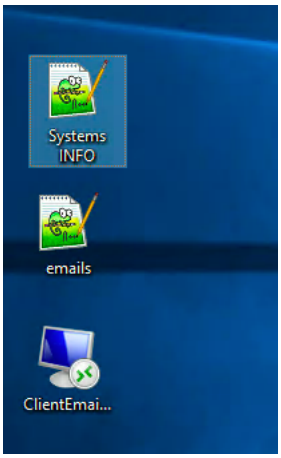
CORE SECURITY
A HelpSystems Company

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.

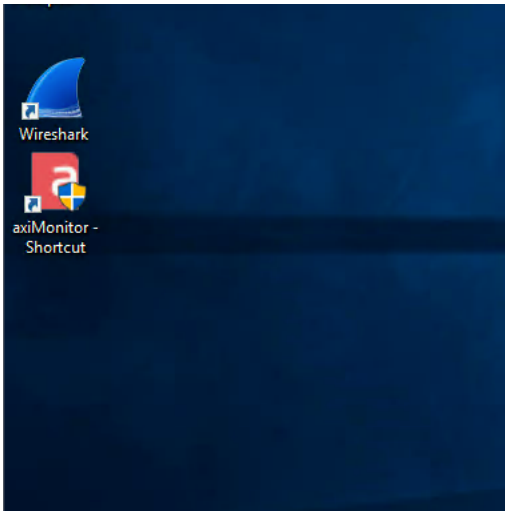


Systems INFO.txt

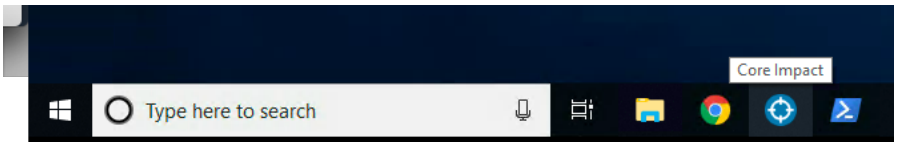
```
Mailserver address:
192.168.123.200
postmaster/ImpactUser

WebApp Test:
http://192.168.123.95/mutillidae/
samurai/samurai **ENTER in Session Mngmt & Services Area**

ClientAccessRdP:
ImpactUser/!ImpactUser!


Phishing Test Redirect URL:
http://www.gorillacorp.com/OopsPage.html

Phishing Clone Form URL:
***Coming Soon***
```

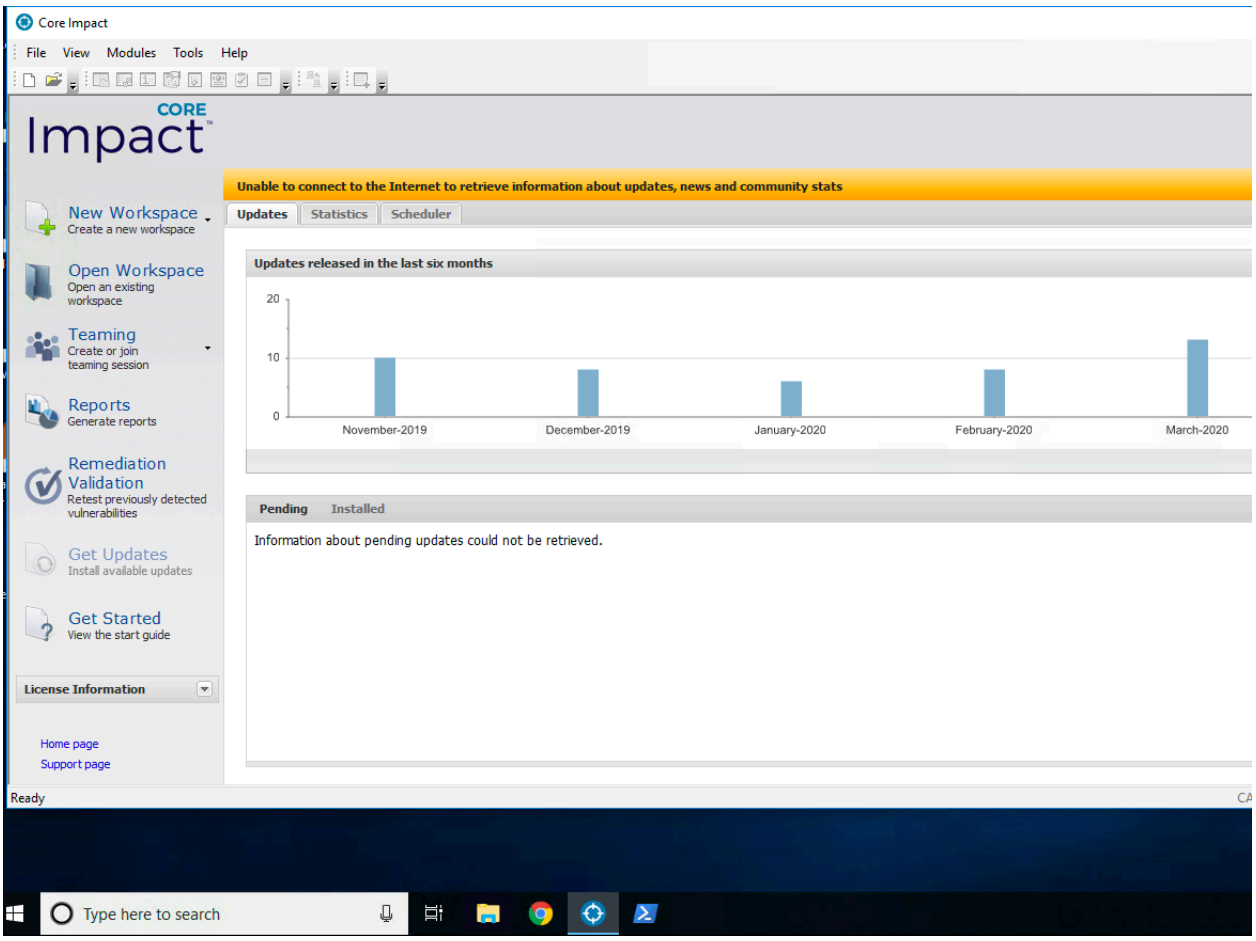
Starting Required Services After Connecting to your Core Impact System

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



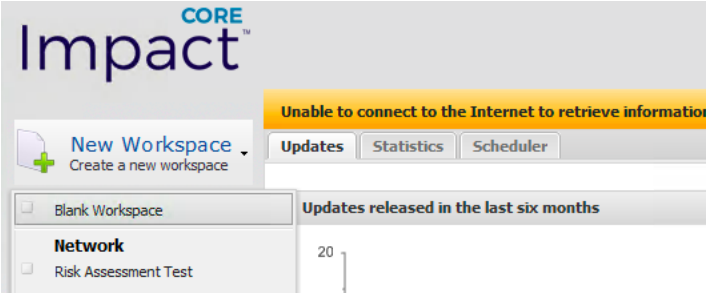
Click on the “Core Impact” icon which is listed on the desktop which will bring you into the IMPACT dashboard as shown below.

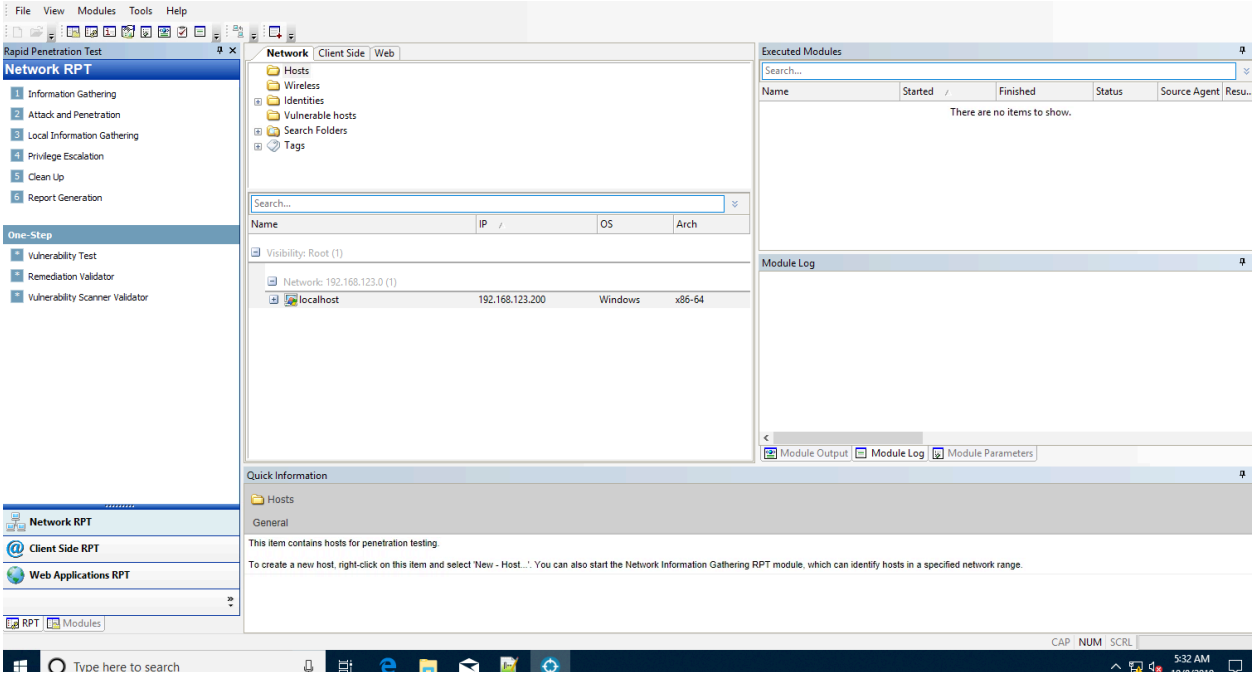




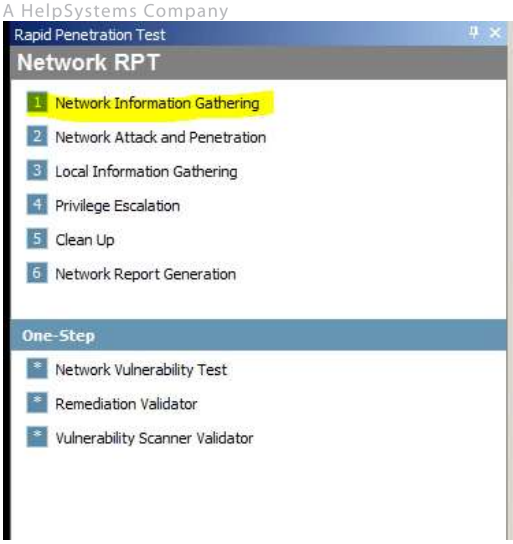
NETWORK TESTING

Now, you are ready to start using use 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.

