Client-side RPT Quick Guide

FORTRA

Thank you for using Core Impact™! This Quick Guide will step you through a basic Client-side Rapid Penetration Test (RPT). To perform these steps, launch Core Impact and open a valid workspace.

Before continuing, make sure you are authorized to perform penetration tests on your perspective target users and systems.

This quick guide is meant to serve as an introduction to the penetration testing capabilities of Core Impact. There are many variations of Core Impact's functionality that are not represented here. For more details, use the Help link within Core Impact.

Client-side RPT Summary

The Client-side RPT is comprised of six steps which, when run in sequence, provide a way for you to test your users and their systems. You will learn how secure your user community is from social engineering attacks.

Client-side Information Gathering - This step uses multiple sources (e.g. search engines, LinkedIn) to locate email addresses of potential target users - the same way a potential attacker would. The Email addresses are stored and used in the Attack and Penetration step of the RPT.

Attack Phase: Attack and Penetration - Using the details from the previous step, Core Impact will send an email to your selected email targets. If recipients of the email take action (e.g. click the included link or open the attachment), their system may be compromised and Core Impact will deploy an agent.

Core Impact's Agent can then serve as a gateway to any compromised systems, allowing you to further penetrate the machine itself or its surrounding network.

Local Information Gathering - This step will do further analysis on any hosts that have an agent installed, exposing user accounts, applications and more.

Privilege Escalation - Depending on the level of access you have on your compromised hosts, this step will attempt to gain elevated privileges for those hosts.

Clean Up - This step disengages and removes any agents that are currently connected.

Client-side Report Generation - As with all Core Impact RPTs, the Report Generation step provides detailed reports on information gathered during the previous steps. These reports are essential in compiling vulnerability data and developing ongoing prevention and remediation strategies.

Run a Client-side RPT

> **TIP:**
> Before beginning the test, you will need the domain of the users you wish to target, and the connection info (address and port) for a valid SMTP server.

Client-side Information Gathering

1. Click the **Client Side RPT** button 

.
2. Click the **Client-side Information Gathering** step.
   This will launch the Information Gathering wizard.
3. Click the **Next** button to get started.
4. Select **Search Engines** for the **Email Address Gathering** and click the **Next** button.
   These are public sources. You can also import your own list of email addresses.

   > **NOTE:**
   > The Core Impact User Guide has further details on how to use LinkedIn to discover potential Client-side targets.

5. Type the domain that corresponds to the email addresses you would like to target.
   For example, **mycompany.com**.
6. Leave the default options for Web Crawling and Search Engine Options and click the **Next** button.
7. Leave the default options for the Client-Side Information Gathering Setup and click **Finish**.

The Information Gathering step will launch the necessary modules - you will see these modules and can monitor their progress in the Executed Modules pane. When the modules are completed, look for new email addresses in the Client Side tab of the Entity Database, then move to the Attack and Penetration step.

Client-side Attack Phase: Attack and Penetration

1. Click **Attack and Penetration** (under Attack Phase) step to launch the Attack and Penetration wizard.
2. Click the **Next** button to get started.

3. Select **Multiple exploits attack** on the **Attack Type Selection** page and click **Next**.

   Single Exploit Attackwill send out 1 attack to each target user.
4. Click the **From:** button and select an email address that will serve as the sender of your attack email, then click **OK**.

   If the email address you want is not yet in the Entity view, you can right-click in the list to create a new one.
5. Click the **To:** button and select one or more email addresses that will be the recipients of your attack email, then click **OK**. Click the **Next** button to proceed with the test.
6. On the **Email Template Selection** step, use the default settings and click **Next**.

   You can use a predefined email template or import one from Outlook or Thunderbird.
7. On the **End User Experience** step, use the default settings and click **Next**.

   These settings form the email that is sent to target users. The email needs to appear legitimate and entice the reader to take action. You can also choose toObfuscate URL to mask the link and further increase the test's chance of success.
8. Leave the options un-checked and click **Finish**.

   You can set advanced actions for mail sending, web server setup and more.

The Attack and Penetration step will launch the necessary modules - monitor the Executed Modules pane to track them. In order for the Attack and Penetration to succeed, one of the email recipients needs to take action in the email. When they do this, if their system is vulnerable, Core Impact will exploit and deploy an agent on their system. If this occurs, you will see the agents attached to new Hosts in the Network tab of the Entity Database. You can now move to the Local Information Gathering step of the RPT.

Local Information Gathering

1. Click the **Local Information Gathering** step to launch the Local Information Gathering wizard.
2. Click the **Next** button to get started.
3. Use the default setting **All connected agents** and click the **Finish** button.

   You can also select from the list of connected agents if you prefer.

The Local Information Gathering step will launch the necessary modules - monitor the Executed Modules pane to track them. When the modules are completed, you will find new details about the host in the Entity Properties pane. The Local Information Gathering modules that are run also show what data they are gathering in the Module Log pane. Now move to the Privilege Escalation step of the RPT.

Privilege Escalation

1. Click the **Privilege Escalation** step to launch the Privilege Escalation wizard.
2. Click the **Next** button to get started.
3. Use the default setting **All connected agents** and click **Next**.

   You can also select from the list of connected agents if you prefer.
4. Use the default settings on the **Exploit Selection** page and click the **Finish** button.

   This will ensure that no services are disabled on the target system. Also the test will stop on a system once an agent is deployed.

The Privilege Escalation step will launch the necessary modules - monitor the Executed Modules pane to track them. If the modules are successful, new agents will be deployed that have more access to the target system (Consider running further Information Gathering from these agents). Move to the Clean Up step.

Clean Up

1. Click the **Clean Up** step to launch the Clean Up wizard.
2. Click the **Next** button to get started.
3. Check the **Select to confirm…** option and then click the **Finish** button.

The Clean Up step will launch the necessary modules - monitor the Executed Modules pane to track them. When the modules are completed, all connected agents will be uninstalled from targeted hosts. Now move on to the Client-side Report Generation step of the RPT.

Client-side Report Generation

1. Click the **Client-side Report Generation** step to launch the Client-side Report Generation wizard.
2. Click the **Next** button to get started.
3. Select the report you wish to run, then click **Next**.

   See below for report types and descriptions.
4. Each report will have one or more additional options - use the default settings for now and click the **Next** button (or **Finish** button if applicable).

   Depending on the report type, you may have to select one or more workspaces.
5. Click the ellipsis button  to view and select the workspace(s) for which you want a report.
6. Select the workspace(s) on the left and click the **Add** button to select them. Then click **OK** to return to the wizard.

   If you select any workspaces that are not currently opened, you will need to enter the workspace password.
7. Click the **Finish** button to run the report.

The report will open in a new window and can be printed or exported in multiple formats such as PDF, HTML and RTF.

Available Client-side RPT Reports

- **FISMA Exploited Vulnerabilities Report**: A report designed to Map Vulnerabilities to NIST 800-53a Controls.
- **Information Publicly Available Report**: A detailed report of the results from the search of documents and any included metadata during Client-side Information Gathering.
- **Client-side Penetration Test Report**: A detailed report of your client-side tests.
- **User Report**: A detailed report about all the users that were discovered and targeted.
- **Delta Report**: A report showing a side-by-side comparison of test statistics for any 2 workspaces.