



Core Impact
21
Assisted Start

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.

202301111010

Table of Contents

Introduction	4
Getting Started	4
Network Testing	7
Network Risk Assessment Testing	7
Vulnerability Scanner Validation	26
Remediation Validator	30
Client-side Testing	33
Exploit-based Client-side Tests	33
Phishing-based Client-side Tests	49
Client-side Workstation Tests	59
Web Applications RPT	62
WebApps Risk Assessment Tests	62
WebApps Vulnerability Scanner Validation	80
Contacting Fortra	84
Fortra Portal	84

Introduction

Core Impact is the only solution that empowers you to replicate multi-staged attacks that pivot across systems, devices and applications, revealing how chains of exploitable vulnerabilities open paths to your organization's mission-critical systems and data.

A penetration-test (or security assessment) is the process of actively evaluating your information security measures. Information systems will be tested to find any security issues, as opposed to a paper-based audit.

From a business perspective, penetration testing helps safeguard an organization against failure, through:

- Preventing financial loss through fraud (i.e. hackers, extortionists and disgruntled employees) or through lost revenue due to unreliable business systems and processes.
- Protecting your brand by avoiding loss of consumer confidence and business reputation.
- Proving due diligence and compliance to your industry regulators, customers and shareholders. Non-compliance can result in losing business, receiving heavy fines, gathering bad PR or ultimately failing. At a personal level it can also mean the loss of your job, prosecution and sometimes even imprisonment.

From an operational perspective, penetration testing helps shape information security strategy through identifying vulnerabilities and quantifying their impact and likelihood so that they can be managed proactively; budget can be allocated and corrective measures implemented.

Getting Started

Prior to performing a penetration test it is important to define the goals and the constraints of the penetration test. These should be understood by both the person/team performing the penetration test and the business unit/point of contact that approves the test.

Goal Definition

Prior to performing a test it is important to have a goal defined for the test. This will help ensure you both know when the test is finished and determine how to treat the results of the test.

Common goals for a penetration test of a network are:

- Meeting a compliance/regulatory requirement
- Determining if a specific network or machine is accessible from a particular zone (i.e. the guest network or the Internet)
- Determining if any exploitable vulnerabilities exist on a specific machine or set of machines
- Perform test from a random network location, time and track response from security team to detect and isolate the attacking machine

Testing Constraints

While the typical attacker is not assumed to have any constraints regarding the actions that can be performed, the internal tester is often required to work within specific constraints. These constraints are typically to minimize risk (real or perceived) associated with the Penetration Test and to define how much time the tester has to conduct the test.

Common Constraints of a Penetration Test are:

- Services cannot be intentionally brought down
- Services may not be disrupted at all
- Testing may only be performed during maintenance window or during non-production hours
- Testing must be completed by a specific date
- Specific (critical) hosts cannot be targeted

When agreeing to the constraints imposed by the business, it is important to ensure the business understands how the constraints reduce the effectiveness of a Test. An attacker may spend weeks or months accessing an environment and waiting for a suitable new vulnerability to be discovered before exploiting the window of time for an organization between the announcement of a vulnerability and the release of a patch.

Notification

While attackers do not have the courtesy of notifying network and system owners of their attacks it is common practice to notify internal groups of upcoming security assessments. This could be a simple notification of the window of time the testing will take place or a detailed overview of the scope of the test.

While there is a risk that system owners may turn off known vulnerable systems or services prior to the test or block the tester's IP, it is better to try and build a cooperative relationship with business owners. It should be a tester's goal to help educate business owners of the

value of frequent security testing as well as the benefits that the resulting improved security can have for their systems.

Methodology

Core Impact uses a built-in testing methodology known as the Rapid Penetration Test or RPT. The RPT is based on years of manual security assessments and the experience that brings. It is designed to guide the operator through the steps of a security assessment from Information Gathering to exploitation, post exploitation and reporting.

To learn more about security assessment methodology visit the site of the Penetration Testing Execution Standard - <http://www.pentest-standard.org>

Network Testing

Core Impact allows you to perform a variety of tests on your networked systems.

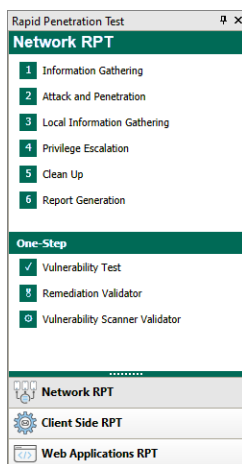
What kind of Network test do you want to perform?

- [Risk Assessment](#)
- [Vulnerability Scanner Validation](#)

Network Risk Assessment Testing

Your organization's servers and workstations make up the backbone of your IT infrastructure and house some of its most important information assets. Perimeter defenses offer these systems a level of protection, but no defensive application is 100% impervious to attack. It is therefore critical to proactively test your organization's ability to detect, prevent and respond to network threats.

Performing a Network Risk Assessment test with Core Impact's RPT enables you to quickly determine the risk present in your environment and priorities the remediation.



The RPT is divided into the following steps - click one to learn more about how to execute the step:

1. [Network Information Gathering](#)
2. [Network Attack and Penetration](#)
3. [Local Information Gathering](#)
4. [Privilege Escalation](#)

5. [Clean Up](#)
6. [Network Report Generation](#)

Information Gathering

The **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.

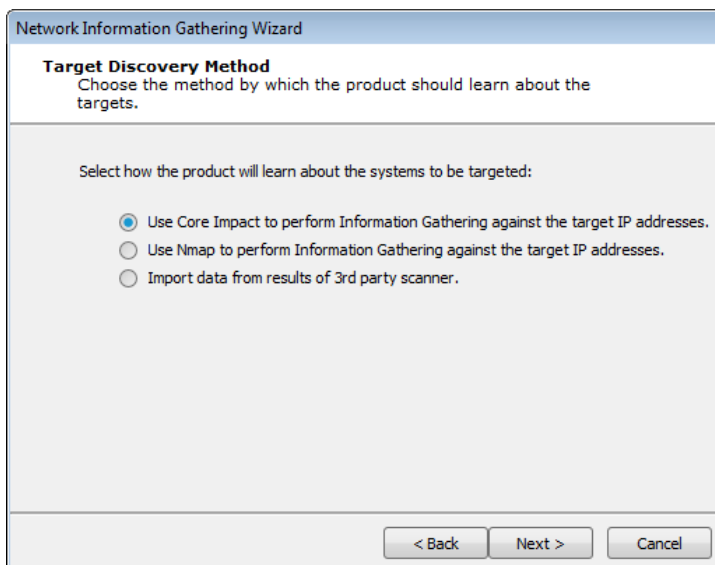
NOTE:

Before running Network Attack and Penetration, you should know the IP address(es) of the system(s) you want the penetration test to target, and you should have permission to do so.

Below are the basic steps to running Information Gathering. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run Information Gathering:

1. Make sure that the **Network RPT** is active.
2. Click on **Information Gathering** to open up the Information Gathering Wizard, then click **Next** to continue.
3. Select **Use Core Impact to perform Information Gathering against the target IP addresses**. Then click **Next** to continue.



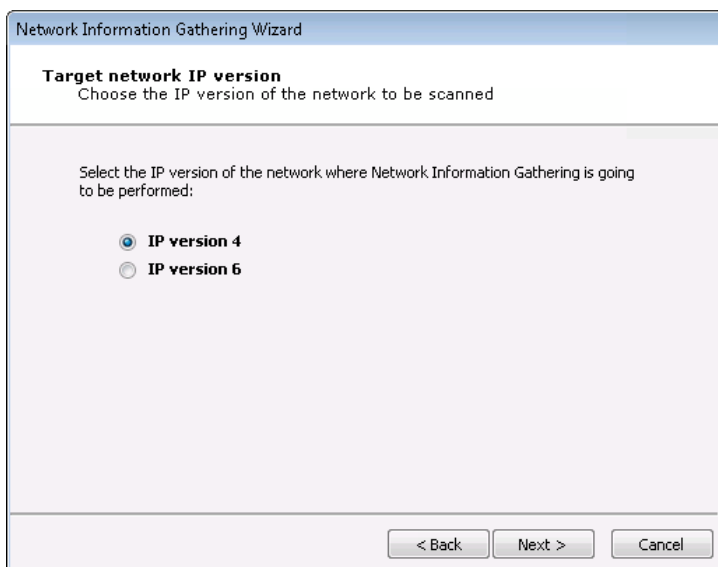
WHY?

You would use this option when you already know the IP address(es) of one or more systems that you want to target in the penetration test.

WHAT ELSE?

You would choose **Use Nmap to perform Information Gathering against the target IP addresses** if you want Nmap to do the information gathering. You would use the **Import data from results of 3rd Party Scanner** option when you have output data from a vulnerability scanner, and you want Core Impact to use the results of that scan to determine which systems to target in the penetration test.

4. Select **IP Version 4**. Then click **Next** to continue.



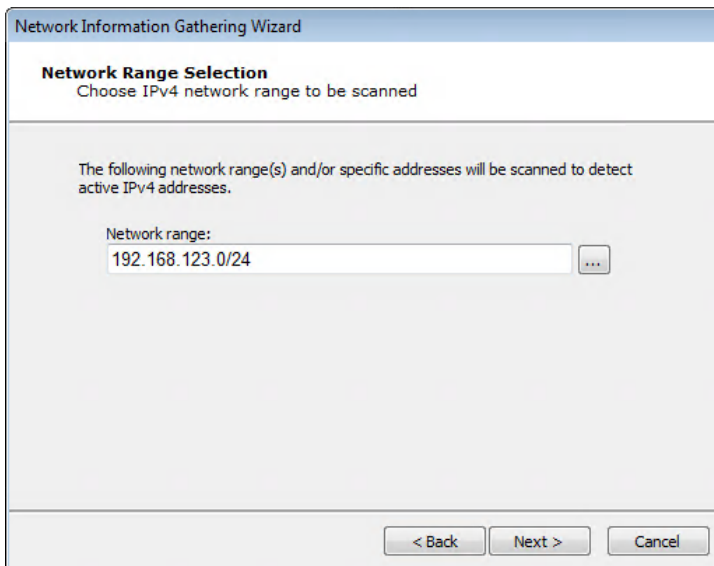
WHY?

You use this option when the systems you want to target use IPv4 as their communication method.

WHAT ELSE?

You would use the **IP Version 6** option when your target systems are actively using IPv6.

5. Type in the target IP address(es) you want to scan. Then click **Next** to continue.



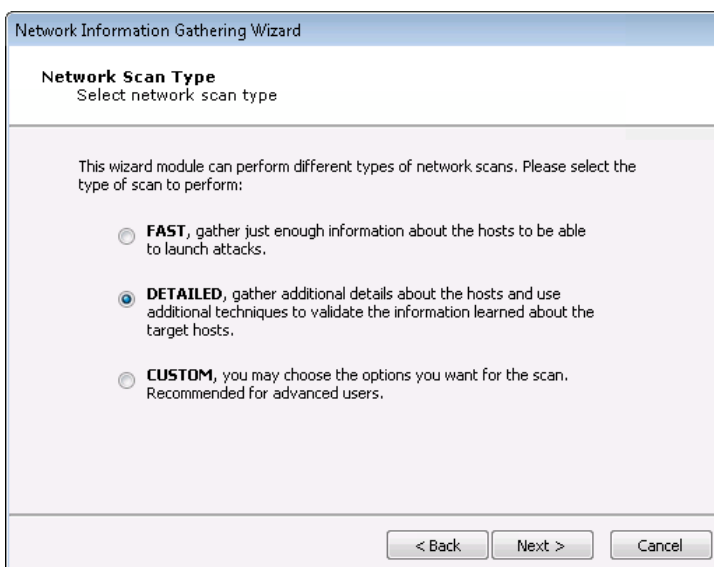
WHY?

This field tells Core Impact which machine(s) you want to target in the penetration test.

WHAT ELSE?

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.

6. Select **Detailed** as the Network Scan Type. Then click **Next** to continue.



WHY?

The **DETAILED** setting runs more modules in order to discover additional, potentially useful details about target systems.

WHAT ELSE?

There are 3 network scan types you can perform:

- **FAST:** The test captures the minimal amount of data needed in order to launch attacks.
 - **DETAILED:** The test runs more modules in order to discover additional, potentially useful details about target systems.
 - **CUSTOM:** You configure how Core Impact will execute the Information Gathering process.
7. Select **Check for Network Exposures** and leave **Perform camera information gathering** checked. Then click **Finish** to start the Information Gathering step of the RPT.

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

WHY?

Core Impact can detect whether any systems in the targeted range are security cameras. If identified, these can then be tested for possibly vulnerabilities. See the User Guide for more details. The RPT can also check for Exposures in targeted hosts. 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 (see <http://cve.mitre.org>).

After starting Information Gathering:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of many modules that will run to complete the overall process.

After Information Gathering has completed:

If your target systems have been successfully found by Core Impact, you will see the systems listed in the Hosts tab of the Entity database. You can then run the [Network Attack and Penetration](#) step of the RPT, which will attempt to exploit any weaknesses in the systems.

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.

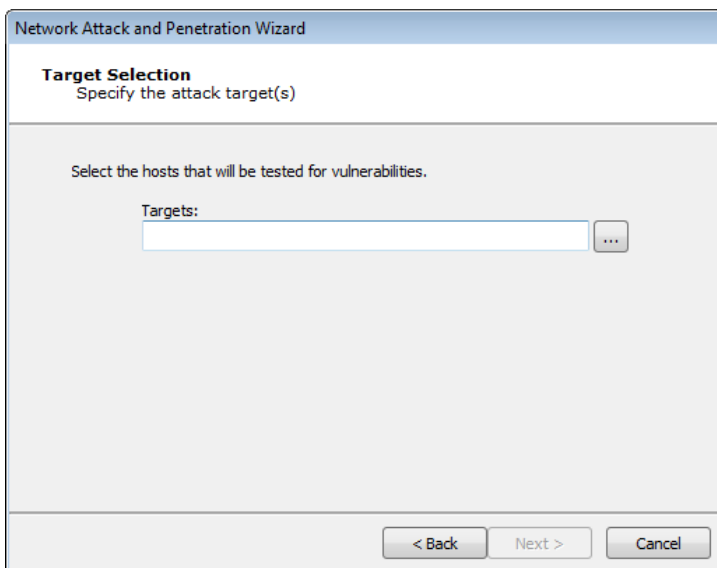
NOTE:

Before running Network Attack and Penetration, you should know the IP address(es) of the system(s) you want the penetration test to target, and you should have permission to do so.