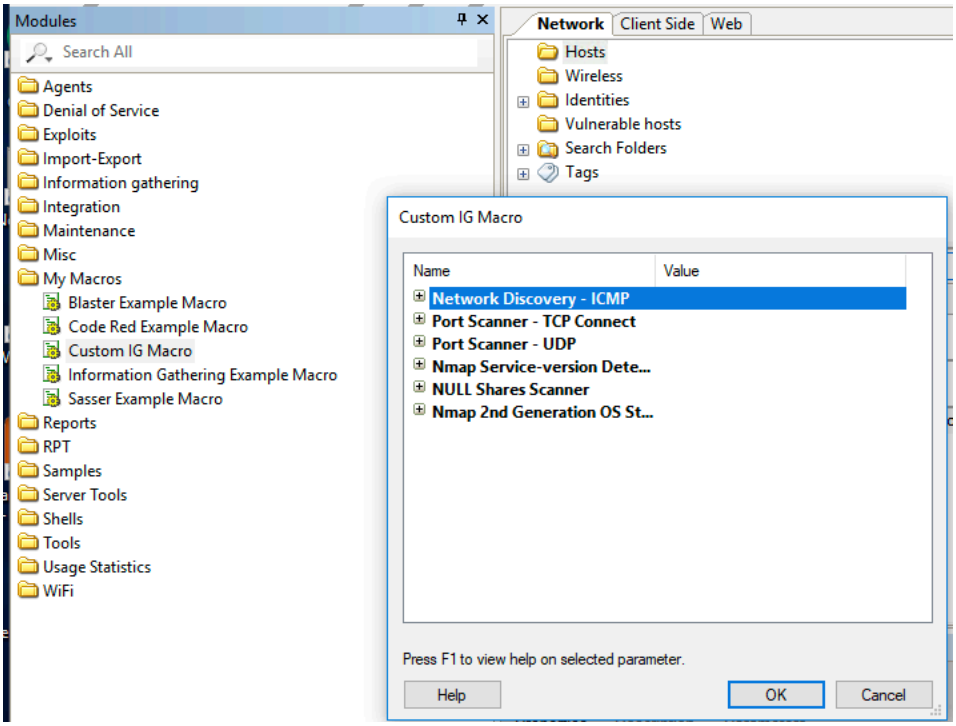




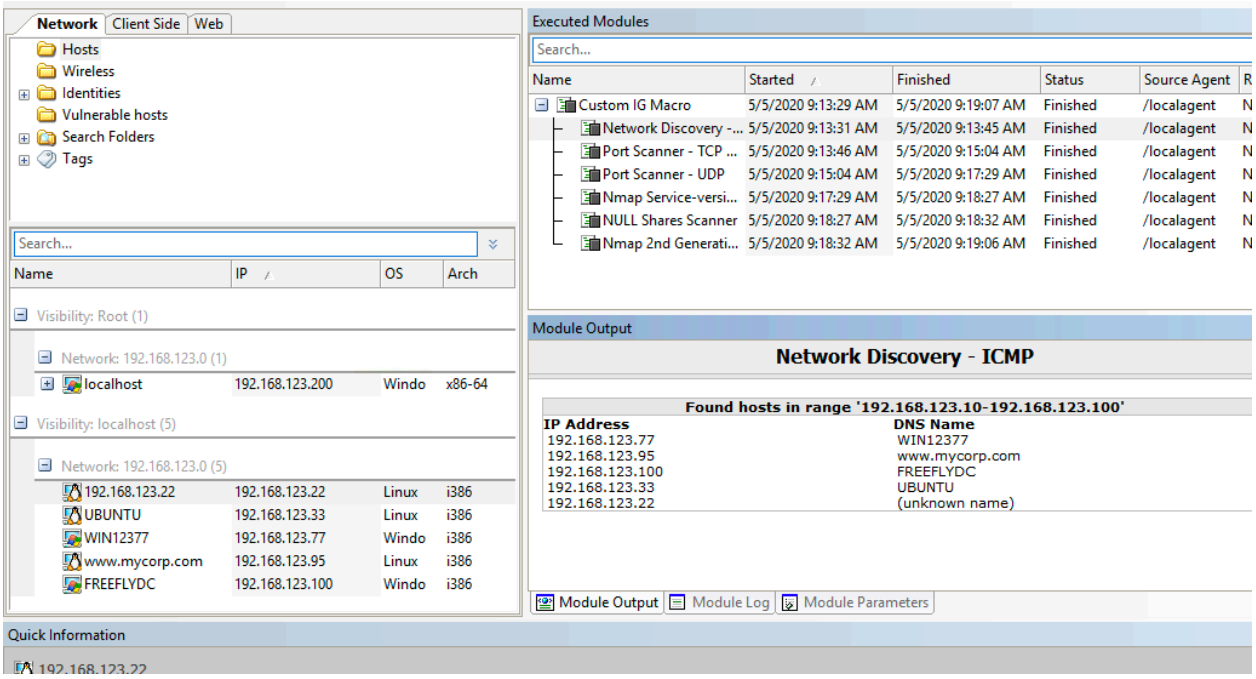
To begin a simple Network Information Gathering, select step # 1 from the Rapid Penetration Test (RPT) on the upper left hand window. Select all defaults when proceeding through the wizard. The results of the gathering is listed below. However, due to within AWS lab, there is a restriction in performing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



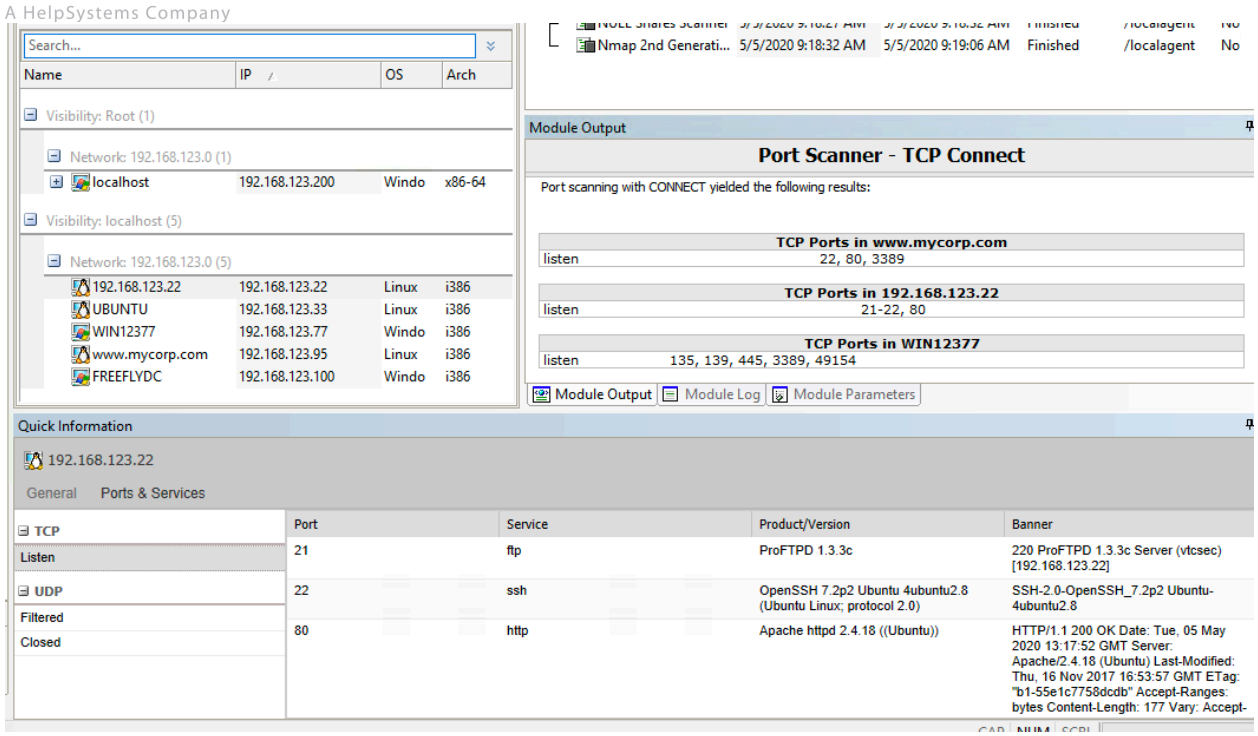
To use alternate module to perform network information gathering in this lab environment, please go to Modules tab, run Custom IG Macro by double clicking the module and click Ok to run the module.



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 :

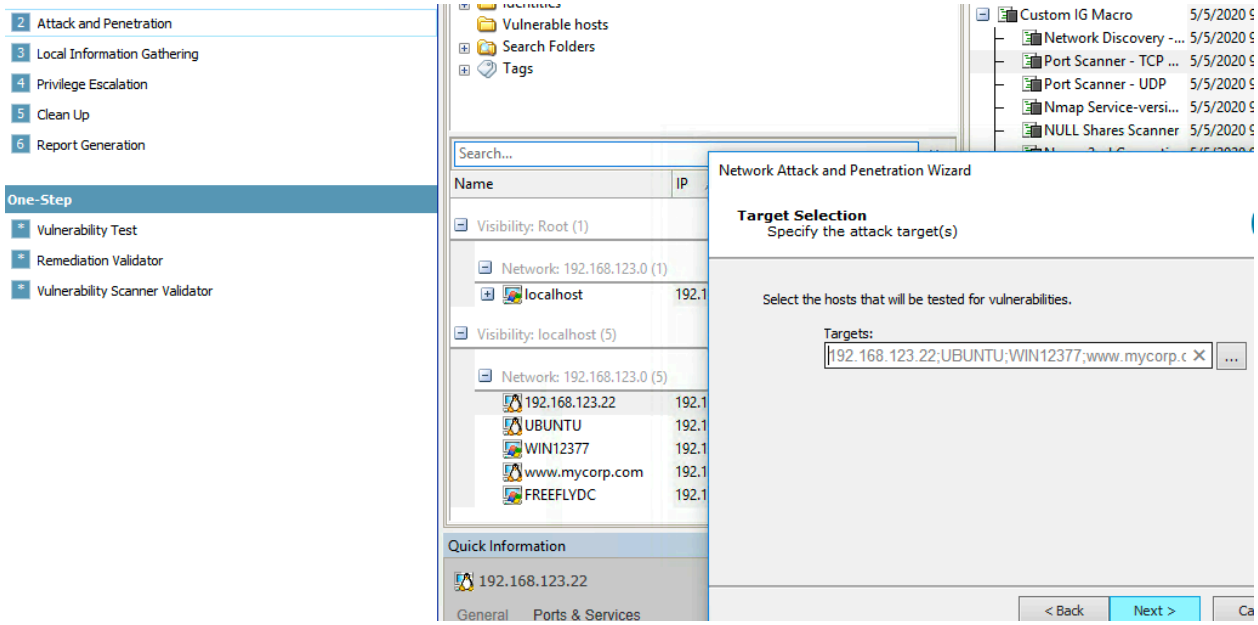


Once the Hosts have been identified and the 1st step completes, Click through the hosts to see some of the information available on them.



