

## Instructions to Access CORE IMPACT lab in the AWS Cloud

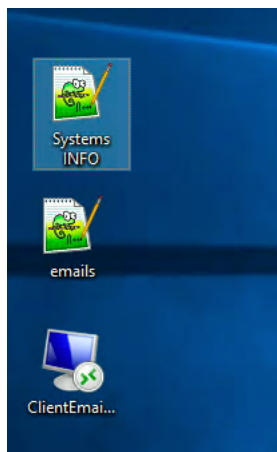
Using Remote Desktop, remote desktop into the Core Impact machine, please use following credential :

Username : ImpactUser

Password : <will be given to you by our se>

## File to assist Core Impact test in AWS lab

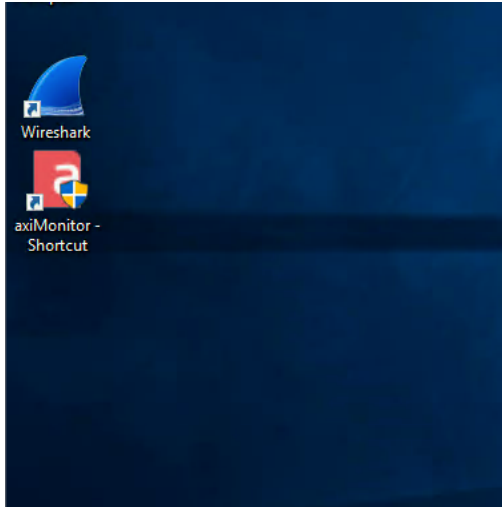
Open Systems INFO file in Desktop. The file consists of all information required to conduct Network Testing, Web Application Penetration Testing and Client side Penetration Testing.



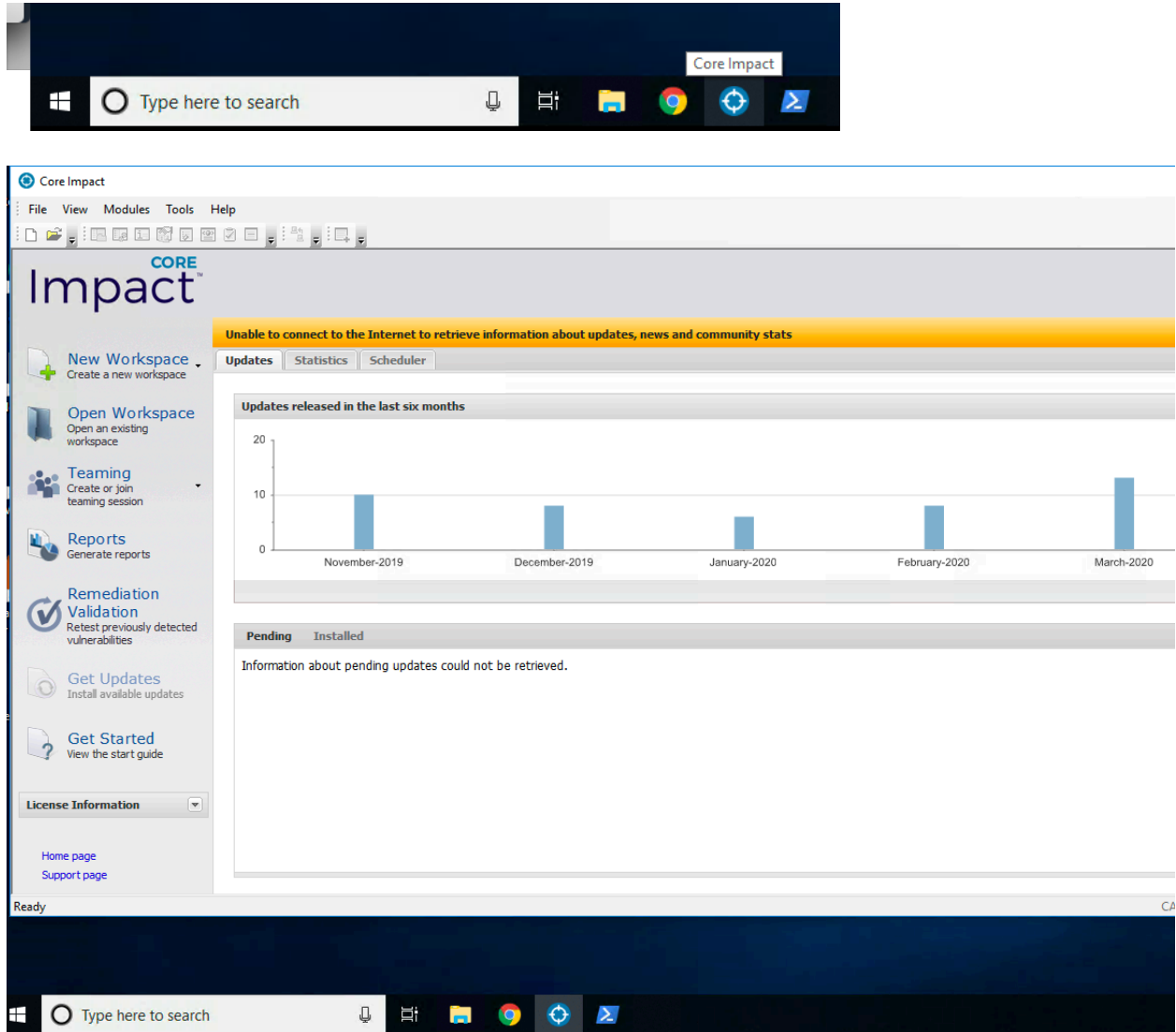
```
Systems INFO.txt
1 Mailserver address:
2 192.168.123.200
3 postmaster/ImpactUser
4
5 WebApp Test:
6 http://192.168.123.95/mutillidae/
7 samurai/samurai **ENTER in Session Mngmt & Services Area**
8
9 ClientAccessRdP:
10 ImpactUser/!ImpactUser!
11
12
13 Phishing Test Redirect URL:
14 http://www.gorillacorp.com/OopsPage.html
15
16 Phishing Clone Form URL:
17 ***Coming Soon***
18
19
```

## Starting Required Services After Connecting to your Core Impact System

Once remote desktop successfully to your Core impact system, please go to Desktop, right click axiMonitor -Shortcut, click Run as Administrator



Click on the “Core Impact” icon which is listed on the desktop which will bring you into the IMPACT dashboard as shown below.



## NETWORK TESTING

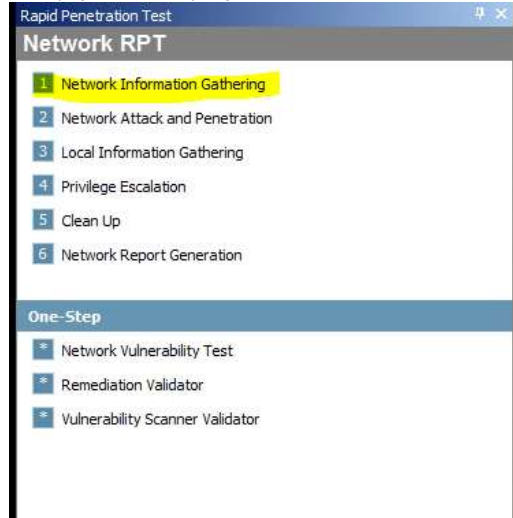
Now, you are ready to start using Core Impact. Create a new “Blank” workspace on the left hand menu in the dashboard and walk through the wizard. A new workspace is created and shown below.

The image shows two screenshots from the Core Impact application. The top screenshot is the dashboard, featuring the 'CORE Impact' logo, a 'New Workspace' button, and a sidebar with options for 'Blank Workspace', 'Network', and 'Risk Assessment Test'. A notification banner at the top states 'Unable to connect to the Internet to retrieve information'. Below this, there are tabs for 'Updates', 'Statistics', and 'Scheduler', and a section titled 'Updates released in the last six months' showing a count of 20.

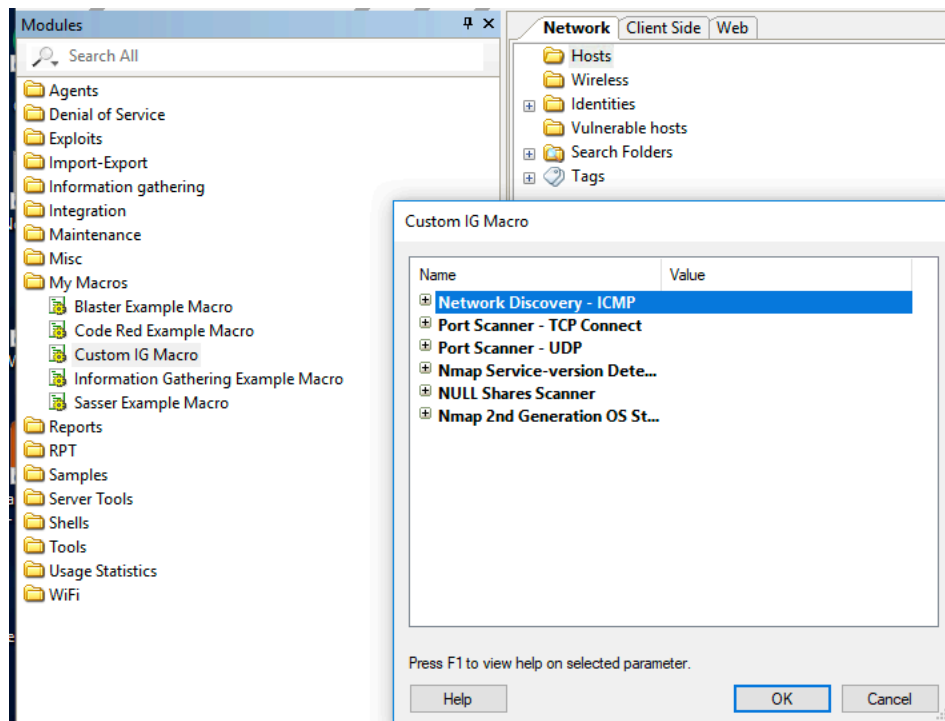
The bottom screenshot is a window titled 'Rapid Penetration Test' with a 'Network RPT' sub-window. The left sidebar lists various modules under 'Network RPT' and 'One-Step'. The main area shows a tree view of hosts under 'Network', including 'localhost' with IP 192.168.123.200, OS Windows, and Arch x86-64. The 'Executed Modules' table is empty, and the 'Module Log' is also empty. The 'Quick Information' section at the bottom provides context for the hosts.

Name	Started	Finished	Status	Source Agent	Resu..
There are no items to show.					

To begin a simple Network Information Gathering, select step # 1 from the Rapid Penetration Test (RPT) on the upper left hand window. Select all defaults when proceeding through the wizard. The results of the gathering is listed below. However, due to within AWS lab, there is a restriction in performing Network Discover – ARP scan. We had created a custom module to perform network information discovery on Vulnerable Systems in this lab environment.



To use alternate module to perform network information gathering in this lab environment, please go to Modules tab, run Custom IG Macro by double clicking the module and click Ok to run the module.



Once Network Information Gathering completed, you can view activity logs in Executed Modules tab and also discovered systems in this lab under Network tab, as shown below :

The screenshot displays the CORE Security interface with two main panels. The left panel, titled 'Network', shows a tree view of discovered hosts under the 'Network: 192.168.123.0 (5)' section. The right panel, titled 'Executed Modules', shows a list of completed tasks, including 'Network Discovery - ICMP', and its corresponding output.

Name	Started	Finished	Status	Source Agent	R
Custom IG Macro	5/5/2020 9:13:29 AM	5/5/2020 9:19:07 AM	Finished	/localagent	N
Network Discovery - ICMP	5/5/2020 9:13:31 AM	5/5/2020 9:13:45 AM	Finished	/localagent	N
Port Scanner - TCP ...	5/5/2020 9:13:46 AM	5/5/2020 9:15:04 AM	Finished	/localagent	N
Port Scanner - UDP	5/5/2020 9:15:04 AM	5/5/2020 9:17:29 AM	Finished	/localagent	N
Nmap Service-versi...	5/5/2020 9:17:29 AM	5/5/2020 9:18:27 AM	Finished	/localagent	N
NULL Shares Scanner	5/5/2020 9:18:27 AM	5/5/2020 9:18:32 AM	Finished	/localagent	N
Nmap 2nd Generati...	5/5/2020 9:18:32 AM	5/5/2020 9:19:06 AM	Finished	/localagent	N

Found hosts in range '192.168.123.10-192.168.123.100'	
IP Address	DNS Name
192.168.123.77	WIN12377
192.168.123.95	www.mycorp.com
192.168.123.100	FREELYDC
192.168.123.33	UBUNTU
192.168.123.22	(unknown name)

Once the Hosts have been identified and the 1st step completes, Click through the hosts to see some of the information available on them.

**Module Output**

### Port Scanner - TCP Connect

Port scanning with CONNECT yielded the following results:

TCP Ports in www.mycorp.com	
listen	22, 80, 3389

TCP Ports in 192.168.123.22	
listen	21-22, 80

TCP Ports in WIN12377	
listen	135, 139, 445, 3389, 49154

Module Output | Module Log | Module Parameters

---

**Quick Information**

192.168.123.22

General | Ports & Services

Protocol	Port	Service	Product/Version	Banner
TCP	21	ftps	ProFTPD 1.3.3c	220 ProFTPD 1.3.3c Server (vtsec) [192.168.123.22]
UDP	22	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)	SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
Filtered	80	http	Apache httpd 2.4.18 ((Ubuntu))	HTTP/1.1 200 OK Date: Tue, 05 May 2020 13:17:52 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Thu, 16 Nov 2017 16:53:57 GMT ETag: "b1-55e1c77580cdb" Accept-Ranges: bytes Content-Length: 177 Vary: Accept-
Closed				

Next select step #2, the attack and penetration in the RPT

Choose all hosts discovered (if you drag and drop step 2 to the target(s) they will automatically be selected.

**2 Attack and Penetration**

3 Local Information Gathering

4 Privilege Escalation

5 Clean Up

6 Report Generation

---

**One-Step**

- \* Vulnerability Test
- \* Remediation Validator
- \* Vulnerability Scanner Validator

Search...