Below are the basic steps to running Network Attack and Penetration. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run Network Attack and Penetration:

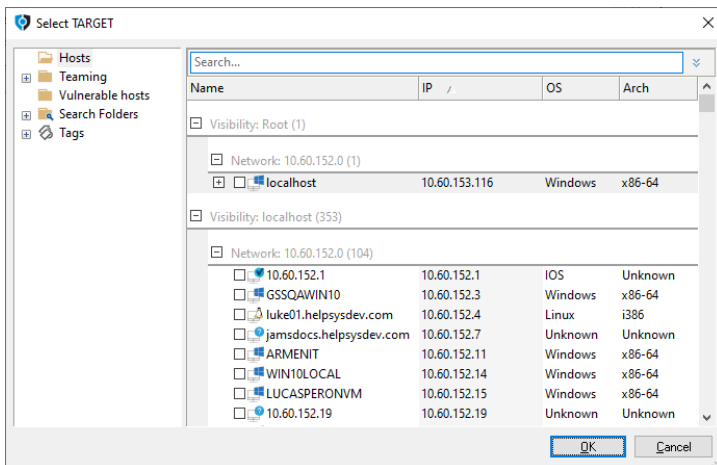
1. Make sure that the **Network RPT** is active.
2. Click on **Network Attack and Penetration** to open up the Wizard, then click **Next** to continue.
3. Click the ellipsis button  next to the **Targets** field.



WHY?

This will open the Entities Selection window from which you can select which system(s) you want to target.

4. In the **Entities Selection** window, select the host(s) that you wish to target with the Attack and Penetration, then click **Ok**. Only hosts that are represented in the Entity View can be targeted.



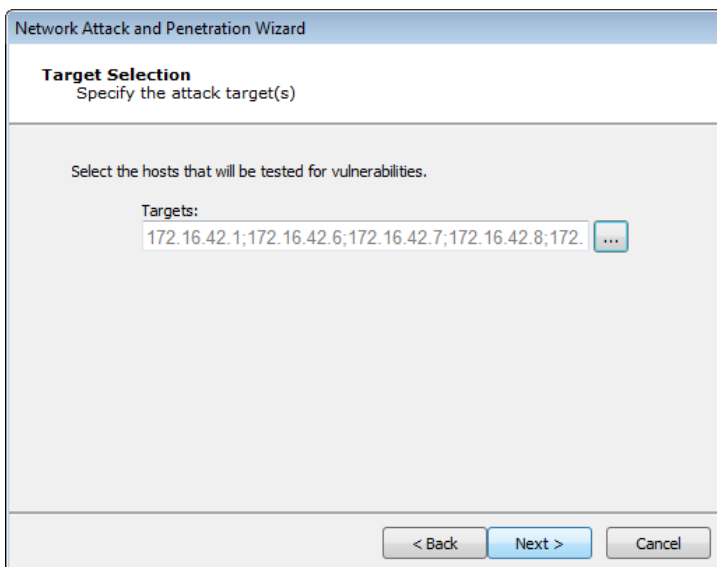
WHY?

The host(s) that you check on this screen will be targeted by the Network Attack and Penetration.

WHAT ELSE?

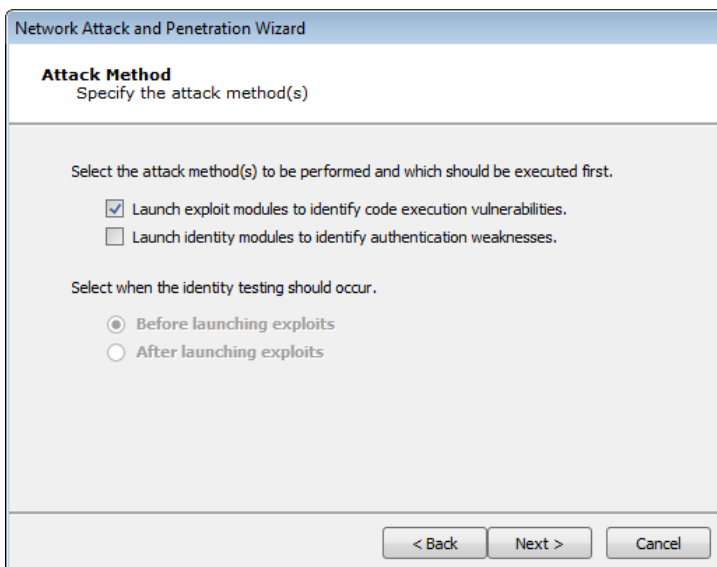
You can manually add a new host at this stage by right-clicking on the Hosts folder, then selecting New. Then enter the host details.

5. On the **Target Selection** step of the wizard, click **Next** to continue.



The screenshot shows the 'Network Attack and Penetration Wizard' window at the 'Target Selection' step. The title bar reads 'Network Attack and Penetration Wizard'. Below the title bar, the text 'Target Selection' is displayed in bold, followed by 'Specify the attack target(s)'. The main area contains the instruction 'Select the hosts that will be tested for vulnerabilities.' Below this, there is a 'Targets:' label and a text input field containing the IP addresses '172.16.42.1;172.16.42.6;172.16.42.7;172.16.42.8;172.' followed by a blue ellipsis button. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

6. In the **Attack Method** window, leave the default selections, then click **Next** to continue.



The screenshot shows the 'Network Attack and Penetration Wizard' window at the 'Attack Method' step. The title bar reads 'Network Attack and Penetration Wizard'. Below the title bar, the text 'Attack Method' is displayed in bold, followed by 'Specify the attack method(s)'. The main area contains the instruction 'Select the attack method(s) to be performed and which should be executed first.' Below this, there are two checkboxes: the first is checked and labeled 'Launch exploit modules to identify code execution vulnerabilities.', and the second is unchecked and labeled 'Launch identity modules to identify authentication weaknesses.' Below these, there is another instruction: 'Select when the identity testing should occur.' Below this, there are two radio buttons: the first is selected and labeled 'Before launching exploits', and the second is unselected and labeled 'After launching exploits'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

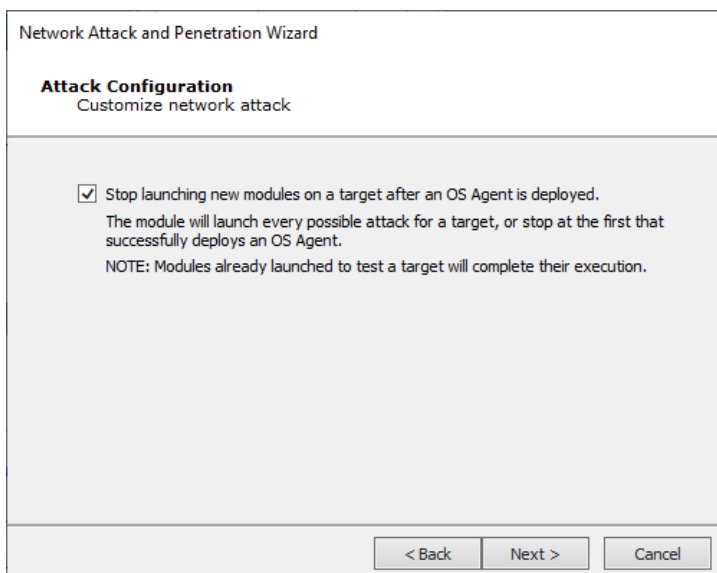
WHY?

The **Launch Exploit modules to identify code execution vulnerabilities** will instruct the Attack and Penetration to attempt to find vulnerabilities in the target hosts' OS or any installed programs.

WHAT ELSE?

Select **Launch Identity modules to identify authentication weaknesses** if you want the Attack and Penetration to attempt to gather identities (usernames/passwords or other credentials) from the target host(s).

7. On the **Exploit Selection** window, leave the default selections and click **Next** to continue.



WHY?

These options determine which exploits will be used during the attack as well as some specific behavior parameters.

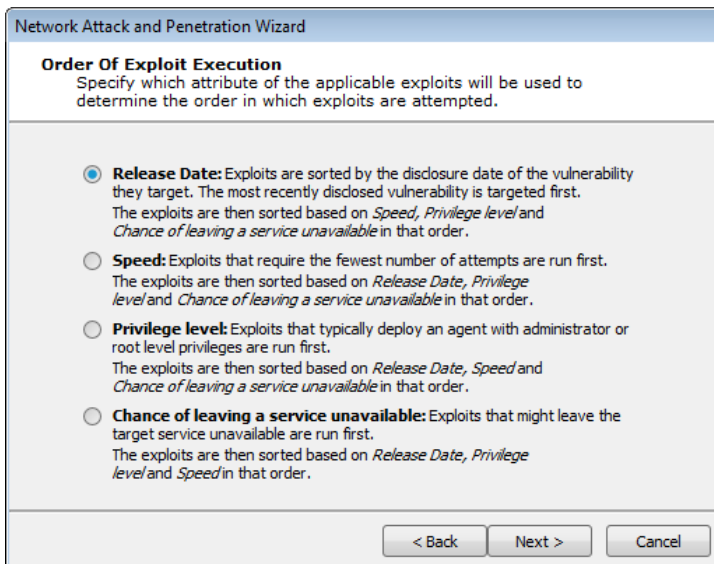
WHAT ELSE?

- 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.
- Check the **Stop launching new exploits after an agent is deployed** check-box if you want the attack to stop after the first agent is deployed. When more than one exploit are running concurrently against

a host, they will be allowed to complete even after an agent is deployed. Because of this, more than one agent may be installed even when this option is checked.

- 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.
- If you want to attempt to penetrate any Network Devices that are among your targets, you can check the **Use Authentication Weakness exploits against Network Devices** check-box.

8. In the **Order of Exploit Execution** window, select how exploits are prioritized during the Attack and Penetration. Then click **Next** to continue.



WHY?

- **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.

WHAT ELSE?

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.

- In the **Exploits - Communication Parameters** window, leave the **Connection Method** and **TCP port** as the default values, then click **Next** to continue.

WHY?

The host(s) that you check on this screen will be targeted by the Network Attack and Penetration.

WHAT ELSE?

The connection method can be one of the following:

- 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.

NOTE:

Only exploits with the specified connection method will be run (if you select "Reuse connection", only exploits with that capability will be selected). 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.

10. In the **Exploits - Agent Expiration Parameters** window, leave the **Agent Expiration** as the default, then click **Next** to continue.

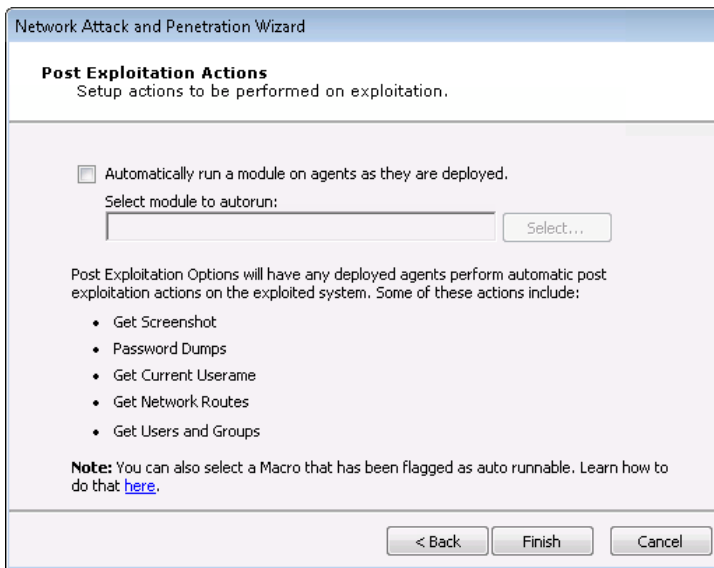
WHY?

For deployed agents, you can set when the agents should expire.

WHAT ELSE?

You can disable Agent Expiration or set a specific time (in days, weeks or months) when the agent(s) should expire.

11. On the **Exploitation Actions** window, click **Finish** to continue.



WHY?

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.

After starting Network Attack and Penetration:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of many modules that will run to complete the overall process.

After Network Attack and Penetration has completed:

If your target systems have been successfully penetrated by Core Impact, you will see the new agent(s) under your systems listed in the Hosts tab of the Entity database. You can then run the [Network Local Information Gathering](#) step of the RPT, which will attempt to gather additional data from the penetrated systems. Once any vulnerabilities have been found and addressed, you can run the [Remediation Validator](#) to verify that vulnerabilities have been fixed.

Local Information Gathering

The **Local Information Gathering** 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.

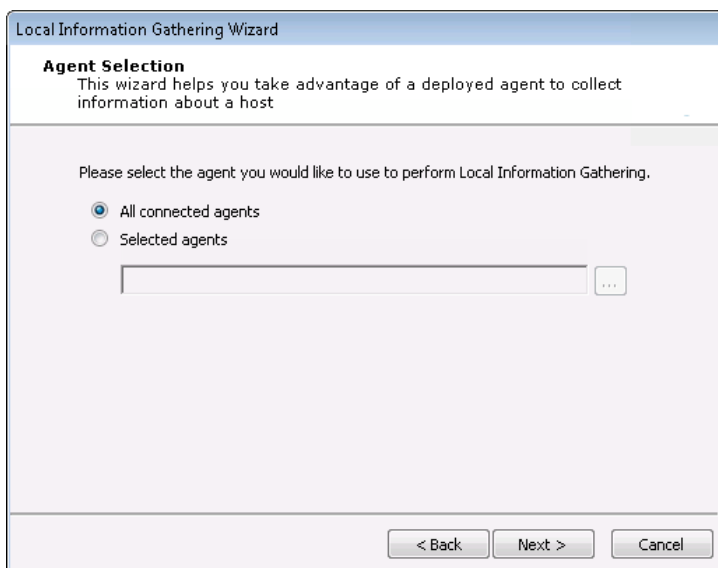
NOTE:

Before running Local Information Gathering, you should have active agents on one or more host targets and permission to run penetration tests on the system(s).

Below are the basic steps to running Local Information Gathering. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.


To run Local Information Gathering:

1. Make sure that the **Network RPT** is active.
2. Click on **Local Information Gathering** to open up the Wizard, then click **Next** to continue.
3. On the **Agent Selection** step of the Wizard, click **Next** to continue.

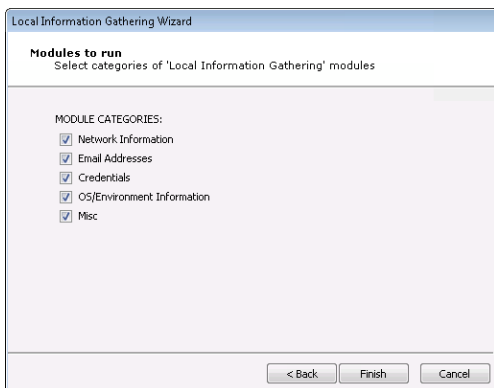
**WHY?**

By default, information will be gathered on all connected agents.

WHAT ELSE?

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.

4. In the **Modules to Run** window, leave the default selections and click **Finish** to continue.



WHY?

The RPT will attempt to gather information in the provided categories.

WHAT ELSE?

You can manually check/uncheck categories based on your testing requirements.

After starting Local Information Gathering:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of multiple modules that will run to complete the overall process.

After Local Information Gathering has completed:

If additional information has been gathered by the RPT, you will be able to view the data in the Entity Properties of the target(s). You can then run the [Privilege Escalation](#) step of the RPT, which will attempt to use the gathered data to gain privileges on the penetrated systems.

Privilege Escalation

The **Privilege Escalation** 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**.