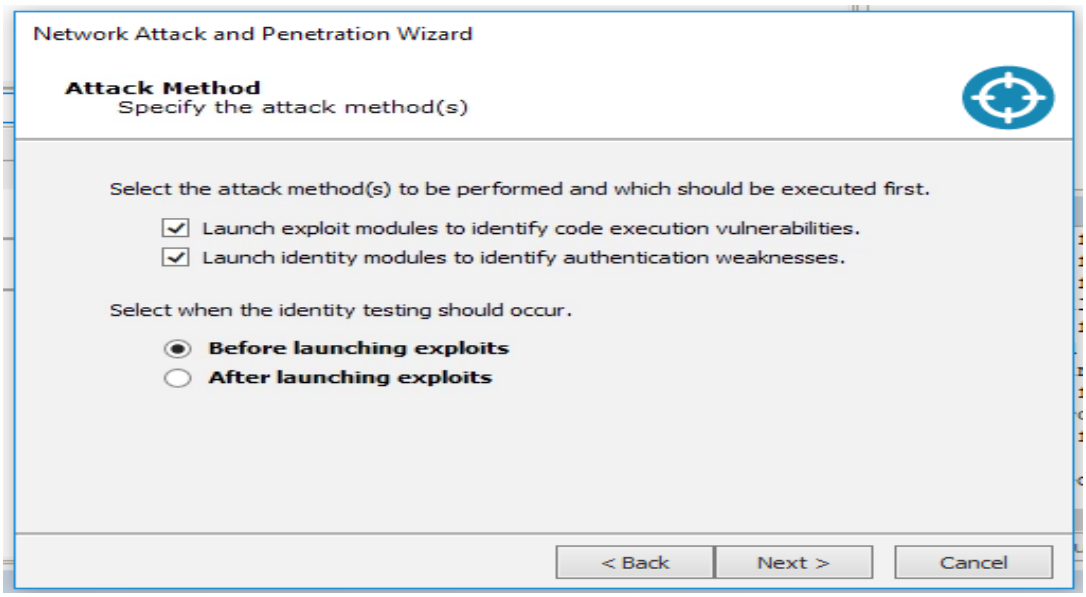
Next select step #2, the attack and penetration in the RPT

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

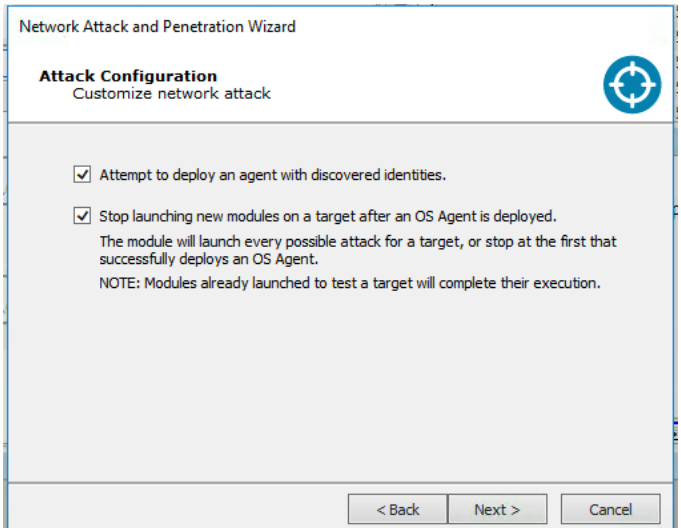


Click Next

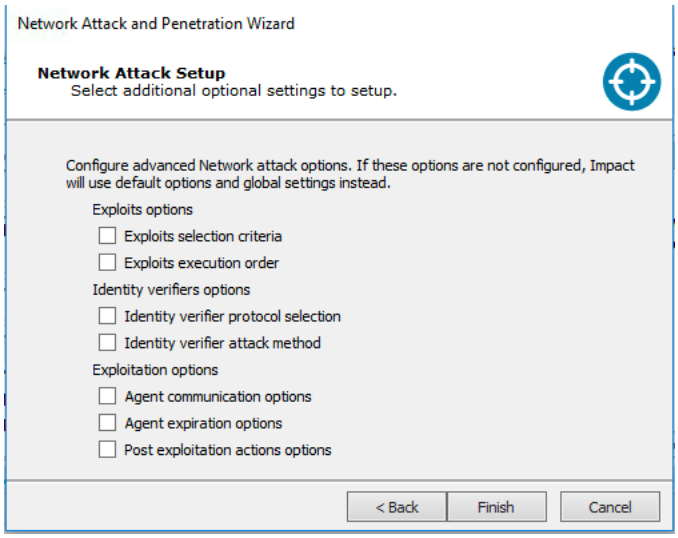
When presented with the Attack Method Select both check boxes



Leave the default options. Select both options highlighted below.



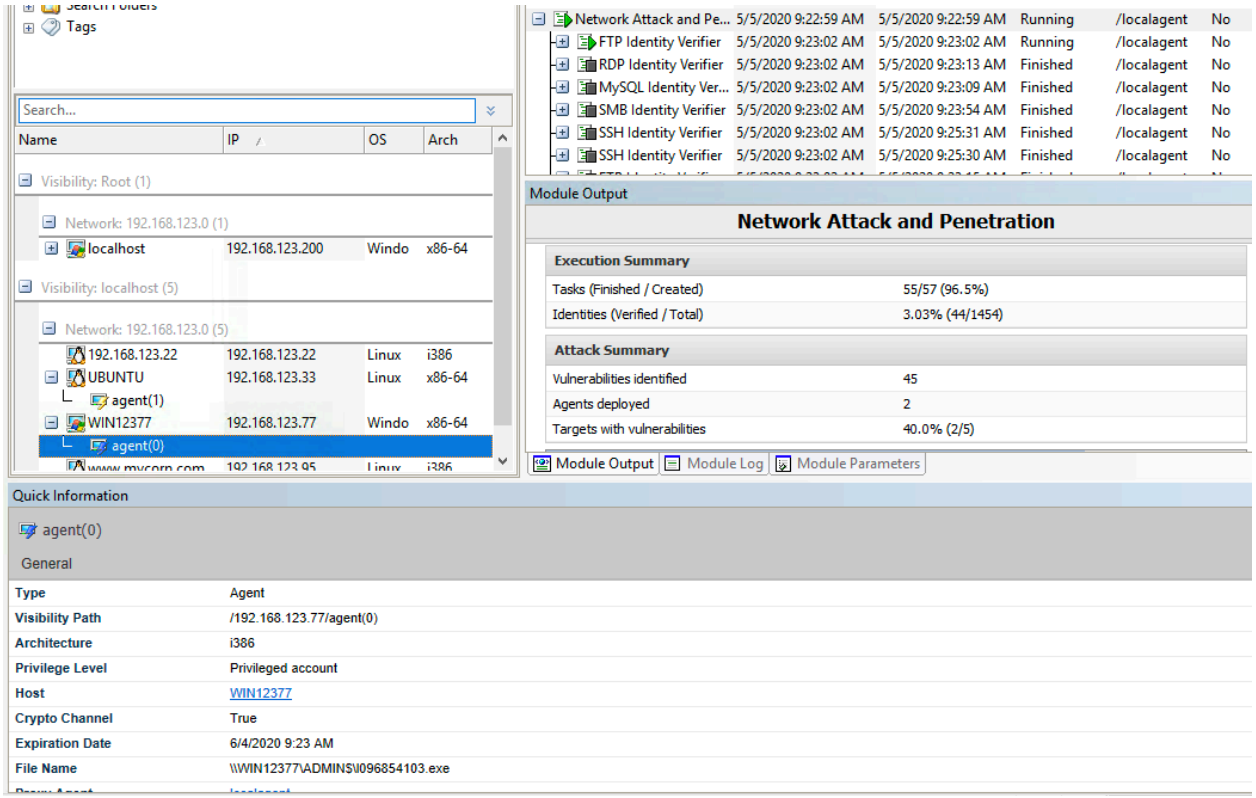
Click Next and leave the default option without checking any advanced Network attack options, and click Finish.



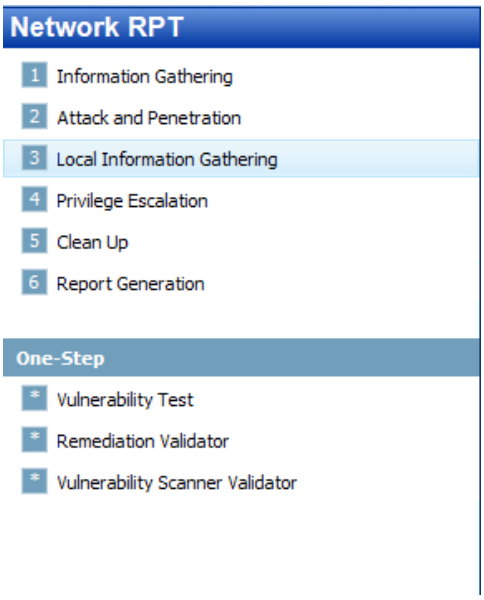
(However, you can individually check the option to see each advance option settings.)