Name	IP
Visibility: Root (1)	
Network: 192.168.123.0 (1)	
localhost	192.168.123.1
Visibility: localhost (5)	
Network: 192.168.123.0 (5)	
192.168.123.22	192.168.123.22
UBUNTU	192.168.123.33
WIN12377	192.168.123.77
www.mycorp.com	192.168.123.95
FREEFLYDC	192.168.123.100

Quick Information

192.168.123.22

General | Ports & Services

**Network Attack and Penetration Wizard**

**Target Selection**  
Specify the attack target(s)

Select the hosts that will be tested for vulnerabilities.

Targets:  
192.168.123.22;UBUNTU;WIN12377;www.mycorp.c

< Back | Next > | Ca

Click Next

When presented with the Attack Method Select both check boxes

The screenshot shows the 'Attack Method' step of the 'Network Attack and Penetration Wizard'. The title bar reads 'Network Attack and Penetration Wizard'. Below the title, the section is titled 'Attack Method' with the subtitle 'Specify the attack method(s)'. A blue circular icon with a white crosshair is in the top right corner. The main content area contains the following text and options:

Select the attack method(s) to be performed and which should be executed first.

- Launch exploit modules to identify code execution vulnerabilities.
- Launch identity modules to identify authentication weaknesses.

Select when the identity testing should occur.

- Before launching exploits**
- After launching exploits**

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

Leave the default options. Select both options highlighted below.

The screenshot shows the 'Attack Configuration' step of the 'Network Attack and Penetration Wizard'. The title bar reads 'Network Attack and Penetration Wizard'. Below the title, the section is titled 'Attack Configuration' with the subtitle 'Customize network attack'. A blue circular icon with a white crosshair is in the top right corner. The main content area contains the following text and options:

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

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

Click Next and leave the default option without checking any advanced Network attack options, and click Finish.

Network Attack and Penetration Wizard

**Network Attack Setup**  
Select additional optional settings to setup.

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

Exploits options

- Exploits selection criteria
- Exploits execution order

Identity verifiers options

- Identity verifier protocol selection
- Identity verifier attack method

Exploitation options

- Agent communication options
- Agent expiration options
- Post exploitation actions options

< Back   Finish   Cancel

(However, you can individually check the option to see each advance option settings.)

Multiple agents will be placed on the targeted systems indicated that a vulnerability exists. This agent is injected into the memory space of the service that is exposed. This will now give you the option of interacting through the agent by “right clicking” on the agent affords you several options including but not limited to opening a shell, getting screen shots and browsing files. All of this will be communicated from the agent to the IMPACT console using AES 256 bit encryption.

You can view each executed Modules activity logs under Executed Modules tab.

The screenshot displays the IMPACT console interface. On the left, a tree view shows the network structure, including a local host and several remote hosts under the network 192.168.123.0. The 'agent(0)' is selected on host WIN12377. The top right pane shows a list of executed modules with columns for Name, Start Time, End Time, Status, Path, and a checkbox. The 'Module Output' window for 'Network Attack and Penetration' provides a summary of execution and attack results. The 'Quick Information' section at the bottom details the agent's configuration.

Name	IP	OS	Arch
localhost	192.168.123.200	Windo	x86-64
192.168.123.22	192.168.123.22	Linux	i386
UBUNTU	192.168.123.33	Linux	x86-64
agent(1)			
WIN12377	192.168.123.77	Windo	x86-64
agent(0)			
www.mycorp.com	192.168.123.95	Linux	i386

Name	Start Time	End Time	Status	Path	Checkbox
Network Attack and Pe...	5/5/2020 9:22:59 AM	5/5/2020 9:22:59 AM	Running	/localagent	No
FTP Identity Verifier	5/5/2020 9:23:02 AM	5/5/2020 9:23:02 AM	Running	/localagent	No
RDP Identity Verifier	5/5/2020 9:23:02 AM	5/5/2020 9:23:13 AM	Finished	/localagent	No
MySQL Identity Ver...	5/5/2020 9:23:02 AM	5/5/2020 9:23:09 AM	Finished	/localagent	No
SMB Identity Verifier	5/5/2020 9:23:02 AM	5/5/2020 9:23:54 AM	Finished	/localagent	No
SSH Identity Verifier	5/5/2020 9:23:02 AM	5/5/2020 9:25:31 AM	Finished	/localagent	No
SSH Identity Verifier	5/5/2020 9:23:02 AM	5/5/2020 9:25:30 AM	Finished	/localagent	No

Execution Summary	
Tasks (Finished / Created)	55/57 (96.5%)
Identities (Verified / Total)	3.03% (44/1454)

Attack Summary	
Vulnerabilities identified	45
Agents deployed	2
Targets with vulnerabilities	40.0% (2/5)

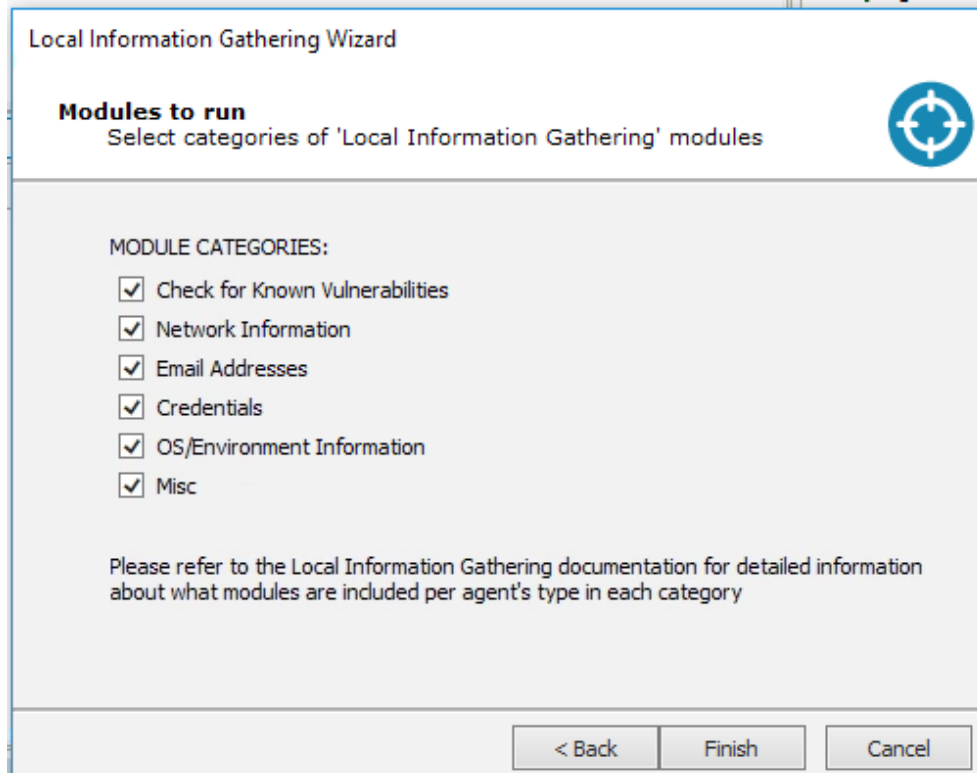
Quick Information	
agent(0)	
General	
Type	Agent
Visibility Path	/192.168.123.77/agent(0)
Architecture	i386
Privilege Level	Privileged account
Host	WIN12377
Crypto Channel	True
Expiration Date	6/4/2020 9:23 AM
File Name	\\WIN12377\ADMIN\$\\096854103.exe

Step #3 in the RPT will allow for local information gathering such as getting network information, gathering email addresses and credentials.

Network RPT	
1	Information Gathering
2	Attack and Penetration
3	Local Information Gathering
4	Privilege Escalation
5	Clean Up
6	Report Generation

One-Step	
*	Vulnerability Test
*	Remediation Validator
*	Vulnerability Scanner Validator



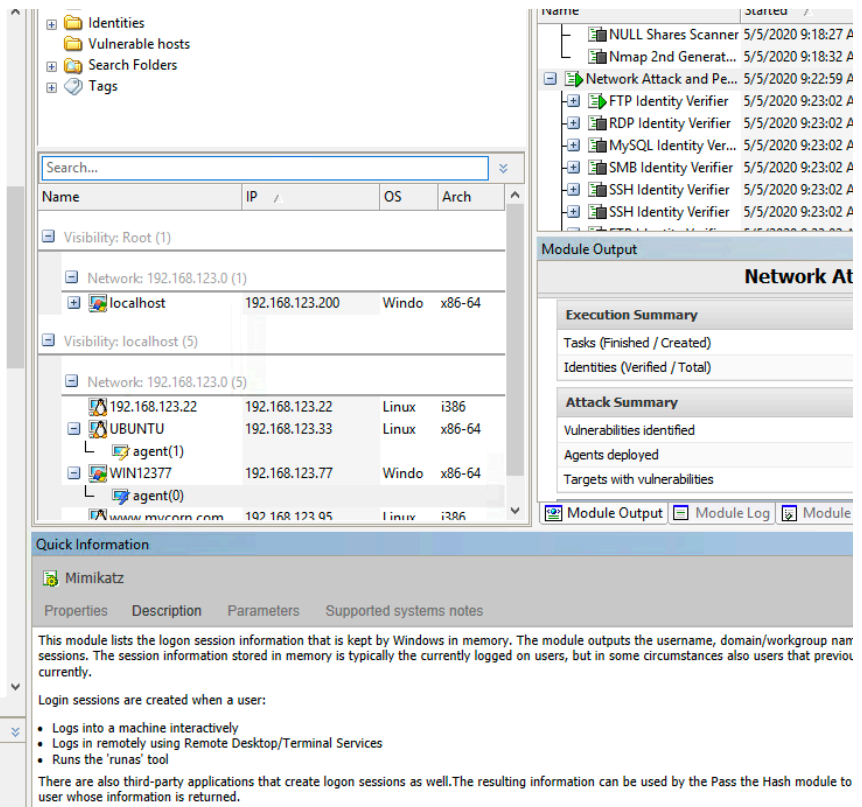
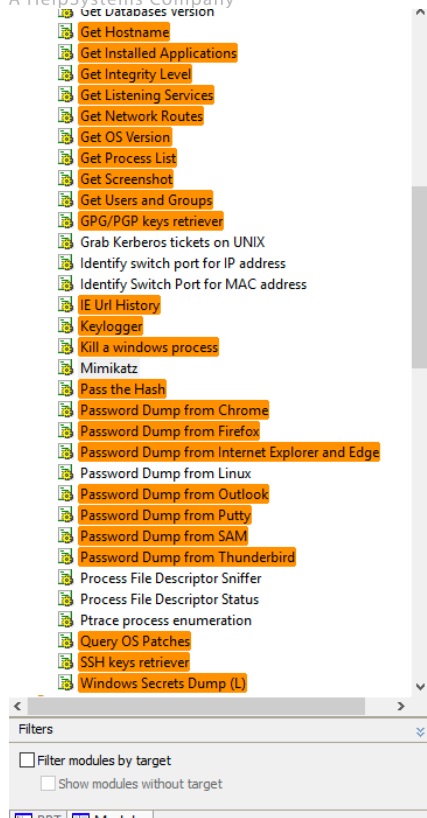
If you would prefer to interact with the individual modules:

Click on the lower left hand side that says Modules.

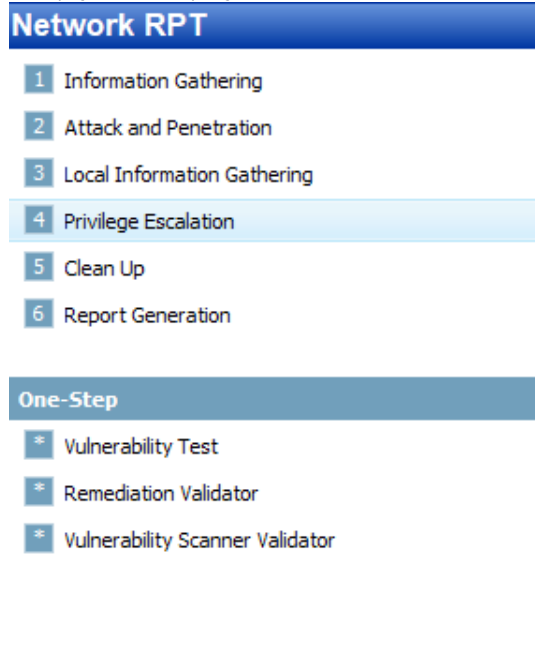
Then click on the Information gathering Folder>Local

Here are a few modules that you can drag and drop to get more information from a compromised system. The highlighted ones indicate the one that can be used on the selected agent on compromised system.

Information on the modules and exploits can be seen in the quick information Panel at the bottom center



Step # 4 will escalate privileges based on user access to printer drivers, graphic drivers, etc....Feel free to run this step against all the system with agents. Not all compromised systems start out with full access.