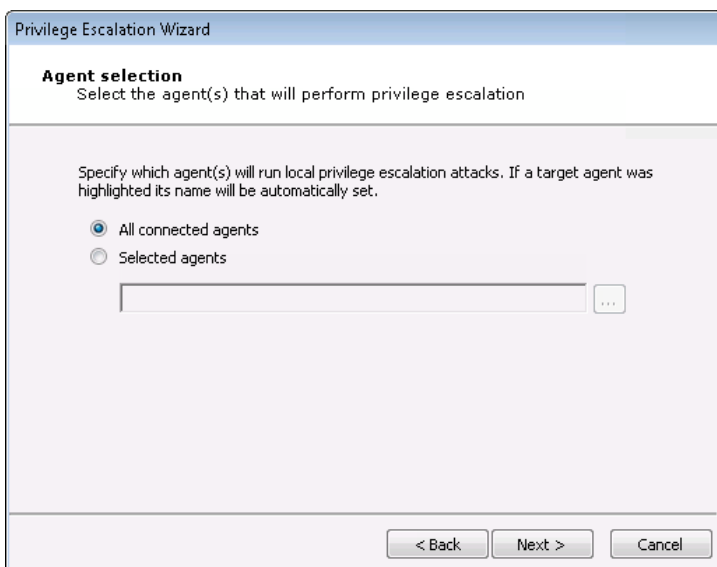
NOTE:

Before running Privilege Escalation , you should have active agents on one or more host targets and permission to run penetration tests on the system(s).

Below are the basic steps to running Privilege Escalation. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.


To run Privilege Escalation:

1. Make sure that the **Network RPT** is active.
2. Click on **Privilege Escalation** to open up the Wizard, then click **Next** to continue.
3. On the **Agent Selection** step of the Wizard, click **Next** to continue.

**WHY?**

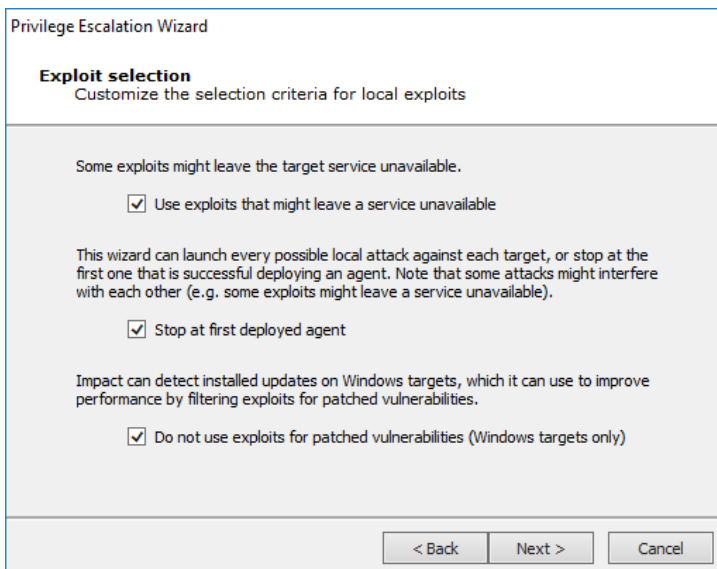
By default, information will be gathered on all connected agents.

WHAT ELSE?

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.

4. In the **Exploits Selection** window, leave the default selections and click **Next** to continue.



The screenshot shows a window titled "Privilege Escalation Wizard" with a sub-header "Exploit selection" and the instruction "Customize the selection criteria for local exploits". The main content 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 of the window are three buttons: "< Back", "Next >", and "Cancel".

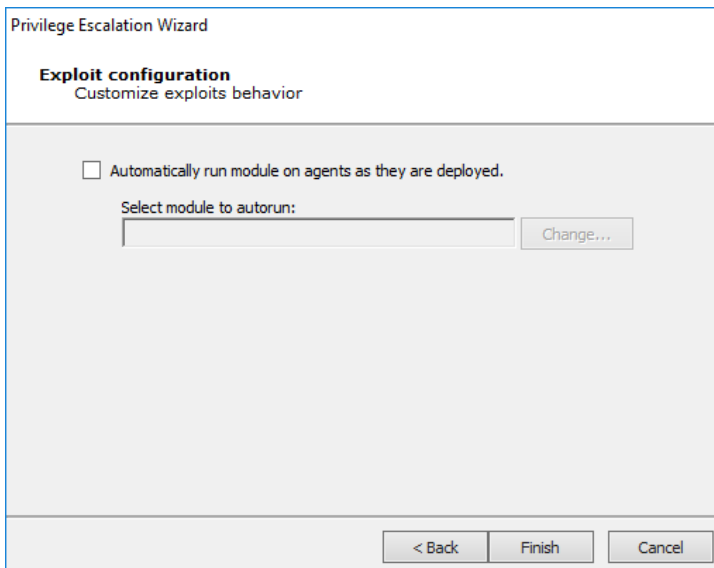
WHY?

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.

WHAT ELSE?

For a more aggressive attack strategy or for better performance, check or uncheck the appropriate check-boxes.

5. In the **Exploits Configuration** window, leave the default selections and click **Finish** to continue.



WHY?

If Privilege Escalation succeeds in deploying an Agent, it can automatically execute a Module of your choosing.

WHAT ELSE?

You could configure the Privilege Escalation test to automatically run a specific Module if an Agent is installed.

After starting Privilege Escalation:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of many modules that will run to complete the overall process.

After Privilege Escalation has completed:

You may want to run the Local Information Gathering step (again) 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.

Clean Up

The Network Clean Up step automatically uninstalls all currently-connected agent(s) that resulted from your Network penetration testing.

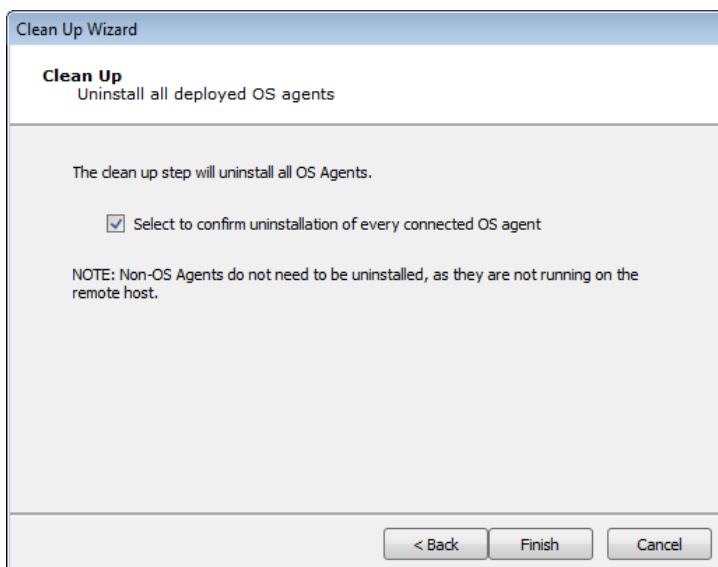
NOTE:

Before running Clean Up, you should have active agents on one or more host targets and permission to run penetration tests on the system(s).

Below are the basic steps to running Clean Up.

To run Clean Up:

1. Make sure that the **Network RPT** is active.
2. Click on **Clean Up** to open up the Wizard, then click **Finish** to continue.



After starting Clean Up:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of multiple modules that will run to complete the overall process.

After Clean Up has completed:

Any agents that were installed on target systems will be removed.

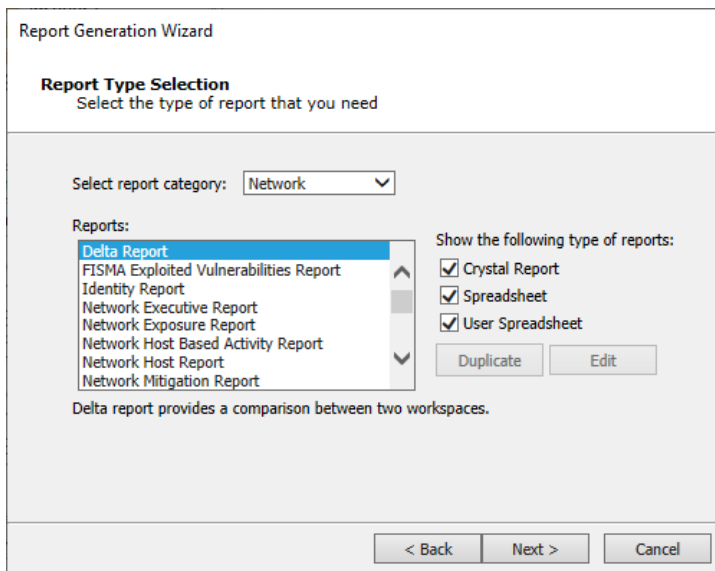
Network Report Generation

The Network 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.

Below are the basic steps to running Network Report Generation. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run Report Generation:

1. Make sure that the **Network RPT** is active.
2. Click on **Network Report Generation** to open up the Wizard, then click **Next** to continue.
3. Select the Report you wish to run, then click **Finish** to continue.



After Network Report Generation has completed:

The report window will open, from which you can view, print, or export the report.

Vulnerability Scanner Validation

Overview

A vulnerability management strategy typically involves multiple steps:

1. Scanning the target systems
2. Identifying which potential vulnerability poses a true risk to the environment
3. Determining the scope of that risk
4. Prioritizing the remediation efforts
5. Re-testing to ensure the remediation was effective

Using Core Impact, you can import the results of a network vulnerability scan and determine which potential threats can be leveraged to expose true risk to data and system integrity via the networked hosts application.

Getting Started

To execute a **Network Vulnerability Scanner Validation**, follow the steps outlined [here](#).

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.

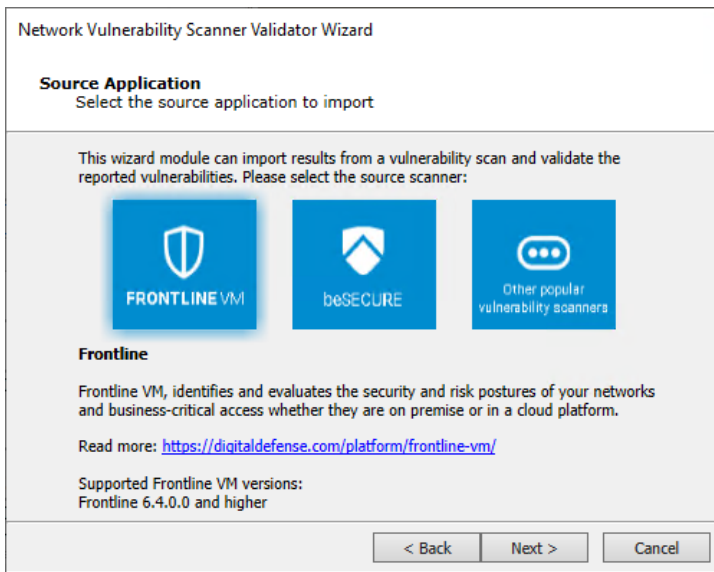
NOTE:

Before running 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

Below are the basic steps to running the Vulnerability Scanner Validator wizard. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

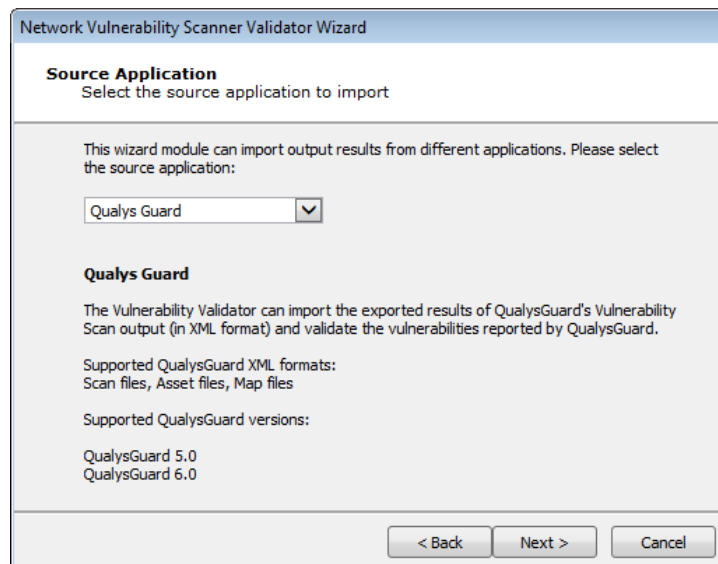
To run the Vulnerability Scanner Validator:

1. Make sure that the **Network RPT** is active.
2. Under the **One-Step** heading, click on **Vulnerability Scanner Validator** to open up the wizard, then click **Next** to continue.
3. 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:

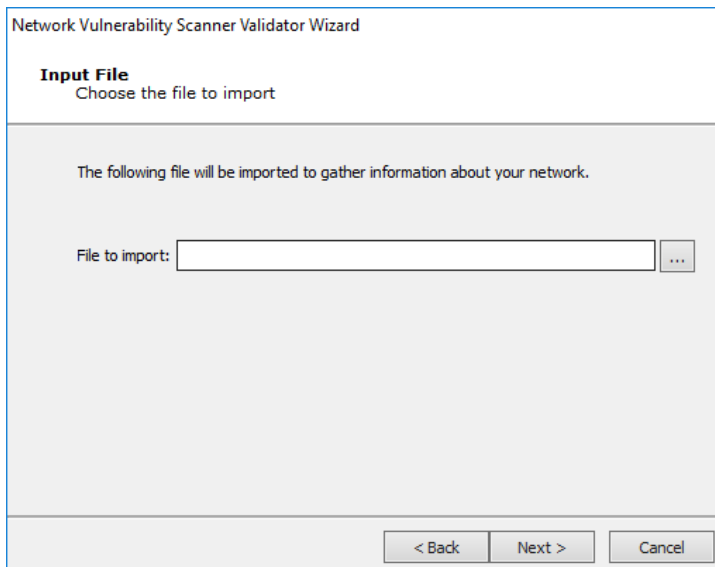


Select one of the three available options and press **Next** to continue.

WHY?

This option tells Core Impact which scanner from which your data originated.

4. Browse to the scanner's output file or enter the details of the scanner's database. Then click **Finish** to start the Vulnerability Scanner Validator.



The screenshot shows a dialog box titled "Network Vulnerability Scanner Validator Wizard". The main heading is "Input File" with the instruction "Choose the file to import". Below this, a message states: "The following file will be imported to gather information about your network." There is a text input field labeled "File to import:" followed by a browse button (three dots). At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

WHY?

The output format you are importing is dependent on the Vulnerability Scanner you selected in the previous step.

WHAT ELSE?

Some scanners export their results to a file while others require you to access their data directly from the scanner's database.

After starting the Vulnerability Scanner Validator:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of multiple modules that will run to complete the overall process.

After the Vulnerability Scanner Validator has completed:

If your target systems have been successfully found by Core Impact, you will see the systems listed in the Hosts tab of the Entity database. You can then run the [Network Attack and Penetration](#) step of the RPT, which will attempt to exploit any weaknesses in the systems. Following that test, you can run the [Remediation Validator](#) to verify that vulnerabilities have been fixed.