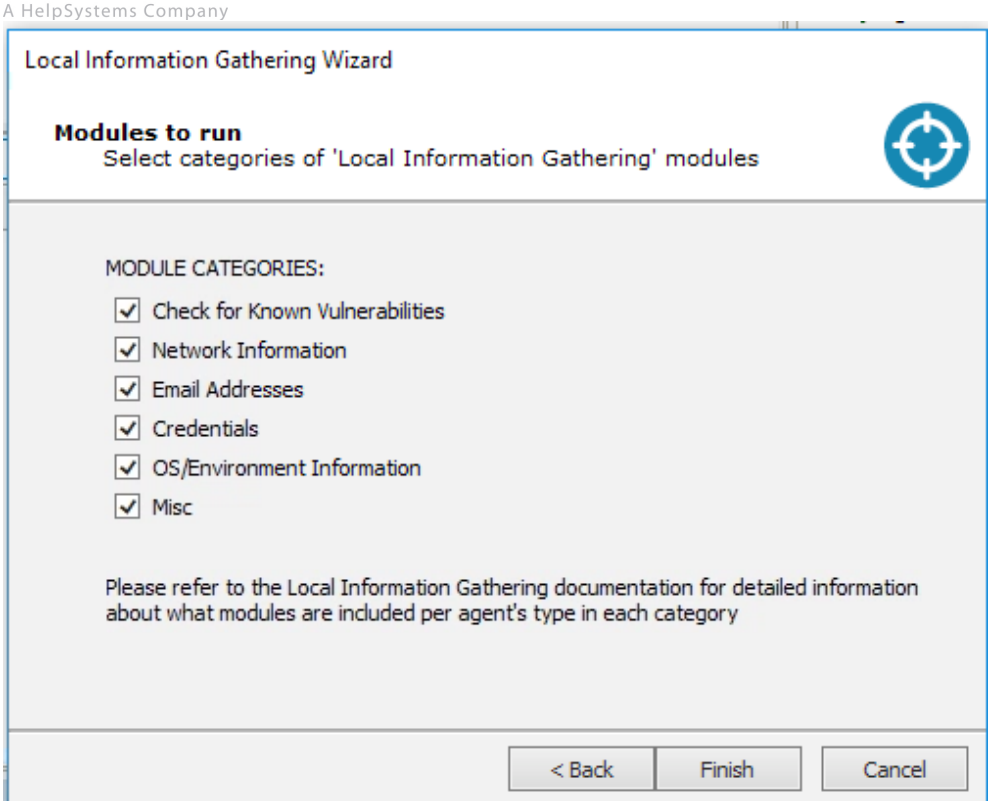
Multiple agents will be placed on the targeted systems indicated that a vulnerability exists. This agent is injected into the memory space of the service that is exposed. This will now give you the option of interacting through the agent by “right clicking” on the agent affords you several options including 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.



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





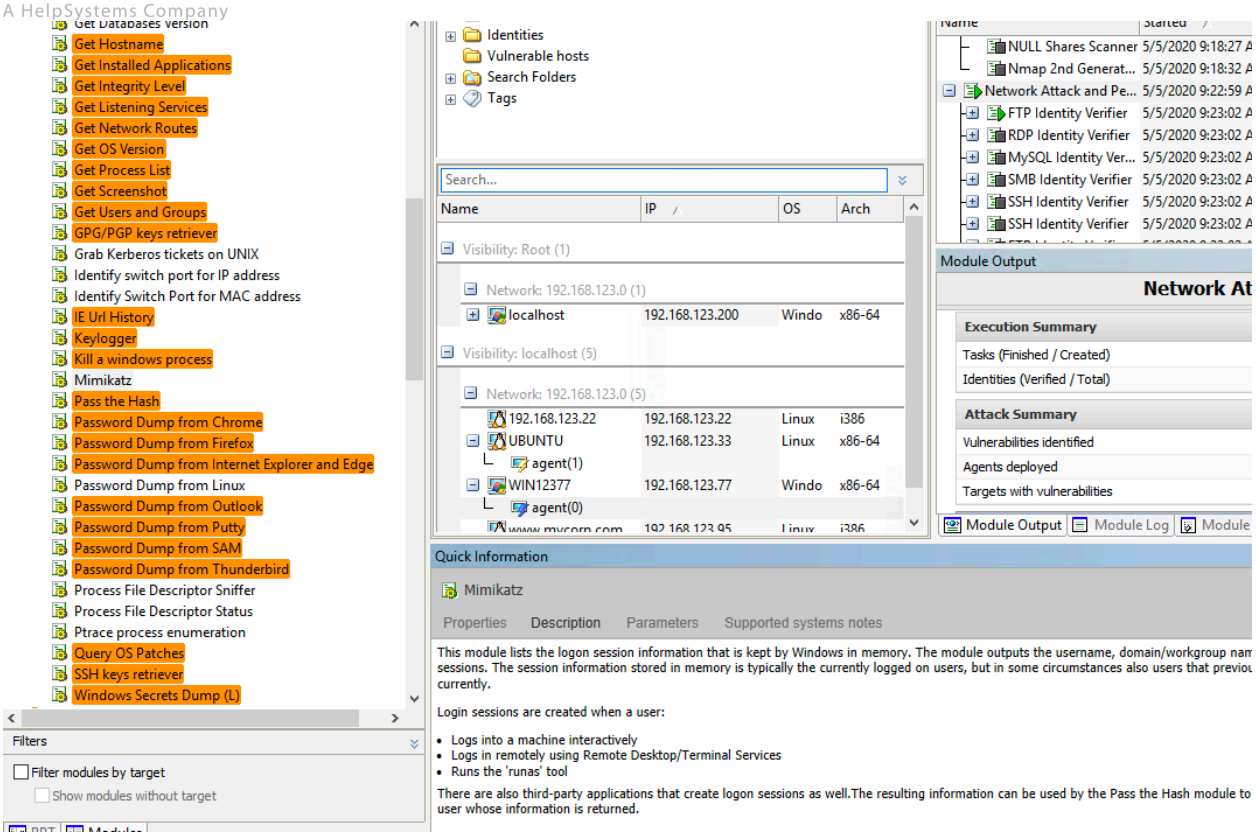
If you would prefer to interact with the individual modules:

Click on the lower left hand side that says Modules.

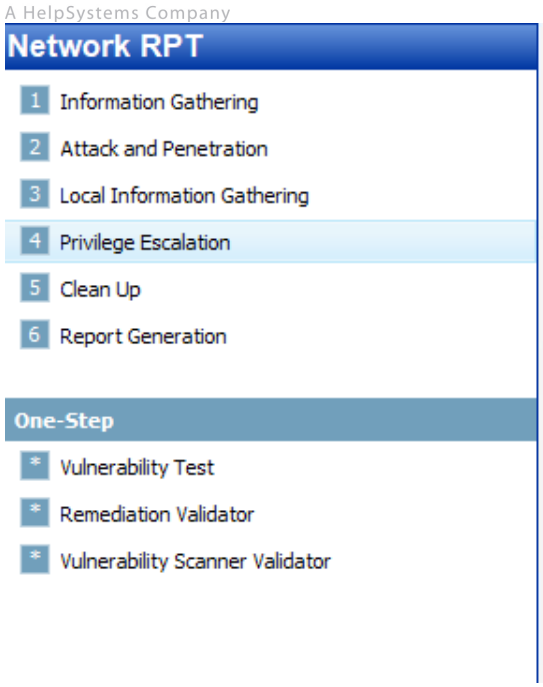
Then click on the Information gathering Folder>Local

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.

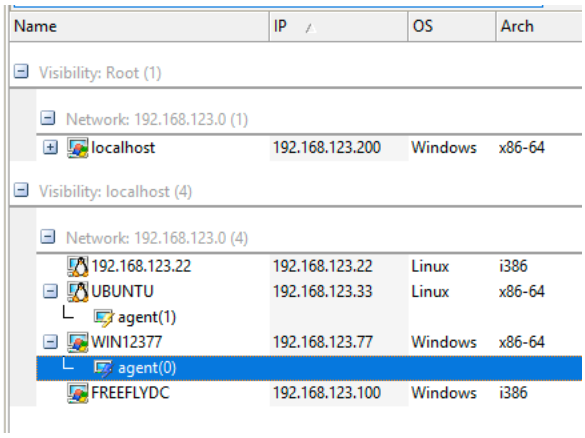
Information on the modules and exploits can be seen in the quick information Panel at the bottom center



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.

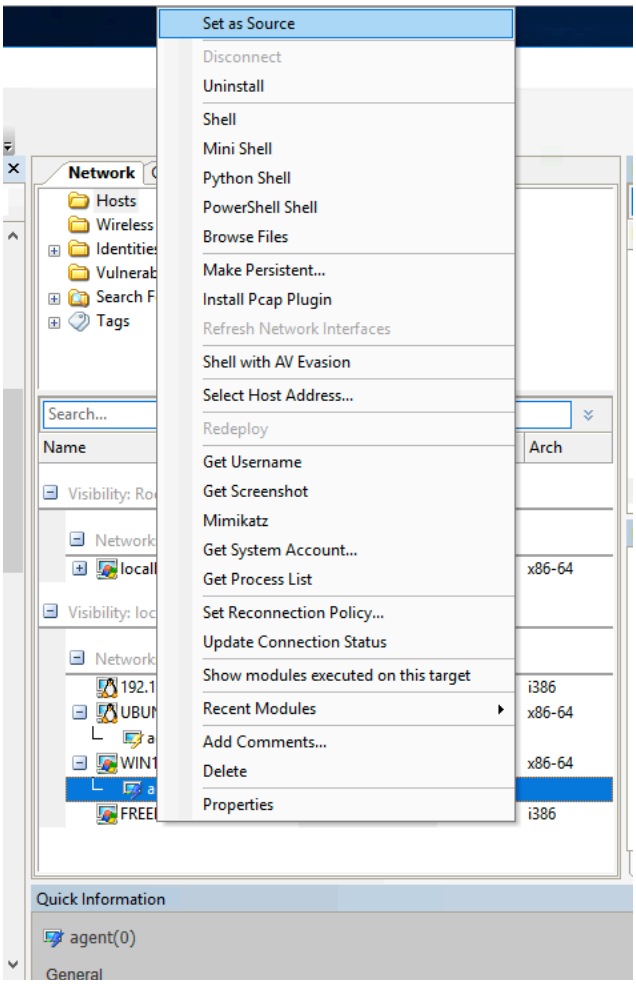


Agent color indicator will indicate type of privilege which agent has. Current screenshot below showed the agent with yellow indicator only has regular user privilege