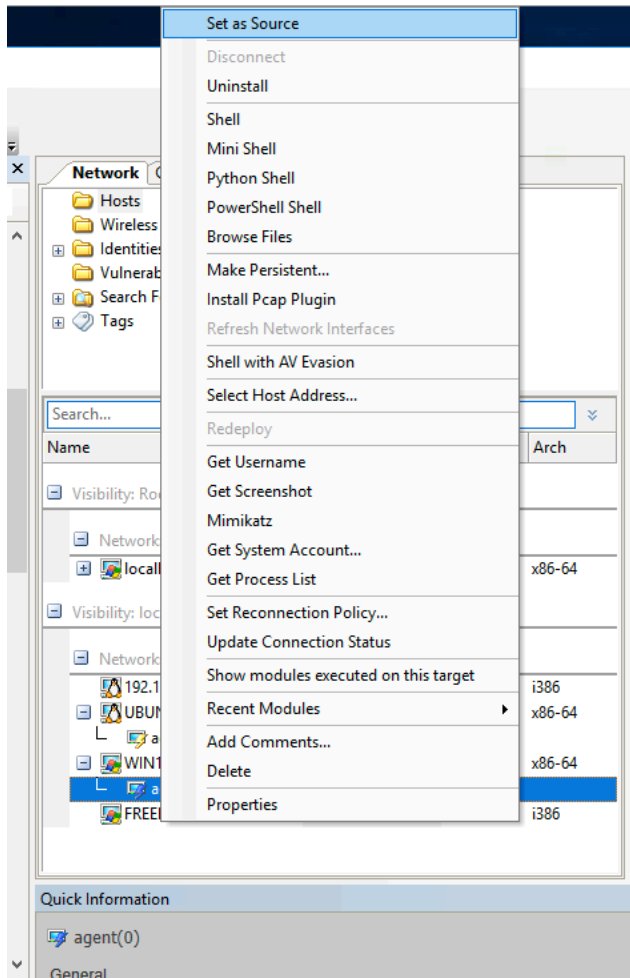


Agent color indicator will indicate type of privilege which agent has. Current screenshot below showed the agent with yellow indicator only has regular user privilege

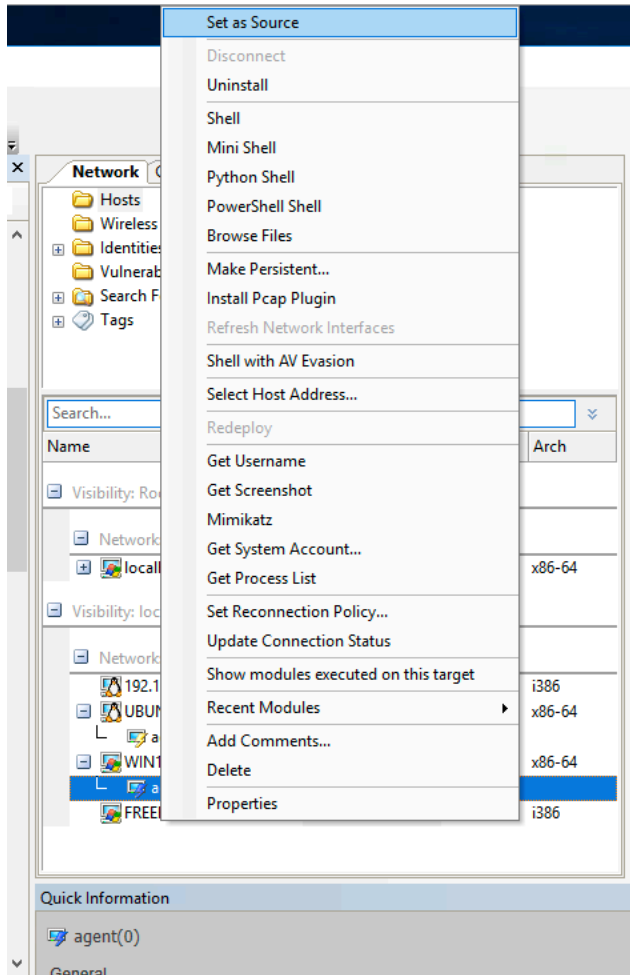
Name	IP	OS	Arch
Visibility: Root (1)			
Network: 192.168.123.0 (1)			
localhost	192.168.123.200	Windows	x86-64
Visibility: localhost (4)			
Network: 192.168.123.0 (4)			
192.168.123.22	192.168.123.22	Linux	i386
UBUNTU	192.168.123.33	Linux	x86-64
agent(1)			
WIN12377	192.168.123.77	Windows	x86-64
agent(0)			
FREEFLYDC	192.168.123.100	Windows	i386

Select which Agents to escalate privilege, click Next and Finish to run Privilege Escalation Exploits on compromised systems

If you escalated any system successfully you can use them as a source agent and pivot off this agent. Simply “right click” and select “set as source.” If you identified another network in the local information gathering (Step #3) then you can use this source agent to pivot into that network.



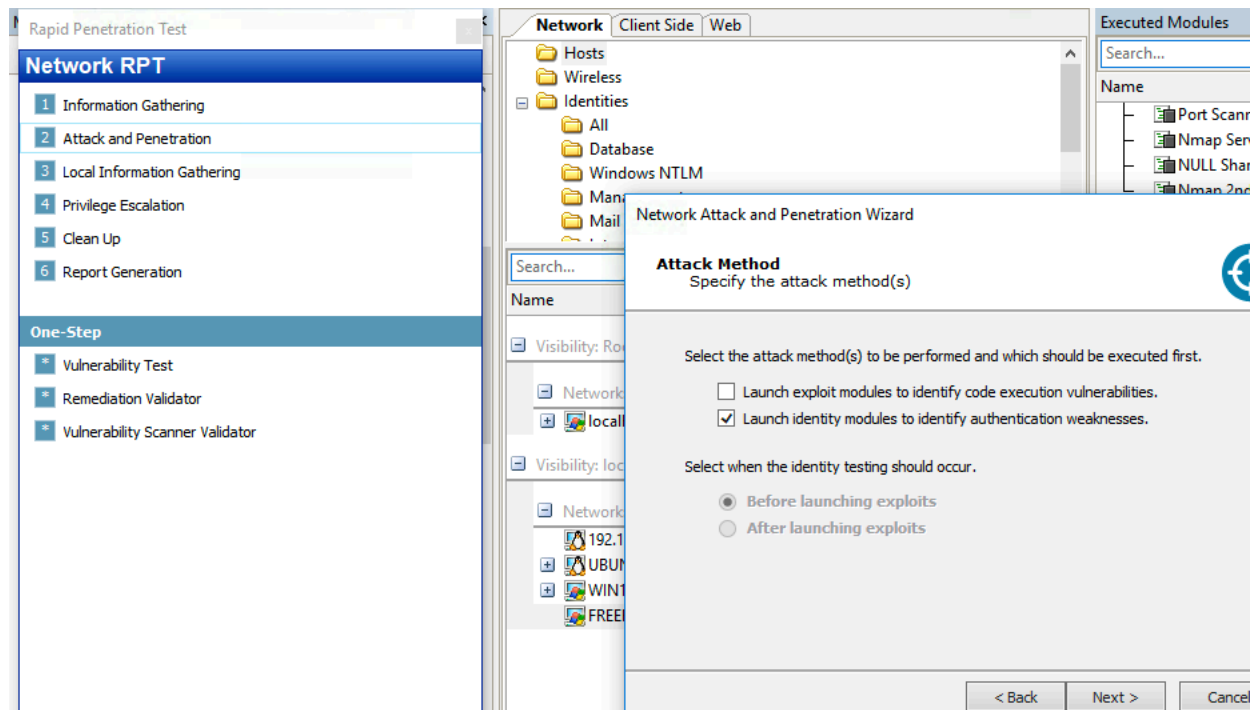
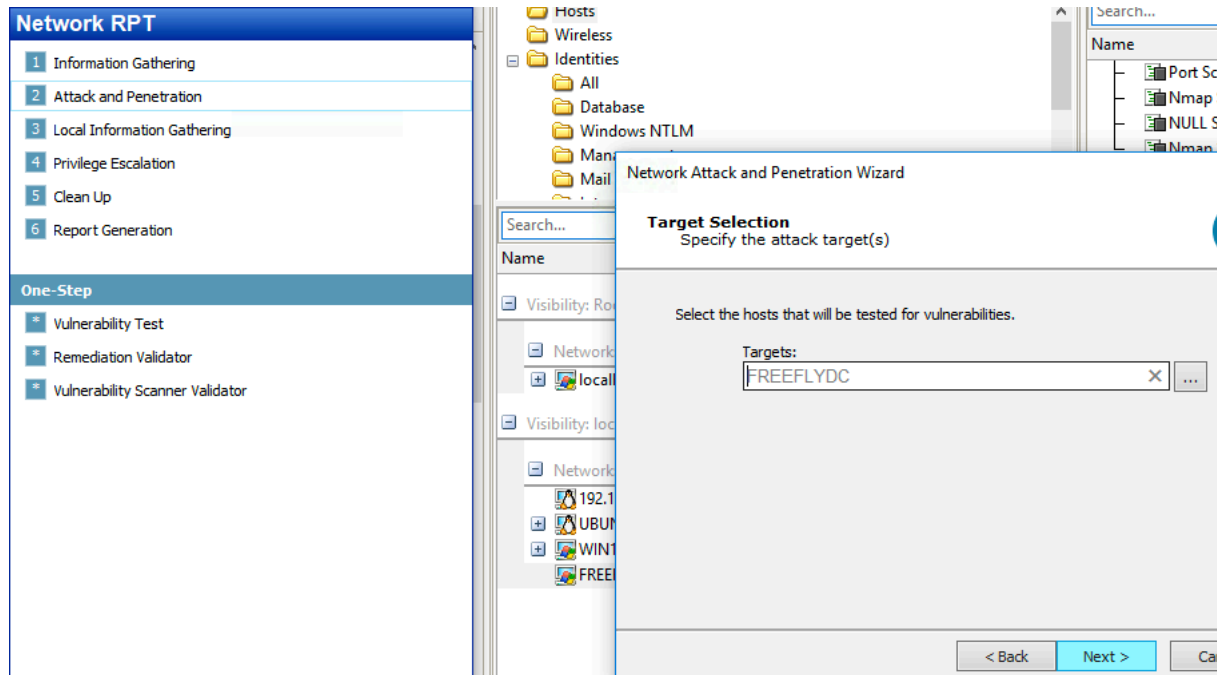
In addition to this there is 1 Windows Client called WIN12377 that gets compromised. If you right click the system and run Mimikatz, you will get the windows credentials dump information from the system.

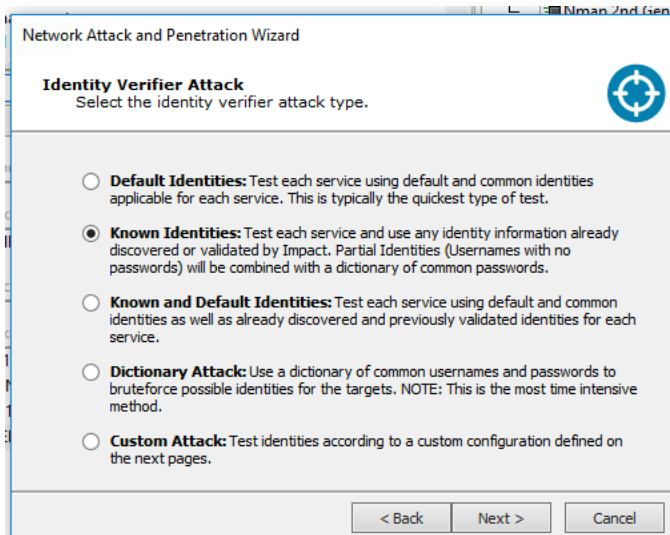
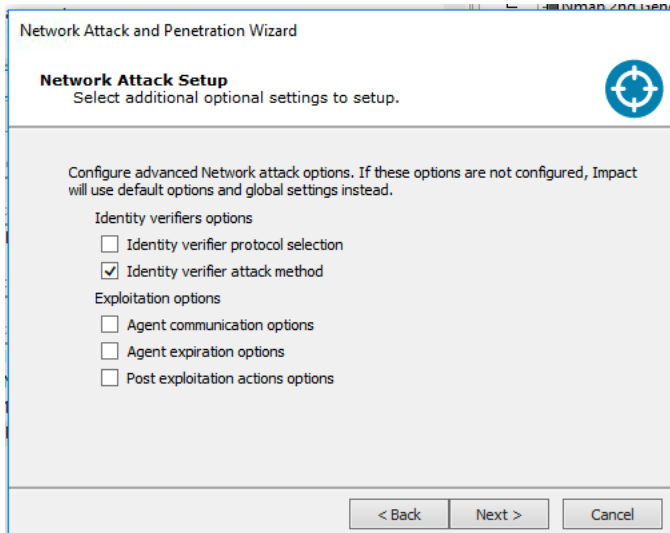


Here is what it should look like:



Choose only Identity modules attack. Leave other options DEFAULT. Check "Identify verifier attack method" under Network Attack Setup. Choose Known Identities in next screen so that Core Impact will use discovered identity information to exploit and gain access to Domain Controller – FREEFLYDC





Leave other options as Default options and click Finish. You will see agent deployed in Domain Controller once exploit successful, as shown below.

The screenshot shows the Core Security console interface. At the top is a search bar. Below it is a table of hosts with columns for Name, IP, OS, and Arch. The hosts are grouped by visibility: 'Root (1)' and 'localhost (4)'. The 'localhost (4)' group contains four entries: '192.168.123.22' (Linux, i386), 'UBUNTU' (Linux, x86-64), 'WIN12377' (Windows, x86-64), and 'FREEFLYDC' (Windows, x86-64). The 'agent(3)' entry is highlighted in blue. Below the table is a 'Quick Information' section for the selected agent, showing details like Type (Agent), Visibility Path (/192.168.123.100/agent(3)), Architecture (i386), Privilege Level (Privileged account), Host (FREEFLYDC), and Crypto Channel (True).

Name	IP	OS	Arch
Visibility: Root (1)			
Network: 192.168.123.0 (1)			
localhost	192.168.123.200	Windows	x86-64
Visibility: localhost (4)			
Network: 192.168.123.0 (4)			
192.168.123.22	192.168.123.22	Linux	i386
UBUNTU	192.168.123.33	Linux	x86-64
WIN12377	192.168.123.77	Windows	x86-64
FREEFLYDC	192.168.123.100	Windows	x86-64
agent(3)			

**Quick Information**  
agent(3)

General

Type	Agent
Visibility Path	/192.168.123.100/agent(3)
Architecture	i386
Privilege Level	Privileged account
Host	<a href="#">FREEFLYDC</a>
Crypto Channel	True

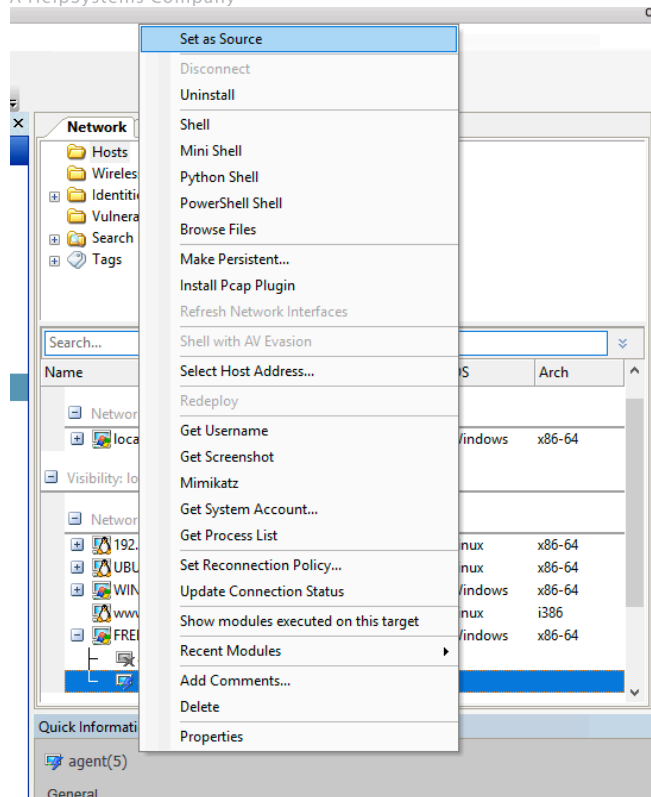
If you escalated any system successfully you can use them as a source agent and pivot off this agent. Simply “right click” and select “set as source.” If you identified another network in the local information gathering (Step #3) then you can use this source agent to pivot into that network.