Remediation Validator

Overview

A vulnerability management strategy typically involves multiple steps:

1. Scanning the target systems
2. Identifying which potential vulnerability poses a true risk to the environment
3. Determining the scope of that risk
4. Prioritizing the remediation efforts
5. Re-testing to ensure the remediation was effective

Using Core Impact's Remediation Validator, you can easily re-test hosts that had been identified as vulnerable, ensuring that remediation steps have been effective.

Getting Started

To execute a **Network Remediation Validator** test, follow the steps outlined [here](#).

Remediation Validator Test


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.

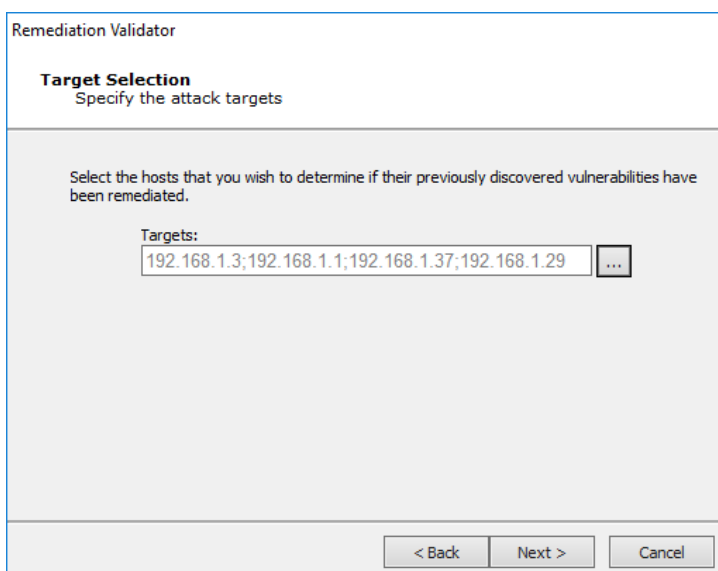
NOTE:

Before running the Remediation Validator, you should know the IP address(es) of the system(s) you want the penetration test to target, and you should have permission to do so.

Below are the basic steps to running the Remediation Validator wizard. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run the Remediation Validator:

1. Make sure that the **Network RPT** is active.
2. Under the **One-Step** heading, click on **Remediation Validator** to open up the wizard, then click **Next** to continue.
3. In the **Target Selection** step, click the ellipsis button  next to the **Targets** field and select the target(s) against which you want to run the Remediation Validator. Then click **Next** to continue.



The screenshot shows a window titled "Remediation Validator" with a "Target Selection" section. The instruction reads: "Specify the attack targets" and "Select the hosts that you wish to determine if their previously discovered vulnerabilities have been remediated." Below this is a "Targets:" input field containing the IP addresses "192.168.1.3;192.168.1.1;192.168.1.37;192.168.1.29" and an ellipsis button. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

WHY?

This will open the Entities Selection window from which you can select which host(s) you want to target. These hosts should be ones that have previously been successfully exploited and have since had their vulnerabilities remediated.

4. Click **Finish** to start the Remediation Validator.

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

WHAT ELSE?

Select the **Consider vulnerabilities as solved** ... option if you want Core Impact to mark vulnerabilities as "solved" (and not "indeterminate") when the original attack patch can not be used.

After starting the Remediation Validator:

Core Impact will execute the same exploits that it used to originally penetrate the host(s). You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of multiple modules that will run to complete the overall process.

After the Remediation Validator has completed:

Run the **Remediation Validation Report** to view a detailed report on the post-remediation test.

Client-side Testing

Core Impact 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 PC should they follow an action prompted by the email contents. You can perform an Exploit-based test where Core Impact uses vulnerabilities in the user's system to install an agent. Or you can perform a Phishing-based test in which users are asked to click a link in the email that sends them to a fake web site where they might insert sensitive data.

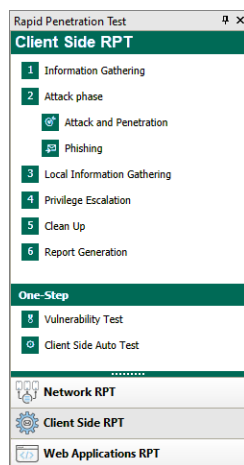
What kind of Client-side test do you want to perform?

- [Exploit-based Test](#)
- [Phishing-based Test](#)
- [Workstation Test](#)

Exploit-based Client-side Tests

Overview

Including exploits in a Client-side test not only tests the end users but also the protective systems on the users' machine. Used in a holistic test, a Client-side exploit-based test can be the first foothold that allows the test to move into the environment and pivot to a network test from a user's compromised workstation.



Getting Started

The RPT is divided into the following steps - click one to learn more about how to execute the step:

1. [Information Gathering](#)
2. [Attack Phase: Attack and Penetration](#)
3. [Local Information Gathering](#)
4. [Privilege Escalation](#)
5. [Clean Up](#)
6. [Client-side Report Generation](#)

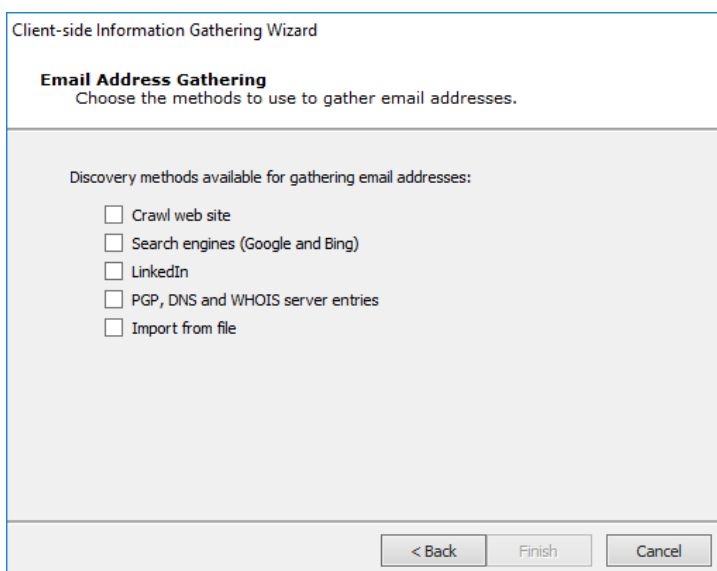
Client-side Information Gathering

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.

Below are the basic steps to running Client-side Information Gathering. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run Client-side Information Gathering:

1. Make sure that the **Client-side RPT** is active.
2. Click on **Client-side Information Gathering** to open up the Information Gathering Wizard, then click **Next** to continue.
3. Set discovery method to **Search engines**. Then click **Next** to continue.



The screenshot shows a dialog box titled "Client-side Information Gathering Wizard". Inside, there is a section titled "Email Address Gathering" with the instruction "Choose the methods to use to gather email addresses." Below this, a list of discovery methods is provided, each with an unchecked checkbox:

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

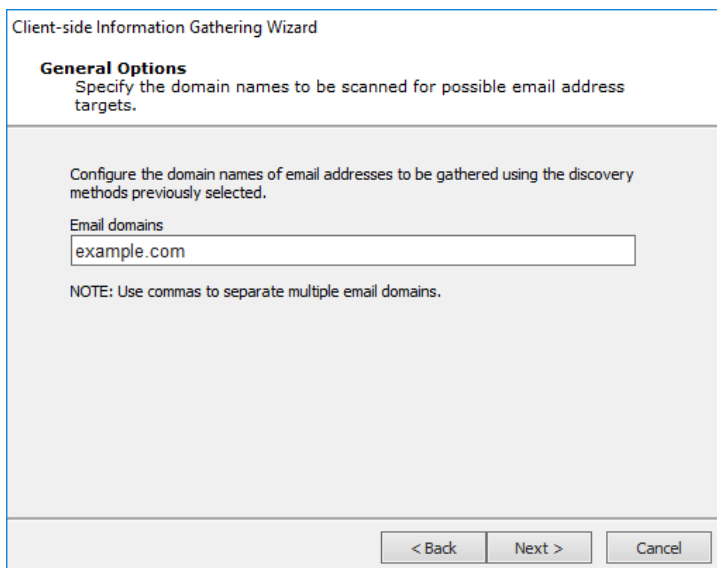
At the bottom of the dialog box, there are three buttons: "< Back", "Finish", and "Cancel".

WHY?

The **Search Engines** setting uses Google or Bing search engines to locate email addresses in public on-line records. An attacker might use the exact same method to locate target email addresses.

WHAT ELSE?

- **Search in PGP, DNS and WHOIS** uses Public Internet Databases to locate email addresses.
 - **Crawl Web Site** to can search within a specific web site to explore for email addresses or documents.
 - **Import from file**: Select this option if you have a local file that contains your target email addresses.
 - **LinkedIn**: Select this option to have CORE Impact search through the web site LinkedIn to locate users for a specific company. If you select this option, you can further configure it in a subsequent step of the wizard.
4. Enter the domain(s) for which you want to discover email addresses. For example, if you enter `company.com`, the crawler will search for an record all email addresses it finds that end in `@company.com`. Then click **Next** to continue.



The screenshot shows a wizard window titled "Client-side Information Gathering Wizard". The "General Options" section is active, with the instruction "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 reads "NOTE: Use commas to separate multiple email domains." At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

WHY?

For example, if you enter `company.com`, the crawler will search for and record all email addresses it finds that end in `@company.com`.

5. Leave the default settings on the **Web Crawling and Search Engines Options** step. Then click **Next** to continue.

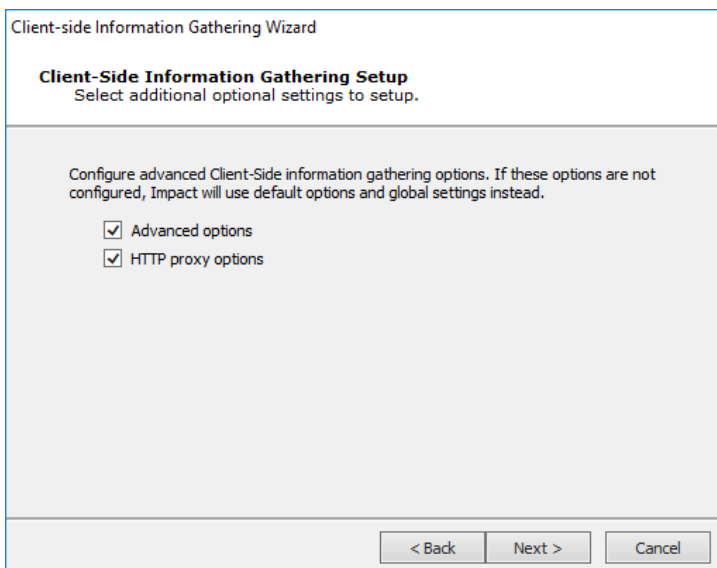
The screenshot shows a wizard window titled "Client-side Information Gathering Wizard" with a sub-header "Web Crawling and Search Engines Options". Below the sub-header is the instruction "Configure options for web site crawling and search engine results." The main area contains two sections of settings. 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 of the window are three buttons: "< Back", "Next >", and "Cancel".

WHY?

These options dictate the scope and depth of the Information Gathering step.

WHAT ELSE?

- 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.
6. Leave the default settings on the **Client-side Information Gathering Setup** step. Then click **Finish** to start the Information Gathering step of the RPT.



WHY?

These options will present additional settings for the RPT.

WHAT ELSE?

- **Search for metadata inside Microsoft Office 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.
- HTTP Proxy options will allow you to configure a Proxy server if one is required for your network access

After starting Client-side Information Gathering:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of multiple modules that will run to complete the overall process.

After Client-side Information Gathering has completed:

If Core Impact, 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. You can then run the [Client-side Attack and Penetration](#) or [Client-side Phishing](#) step of the RPT.

Client-side Attack Attack and Penetration

Using the **Client-side Attack and Penetration** wizard, you can execute an exploit-based test on your email users.

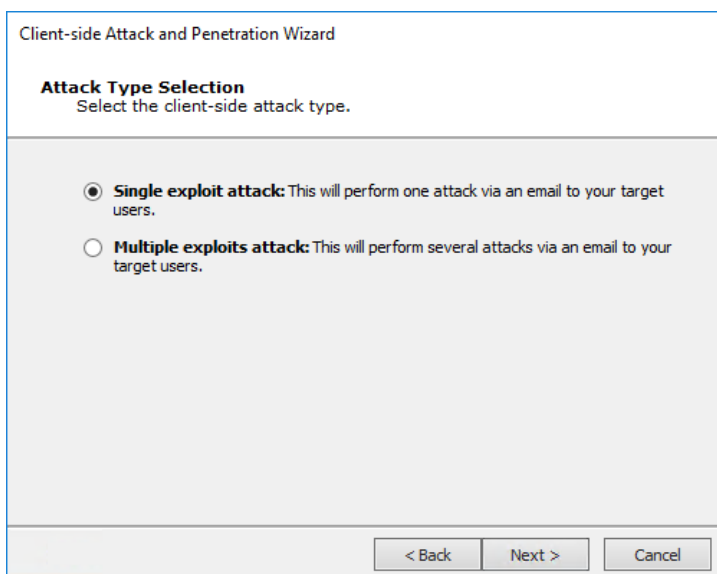
NOTE:

Before running Client-side Attack and Penetration, you should know the email addresses of the users you want the penetration test to target, and you should have permission to do so.

Below are the basic steps to running Client-side Attack and Penetration. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run an exploit-based Client-side Attack and Penetration:

1. Make sure that the **Client-side RPT** is active.
2. Click on **Attack and Penetration** under Attack Phase to open up the Attack and Penetration Wizard, then click **Next** to continue.
3. Leave the default setting of **Single Exploit Attack** on the **Attack Type Selection** step. Then click **Next** to continue.



The screenshot shows a wizard window titled "Client-side Attack and Penetration Wizard". The current step is "Attack Type Selection" with the instruction "Select the client-side attack type." There are two radio button options: "Single exploit attack: This will perform one attack via an email to your target users." (which is selected) and "Multiple exploits attack: This will perform several attacks via an email to your target users." At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

WHY?

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

WHAT ELSE?

The **Multiple exploits attack** option will send several different attacks via email to your targets.

4. Leave the default setting of **Web Browser** on the **Targeting with Single Exploit** step. Then click **Next** to continue.

The screenshot shows a wizard window titled "Client-side Attack and Penetration Wizard". The current step is "Targeting with Single Exploit" with the instruction "Select the client-side exploit type." There are four radio button options:

- 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.

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

WHY?

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 which will be pre-established by Core Impact to launch an attack against the user's system.

WHAT ELSE?

You can select other methods to use a single exploit in the Client-side Attack and Penetration:

- **Mail Client:** These exploits take advantage of vulnerabilities in the recipient's email client software. If you choose Mail Client, click the Next button to configure the Exploit Selection Method.
- **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. If you choose Attach, click the Next button to configure the Exploit Selection Method.

- **Trojan:** These involve attaching an agent to the email. If a user executes the attachment, the agent is deployed on their machine.
5. Leave the default setting of **Exploit List** on the **Exploit selection method** step and click the **Change** button to select a specific exploit for the test to use. Then click **Next** to continue.