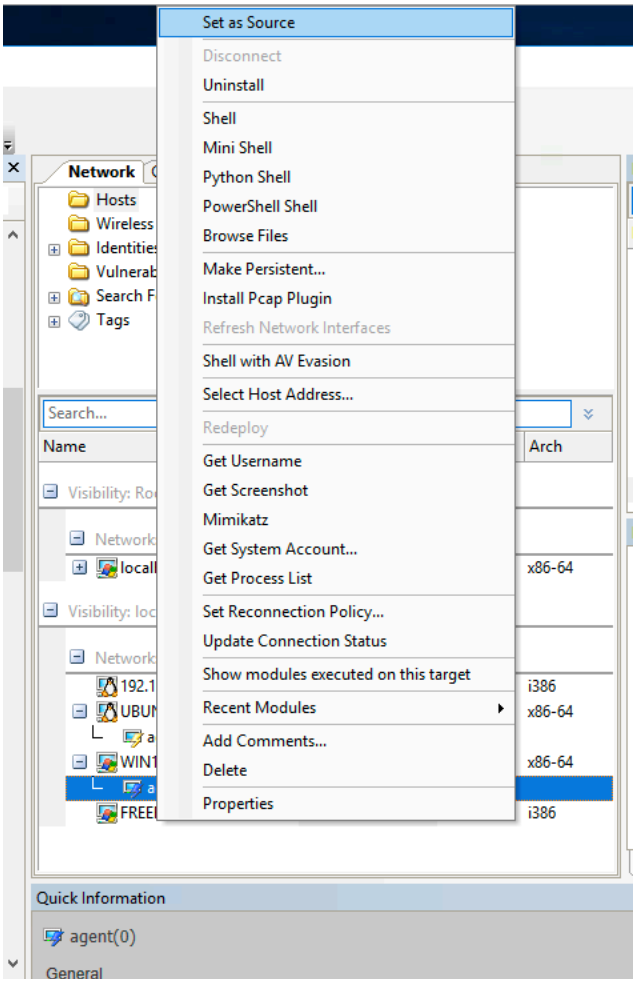


Select which Agents to escalate privilege, click Next and Finish to run Privilege Escalation Exploits on compromised systems

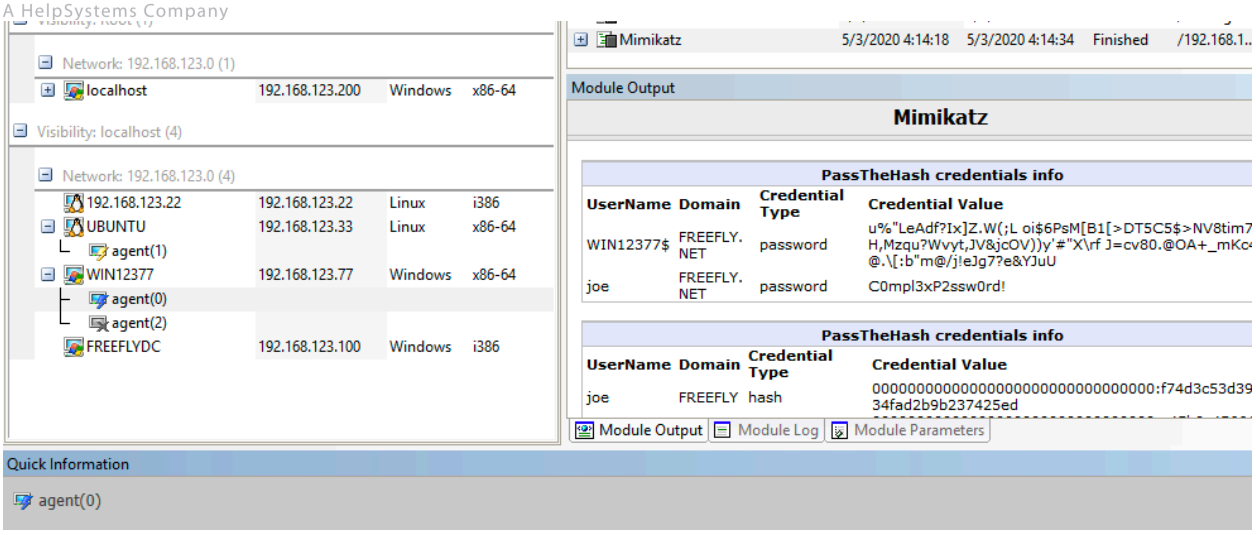
If you escalated any system successfully you can use them as a source agent and pivot off this agent. Simply “right click” and select “set as source.” If you identified another network in the local information gathering (Step #3) then you can use this source agent to pivot into that network.



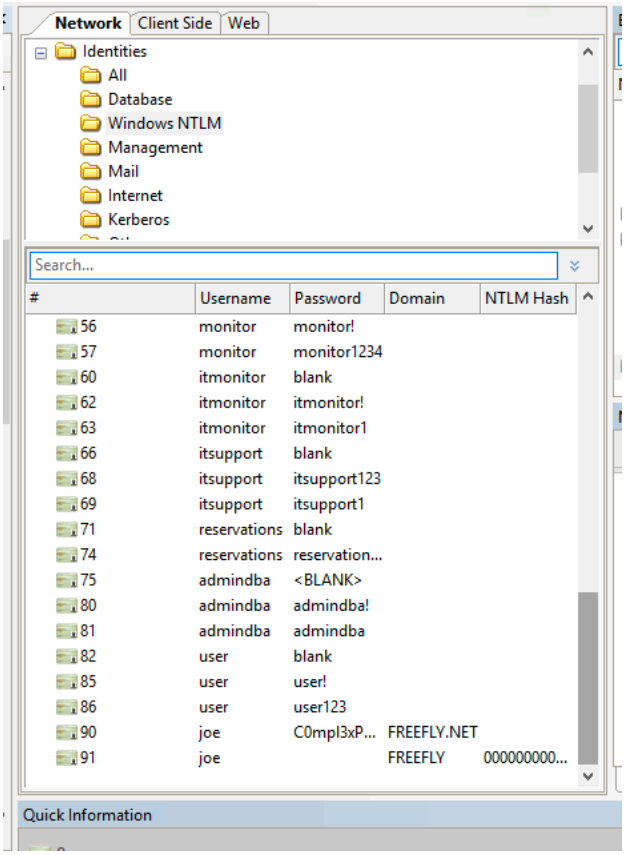
In addition to this there is 1 Windows Client called WIN12377 that gets compromised. If you right click the system and run Mimikatz, you will get the windows credentials dump information from the system.



Here is what it should look like:

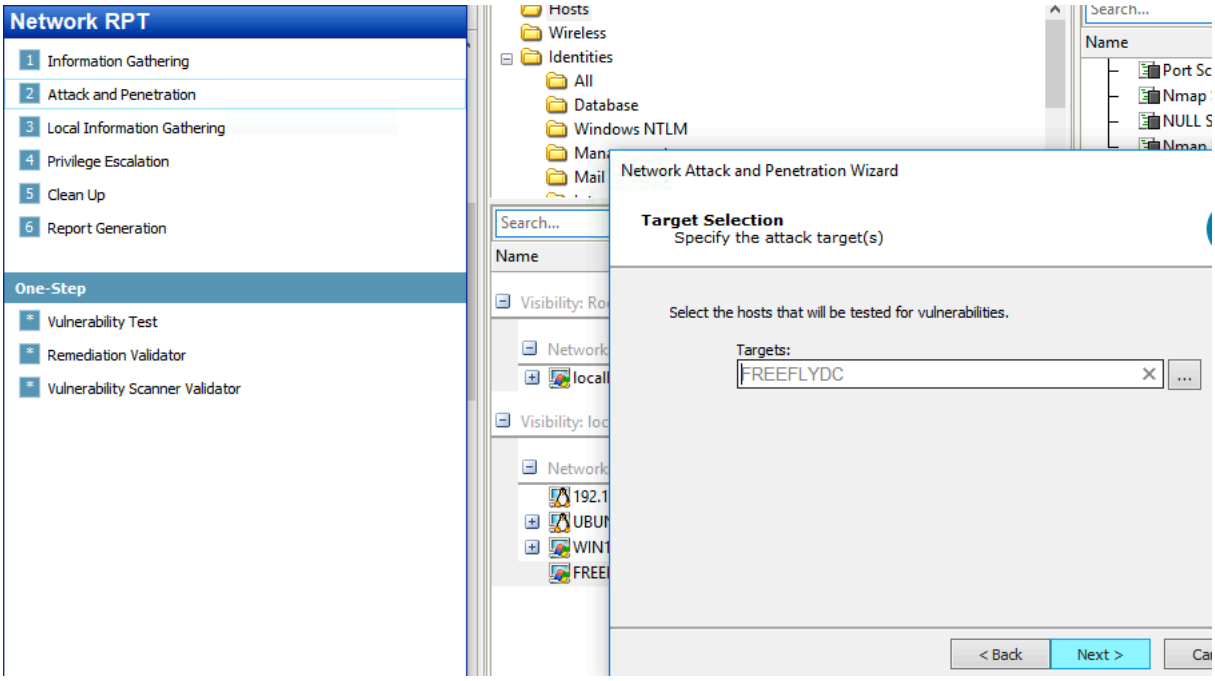


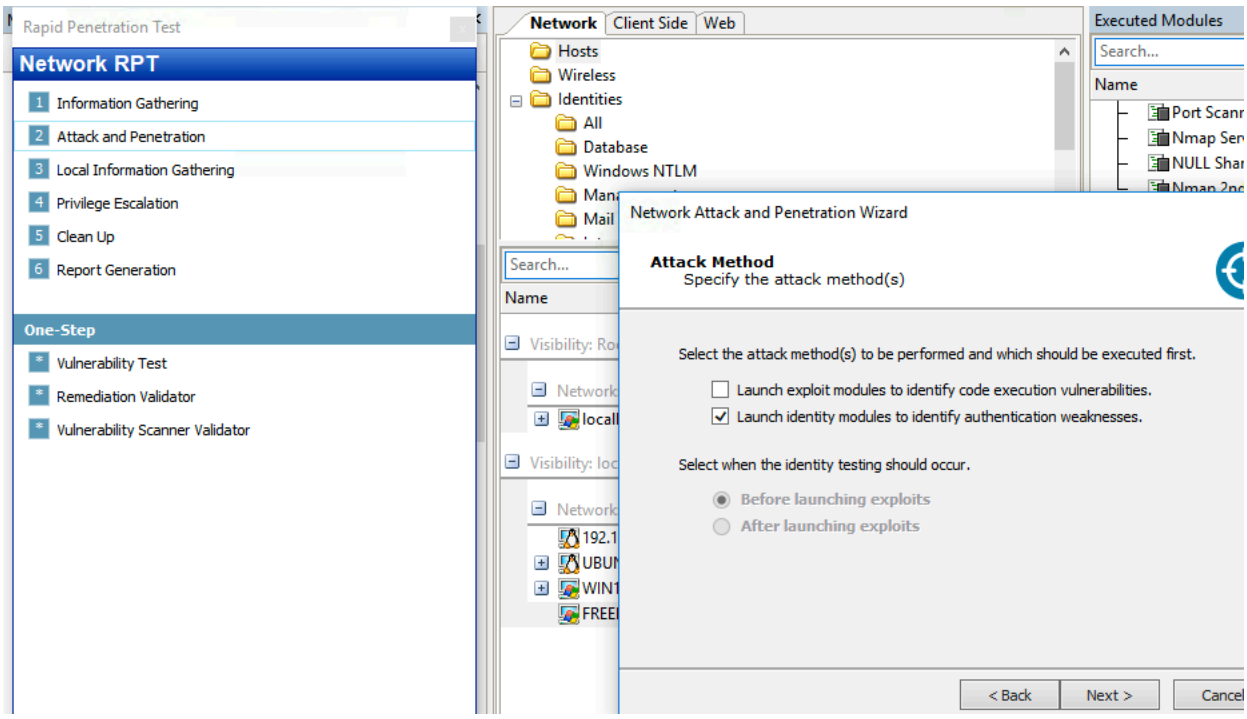
Once that is done select the Identities>All folder in as shown below and all the captured Identities will be displayed. These identities gathered can and will now be used against other systems.

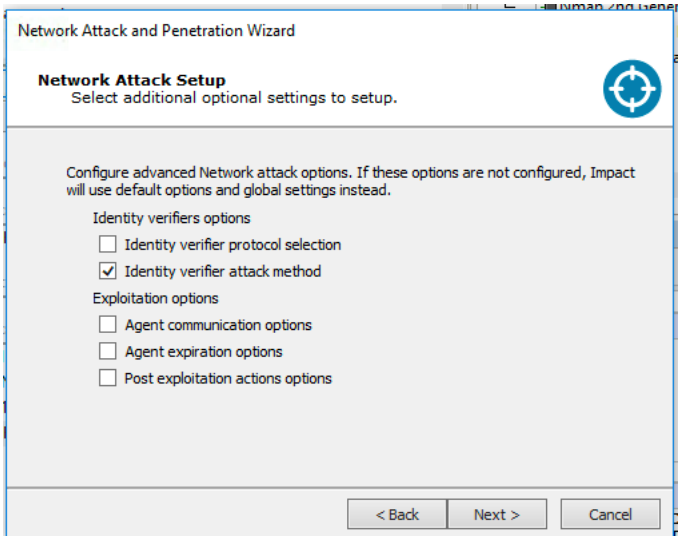


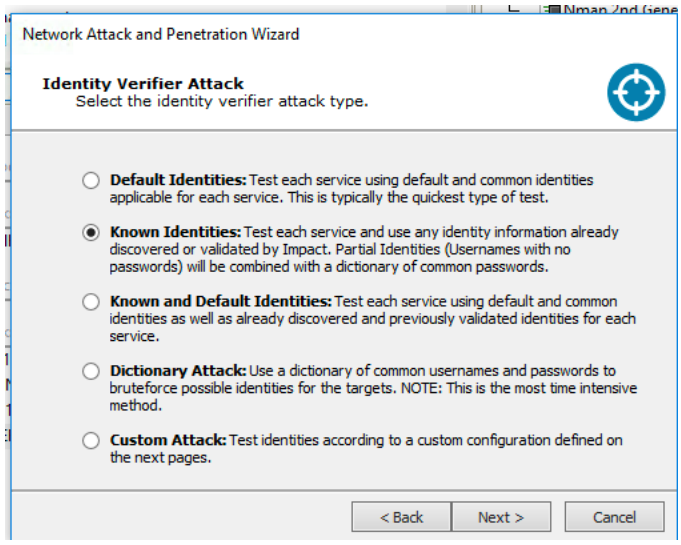
Select Step 2. Attack and Penetration on Domain Controller – FREEFLYDC, as screenshot attached.

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

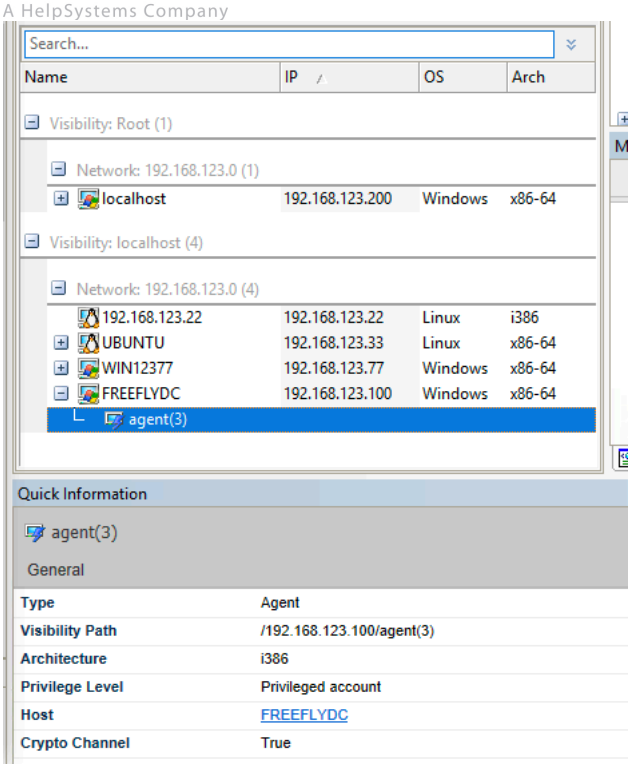




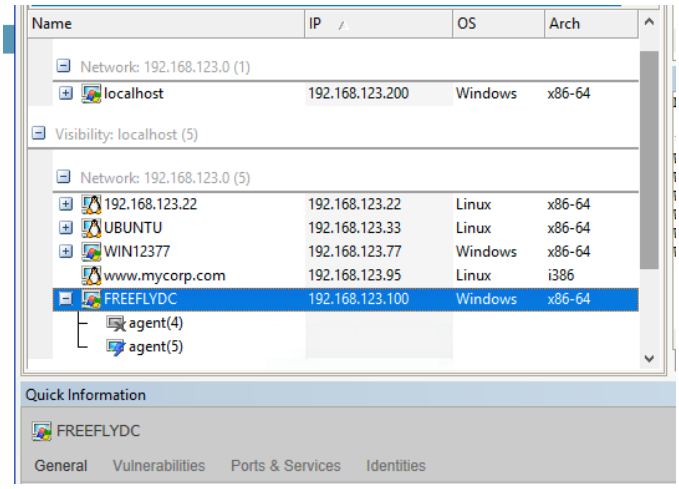


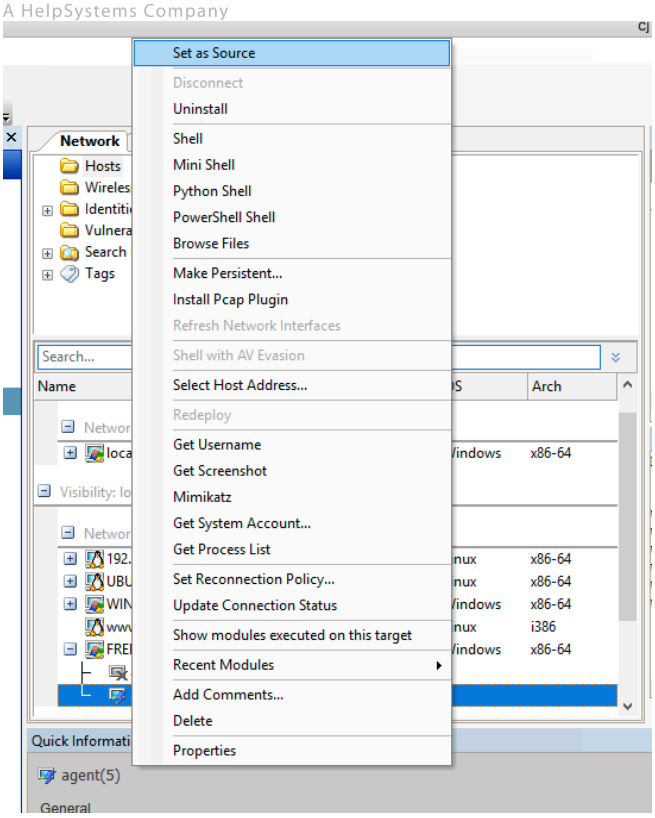


Leave other options as Default options and click Finish. You will see agent deployed in Domain Controller once exploit successful, as shown below.