The screenshot shows the Core Security console interface. The host list table is similar to the previous one, but now includes two agent entries under the 'FREEFLYDC' host: 'agent(4)' and 'agent(5)'. The 'FREEFLYDC' entry is highlighted in blue. Below the table is a 'Quick Information' section for the selected host, showing tabs for General, Vulnerabilities, Ports & Services, and Identities.

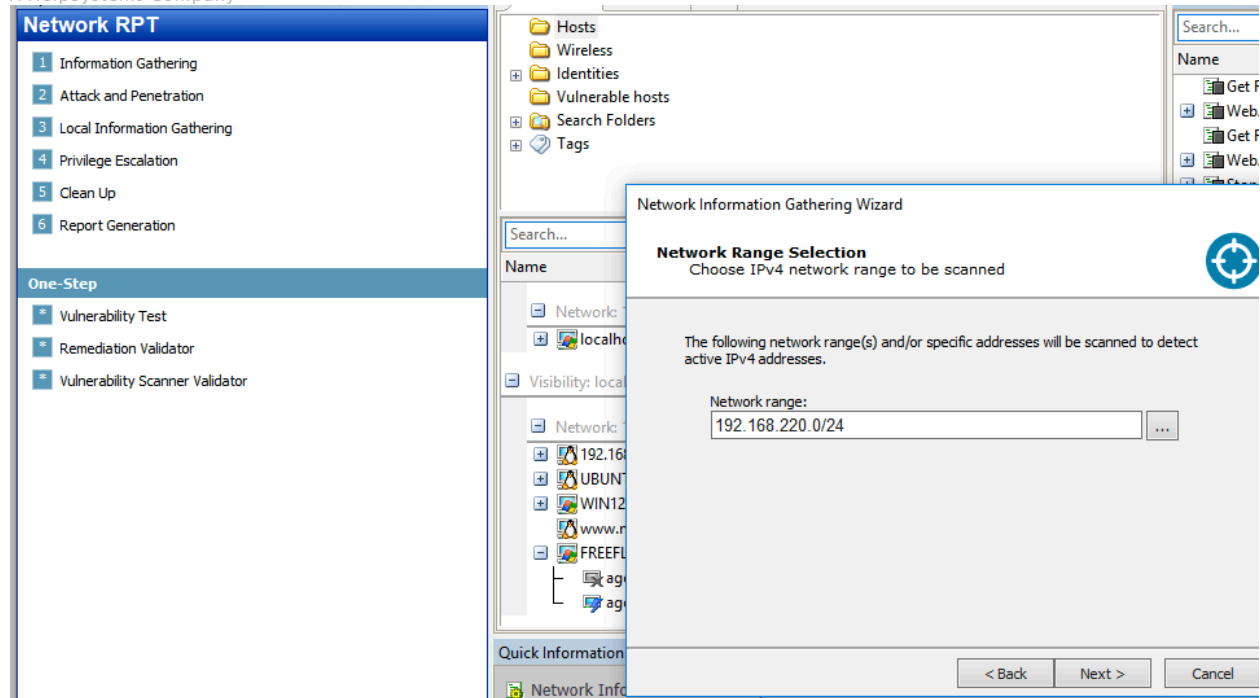
Name	IP	OS	Arch
Network: 192.168.123.0 (1)			
localhost	192.168.123.200	Windows	x86-64
Visibility: localhost (5)			
Network: 192.168.123.0 (5)			
192.168.123.22	192.168.123.22	Linux	x86-64
UBUNTU	192.168.123.33	Linux	x86-64
WIN12377	192.168.123.77	Windows	x86-64
www.mycorp.com	192.168.123.95	Linux	i386
FREEFLYDC	192.168.123.100	Windows	x86-64
agent(4)			
agent(5)			

**Quick Information**  
FREEFLYDC

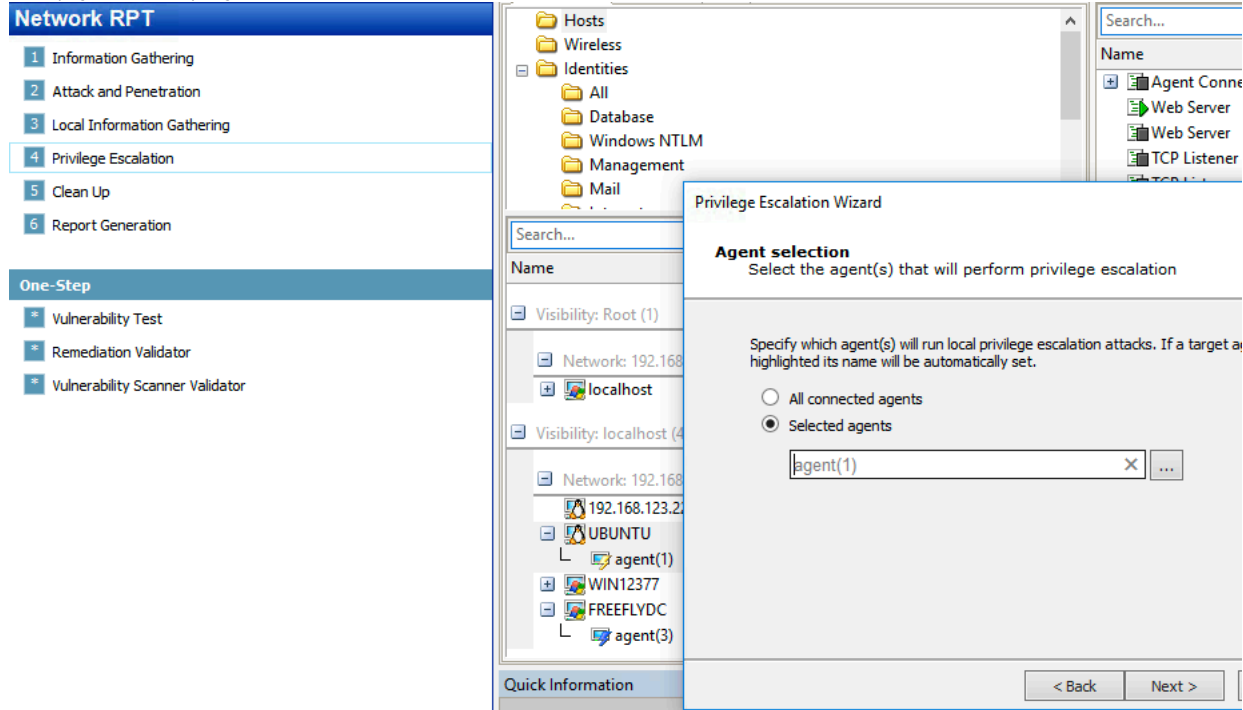
General Vulnerabilities Ports & Services Identities



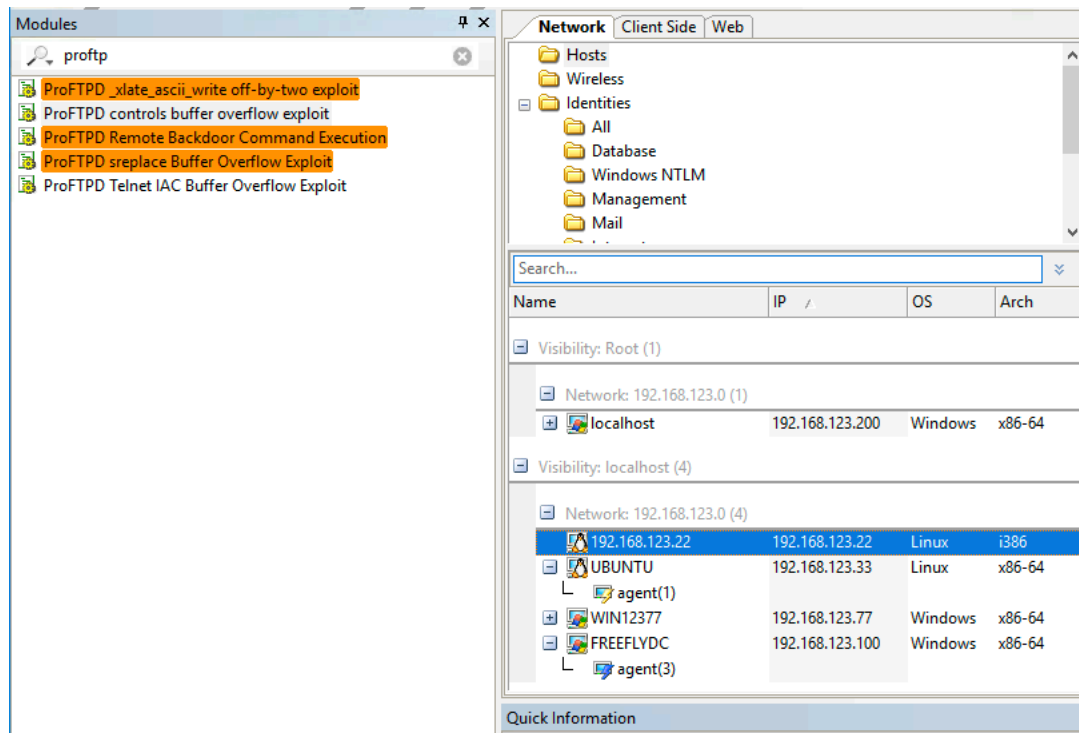
Go to Network RPT – Step 1. Information Gathering, perform information gathering on 192.168.220.0/24. You will successfully pivot to deeper internal networks via domain controller machine which is dual home.

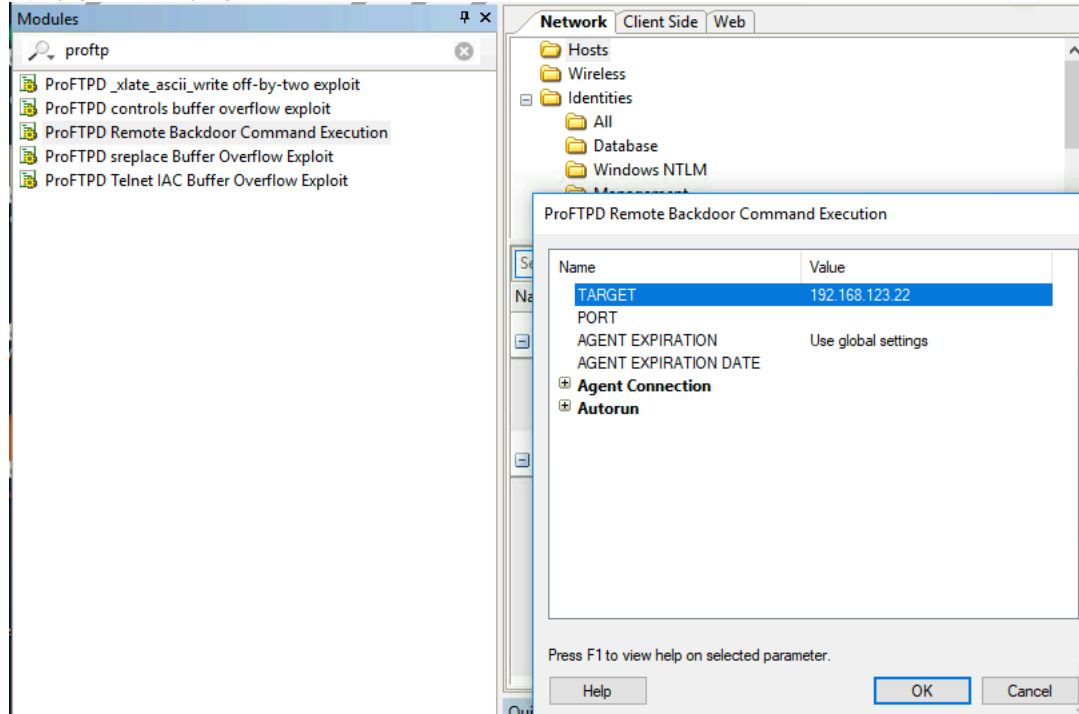


Select Step 4, Privilege Escalation attack on agent belonged to UBUNTU server to gain privilege access to this system

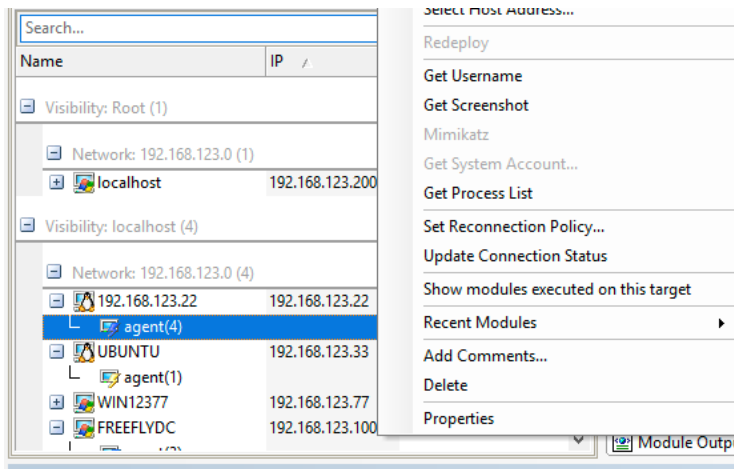


To perform manual testing, select 192.168.123.22 system. Go to Modules tab, and filter exploits by typing application name – Proftpd. Run module – ProFTPD Remote Backdoor Command Execution Exploit to 192.168.123.22 system by pulling the module to the system.