Client-side Attack and Penetration Wizard

Exploit selection method
Define how you would like the exploit to be chosen.

Exploit list: View the complete list of available exploits and choose the specific exploit you wish to use.

Exploit:
Advantech WebAccess nvA1Media Caption Hea

Target application list: Select the application you wish to target. The wizard will use the most recent exploit available that targets your chosen application.

Application:
NTR.ActiveX

WHY?

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 which will be pre-established by Core Impact to launch an attack against the user's system.

WHAT ELSE?

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.

6. 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. Then click **Next** to continue.

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

7. Leave the default settings on the **Email Template Selection** step. Then click **Next** to continue.

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

WHY?

Core Impact ships with several email templates that you can customize when planning a Client-side test.

WHAT ELSE?

You can import an email that has been exported from Outlook or Thunderbird and use that as the basis for your email.

8. Leave the default settings on the **End User Experience** step. Then click **Next** to continue.

The screenshot shows a dialog box titled "Client-side Attack and Penetration Wizard" with the sub-header "End User Experience". Below the sub-header is the instruction "Define the email to be sent and page to be displayed to victims." The main area contains four fields: a text box for "Select a email template (or browse for HTML page to be used as the attack email's body):" with the value "C:\ProgramData\IMPACT\components\modules\classic\install\temp" and a browse button "..."; an "Email Subject:" field with the value "Undelivered Mail Returned to Sender"; a "Message priority:" dropdown menu set to "Normal"; and a "Select CSV file for targets' data tags:" field with a browse button "...". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

WHY?

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. Enter the path to the email template and then click the **Change** button. The email subject should be one that cause users to open the email and trust the contents.

WHAT ELSE?

Optionally, select a CSV file or targets' data tags.

9. Leave the default settings on the **Client-side Attack Setup** step. Then click **Finish** to start the Attack step of the RPT.

The screenshot shows a dialog box titled "Client-side Phishing Wizard" with the sub-header "Client-Side Phishing Attack Setup". Below the sub-header is the instruction "Select additional optional settings to setup." The main area contains a paragraph: "Configure advanced phishing attack options. If these options are not configured, Impact will use default options and global settings instead." Below this are three checked checkboxes: "Advanced options", "Mail sending options", and "Web server options". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

WHY?

These options will present additional settings for the RPT.

WHAT ELSE?

- Advanced options include URL Obfuscation and Grab SMB
- HTTP Proxy options will allow you to configure a Proxy server if one is required for your network access
- Post Exploitation Actions
- Agent Communications Settings

After starting Client-side Attack and Penetration:

Core Impact will send email(s) to the target user(s) you specified in setting up the attack. If any of the target users opens the email and clicks on the link inside of the email, their system will be exploited and an agent installed.

After Client-side Attack and Penetration has completed:

If Core Impact has successfully exploited any users' systems, you will be able to view the agent - and the user's system - in the Network Entity View. You can then run the [Local Information Gathering](#) step of the RPT, which will attempt to use the installed agent(s) to gather further information from the penetrated system(s).

Client-side Local Information Gathering

The **Local Information Gathering** 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.

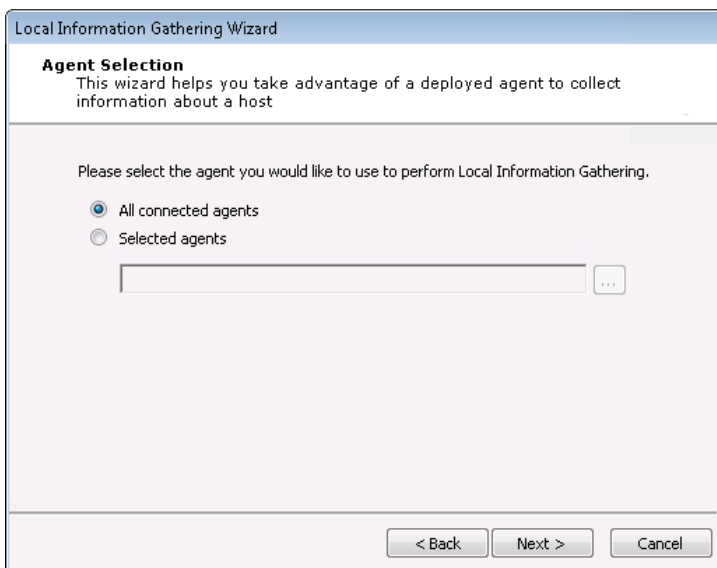
NOTE:

Before running Local Information Gathering, you should have active agents on one or more host targets and permission to run penetration tests on the system(s).

Below are the basic steps to running Local Information Gathering. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run Local Information Gathering:


1. Make sure that the **Client-side RPT** is active.
2. Click on **Local Information Gathering** to open up the Wizard, then click **Next** to continue.
3. On the **Agent Selection** step of the Wizard, click **Next** to continue.



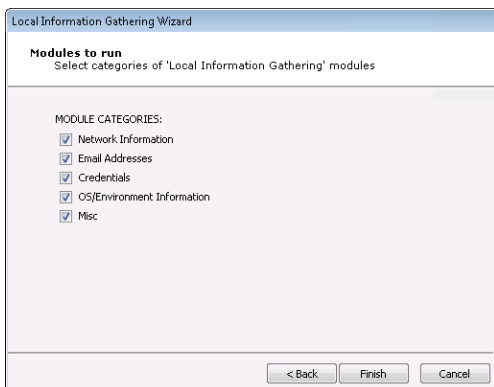
WHY?

By default, information will be gathered on all connected agents.

WHAT ELSE?

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.

4. In the **Modules to Run** window, leave the default selections and click **Finish** to continue.



WHY?

The RPT will attempt to gather information in the provided categories.

WHAT ELSE?

You can manually check/uncheck categories based on your testing requirements.

After starting Local Information Gathering:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of multiple modules that will run to complete the overall process.

After Local Information Gathering has completed:

If additional information has been gathered by the RPT, you will be able to view the data in the Entity Properties of the target(s). You can then run the [Privilege Escalation](#) step of the RPT, which will attempt to use the gathered data to gain privileges on the penetrated systems.

Client side Privilege Escalation

The **Privilege Escalation** 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**.

NOTE:

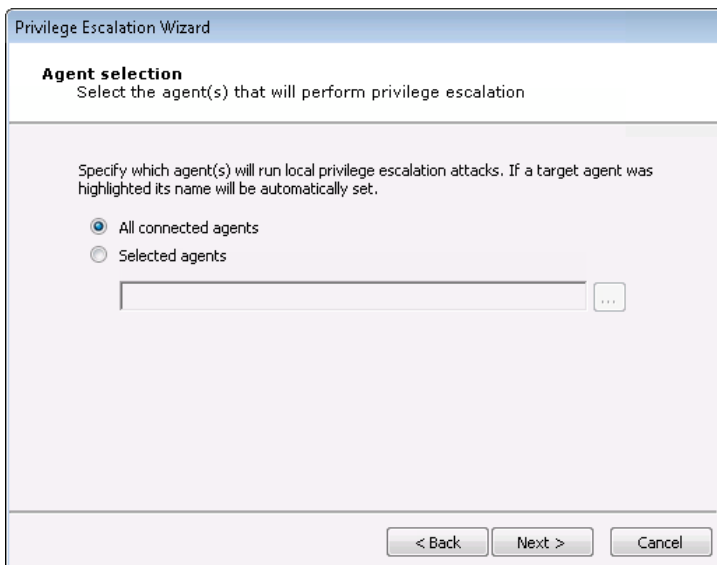
Before running Privilege Escalation, you should have active agents on one or more host targets and permission to run penetration tests on the system(s).

Below are the basic steps to running Privilege Escalation. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run Client-side Privilege Escalation:

1. Make sure that the **Client-side RPT** is active.
2. Click on **Privilege Escalation** to open up the Wizard, then click **Next** to continue.

3. On the **Agent Selection** step of the Wizard, click **Next** to continue.




The screenshot shows a window titled "Privilege Escalation Wizard" with a sub-header "Agent selection". Below the sub-header is the instruction "Select the agent(s) that will perform privilege escalation". A larger block of text explains: "Specify which agent(s) will run local privilege escalation attacks. If a target agent was highlighted its name will be automatically set." There are two radio buttons: "All connected agents" (which is selected) and "Selected agents". Below the "Selected agents" radio button is an empty text input field followed by an ellipsis button "...". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

WHY?

By default, information will be gathered on all connected agents.

WHAT ELSE?

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.

4. In the **Exploits Selection** window, leave the default selections and click **Finish** to continue.

The screenshot shows a window titled "Privilege Escalation Wizard" with a sub-header "Exploit selection" and the instruction "Customize the selection criteria for local exploits". The main content 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 of the window are three buttons: "< Back", "Next >", and "Cancel".

WHY?

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.

WHAT ELSE?

For a more aggressive attack strategy, check or uncheck the appropriate check-boxes.

After starting Privilege Escalation:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of many modules that will run to complete the overall process.

After Privilege Escalation has completed:

You may want to run the [Local Information Gathering](#) step (again) 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.

Clean Up

The **Clean Up** step automatically uninstalls all currently-connected agent(s) that resulted from your Client-side penetration testing.

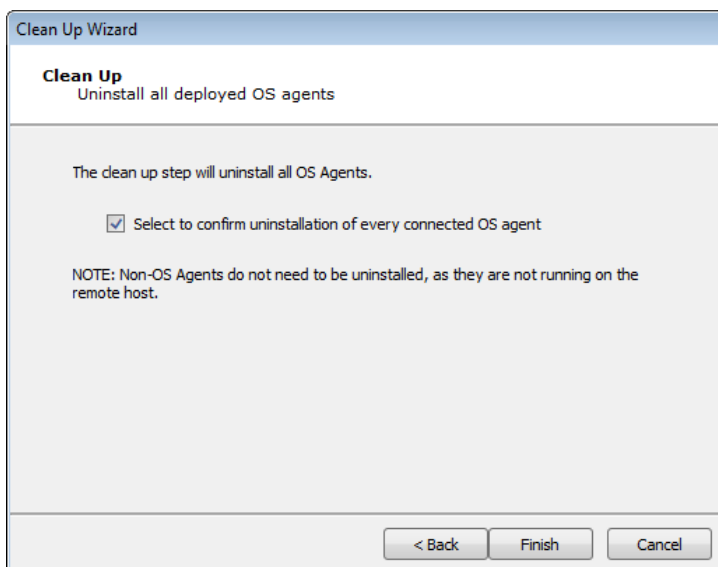
NOTE:

Before running Clean Up, you should have active agents on one or more host targets and permission to run penetration tests on the system(s).

Below are the basic steps to running Clean Up.

To run Clean Up:

1. Make sure that the **Client-side RPT** is active.
2. Click on **Clean Up** to open up the Wizard, then click **Finish** to continue.



After starting Clean Up:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of multiple modules that will run to complete the overall process.

After Clean Up has completed:

Any agents that were installed on target users' systems will be removed.

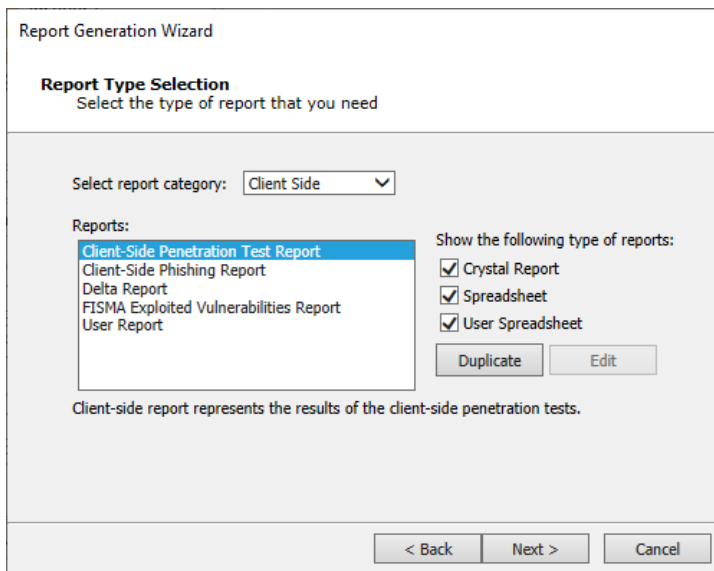
Client-side Report Generation

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.

Below are the basic steps to running Report Generation. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run Report Generation:

1. Make sure that the **Client-side RPT** is active.
2. Click on **Client-side Report Generation** to open up the Wizard, then click **Next** to continue.
3. Select the Report you wish to run, then click **Finish** to continue.



After Client-side Report Generation has completed:

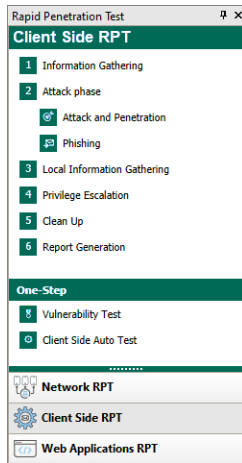
The report window will open, from which you can view, print, or export the report.

Phishing-based Client-side Tests

Overview

Core Impact makes it easy for you to frequently assess your organization's susceptibility to phishing, spear phishing and other social engineering techniques. Core Impact safely replicates email-based attacks to test end-user awareness and security practices. Phishing

testing will enable you to learn how many of your users would expose your environment to attack by measuring how many would click on a link in an unsolicited email they receive. Coupled with the results of a Client-side workstation Test you can paint a full picture of the amount of risk that users introduce to the environment.



Getting Started

A Client-side Phishing test is comprised of the following steps - click one to learn more about how to execute the step:

1. [Information Gathering](#)
2. [Attack Phase: Phishing](#)
3. [Client-side Report Generation](#)

Client-side Information Gathering

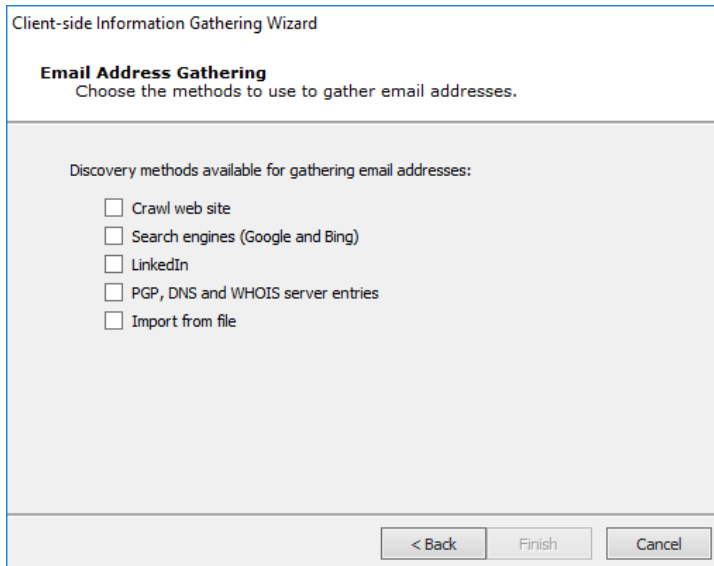
Using the **Client-side Information Gathering** wizard, you can harvest email addresses that are visible from the Internet or your intranet. Harvesting email addresses from your registered domain in the Internet gives you a good idea of your end-users' exposure to identification by external attackers.