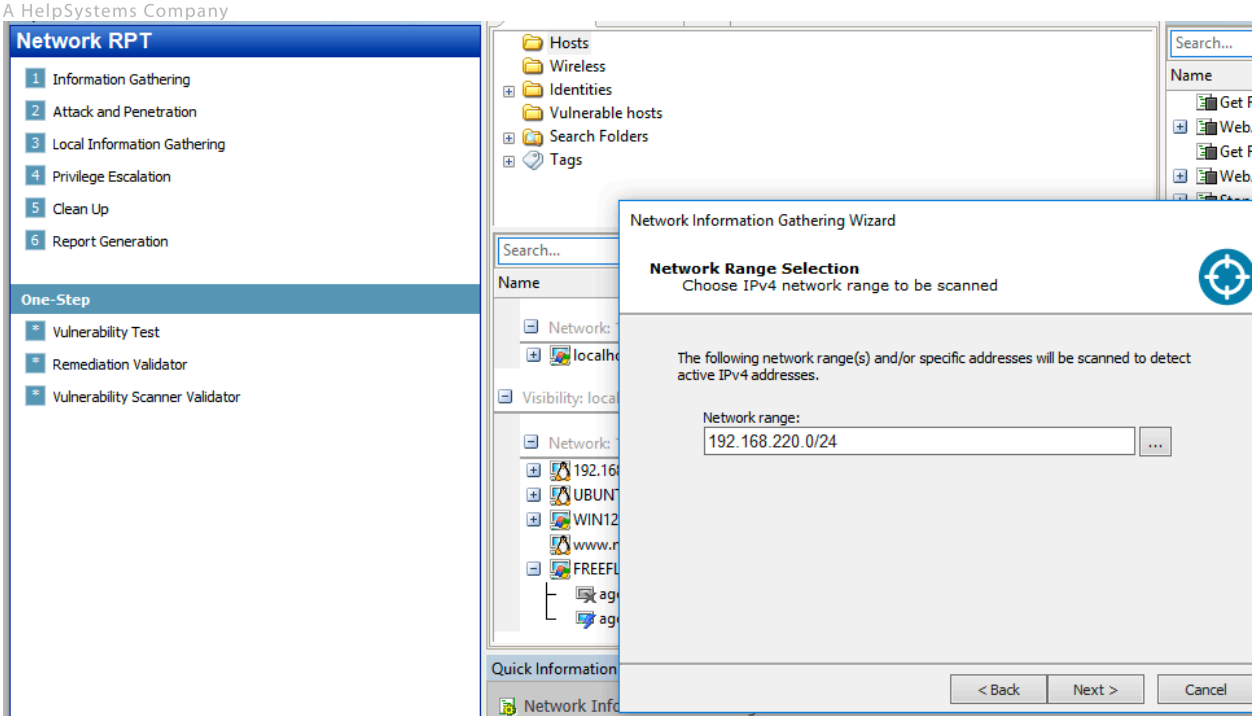


If you escalated any system successfully you can use them as a source agent and pivot off this agent. Simply “right click” and select “set as source.” If you identified another network in the local information gathering (Step #3) then you can use this source agent to pivot into that network.

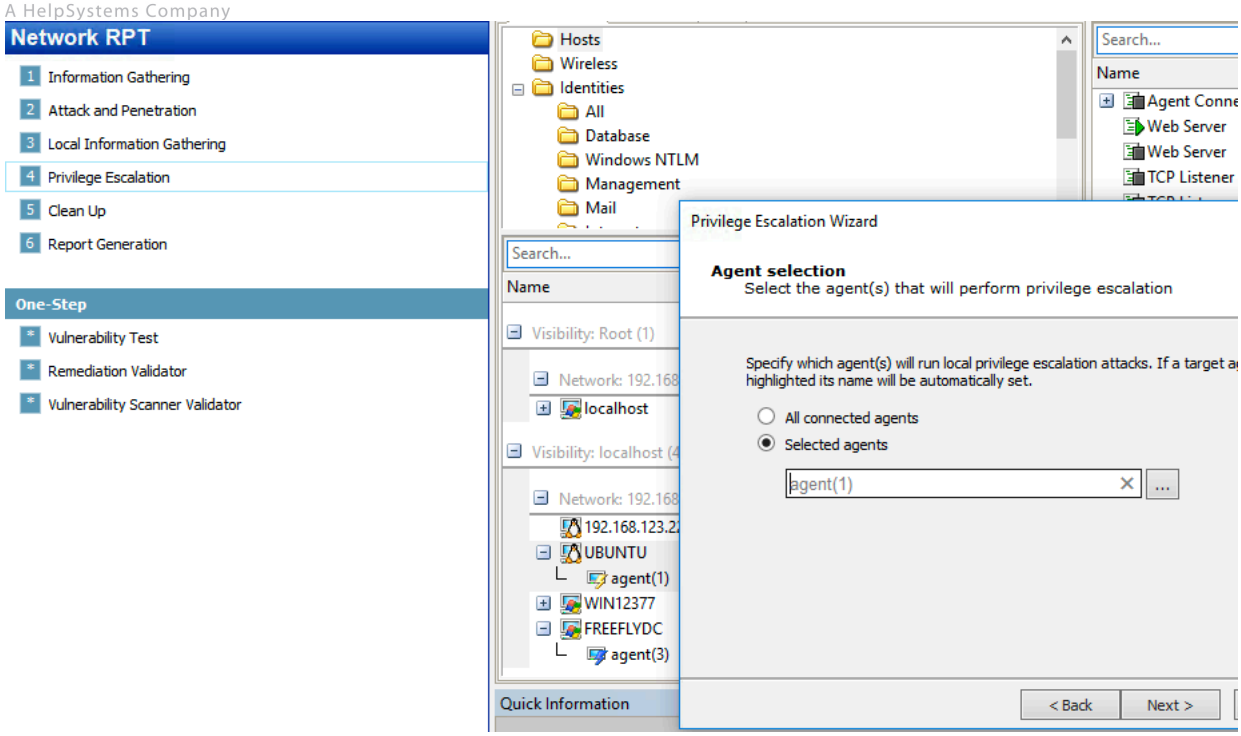




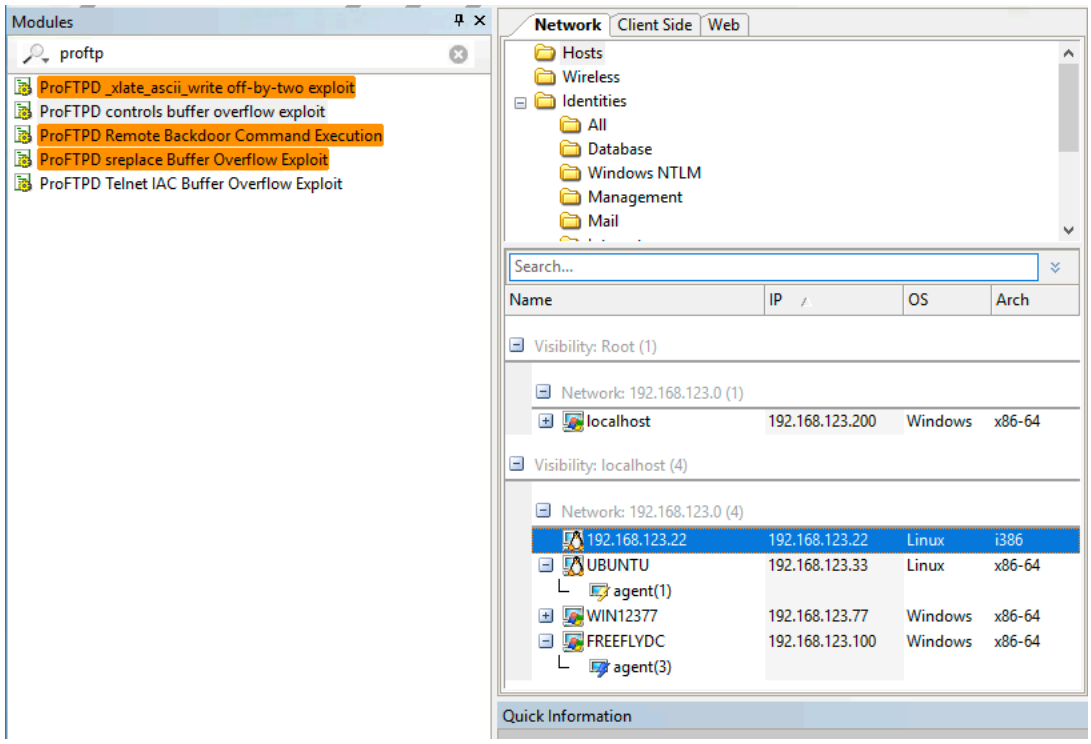
Go to Network RPT – Step 1. Information Gathering, perform information gathering on 192.168.220.0/24. You will successfully pivot to deeper internal networks via domain controller machine which is dual home.

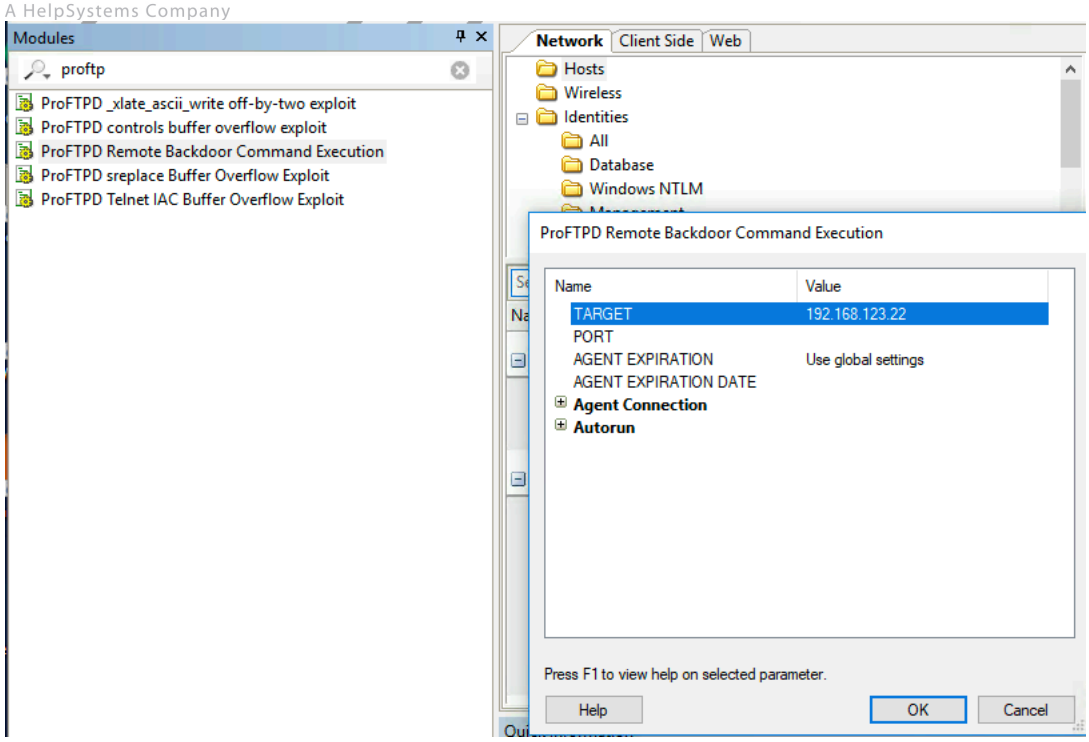


Select Step 4, Privilege Escalation attack on agent belonged to UBUNTU server to gain privilege access to this system

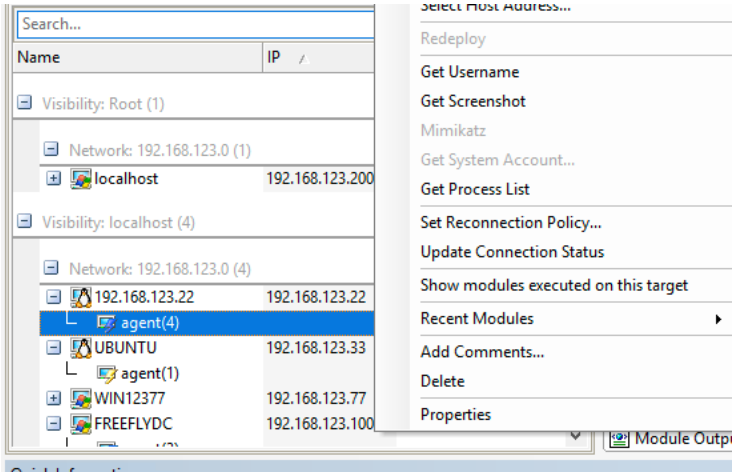


To perform manual testing, select 192.168.123.22 system. Go to Modules tab, and filter exploits by typing application name – Proftp. Run module – ProFTPD Remote Backdoor Command Execution Exploit to 192.168.123.22 system by pulling the module to the system.