After exploit successful, you will able to gain privilege access to 192.168.123.22 system.



Once the evidence has been obtained all that is needed is the cleanup and report generation. Step #5 in the RPT will cleanup and remove all agents and then step #5 will allow for a choice of reports.

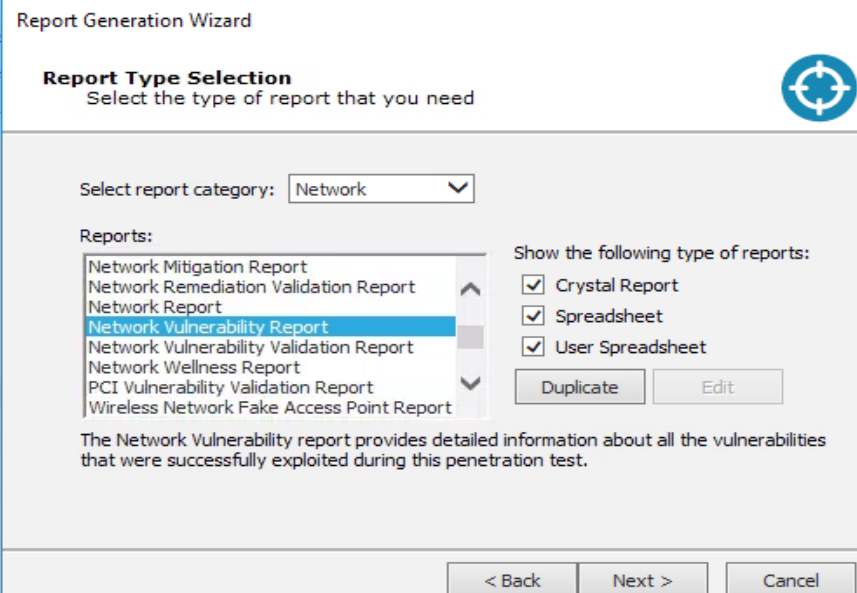
Rapid Penetration Test    
**Network RPT**

- 1 Information Gathering
- 2 Attack and Penetration
- 3 Local Information Gathering
- 4 Privilege Escalation
- 5 Clean Up
- 6 Report Generation

**One-Step**

- \* Vulnerability Test
- \* Remediation Validator
- \* Vulnerability Scanner Validator

In the latest version of IMPACT you can actually customize the reports from the wizard and download the XLS version to edit it under Step #6 in RPT. Below are some of the ones you can do this to.



Report Generation Wizard

**Report Type Selection**  
Select the type of report that you need

Select report category: Network

Reports:

- Network Mitigation Report
- Network Remediation Validation Report
- Network Report
- Network Vulnerability Report**
- Network Vulnerability Validation Report
- Network Wellness Report
- PCI Vulnerability Validation Report
- Wireless Network Fake Access Point Report

Show the following type of reports:

- Crystal Report
- Spreadsheet
- User Spreadsheet

Duplicate Edit

The Network Vulnerability report provides detailed information about all the vulnerabilities that were successfully exploited during this penetration test.

< Back Next > Cancel

Here is an example of a Network Vulnerability report generated from IMPACT.

# Network Vulnerability Report

May 3, 2020 at 4:34 AM

This report provides detailed information about all the vulnerabilities that were successfully exploited by Core Impact during this test. Each one of the reported vulnerabilities was actively exploited in order to obtain control, elevate privileges or obtain information about the vulnerable host. None of these results are potential, all of them were practically tested as part of this test.

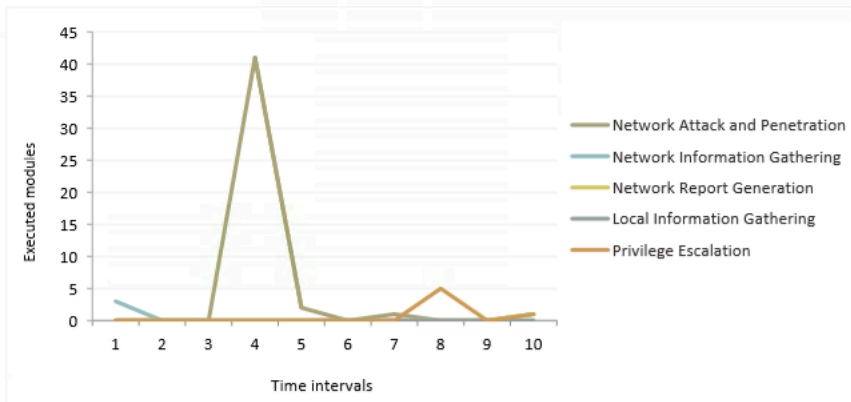
This information provides a practical approach to determine the key vulnerable points in the tested network, and to assess the risk associated with such vulnerabilities.

SECTION	PAGE
<a href="#">Workspace information</a>	2
<a href="#">Effort chart</a>	3
<a href="#">Summary</a>	4
<a href="#">Confirmed vulnerabilities</a>	5
<a href="#">Exploited hosts</a>	6
<a href="#">Critical vulnerabilities</a>	7
<a href="#">Vulnerabilities</a>	8
<a href="#">Vulns container details</a>	11
<a href="#">Vulns extra links</a>	19

## Effort chart

The chart report lifespan was divided into 10 time intervals, time interval 1 begins when the first task started, and time interval 10 ends when the last task finished running.

Distribution of modules in time



Workspace	Visibility Path	Host Name	Vulnerability Identifier	CVSS	Vector Description	Vulnerability Description	Affected Port	Module Name	Remediation URL
cj-test2	/192.168.123.100	FREELYDC	CVE-1999-0505	7.2	Access Vector: Locally exploitable, Access Complexity: Low, Authentication: Not required to exploit, Confidentiality Impact: Allows unauthorized disclosure of information (Complete), Integrity Impact: Allows unauthorized modification (Complete), Availability Impact: Allows disruption of service (Complete)	A Windows NT domain user or administrator account has a guessable password.	445	SMB Identity Verifier	
cj-test2	/192.168.123.100	FREELYDC	CVE-1999-0518	7.5	Access Vector: Network exploitable, Access Complexity: Low, Authentication: Not required to exploit, Confidentiality Impact: Allows unauthorized disclosure of information (Partial), Integrity Impact: Allows unauthorized modification (Partial), Availability Impact: Allows disruption of service (Partial)	A NETBIOS/SMB share password is guessable.	445	SMB Identity Verifier	
cj-test2	/192.168.123.22	192.168.123.22	NOCVE-9999-46189	0		A backdoor introduced by attackers allows unauthenticated users remote root access to systems which run the maliciously modified version of the ProFTPD daemon.	21	ProFTPD Remote Backdoor Command Execution	



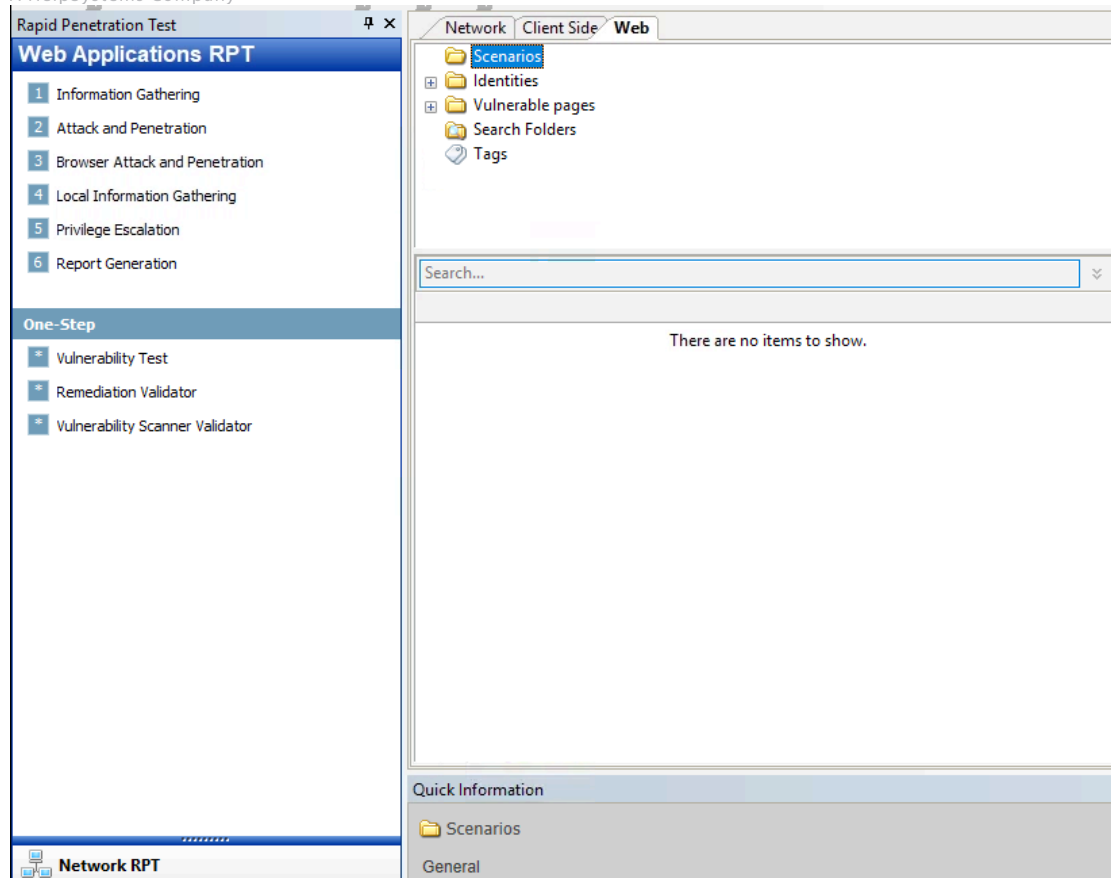
Vulnerabilities extra links

Workspace Name	CVE	URL
cj-test2	CVE-1999-0501	<a href="http://xforce.iss.net/static/1005.php">http://xforce.iss.net/static/1005.php</a>
cj-test2	CVE-1999-0502	<a href="http://xforce.iss.net/static/2941.php">http://xforce.iss.net/static/2941.php</a>
cj-test2	CVE-1999-0502	<a href="http://xforce.iss.net/static/774.php">http://xforce.iss.net/static/774.php</a>
cj-test2	CVE-1999-0503	<a href="http://xforce.iss.net/static/1328.php">http://xforce.iss.net/static/1328.php</a>
cj-test2	CVE-1999-0503	<a href="http://xforce.iss.net/static/282.php">http://xforce.iss.net/static/282.php</a>
cj-test2	CVE-1999-0505	<a href="http://xforce.iss.net/static/1329.php">http://xforce.iss.net/static/1329.php</a>
cj-test2	CVE-1999-0505	<a href="http://xforce.iss.net/static/3421.php">http://xforce.iss.net/static/3421.php</a>
cj-test2	CVE-1999-0518	<a href="http://xforce.iss.net/static/182.php">http://xforce.iss.net/static/182.php</a>
cj-test2	CVE-1999-0519	<a href="http://xforce.iss.net/static/1.php">http://xforce.iss.net/static/1.php</a>
cj-test2	CVE-1999-0519	<a href="http://xforce.iss.net/static/12.php">http://xforce.iss.net/static/12.php</a>
cj-test2	CVE-1999-0519	<a href="http://xforce.iss.net/static/19.php">http://xforce.iss.net/static/19.php</a>
cj-test2	CVE-1999-0519	<a href="http://xforce.iss.net/static/2.php">http://xforce.iss.net/static/2.php</a>
cj-test2	CVE-1999-0519	<a href="http://xforce.iss.net/static/20.php">http://xforce.iss.net/static/20.php</a>
cj-test2	CVE-1999-0519	<a href="http://xforce.iss.net/xforce/xfdb/170">http://xforce.iss.net/xforce/xfdb/170</a>
cj-test2	CVE-2009-4893	<a href="http://security.gentoo.org/glsa/glsa-201006-21.xml">http://security.gentoo.org/glsa/glsa-201006-21.xml</a>
cj-test2	CVE-2009-4893	<a href="http://www.openwall.com/lists/oss-security/2010/06/14/13">http://www.openwall.com/lists/oss-security/2010/06/14/13</a>
cj-test2	CVE-2009-4893	<a href="http://www.securityfocus.com/bid/42077">http://www.securityfocus.com/bid/42077</a>
cj-test2	CVE-2009-4893	<a href="http://www.securityfocus.com/bid/42077/solution">http://www.securityfocus.com/bid/42077/solution</a>
cj-test2	CVE-2009-4893	<a href="http://www.unrealircd.com/txt/unrealsecadvisory.20090413.txt">http://www.unrealircd.com/txt/unrealsecadvisory.20090413.txt</a>
cj-test2	NOCVE-9999-	

## **Web Application Testing**

Core IMPACT AWS lab allows for testing a custom web application identified as <http://www.mycorp.com/mutillidae>

You will be required to switch to the Web Applications RPT tab as indicated below.



Once in the Web Attack Vector you can start by running the Web Apps Information Gathering in Step #1 of the RPT. Create a scenario called "MUTILLIDAE" and accept all defaults. Under Automatic web crawling, please enter following URL : <http://www.mycorp.com/mutillidae>

## WebApps Information Gathering Wizard

### Information Gathering mode selection

Select how the information gathering phase will find web applications



Select the information gathering mode to be performed by the module

- Crawl a known web application

NOTE: You can either provide a URL to be crawled automatically or manually by interactive web crawling.

- Discover web applications in hosts running HTTP servers

< Back

Next >

Cancel

## 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

WebApps Information Gathering Wizard

**Automatic Crawling Options**  
Configure how to crawl your web site

Select web browser to impersonate: Google Chrome 62 (Windows 10) ▼

Custom user agent:

Max. number of pages the crawler should process 300 ▼

Max. depth level to crawl 3 ▼

Restrict crawling to starting page domain

Additional domains to allow during crawling (for example: \*.coresecurity.com)

NOTE: Use semicolons ( ; ) to separate entries.