Below are the basic steps to running Client-side Information Gathering. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run Client-side Information Gathering:

1. Make sure that the **Client-side RPT** is active.
2. Click on **Client-side Information Gathering** to open up the Information Gathering Wizard, then click **Next** to continue.

3. Set discovery method to **Search engines**. Then click **Next** to continue.



The screenshot shows a window titled "Client-side Information Gathering Wizard" with a sub-header "Email Address Gathering". Below the sub-header is the instruction "Choose the methods to use to gather email addresses." The main area is titled "Discovery methods available for gathering email addresses:" and contains five unchecked checkboxes: "Crawl web site", "Search engines (Google and Bing)", "LinkedIn", "PGP, DNS and WHOIS server entries", and "Import from file". At the bottom of the window are three buttons: "< Back", "Finish", and "Cancel".

WHY?

The **Search Engines** setting uses Google or Bing search engines to locate email addresses in public on-line records. An attacker might use the exact same method to locate target email addresses.

WHAT ELSE?

- **Search in PGP, DNS and WHOIS** uses Public Internet Databases to locate email addresses.
 - **Crawl Web Site** to can search within a specific web site to explore for email addresses or documents.
 - **Import from file:** Select this option if you have a local file that contains your target email addresses.
 - **LinkedIn:** Select this option to have CORE Impact search through the web site LinkedIn to locate users for a specific company. If you select this option, you can further configure it in a subsequent step of the wizard.
4. Enter the domain(s) for which you want to discover email addresses. For example, if you enter company.com, the crawler will search for an record all email addresses it finds that end in @company.com. Then click **Next** to continue.

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

WHY?

For example, if you enter company.com, the crawler will search for and record all email addresses it finds that end in @company.com.

5. Leave the default settings on the **Web Crawling and Search Engines Options** step. Then click **Next** to continue.

Client-side Information Gathering Wizard

Web Crawling and Search Engines Options
Configure options for web site crawling and search engine results.

Configure web site crawling restrictions (this also applies to web sites crawled based on search engine results).

Max. link depth to crawl

Max. number of pages the crawler should process

Max. web resource download size (in kilobytes)

Configure the number of results from search engines to process.

Max. number of results from Google to process

Max. number of results from Bing to process

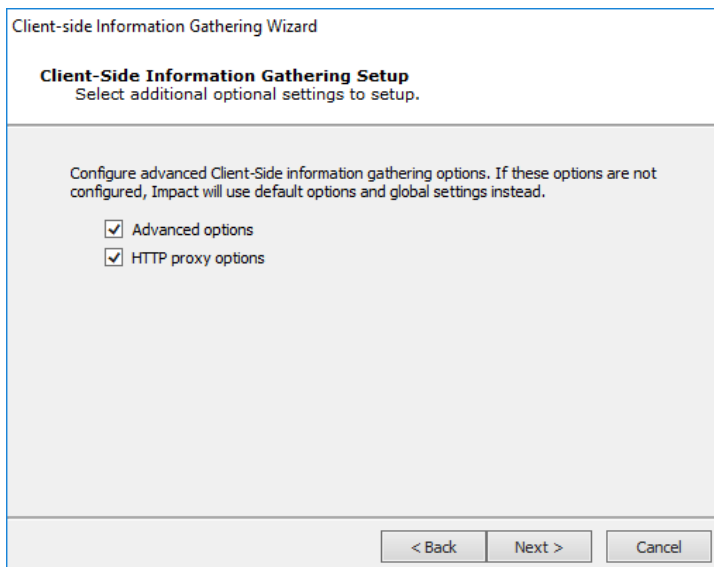
< Back Next > Cancel

WHY?

These options dictate the scope and depth of the Information Gathering step.

WHAT ELSE?

- 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.
6. Leave the default settings on the **Client-side Information Gathering Setup** step. Then click **Finish** to start the Information Gathering step of the RPT.



The screenshot shows a wizard window titled "Client-side Information Gathering Wizard". The current step is "Client-Side Information Gathering Setup", with the instruction "Select additional optional settings to setup." Below this, a text block reads: "Configure advanced Client-Side information gathering options. If these options are not configured, Impact will use default options and global settings instead." Two options are listed with checked checkboxes: "Advanced options" and "HTTP proxy options". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

WHY?

These options will present additional settings for the RPT.

WHAT ELSE?

- **Search for metadata inside Microsoft Office 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.
- HTTP Proxy options will allow you to configure a Proxy server if one is required for your network access

After starting Client-side Information Gathering:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of multiple modules that will run to complete the overall process.

After Client-side Information Gathering has completed:

If Core Impact, 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. You can then run the [Client-side Attack and Penetration](#) or [Client-side Phishing](#) step of the RPT.

Client-side Phishing

Using the **Client-side Phishing** wizard, you can execute a Phishing-based test on your email users.

NOTE:

Before running Client-side Phishing , you should know the email addresses of the users you want the penetration test to target, and you should have permission to do so.

Below are the basic steps to running Client-side Phishing test. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run a Client-side Phishing test:

1. Make sure that the **Client-side RPT** is active.
2. Click on **Phishing** under Attack Phase to open up the Phishing Wizard, then click **Next** to continue.
3. Leave the default setting of **Web Page Redirect** on the **Phishing Type Selection** step and enter in the URL where the browser is redirected after the user clicks the link. Then click **Next** to continue.

The screenshot shows a window titled "Client-side Phishing Wizard" with a section "Phishing Type Selection" and the instruction "Select the kind of client-side Phishing you want to perform". There are two radio button options: "Web Page Redirect" (selected) and "Web Page Clone". The "Web Page Redirect" option includes a text field containing "www.google.com". The "Web Page Clone" option includes a text field for the URL to be impersonated, three checkboxes for "Save submitted form data" (checked), "Ignore forms without credentials" (checked), and "Redirect user after data submission" (unchecked), and another text field for the URL of the web form to be redirected. At the bottom are buttons for "< Back", "Next >", and "Cancel".

WHY?

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.

WHAT ELSE?

The Web Page Clone 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).

4. 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. Then click **Next** to continue.

Client-side Phishing 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

5. Leave the default settings on the **Email Template Selection** step. Then click **Next** to continue.

Client-side Phishing 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

WHY?

Core Impact ships with several email templates that you can customize when planning a Phishing test.

WHAT ELSE?

You can import an email that has been exported from Outlook or Thunderbird and use that as the basis for your Phishing email.

6. Leave the default settings on the **End User Experience** step. Then click **Next** to continue.

Client-side Phishing 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: ▾

Inserts an image into the email body and registers the targets that have requested it

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

< Back Next > Cancel

WHY?

Core Impactships 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. Enter the path to the email template and then click the Change button. The email subject should be one that cause users to open the email and trust the contents.

WHAT ELSE?

Optionally, opt to insert an image into the body of the email. With this method, Core Impact will be able to detect if a recipient of the email opens the email, which will cause a request for the image. Also, select Obfuscate URL to mask the URL that will be used in the email.

7. Leave the default settings on the **Client-side Phishing Attack Setup** step. Then click **Finish** to start the Attack step of the RPT.

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

< Back Next > Cancel

WHY?

These options will present additional settings for the RPT.

WHAT ELSE?

- Advanced options include URL Obfuscation and Grab SMB
- HTTP Proxy options will allow you to configure a Proxy server if one is required for your network access

After starting Client-side Phishing:

Core Impact will send email(s) to the target user(s) you specified in setting up the attack. If any of the target users opens the email and clicks on the link inside of the email, Core Impact will record this information.

After Client-side Phishing has completed:

If any users have clicked on the link provided in the attack, this information will be stored in the Client Side entity view. You can then run [Client-side Reports](#) to learn more.

Client-side Report Generation

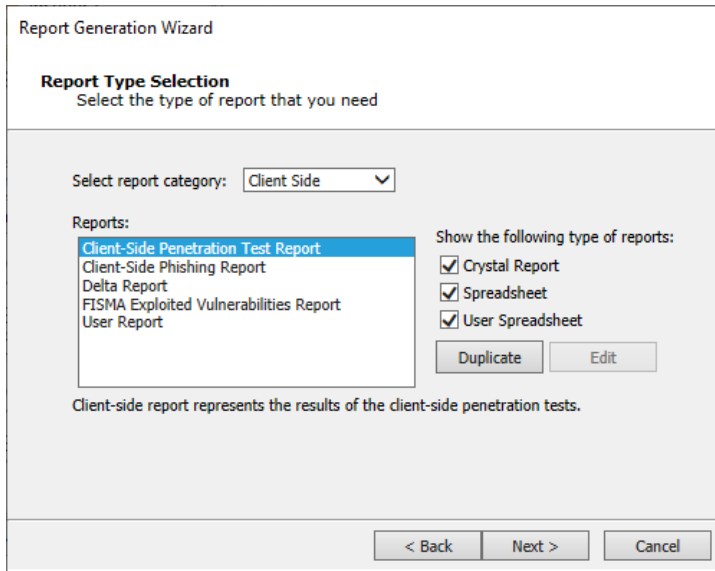
The Client-side Report Generation step allows you to automatically generate robust system reports by processing information collected about the target systems and the different penetration tests you have performed.

Below are the basic steps to running Report Generation. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run Report Generation:

1. Make sure that the **Client-side RPT** is active.
2. Click on **Client-side Report Generation** to open up the Wizard, then click **Next** to continue.

3. Select the Report you wish to run, then click **Finish** to continue.



After Client-side Report Generation has completed:

The report window will open, from which you can view, print, or export the report.

Client-side Workstation Tests

Overview

In some environments, the aim is to include users in the client-side testing. In others, the security team must review new versions of standard desktop builds. By automating the execution of client-side exploits against an end user machine provided to the security tester, Core Impact can return a list of the exploits that are capable of compromising the target. This can allow the security team to easily determine the risk(s) that the image or machine contains.

Getting Started

To execute a **Client-side Auto Test**, follow the steps outlined [here](#).

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.

NOTE:

Before running Client-side Auto Test, you should have a single machine that ready to test, and you should have permission to do so.

Below are the basic steps to running Client-side Auto Test. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run a Client-side Auto Test:

1. Make sure that the **Client-side RPT** is active.
2. Click on **Client-side Auto Test** to open up the Wizard, then click **Next** to continue.
3. On the **Agent Selection** step, click the ellipsis button  and choose an agent from the entity list, then click **Ok**. Back on the Wizard, click **Next** to continue.

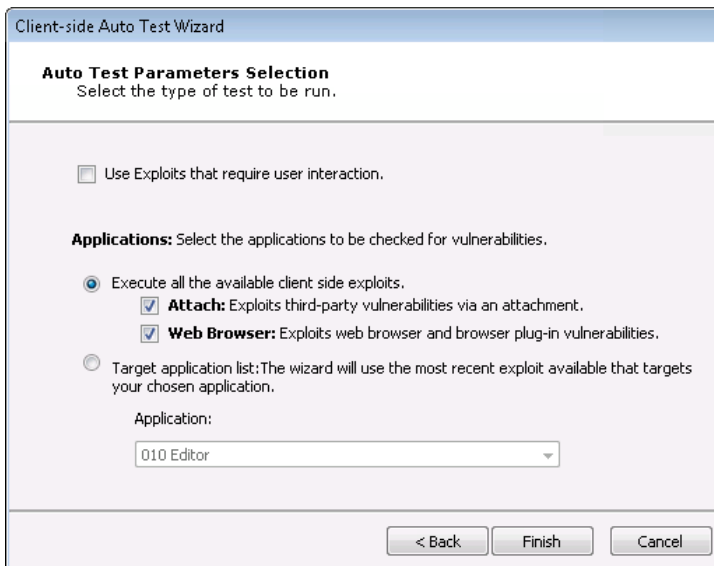
WHY?

The test needs an agent in order to run on the target host.

WHAT ELSE?

You can choose and configure the **Install Agent using SMB** option to manually install an agent as a part of the Auto Test.

4. Leave the default settings on the **Auto Test Parameters Selection** step. Then click **Finish** to start the test.



WHAT ELSE?

You can select other options for the Auto Test:

- Check the **Use Exploits that require user interaction** box if you want the test to use exploits that would require a user to take action in order for the exploit to succeed.
- Select which applications are to be checked for vulnerabilities:
 - Execute all available client-side exploits (**Attach** and/or **Web Browser** exploits).
 - Select a specific application to target from the **Application** drop-down menu.

After starting Client-side Auto Test:

You can view the Modules panel and see the progress of each step in the process.

After Client-side Auto Test has completed:

You can view a list of successful and failed (defended) exploits on the Module Output tab of the Modules pane. You can then focus on addressing any vulnerabilities before deploying the desktop image to your user community.

Web Applications RPT

The Web Applications RPT allows you to target your Web Applications and test for potentially vulnerable pages.

What kind of WebApps test do you want to perform?

- [Risk Assessment](#)
- [Vulnerability Scanner Validation](#)

WebApps Risk Assessment Tests

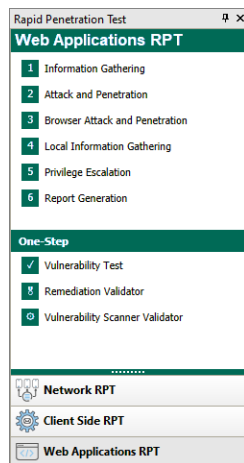
Overview

More and more organizations are moving their services and workflows to web applications. These web applications could contain vulnerabilities that expose not only that application's data to risk but the systems around it. It is therefore critical to proactively test your organization's ability to detect, prevent and respond to web application threats.

Performing a WebApps Risk Assessment test with Core Impact's RPT enables you to quickly determine the risk present in your environment and priorities the remediation.

Getting Started

To execute a **WebApps Risk Assessment**, follow the steps outlined here.



The RPT is divided into the following steps - click one to learn more about how to execute the step:

1. [WebApps Information Gathering](#)
2. [WebApps Attack and Penetration](#)
3. [WebApps Browser Attack and Penetration](#)
4. [WebApps Local Information Gathering](#)
5. [WebApps Report Generation](#)

WebApps Information Gathering

The **WebApps Information Gathering** scans the domain of a known web-based application and identifies pages which can subsequently be tested for vulnerabilities.

