

# Network RPT (IPv6) Quick Guide



Thank you for using Core Impact™! This Quick Guide will step you through a basic Network Rapid Penetration Test (RPT) using IPv6. 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 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.

## Network RPT Summary

The Network RPT is comprised of six steps which, when run in sequence, provide a comprehensive test of your systems and their vulnerabilities.

**Network Information Gathering** - This step scans a range of IP addresses and reports back any hosts or Network Devices that are discovered. Hosts are then shown on the Network tab of Core Impact's Entity Database. The information that is detected about the hosts is then used in subsequent steps of the RPT.

**Network Attack and Penetration** - Using the information gained in the previous step, Core Impact attempts to exploit vulnerabilities and deploy an Agent on each discovered host. Core Impact's Agents serve as gateways to compromised hosts, allowing you to further interact with the machine itself or penetrate its surrounding network.

**Local Information Gathering** - This step will do further analysis on any hosts that have an agent installed.

**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.


**Network 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 remediation strategies.

## Run a Network RPT

**TIP:**

Before beginning the test, you will need the IP address(es) or range of addresses for the systems that you wish to test.

### Network Information Gathering:


1. Click the **Network RPT** button  **Network RPT** .
2. Click the **Network Information Gathering** step to launch the Attack and Penetration wizard, then click the **Next** button to get started.
3. Select **Use Core Impact to perform Information Gathering...** and click **Next**.  
Alternatively, you can opt to import data from a 3rd party vulnerability scanner or use Nmap.
4. Select **IP version 6** as the network type to be scanned.
5. Select either **Passive Discovery** or **Provide IPv6 addresses**.  
Passive Discovery will cause the RPT to listen to network traffic and identify hosts communicating on IPv6.
6. Use the **Detailed** network scan and click **Next**.  
Custom will allow you to set other parameters.
7. Core Impact will **perform camera information gathering by default** which will check targeted systems to learn whether they are security cameras. To check targeted hosts for **Exposures**, check the desired options, then click **Finish**. To check targeted hosts for **Exposures**, check the desired options, then click **Finish**.

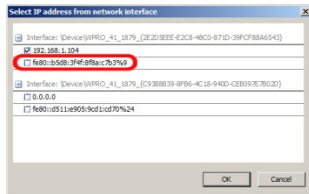
The Information Gathering step will launch the necessary modules - you will see these modules and can monitor their progress in the Executed Modules pane. When the modules are completed, look for newly-discovered hosts in the Network tab of the Entity Database, then move to the Attack and Penetration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

### Change Host Address to IPv6 (OPTIONAL):

Before running the Attack and Penetration, you can force any installed agents to communicate back to the Core Impact console using IPv6.


1. Open the **Network Entity** view and right-click on the **localagent**.
2. On the right-click menu, click **Select host address...**

3. Click inside the field that displays the current host IP address.
4. Click the ellipsis button  to open the network interface address selector.
5. Place a check next to the IPv6 address for your network interface.



6. Click **OK** until you return to the Core Impact workspace.

## Network Attack and Penetration:

1. Click the **Network Attack and Penetration** step to launch the Attack and Penetration wizard, then click the **Next** button to get started.
2. Click the ellipsis button  to see a list of known hosts. Place a check next to each host you wish to target, then click **OK**. You will return to the wizard, then click the **Next** button to proceed with the test.
3. Use the default selections on the **Exploit Selection** page and click **Next**.  
This step dictates the type of exploits attempted and when Core Impact should stop testing each target. It also offers to use exploits against Network Devices.
4. Use the default selection of **Speed** for **Order of Exploit Execution** and click **Next**.  
These options set the order in which the exploits are attempted.
5. Use the default settings for **Exploits - Communication Parameters** and click **Next**.  
This determines how the deployed agents will communicate with the Core Impact console.
6. Use the default settings for **Antivirus Evasion Options** and click **Next**.  
Core Impact can attempt to evade antivirus tools on the targeted system(s)
7. On the **Metasploit Exploits** form, click **Next**.  
Core Impact can run the Metasploit Framework. Leave this option unchecked if you are unsure whether this applies to your system.
8. On the **Exploitation Actions** form, click **Finish**.  
Using this step, you can configure a module (or macro-module) to run as soon as an agent is deployed.

The Attack and Penetration step will launch the necessary modules - monitor the Executed Modules pane to track them. When the modules are completed, locate your targeted hosts to verify that one or more agents were launched and are now attached to them, then move to the Local Information Gathering step.

## Local Information Gathering:

1. Click the **Local Information Gathering** step to launch the Local Information Gathering wizard, then click the **Next** button to get started
2. Use the default setting **All connected agents** and click the **Finish** button.  
You can 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, then click the **Next** button to get started.
2. Use the default setting **All connected agents** and click **Next**.  
You can also select from the list of connected agents if you prefer.
3. 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 systems. With higher privileges, consider running further Local Information Gathering from these agents to learn more about and gain deeper access into targeted hosts.

### TIP:


You can also right-click on any of the deployed agents and select **Set as Source**. This will enable you to repeat the previous sequence of steps from the point of view of the compromised machine, and thus move around the network in a similar manor as an attacker would.

## Clean Up:

1. Click the **Clean Up** step to launch the Clean Up wizard, then click the **Next** button to proceed with the test.
2. 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 modules will be uninstalled from targeted hosts. Now move on to the Network Report Generation step of the RPT.

## Network Report Generation:

1. Click the **Network Report Generation** step to launch the Network 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 a workspace.
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 Network RPT Reports

- **Delta Report:** A report showing a side-by-side comparison of test statistics for any 2 workspaces.
- **Identity Report:** A report containing information about the various identities discovered during Network tests.
- **Network Exposure Report:** Details exposures that found during the Information Gathering stage of the RPT.
- **FISMA Exploited Vulnerabilities Report:** 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 US Government Federal Information Security Management Act (FISMA).
- **Network Host Based Activity Report:** A report showing all modules run for each detected host.
- **Network Host Report:** A detailed report showing all hosts that were detected by the RPT.
- **Network Mitigation Report:** Provides detailed information about the vulnerabilities found, organized as a checklist to have a reference for the issues that need to be remediated.

- **Network Executive Report:** Summarized customizable report of the RPT.
- **Network Vulnerability Report:** A detailed report showing all vulnerabilities that were found by the RPT.
- **PCI Vulnerability Validation Report:** A report that validates vulnerabilities imported from an external scanner.
- **Network Remediation Validation Report:** Provides a comparison of the original workspace with the remediation result.
- **Network Vulnerability Report:** Detailed report of all vulnerabilities found.
- **Network Vulnerability Validation Report:** Report containing validation information for vulnerabilities imported from external vulnerability scanners.
- **Network Wellness Report:** This report indicates the amount of testing that was performed and shows which tests resulted a vulnerability being found on the selected targets.
- **Wireless Network Fake Access Point Report:** Provides information about the attacks of WiFi Fake Access Points.
- **Wireless Network MitM Report:** Provides information about WiFi Man in the Middle attacks.
- **Wireless Network Report:** Provides information about all the known WiFi relationships that have been discovered as part of this penetration test.



#### About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey.

Learn more at [fortra.com](https://fortra.com).