Detect web application framework

< Back   Next >   Cancel

Check “use session management in your website” under Automatic Crawling options.

WebApps Information Gathering Wizard

**Automatic Crawling Options (contd)**  
Configure how to crawl your web site

Evaluate JavaScript code included in web site

Follow links in robots.txt files in web site

Send forms found in web pages: Send with default values ▼

To do custom parsing on pages' links, provide the name of a module here:

Link parsing module  ... Clear

If your web application requires a user to authenticate to access all its functionality, you can configure credentials for the crawler to perform authentication when required.

Use session management in your website

< Back   Next >   Cancel

Select Form-based and enter username/password which are samurai/samurai

WebApps Information Gathering Wizard

**Session Management (contd)**  
Provide credentials to authenticate

Provide credentials to authenticate against the website:

Username: samurai Password: samurai

Identity:

< Back Next > Cancel

Click Next until Web Services Discovery Options.

Check “Append ‘?wsdl’ to every found UR” option. Select SOAP WS-Security and enter samurai as username and samurai as password

WebApps Information Gathering Wizard

**Web Services Discovery Options**  
Configure how to search for web services

Search for SOAP web services definitions

Append '?wsdl' to every found URL

How method parameters values should be filled: Complete with default values

How SOAP operations found in a definition file should authenticate:

Use the same as for crawling web pages

Use SOAP WS-Security

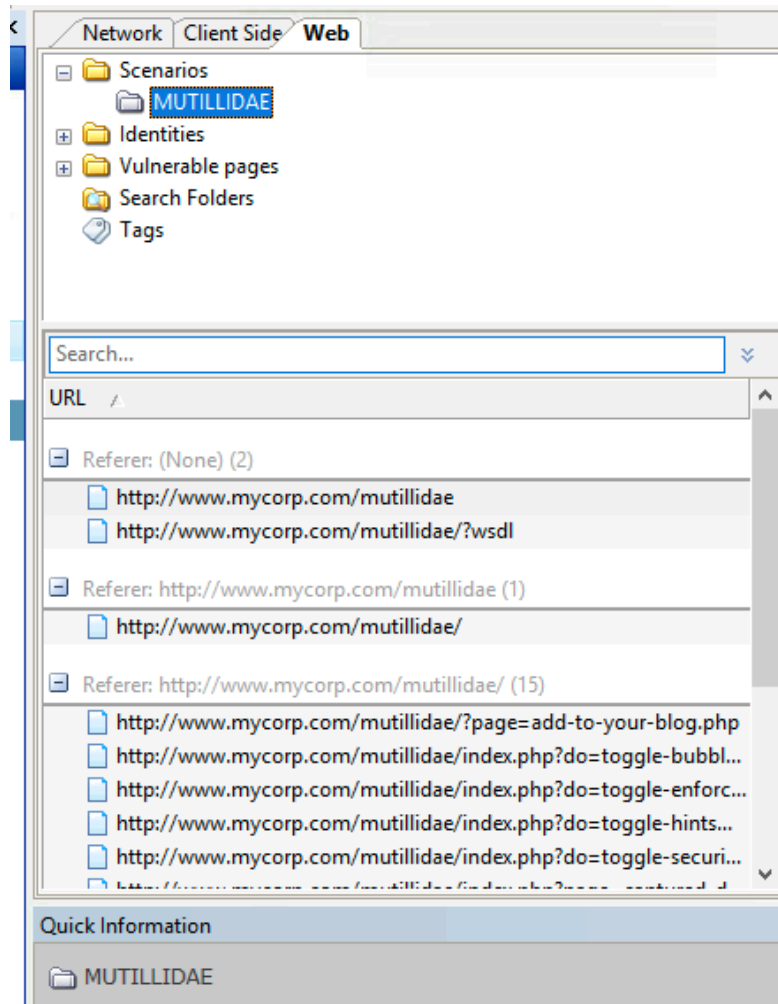
Username: samurai Password: samurai

Identity:

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

< Back Finish Cancel

Once the scenario is created and the crawling process has started you will see multiple pages in the main view as shown below.



Once you have your pages in view you can begin by running the “web apps attack and penetration” in step #2 of the RPT. You can “double click” on this option or “drag and drop” onto the scenario or referer pages. Select only A1, A4, and A7 for injection, XML web services and XSS and the remainder of all defaults. The results will yield “logical” web agents on each vulnerable page as shown below.

WebApps Attack and Penetration Wizard

**Risk Types**  
Select the OWASP Top 10 risk types that will be tested on web pages

- A1 - Injection
  - Look for SQL Injection vulnerabilities
  - Look for OS Command Injection vulnerabilities
- A2 - Broken Authentication
- A3 - Sensitive Data Exposure
  - Look for Sensitive Information in documents
  - Look for Weak SSL Ciphers

NOTE: Analysis of sensitive data exposure in databases can be performed running Local Information Gathering RPT on configured SQL Injection agents.

< Back    Next >    Cancel

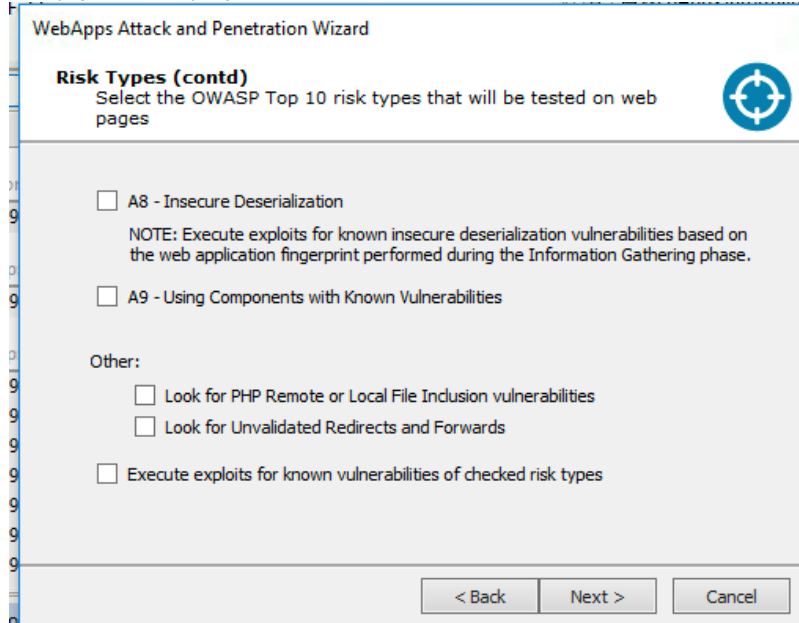
WebApps Attack and Penetration Wizard

**Risk Types (contd)**  
Select the OWASP Top 10 risk types that will be tested on web pages

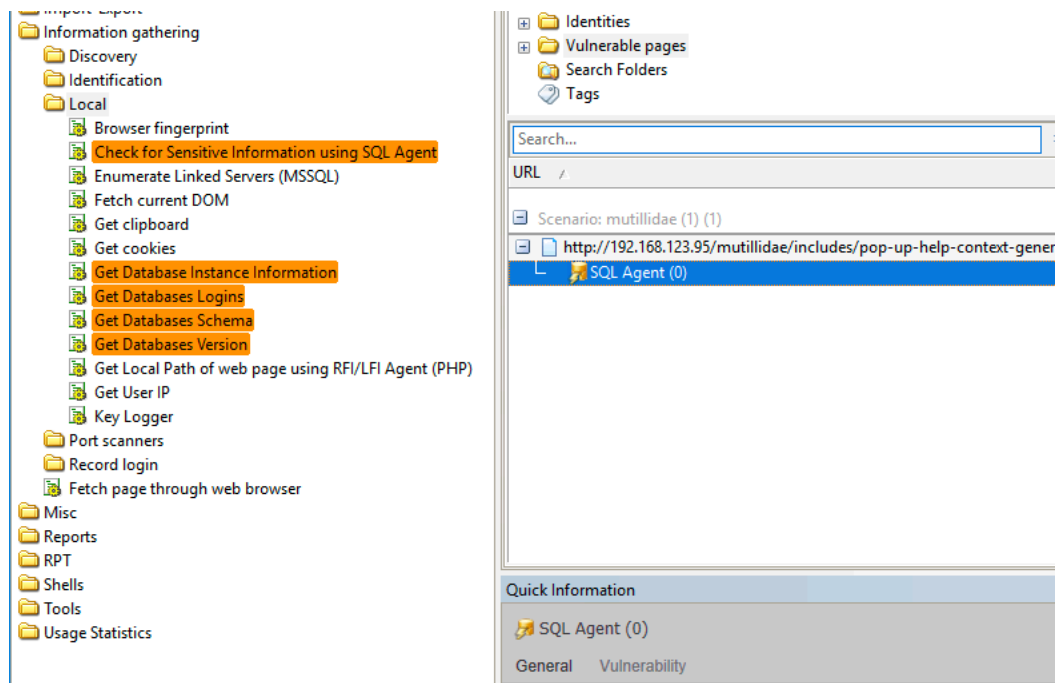
- A4 - XML External Entities
- A5 - Broken Access Control

NOTE: Broken access control detection need user interaction to obtain session cookies. It can be performed running the Broken Access Control Analyzer module that have a separate wizard to guide the test configuration.
- A6 - Security Misconfiguration
  - Look for known security misconfiguration issues
  - Look for WebDAV vulnerabilities
  - Look for default host credentials
- A7 - Cross Site Scripting (XSS)

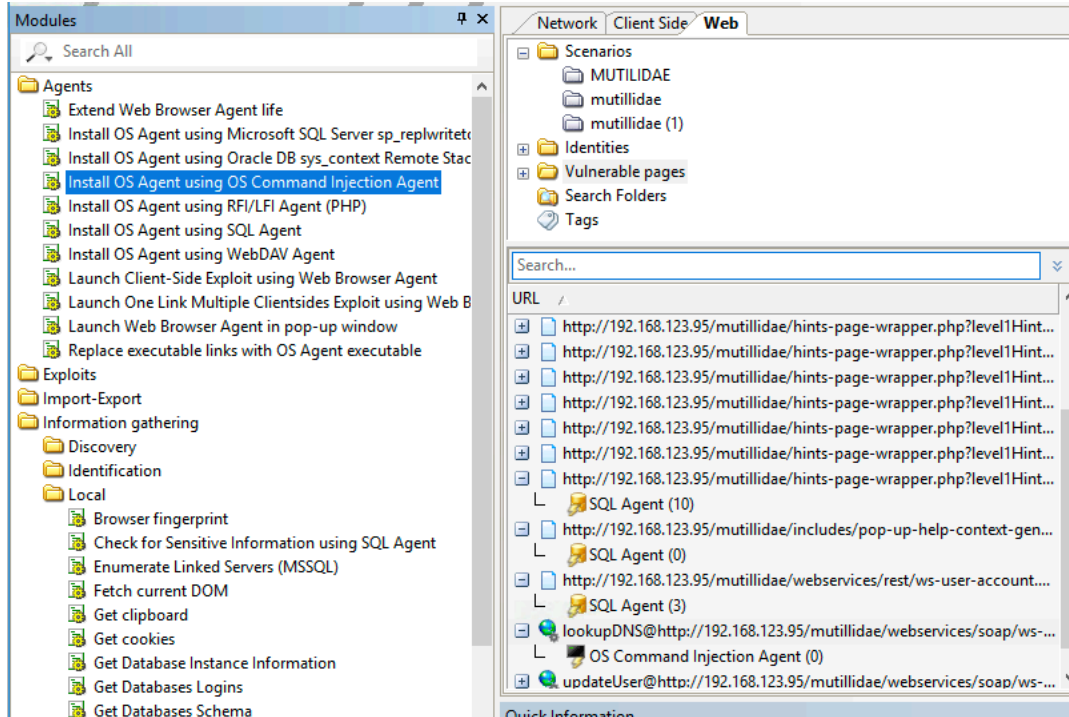
< Back    Next >    Cancel



All of the above agents can be leveraged to gain additional information such as getting the DB schema, Logins or DB version. Simply “drag and drop” the highlighted module onto the logical agent



You now have the ability to leverage that vulnerability and challenge the Web Application Firewall (WAF) by attempting to deploy an OS Agent via the vulnerable web application. Simply “drag and drop” the “install OS agent using OS Command Injection” module onto the OS Command Injection agent as shown below.



The result will be as shown an OS agent deployed from the OS Command Injection agent and we end up back onto the network with the OS deployed onto the windows server hosting the web application

The screenshot shows the Agent Connector Manager interface. On the left, a tree view displays the network structure under 'localhost (5)'. The 'Network: 192.168.123.0 (5)' folder is expanded, showing several agents: agent(1) on 192.168.123.22 (Linux), agent(0) on 192.168.123.33 (Linux), agent(2) on 192.168.123.77 (Windows), agent(5) on 192.168.123.95 (Linux), and agent(5) on 192.168.123.100 (Windows). The 'Quick Information' panel for agent(5) is shown below, with the following details:

Visibility Path	/192.168.123.95/agent(5)
Architecture	x86-64
Privilege Level	Regular account
Host	<a href="http://www.mycorp.com">www.mycorp.com</a>
Crypto Channel	True
Expiration Date	6/4/2020 10:16 AM
Proxy Agent	<a href="#">localagent</a>
Deployed With	Install OS Agent using OS Command Injection Agent

All that is required now is to run reports as no cleanup is required on a logical agent!

Here is an example of a Web Application Vulnerability report generated from IMPACT.

The screenshot shows the 'Report Generation Wizard' in IMPACT. The 'Report Type Selection' step is active, with the instruction 'Select the type of report that you need'. The 'Select report category' dropdown is set to 'WebApps'. The 'Reports' list includes:

- WebApps Delta Report
- WebApps Executive Report
- WebApps Remediation Validation Report
- WebApps Vulnerability Report** (highlighted)

On the right, the 'Show the following type of reports:' section has three checked options: 'Crystal Report', 'Spreadsheet', and 'User Spreadsheet'. A 'Duplicate' button and an 'Edit' button are also visible. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons. A blue information box at the bottom left states: 'This RPT works with Web view, which is not currently selected. You should switch to that view to use these RPT steps.'