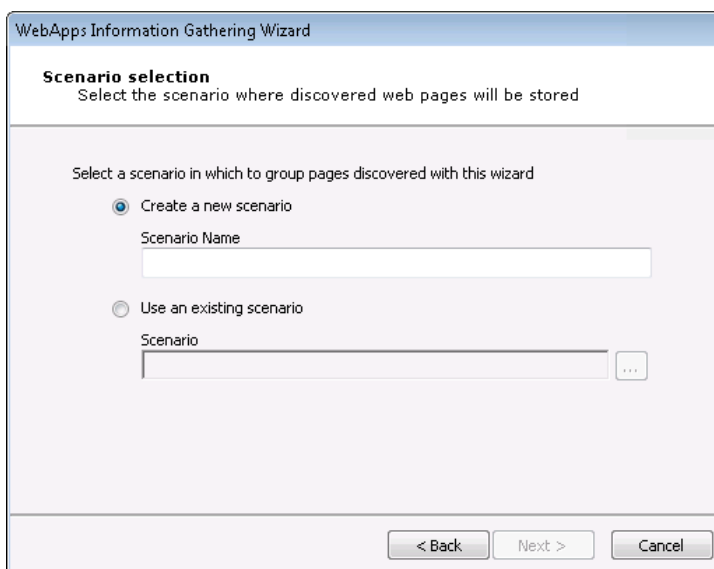
NOTE:

Before running WebApps Information Gathering, you should know the IP address(es) or URL(s) of the web application(s) you want the penetration test to target, and you should have permission to do so.

Below are the basic steps to running WebApps Information Gathering. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run WebApps Information Gathering:

1. Make sure that the **WebApps RPT** is active.
2. Click on **WebApps Information Gathering** to open up the Information Gathering Wizard, then click **Next** to continue.
3. Leave the default option of **Create a new Scenario**, then enter a **Scenario Name**. Then click **Next** to continue.




The screenshot shows a dialog box titled "WebApps Information Gathering Wizard". The main heading is "Scenario selection" with the instruction "Select the scenario where discovered web pages will be stored". Below this, there is a sub-instruction: "Select a scenario in which to group pages discovered with this wizard". There are two radio button options: "Create a new scenario" (which is selected) and "Use an existing scenario". Under "Create a new scenario", there is a text input field labeled "Scenario Name". Under "Use an existing scenario", there is a text input field labeled "Scenario" followed by a browse button (three dots). At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

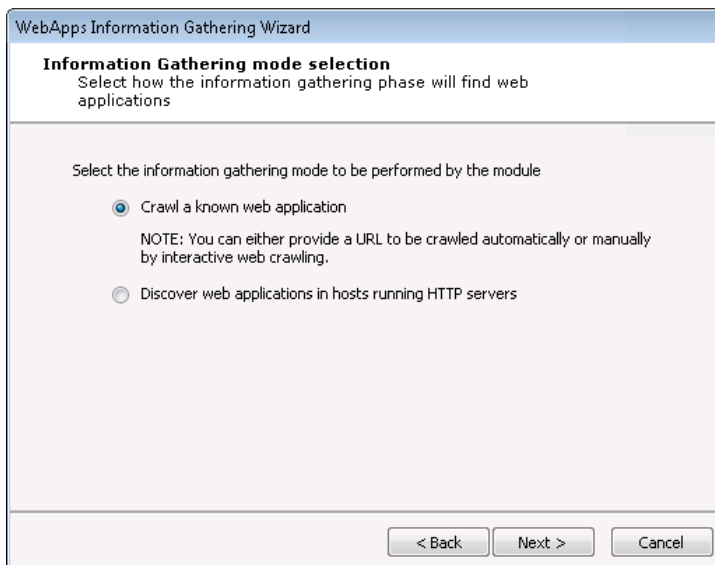
WHY?

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.

WHAT ELSE?

If you already have a Scenario in your entity database, you can choose the **Use an existing scenario** option, then click the ellipsis button  to select your Scenario.

4. Leave the default option of **Crawl a known web application**, then click **Next** to continue.



WHY?

You use this option when you know of and want to target specific web applications in your environment.

WHAT ELSE?

If you do not know of running web applications, or you want to test the ability of web applications being detected, select the **Discover web applications in hosts running HTTP servers** option. Core Impact will scan known hosts to detect whether there are HTTP servers running on them. If

there are, Core Impact will target those servers in the WebApps test.

5. Leave the default option of **Automatic web crawling**, then enter the **URL** to your web application. Then click **Next** to continue.

WebApps Information Gathering Wizard

Crawling mode selection
Select the crawling mode to be used

Select the web crawling mode to be used to learn the web site structure

Automatic web crawling
URL

Interactive web crawling
 Interactive crawling of a mobile application backend
 Import web resources from Burp Suite

< Back Next > Cancel

WHY?

With this option, Core Impact will automatically crawl (navigate) the target web application and look for pages that might be vulnerable.

WHAT ELSE?

- With the **Interactive web crawling** option, you set your web browser to use Core Impact as a proxy and then navigate your web application manually. 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.
 - With the **Interactive crawling of a mobile backend** option, you set your mobile device to use Core Impact as a proxy and then use your mobile app manually. As you use the app, Core Impact will harvest the traffic and evaluate web services that may be vulnerable.
6. Configure the **Proxy Settings** that correspond to your environment. Then click **Next** to continue.

The screenshot shows the 'Proxy Settings' step of the 'WebApps Information Gathering Wizard'. The title bar reads 'WebApps Information Gathering Wizard'. Below the title, the section is titled 'Proxy Settings' with the subtitle 'Configure the proxy required to crawl your website'. There are four radio button options: 'Direct connection to the web site' (selected), 'Use the proxy settings defined in the global Network options', 'Use Internet Explorer proxy settings', and 'Use custom proxy settings'. Below these are input fields for 'Address', 'Port' (set to 8080), 'Username', 'Password', and an 'Exception List' text area. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

WHY?

Core Impact needs to have access to the target web application so, if a proxy is needed, you will have to configure it accordingly.

7. Leave the default options on the **Automatic Crawling Options** step, then click **Next** to continue.

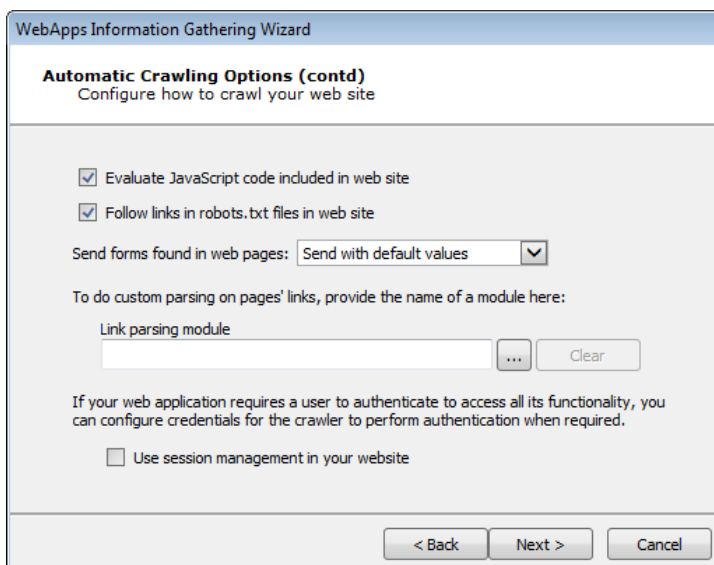
The screenshot shows the 'Automatic Crawling Options' step of the 'WebApps Information Gathering Wizard'. The title bar reads 'WebApps Information Gathering Wizard'. Below the title, the section is titled 'Automatic Crawling Options' with the subtitle 'Configure how to crawl your web site'. It features a dropdown menu for 'Select web browser to impersonate:' set to 'Internet Explorer 11.0'. There is a text field for 'Custom user agent:'. Below are several checked checkboxes: 'Max. number of pages the crawler should process' (set to 300), 'Max. depth level to crawl' (set to 3), 'Restrict crawling to starting page domain', and 'Detect web application framework'. There is also a text field for 'Additional domains to allow during crawling (for example: *.coresecurity.com)' with a note below it: 'NOTE: Use semicolons (;) to separate entries.' At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

WHY?

Using these options, you can further control how the test is performed.

WHAT ELSE?

- 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.
8. Leave the default options on the **Automatic Crawling Options (Cont.)** step, then click **Next**.



The screenshot shows a dialog box titled "WebApps Information Gathering Wizard" with the subtitle "Automatic Crawling Options (contd) Configure how to crawl your web site". The dialog contains several options:

- 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 (dropdown menu)
- To do custom parsing on pages' links, provide the name of a module here:
Link parsing module: [text input] [Browse] [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

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

WHY?

Using these options, you can further control how the test is performed.

WHAT ELSE?

- 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.
 - If you want the web crawler to log in to the web application, check the **Use session management in your website** check-box.
9. Leave the default options on the **Web Services Discovery Options** step, then click **Finish** to start the test.

The screenshot shows the 'Web Services Discovery Options' step of the 'WebApps Information Gathering Wizard'. The window title is 'WebApps Information Gathering Wizard'. The main heading is 'Web Services Discovery Options' with the subtitle 'Configure how to search for web services'. The options are as follows:

- Search for SOAP web services definitions
- Append '?wsdl' to every found URL
- How method parameters values should be filled: Complete with default values (dropdown menu)
- How SOAP operations found in a definition file should authenticate:
 - Use the same as for crawling web pages
 - Use SOAP WS-Security
- Username: [text input field]
- Password: [text input field]

NOTE: To detect web service calls done in web pages the JavaScript evaluation option in the Automatic Crawling Options should be enabled.

Buttons at the bottom: < Back, Finish, Cancel

WHY?

Using these options, you can opt for the RPT to look for any SOAP-based web services.

WHAT ELSE?

- **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.

After starting WebApps Information Gathering:

- You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of many modules that will run to complete the overall process.
- If your target web application has been successfully found by Core Impact, a list of web pages from the application will be listed in the Web view of the Entity database (under the associated Scenario). You can then run the [WebApps Attack and Penetration](#) step of the RPT, which will attempt to identify potential vulnerabilities in the found pages.

WebApps Attack and Penetration


The **WebApps Attack and Penetration** scans web pages found during WebApps Information Gathering and identifies pages that may be vulnerable to potential attacks.

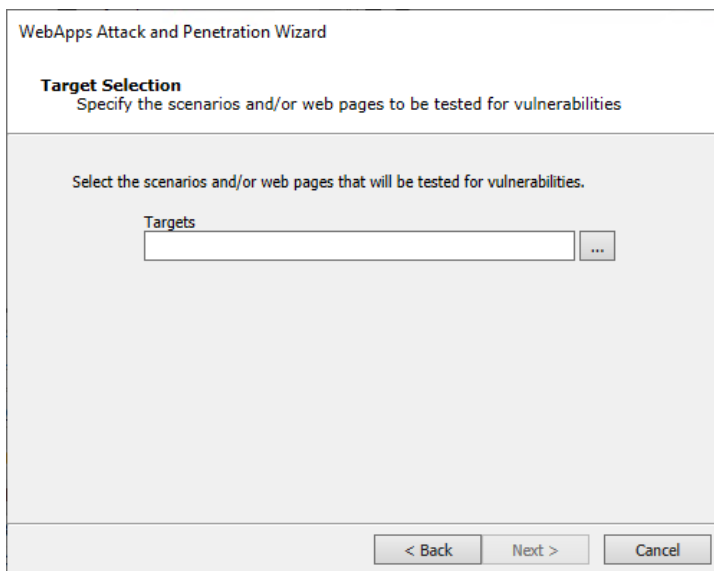
NOTE:

Before running WebApps Attack and Penetration, you should have already identified one or more web pages from web application. The pages will be listed in the Web view of the entity database under the associated Scenario.

Below are the basic steps to running WebApps Attack and Penetration. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run WebApps Attack and Penetration:

1. Make sure that the **WebApps RPT** is active.
2. Click on **WebApps Attack and Penetration** to open up the Attack and Penetration Wizard, then click **Next** to continue.
3. On the **Target Selection** step, click the ellipsis button  and select the web page (s) or Scenarios that you want to test for vulnerabilities. Click **Ok**, then click **Next** to continue.



The screenshot shows a dialog box titled "WebApps Attack and Penetration Wizard" with the "Target Selection" step selected. The subtitle reads "Specify the scenarios and/or web pages to be tested for vulnerabilities". The main instruction is "Select the scenarios and/or web pages that will be tested for vulnerabilities." Below this is a text input field labeled "Targets" with an ellipsis button to its right. At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

WHY?

WebApps Attack and Penetration step can detect whether those pages will be vulnerable to a number of different attack types.

4. Leave the default selections on the **Risk Types** step, then click **Next** to continue.

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

WHY?

Core Impact provides test capabilities that correspond to the OWASP Top 10 vulnerabilities for web applications.

WHAT ELSE?

Select the test categories you wish to run against your web pages. Each option will add configuration steps in the Wizard.

5. Leave the default selections on the **Risk Types (contd)** step, then click **Next** to continue.

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

WHY?

Core Impact provides test capabilities that correspond to the OWASP Top 10 vulnerabilities for web applications.

WHAT ELSE?

Select the test categories you wish to run against your web pages. Each option will add configuration steps in the Wizard.

- Leave the default selections on the **Risk Types (contd)** step, then click **Next** to continue.

WHY?

In addition to the OWASP Top 10 categories, Core Impact can **Look for PHP remote local file inclusion vulnerabilities** in your web apps as well as **Invalid redirects or lookups** and **Hidden/Backup pages**.

WHAT ELSE?

Check the **Execute exploits for known vulnerabilities** option if you want Core Impact to attempt to execute exploits as a part of the test.

- Leave the default options on the **SQL Injection tests configuration** step, then click **Next** to continue.

WebApps Attack and Penetration Wizard

SQL Injection tests configuration
Customize parameters for SQL Injection tests

Select which web page's parameters to test for SQL Injection:

Request parameters Request cookies

Select depth of SQL Injection tests to be applied to web pages' input:

To configure a custom error page detection to identify SQL Injection vulnerabilities, check the following option:

Use custom error page detection

< Back Next > Cancel

WHY?

Because the **A1 - Injection** option was selected as a Risk Type, the test requires additional setup. SQL Injection tests can be performed for **Request parameters** or **Request cookies**.

WHAT ELSE?

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. This will require additional configurations in the Wizard.

8. Depending on which Risk Type(s) were selected in the wizard, you will see additional steps to configure options. When you've reached the final wizard page, click **Finish** to start the test.

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
 ...

To configure a module to prevent crawling links that may terminate the session, provide the name of a module here:

Logout forbidden link module
 ...

< Back **Finish** Cancel

After starting WebApps Attack and Penetration:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of many modules that will run to complete the overall process.

After WebApps Attack and Penetration has completed:

If any target web pages have potential vulnerabilities, you will see WebApps agents under the page(s) in the Web view of the Entity database. You can view pages under the corresponding risk category or under the Scenario itself.

If you opted to search for SQLi or PHP-RFI, you can then run the [WebApps Local Information Gathering](#) step of the RPT.

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 attempt to exploit any vulnerable web pages.

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.