# Webapps Vulnerability Report

May 3, 2020 at 5:59 AM

This report provides detailed information regarding each web application vulnerability found by Core Impact during the course of the testing. These vulnerabilities represent key vulnerable points within the tested applications and can be used to better understand the risk associated with the web application.

For more information regarding the types of vulnerabilities found, consult the Vulnerability Descriptions at the end of the report.

SECTION	PAGE
<a href="#">Workspace information</a>	2
<a href="#">Starting urls</a>	3
<a href="#">Summary</a>	4
<a href="#">Vulnerabilities breakdown</a>	5
<a href="#">Vulnerability analysis</a>	6
<a href="#">A1. SQLi - vulnerabilities</a>	8
<a href="#">A1. SQLi - vulns. details</a>	12
<a href="#">A1. SQLi - requests</a>	22
<a href="#">A1. SQLi - ws request method</a>	26
<a href="#">A1. SQLi - ws request method ns</a>	28
<a href="#">A1. OSCI - vulnerabilities</a>	30
<a href="#">A1. OSCI - parameters</a>	31
<a href="#">A1. OSCI - ws request method</a>	32
<a href="#">A1. OSCI - ws request method ns</a>	33
<a href="#">A7. XSS - vulnerabilities</a>	34
<a href="#">A7. XSS - basic info</a>	36
<a href="#">A7. XSS - attack info</a>	37
<a href="#">A7. XSS - attack info (cont)</a>	38
<a href="#">A7. XSS - requests</a>	39

Summary

Risks

Vulnerabilities	Total
Successfully exploited	27
Exploited in webpages	27
Exploited in hosts	0

Assets

URLs	Total
Found	122
At Risk (confirmed vulnerabilities)	23
Broken links	0

Hosts	Total
Found (by 'WebApps Web Server Network Vulnerability Test' module)	0
At Risk (confirmed vulnerabilities)	0

General

Effort	Total
Modules run	245

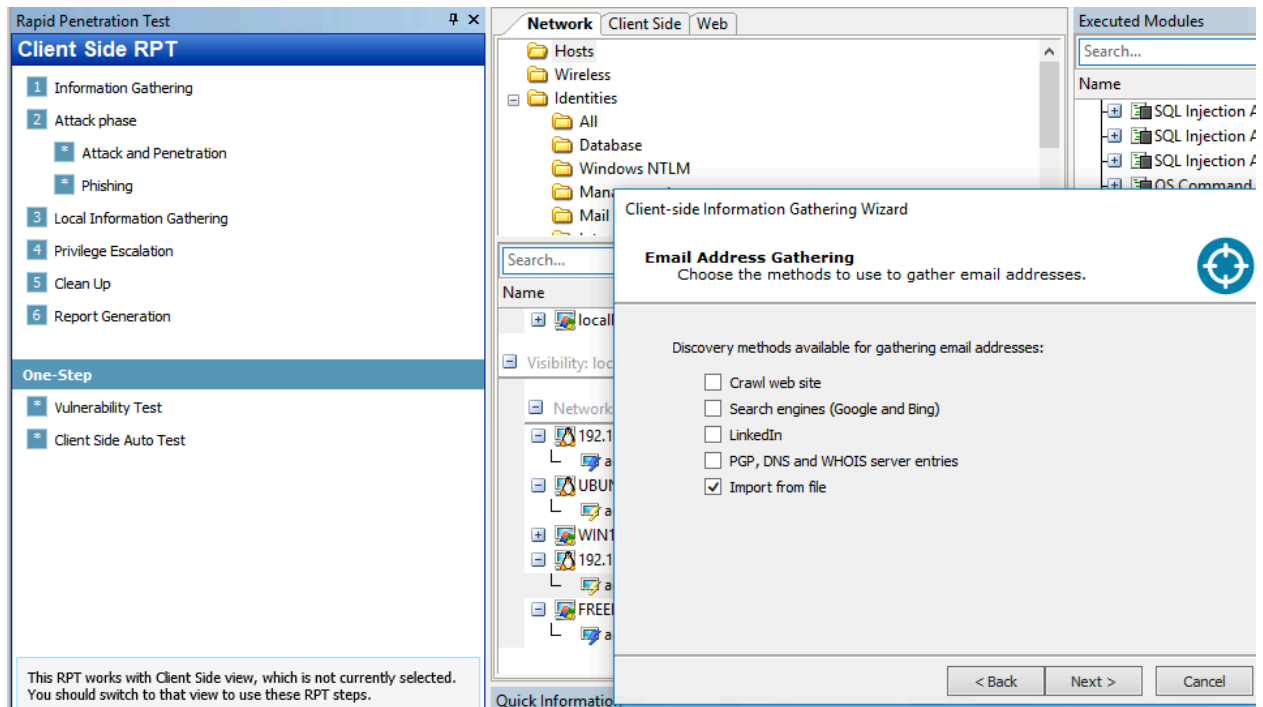
A1. SQL injection - vulnerabilities

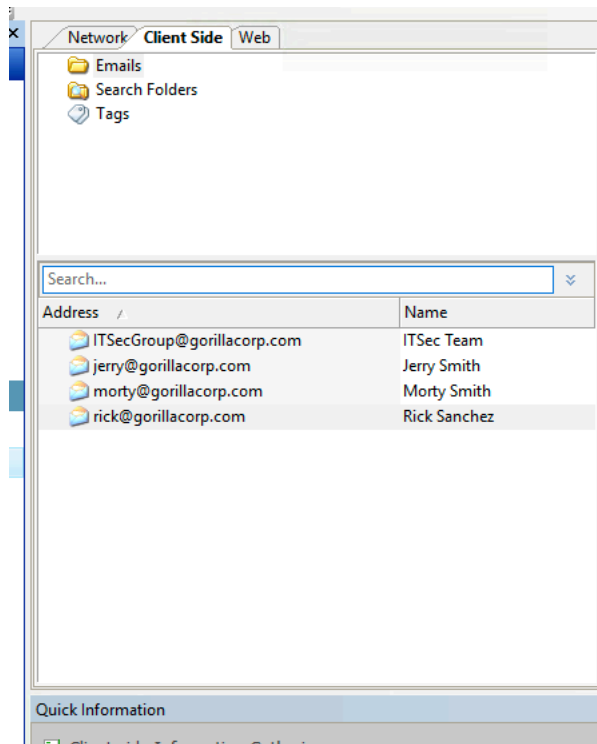
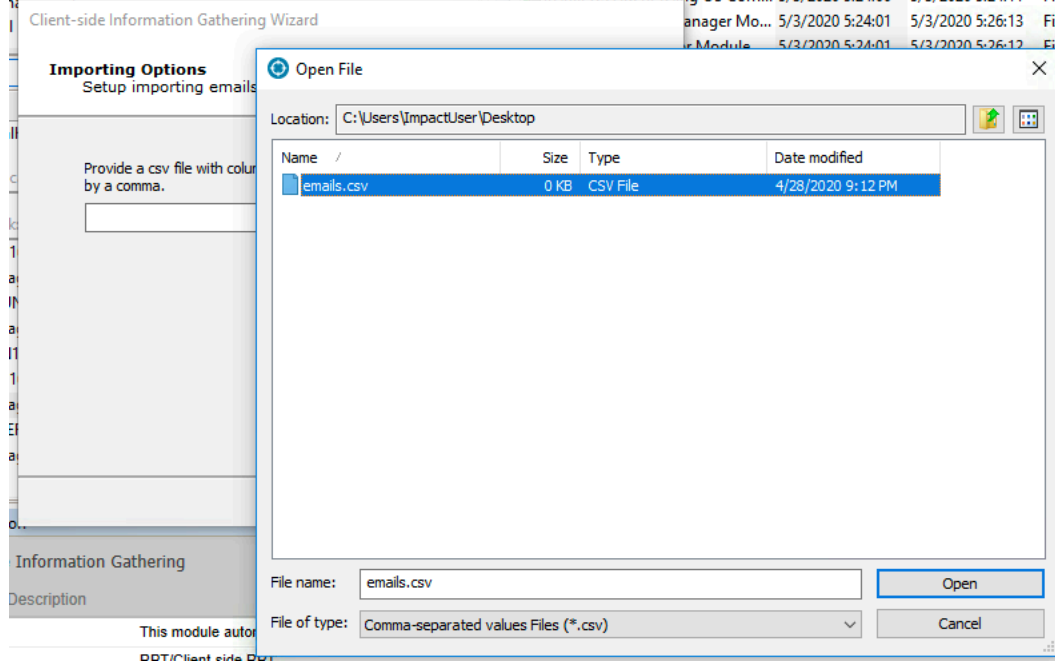
Workspace	Scenario	Web Page	Vuln Id	Documentation	Basic Information
cj-test2	mutillidae (1)	http://192.168.123.95/mutillidae/hints-page-wrapper.php?level1HintIncludeFile=62	1	Description The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization. There, it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques.	-Agent Configured : true -SQL Vuln Type : Blind -Detected by : ASCIIDeltaErrorDecoder -Param Name : level1HintIncludeFile -Param Type : GET -Triggers : "1=1", "-1.0", "1.0", "-1", "1", "0", "@"
cj-test2	mutillidae (1)	http://192.168.123.95/mutillidae/hints-page-wrapper.php?level1HintIncludeFile=59	1	Description The parameter is being used without sanitization inside a SQL statement as a number, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization. The query being performed should look like SELECT ... WHERE [column]=<level1HintIncludeFile parameter>	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : SqlErrorStringPage -Param Name : level1HintIncludeFile -Param Type : GET -Triggers : "A", "a", "--", ""
cj-test2	mutillidae (1)	http://192.168.123.95/mutillidae/hints-page-wrapper.php?level1HintIncludeFile=59	2	Description The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization. There, it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques.	-Agent Configured : true -SQL Vuln Type : Blind -Detected by : ASCIIDeltaErrorDecoder -Param Name : level1HintIncludeFile -Param Type : GET -Triggers : "1=1", "-1.0", "1.0", "-1", "1", "0", "@"

## Client Side Penetration Testing

Click on the TAB labeled Client Side RPT, this brings you into the Client Vector in the workspace.

Select Step 1. Information gathering, choose “Import from file”, select emails.csv from Desktop





Under Step 2 – attack phase, select Phishing, under Web Page Redirect, type <http://www.gorillacorp.com/OopsPage.html>. This can be a security awareness website whereby users will be redirected to a site that notify users that they had been phished and will receive an email soon to attend security awareness training programme. There is an option to clone web page whereby Core

Impact will host and impersonate the web page entered, customer submitted form data including username & password can be captured by Core Impact under this cloned web page

The screenshot shows the 'Client-side Phishing Wizard' window. The title bar reads 'Client-side Phishing Wizard'. Below the title bar, the section is titled 'Phishing Type Selection' with 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 has a text box containing 'http://www.gorillacorp.com/OopsPage.html'. The 'Web Page Clone' option has a text box for 'Enter the URL of the web page to be impersonated'. Below these are three checkboxes: 'Save submitted form data' (checked), 'Ignore forms without credentials' (checked), and 'Redirect user after data submission' (unchecked). There is also a text box for 'Enter the URL of the web form to be redirect'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

For the From: column email, choose [itsecgroup@gorillacorp.com](mailto:itsecgroup@gorillacorp.com) For the To: column email, choose [morty@gorillacorp.com](mailto:morty@gorillacorp.com)

The screenshot shows the 'Client-side Phishing Wizard' window. The title bar reads 'Client-side Phishing Wizard'. Below the title bar, the section is titled 'Email Target Selection' with the instruction 'Specify the target email addresses.'. There are two text boxes: 'From: ITSecGroup@gorillacorp.com' and 'To: morty@gorillacorp.com'. A note states: '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.'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

You can choose the email template or upload your own email template

## 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):

C:\ProgramData\IMPACT\components\modules\classic\install\te X ...

Email Subject:

Security policies update - Please read

Message priority: Normal v

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

1. Select mail sending options and put 192.168.123.200 as the smtp server. User as postmaster, password is ImpactUser

## 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

### Client-side Phishing Wizard

#### Email Sending Settings

Customize the settings for sending emails.

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.

SMTP server:

SMTP port:  Connection security:

User name:

Password:

Numbers of targets in each chunk

Chunk size:

Set the time to wait between chunks (in seconds)

Delay(s):

< Back Finish Cancel

Checked Executed Modules log to make sure email was successfully sent

Client-side Phishing	5/5/2020 10:27:00 AM	5/5/2020 10:27:00 AM	Running	/localagent	Yes
Client-side Phishin...	5/5/2020 10:27:01 AM	5/5/2020 10:27:01 AM	Running	/localagent	No

```

Module Log
*** Debugging mode is enabled
randomPrefix ONLOADWINDOWTNRkDTbtstbdYclrLHGW1Qaa
Trying prefix: ONLOADWINDOWTNRkDTbtstbdYclrLHGW1Qaa
Web Browser Agent environment established
Target: "Morty Smith" <morty@gorillacorp.com> URL:
http://192.168.123.200/rpt/a9e53215004a16f8/ONLOADWINDOWTNRkDTbtstbdYclrLHGW1Qaa/list.ht
Trying to send mails using preferred SMTP server.
Connected to server 192.168.123.200:25.
* The server is offering the following Auth methods: PLAIN, LOGIN, CRAM-MD5, GSSAPI, DI
Mail sent successfully to: "Morty Smith" <morty@gorillacorp.com>.
Disconnected from server.
Sending mails using preferred SMTP server done.
  
```

Module Output | Module Log | Module Parameters

2. Activity log will show that users had not viewed or clicked any link in the email.

Module Name	Start Time	End Time	Status	Agent	Enabled
Client-side Phishing	5/5/2020 10:27:00 AM	5/5/2020 10:27:00 AM	Running	/localagent	Yes
Client-side Phishin...	5/5/2020 10:27:01 AM	5/5/2020 10:27:01 AM	Running	/localagent	No
CS Image Tag	5/5/2020 10:27:02 AM	5/5/2020 10:27:02 AM	Running	/localagent	No
CS-WBA Brows...	5/5/2020 10:27:02 AM	5/5/2020 10:27:02 AM	Running	/localagent	No

**Module Output**

### Client-side Phishing

**Attack Information**

Redirect to	<a href="http://www.qorillacorp.com/OopsPage.html">http://www.qorillacorp.com/OopsPage.html</a>
Started	5/5/2020 10:27 AM
Finish	Until stopped by user

**Targets**

Target	Viewed	Clicked
<a href="mailto:morty@qorillacorp.com">morty@qorillacorp.com</a>	No	No

Module Output
Module Log
Module Parameters

Go to Email Client to test phishing email.