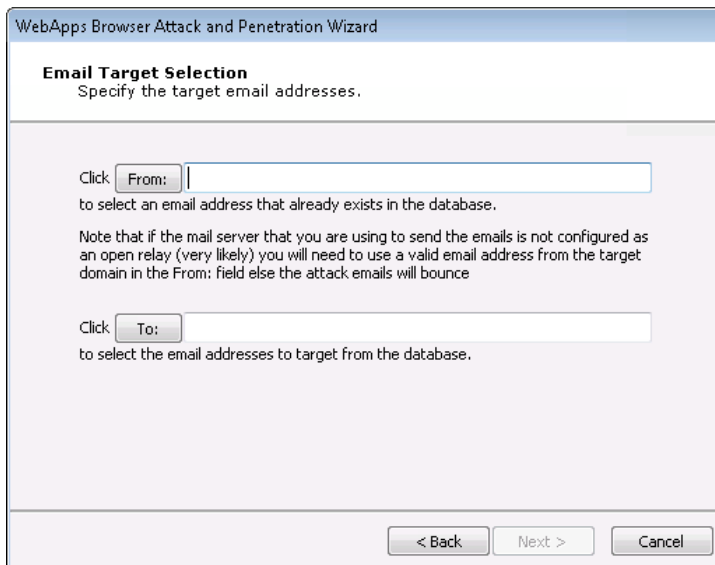
NOTE:

Before running WebApps Browser Attack and Penetration, you should have already identified one or more web pages from web application that have XSS agents attached to them. The pages will be listed in the Web view of the entity database under the associated Scenario.

Below are the basic steps to running WebApps Browser Attack and Penetration. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run WebApps Browser Attack and Penetration:

1. Make sure that the **WebApps RPT** is active.
2. Click on **WebApps Browser Attack and Penetration** to open up the Attack and Penetration Wizard, then click **Next** to continue.
3. On the **Email Target Selection** step, 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. Then click **Next** to continue.

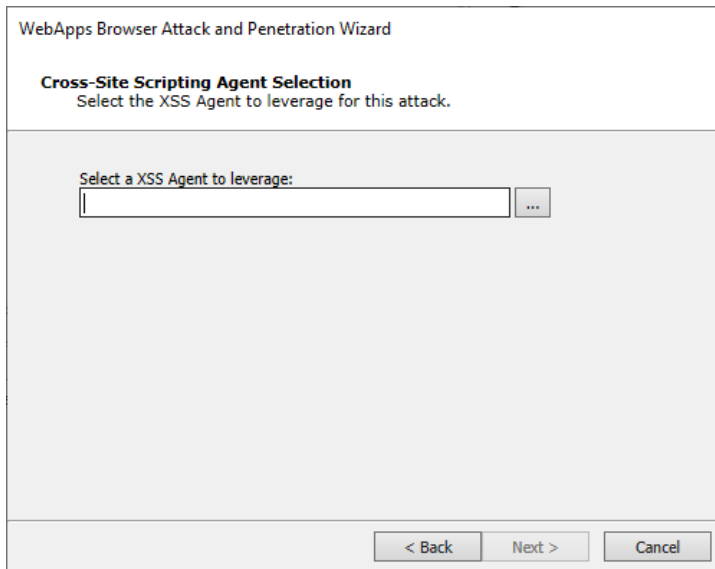


The screenshot shows a window titled "WebApps Browser Attack and Penetration Wizard" with the "Email Target Selection" step. The instruction is "Specify the target email addresses." There are two input fields: "From:" and "To:". The "From:" field has a button labeled "From:" to its left and a text box. Below it, the text says "to select an email address that already exists in the database." A note follows: "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". The "To:" field has a button labeled "To:" to its left and a text box. Below it, the text says "to select the email addresses to target from the database." At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

WHY?

This RPT will email the users in the **To:** field. The email will appear to come from the user in the **From:** field.

- Click the ellipsis button next to the **Select a XSS Agent to leverage** field and select a XSS agent from the Entity database. Click Ok, then click **Next** to continue with the Wizard.



WHY?

Core Impact will send an email to targeted users and provide a link which, when clicked, will exploit the XSS vulnerability.

WHAT ELSE?

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. Enter the path to the email template and then click the **Change** button. The email subject should be one that cause users to open the email and trust the contents.

- Enter details for your **SMTP Server** and **SMTP Port**, then click **Finish** to start the test.

The screenshot shows a wizard window titled "WebApps Browser Attack and Penetration Wizard" with a sub-section "Email Sending Settings" and the instruction "Customize the settings for sending emails." Below this, a note states: "If a SMTP server is not provided, a DNS query will be done to find the MX record for the SMTP server for each target domain." The form contains several input fields: "SMTP server:" (empty), "SMTP port:" (25), "Connection security:" (None), "User name:" (empty), "Password:" (empty with a small 'A' icon), "Numbers of targets in each chunk" section with "Chunk size:" (100) and "Set the time to wait between chunks (in seconds)" section with "Delay(s):" (1). At the bottom are three buttons: "< Back", "Finish", and "Cancel".

WHY?

Core Impact will send an email to targeted users and therefore needs access to a functioning SMTP server.

After starting WebApps Browser Attack and Penetration:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of many modules that will run to complete the overall process. 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 from the RPT.

After WebApps Browser Attack and Penetration has completed:

If any targeted users click on the link contained in the email, an agent will be installed on their system. At this point, you have successfully exploited a XSS vulnerability in your web application. You can also take the test another step by performing Local Information Gathering on any user machines that now have an agent installed.

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 both SQLi and PHP-RFI Agents, the RPT will run the following modules:

- Get Databases Version
- Get Databases Logins
- Get Databases Schema
- Check for Sensitive Information


For PHP-RFI Agents only, the RPT will also run the module **Get Local Path of web page using RFI Agent (PHP)**.

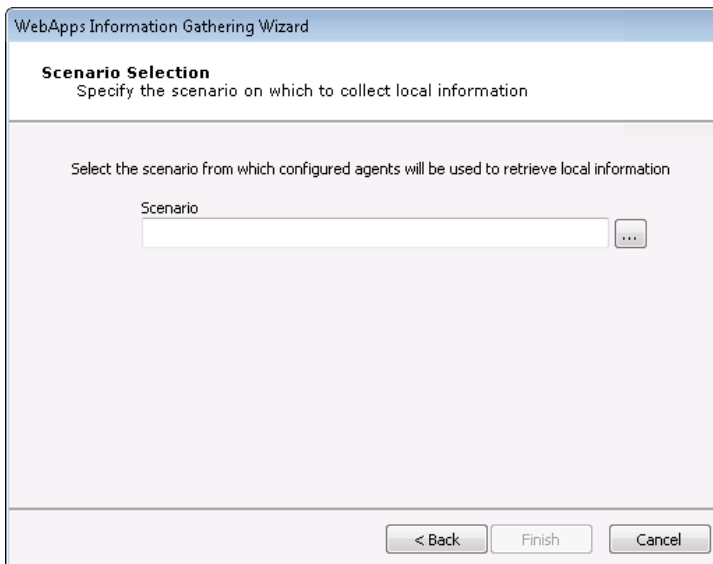
NOTE:

Before running WebApps Local Information Gathering, you should have SQLi or PHP-RFI agents already attached to web pages in your entity database.

Below are the basic steps to running WebApps Local Information Gathering. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run WebApps Local Information Gathering:

1. Make sure that the **WebApps RPT** is active.
2. Click on **WebApps Local Information Gathering** to open up the Information Gathering Wizard, then click **Next** to continue.
3. On the **Scenario Selection** step, click the ellipsis button  and select the Scenario (s) for which you want to do Local Information Gathering. Click **Ok**, then click **Finish** to start the test.



WHY?

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.

After starting WebApps Local Information Gathering:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of many modules that will run to complete the overall process.

After WebApps Local Information Gathering has completed:

If your target web pages have been successfully exploited by Core Impact, details about the web application's underlying database server will be added to the appropriate category in the **Identities** folder of the Entity database. At this point, your WebApps Local Information gathering has successfully used SQLi or PHP-RFI vulnerabilities in the web application and exposed potentially sensitive and exploitable data in the application's data storage.

WebApps Report Generation

The WebApps 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.

Below are the basic steps to running WebApps Report Generation. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run WebApps Report Generation:

1. Make sure that the **WebApps RPT** is active.
2. Click on **WebApps Report Generation** to open up the Wizard, then click **Next** to continue.
3. Select the Report you wish to run, then click **Finish** to continue.

After WebApps Report Generation has completed:

The report window will open, from which you can view, print, or export the report.

WebApps Vulnerability Scanner Validation

Overview

A vulnerability management strategy typically involves multiple steps:

1. Scanning the target web application
2. Identifying which potential vulnerability poses a true risk to the environment
3. Determining the scope of that risk
4. Prioritizing the remediation efforts
5. Re-testing to ensure the remediation was effective

Using Core Impact you can import the results of a web application vulnerability scan and determine which potential threats can be leveraged to expose true risk to data and system integrity via the web application.

Getting Started

To execute a **WebApps Vulnerability Scanner Validation**, follow the steps outlined [here](#).

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 **WebApps Vulnerability Scanner Validator**. Core Impact will evaluate the scan's output and determine whether each vulnerability can be exploited, providing you with a prioritized validation of your system's weaknesses.

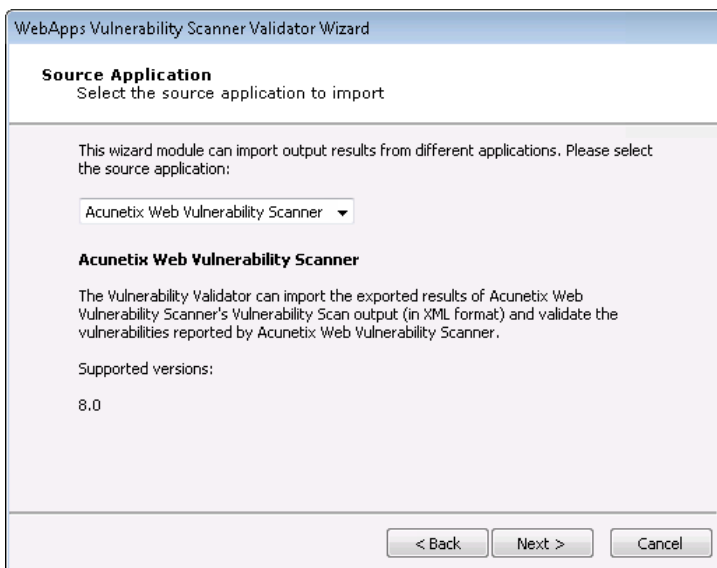
NOTE:


Before running WebApps 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.

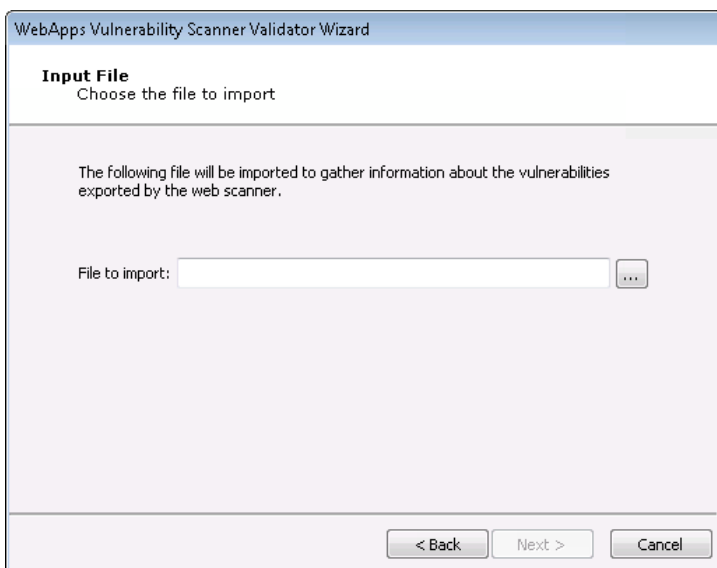
Below are the basic steps to running WebApps Vulnerability Scanner Validator. Hover over the images and expand the **WHY?** and **WHAT ELSE?** sections to learn more about each step.

To run the WebApps Vulnerability Scanner Validator:

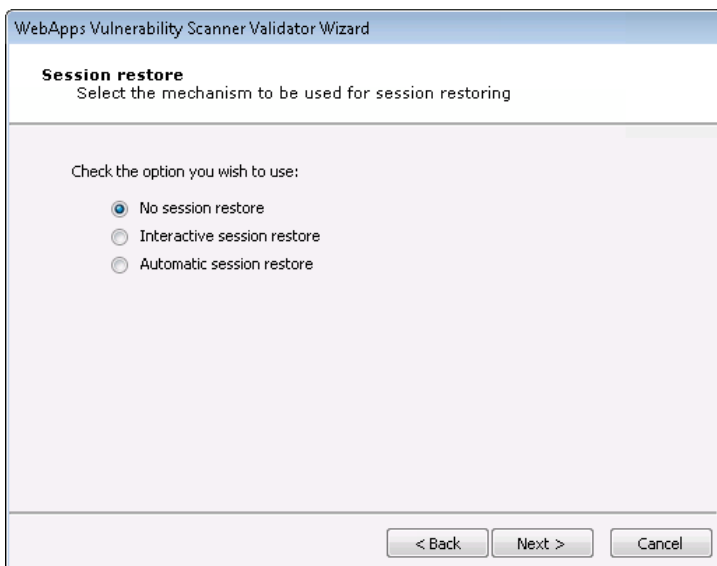
1. Make sure that the **WebApps RPT** is active.
2. Click on **WebApps Vulnerability Scanner Validator** to open up the Wizard, then click **Next** to continue.
3. On the **Source Application** step, use the drop-down menu to select the third-party scanner from which you got your results. Then click **Next** to continue.



- Next to the **File to import** field, click the ellipsis button  and locate/select the output file from the third-party scanner. Then click **Next** to continue.



- Leave the default selection on the **Session Restore** step, then click **Next** to continue.



WHY?

Core Impact can attempt to reestablish a connection to the target web application. Selecting **No session restore** will prevent Core Impact from attempting to log into the target web application.

WHAT ELSE?

- **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.
- **Automatic session restore:** With this option, you define the credentials Core Impact should use in authenticating in your web application.

6. Configure the **Proxy Settings** that correspond to your environment. Then click **Finish** to start the test.

The screenshot shows a dialog box titled "WebApps Vulnerability Scanner Validator Wizard" with a sub-section "Proxy Settings" and the instruction "Configure the proxy required to request webpages". There are four radio button options: "Direct connection to the internet" (selected), "Use the proxy settings defined in the global Network options", "Use Internet Explorer proxy settings", and "Use custom proxy settings". Below these are input fields for "Address" and "Port" (with "8080" in the port field), "Username" and "Password" (with a "A" button next to the password field), and an "Exception List" text area. At the bottom are "< Back", "Finish", and "Cancel" buttons.

WHY?

Core Impact needs to have access to the target web application so, if a proxy is needed, you will have to configure it accordingly.

After starting the WebApps Vulnerability Scanner Validator:

You can view the Modules panel and see the progress of each step in the process - each RPT step is made up of many modules that will run to complete the overall process.

After the WebApps Vulnerability Scanner Validator has completed:

Any target web pages that have potential vulnerabilities will be listed under Web view of the Entity database. You can view pages under the corresponding risk category or under the Scenario itself.

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 Community Portal](https://community.fortra.com) at <https://community.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.