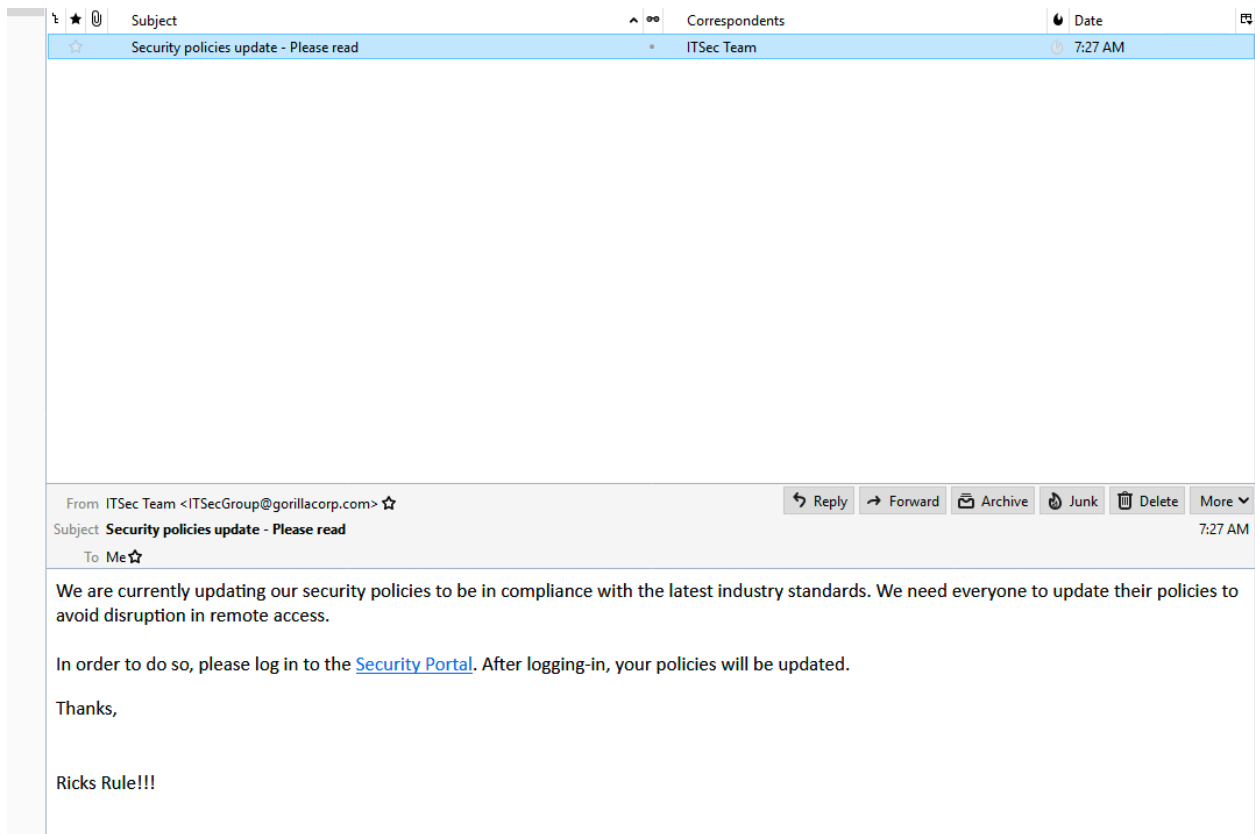
Go to Windows Search -> type mstsc . Select Remote Desktop connection.

Type ip address 192.168.123.140. Login into the email client with following username and password

Username : morty

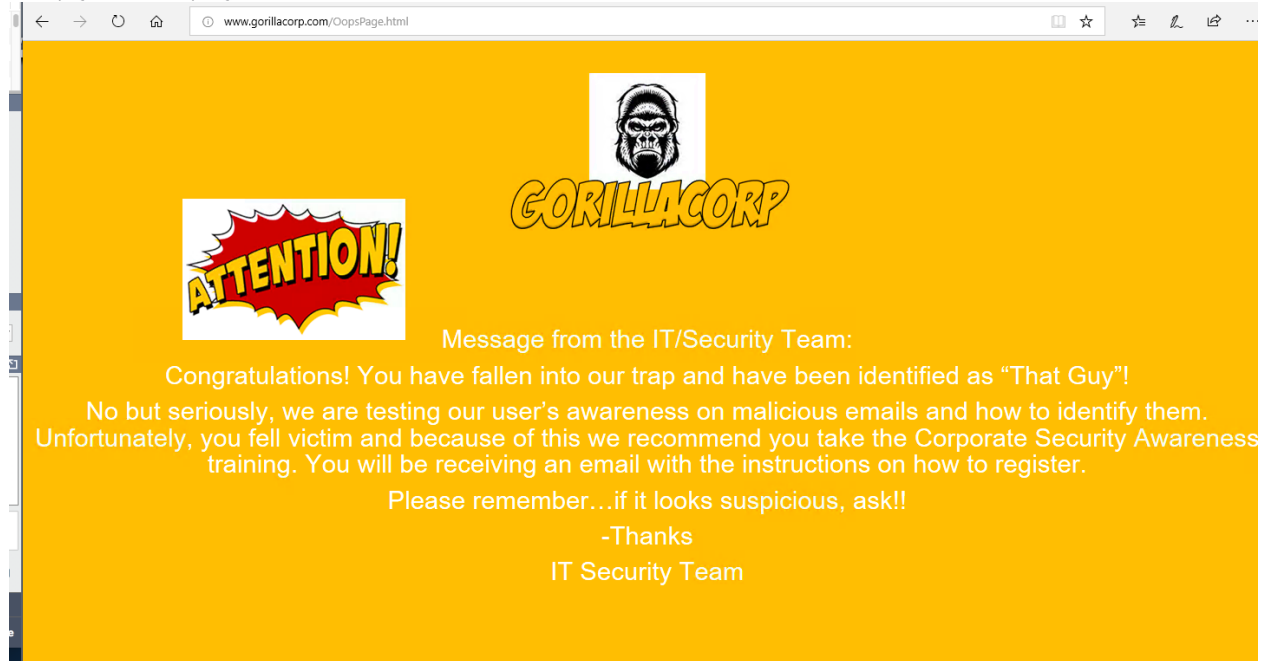
Password :P1ckl3R1ck!

Open Mozilla Thunderbird email application in Desktop after login



When the email has arrived open it and take a look at an email borne attack through the eyes of a victim.

1. You will notice there is an email with a link in it, click on it. A browser will open and redirect to an IT Security Team warning site.



2. After clicking on the link, refer back to your IMPACT console. The executed modules pane will display if phishing is successful.

Module	Start Time	End Time	Status	Agent	Success
Client-side Phishing	5/5/2020 10:27:00 AM	5/5/2020 10:27:00 AM	Running	/localagent	Yes
Client-side Phishin...	5/5/2020 10:27:01 AM	5/5/2020 10:27:01 AM	Running	/localagent	No
CS Image Tag	5/5/2020 10:27:02 AM	5/5/2020 10:27:02 AM	Running	/localagent	No
CS-WBA Brows...	5/5/2020 10:27:02 AM	5/5/2020 10:27:02 AM	Running	/localagent	No

**Module Output**

**Client-side Phishing**

**Attack Information**

Redirect to: <http://www.qorillacorp.com/OopsPage.html>

Started: 5/5/2020 10:27 AM

Finish: Until stopped by user

**Targets**

Target	Viewed	Clicked
<a href="mailto:morty@qorillacorp.com">morty@qorillacorp.com</a>	Yes	Yes

Module Output | Module Log | Module Parameters

Under Browser fingerprint, there is information such as plugins available on client browser to plan for your next client side attack, which is sending exploit through email. If sending exploit through email is successful, a Memory Resident OS Agent will be reflected in association with the IP address of the user's system in the Network View. At this time it may be desired to interact with the OS Agent via the use of the *Local Information Gathering* wizard, *Shell*, *Browse Files* options, or to consider setting the OS Agent as a Pivot Point to perform testing against other systems in the network the user's system resides within.

Client-side Phishing	5/5/2020 10:27:00 AM	5/5/2020 10:27:00 AM	Running	/localagent	Yes
Client-side Phishing (We...	5/5/2020 10:27:01 AM	5/5/2020 10:27:01 AM	Running	/localagent	No
CS Image Tag	5/5/2020 10:27:02 AM	5/5/2020 10:27:02 AM	Running	/localagent	No
CS-WBA Browser fing...	5/5/2020 10:27:02 AM	5/5/2020 10:27:02 AM	Running	/localagent	No

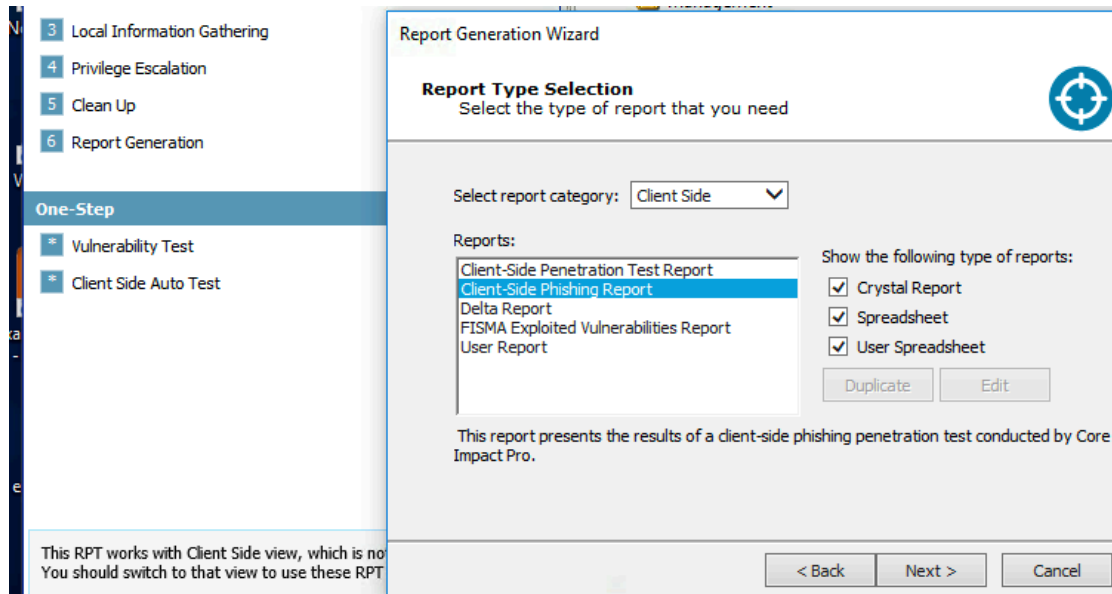
**Module Output**

```

appName: Netscape
appCodeName: Mozilla
timestamp: 05-05-2020 10:31:36
productSub: 20030107
cookieEnabled: true
appVersion: 5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
browser_name: Google Chrome
platform: Win32
browser_version: 64
onLine: true
userAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Plugins:
Edge PDF Viewer
        
```

Module Output
Module Log
Module Parameters

Here is an example of Client-side Phishing report generated from IMPACT.



## Client-Side Phishing Report

### Introduction

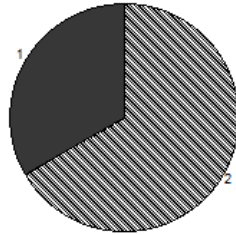
This report presents the results of a client-side phishing exercise conducted by Core Impact. A phishing attack sends an email to one or more email addresses attempting to trick the recipients into following a link that could either redirect them to an external webpage (*Web Page Redirect*) or to a webpage controlled by the tester that will impersonate a login page or other web form (*Web Page Clone*).

The goal of the *Web Page Clone* attack is to learn recipients' credentials (or other sensitive information) for a particular service requiring the end user to enter such information. Although control of hosts is not directly obtained, credentials gathered could be used to further abuse the service being impersonated. Information not otherwise available may be obtained using victims' credentials.

### Workspace Summary

WORKSPACE NAME	STARTED	FINISHED	EXACT TIME	RUNNING TIME	COMPANY/TEST AREA NAME
cj-test	05/05/20 09:13 am	05/05/20 10:34 am	1 h 21m 50s	1 h 15m 29s	N/A

## Phishing Attacks



Web Page Redirect

### Phishing Attacks Details

Total Emails Sent: 3  
Total Clicked Links(\*): 1  
Data Submissions: 0

Attacks with no result	66.7%
Clicked link on phishing site	33.3%
Data logged on phishing site	0.0%
<b>Total:</b>	<b>100.0%</b>

(\* In case of a Web Page Clone attack where the target submitted data, the click isn't counted.

### Details of Phishing Attacks

Name	Email	Attack Type	Total Clicks	Data Submitted	Last Activity Date
Morty Smith	morty@gorillacorp.com	Web Page Redirect	0	-	
Morty Smith	morty@gorillacorp.com	Web Page Redirect	0	-	
Morty Smith	morty@gorillacorp.com	Web Page Redirect	1	-	05-05-2020 10:31:36

### Details of Web Page Redirect Attacks

---

Users tricked to visit the phishing site

Name	Email	Browser Data	Date
Morty Smith	morty@gorillacorp.com	IP: Browser: Google Chrome Version: 64 List of Plugins • Edge PDF Viewer	05-05-2020 10:31:36

### Details of Web Page Clone Attacks

---

- No Web Page Clone attacks were found on the selected workspace

This completes the basic usage of the Core Impact. There are many other modules and tests that can be used, please feel free to continue and try other modules and not use the RPTs to get a feel of how you can customize the tool yourself. Under the file>modules area you should see the option to create a Macro, feel free to utilize this Wizard to run your own automated steps.

If you have any further questions or issue, your Sales Engineer should be able to assist.