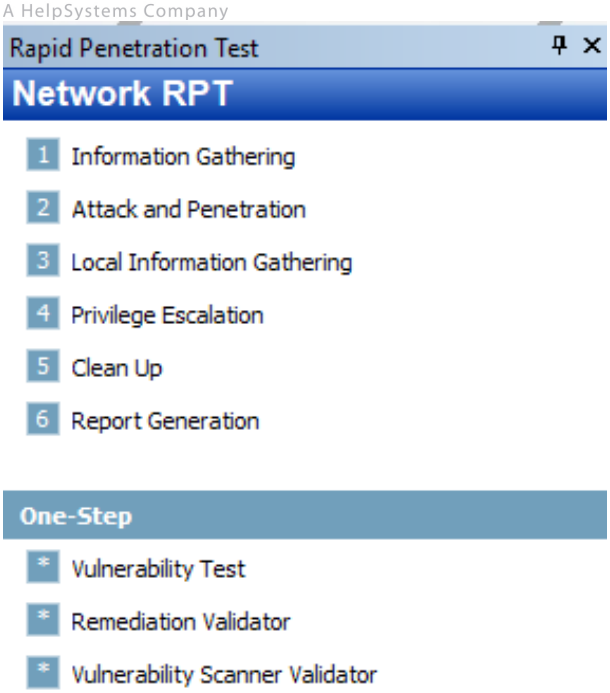


After exploit successful, you will able to gain privilege access to 192.168.123.22 system.

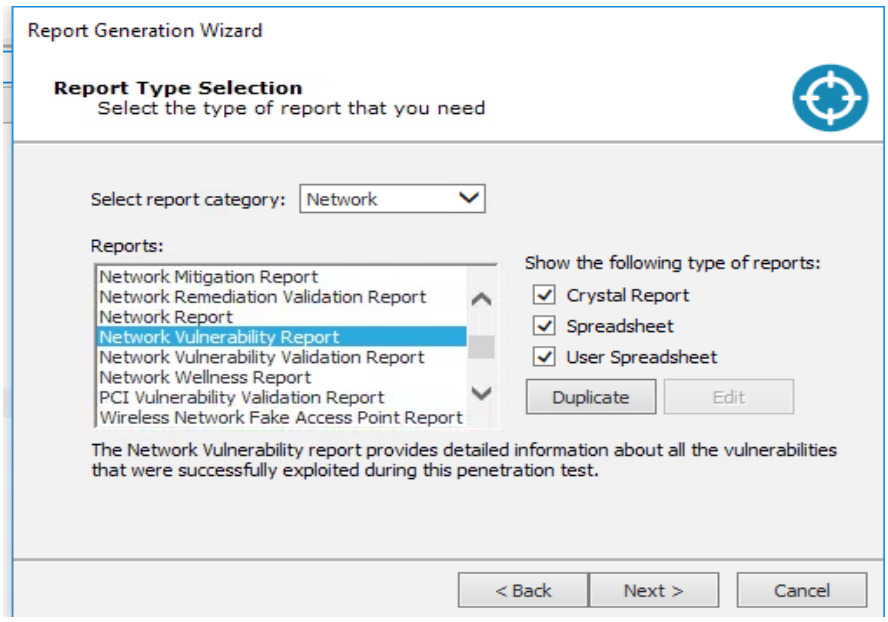


Once the evidence has been obtained all that is needed is the cleanup and report generation. Step #5 in the RPT will cleanup and remove all agents and then step #5 will allow for a choice of reports.

CORE SECURITY
A HelpSystems Company



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.



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

CORE SECURITY
A HelpSystems Company

CORE 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.

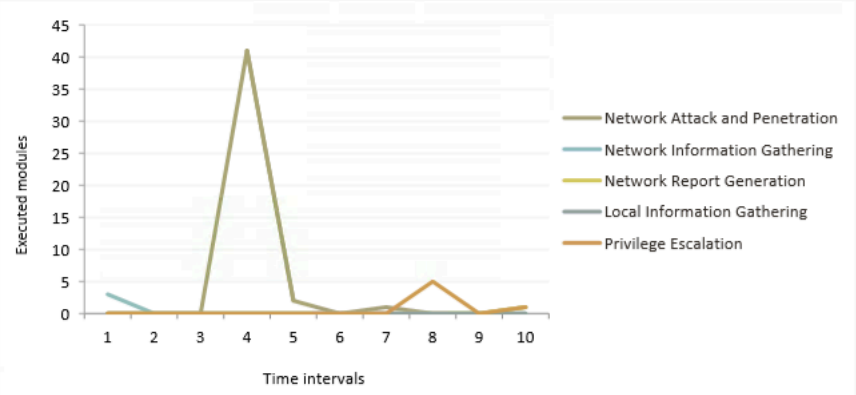
This information provides a practical approach to determine the key vulnerable points in the tested network, and to assess the risk associated with such vulnerabilities.

CORE Impact

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



CORE SECURITY
A HelpSystems Company

Vulnerabilities

Workspace	Visibility Path	Host Name	Vulnerability Identifier	CVSS	Vector Description	Vulnerability Description	Affected Port	Module Name	Remediation URL
cj-test2	/192.168.123.100	FREEFLYDC	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	FREEFLYDC	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	

CORE Impact

Vulnerabilities extra links

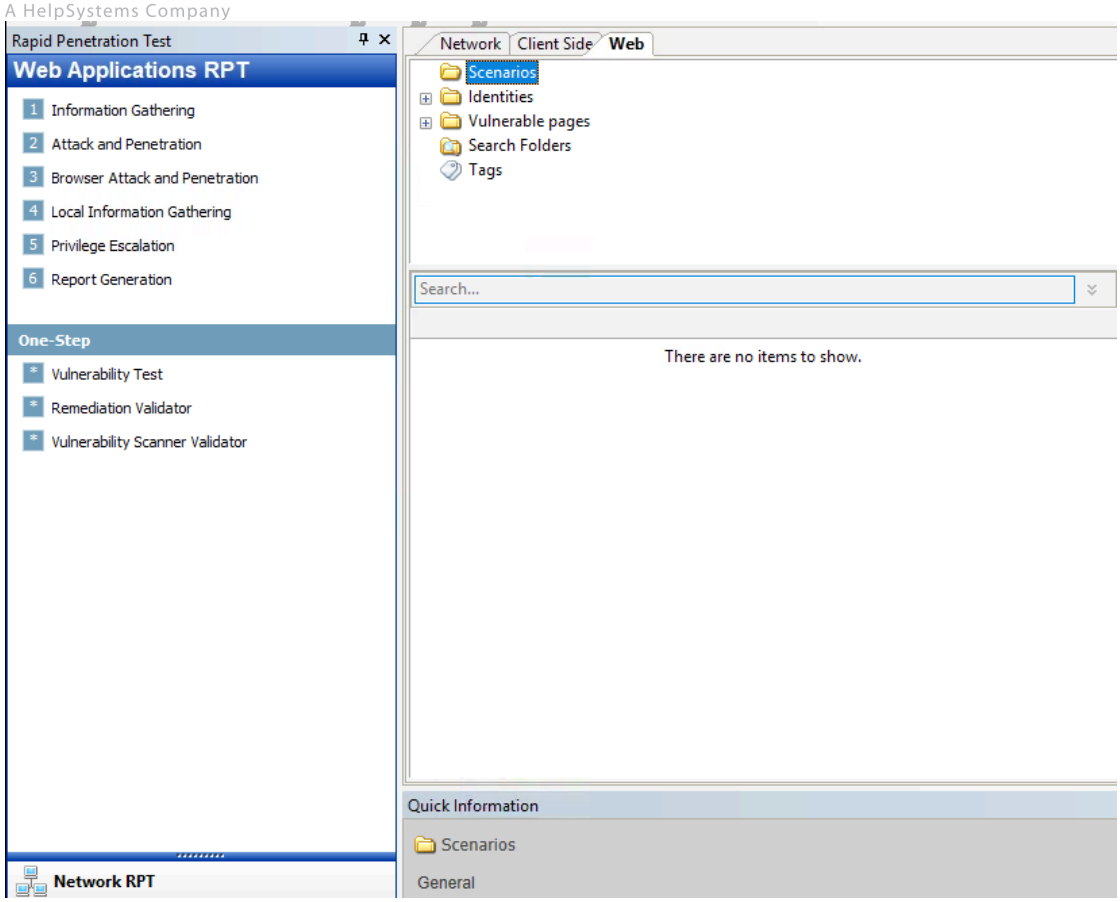
Workspace Name	CVE	URL
cj-test2	CVE-1999-0501	http://xforce.iss.net/static/1005.php
cj-test2	CVE-1999-0502	http://xforce.iss.net/static/2941.php
cj-test2	CVE-1999-0502	http://xforce.iss.net/static/774.php
cj-test2	CVE-1999-0503	http://xforce.iss.net/static/1328.php
cj-test2	CVE-1999-0503	http://xforce.iss.net/static/282.php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

CORE SECURITY
A HelpSystems Company

Web Application Testing

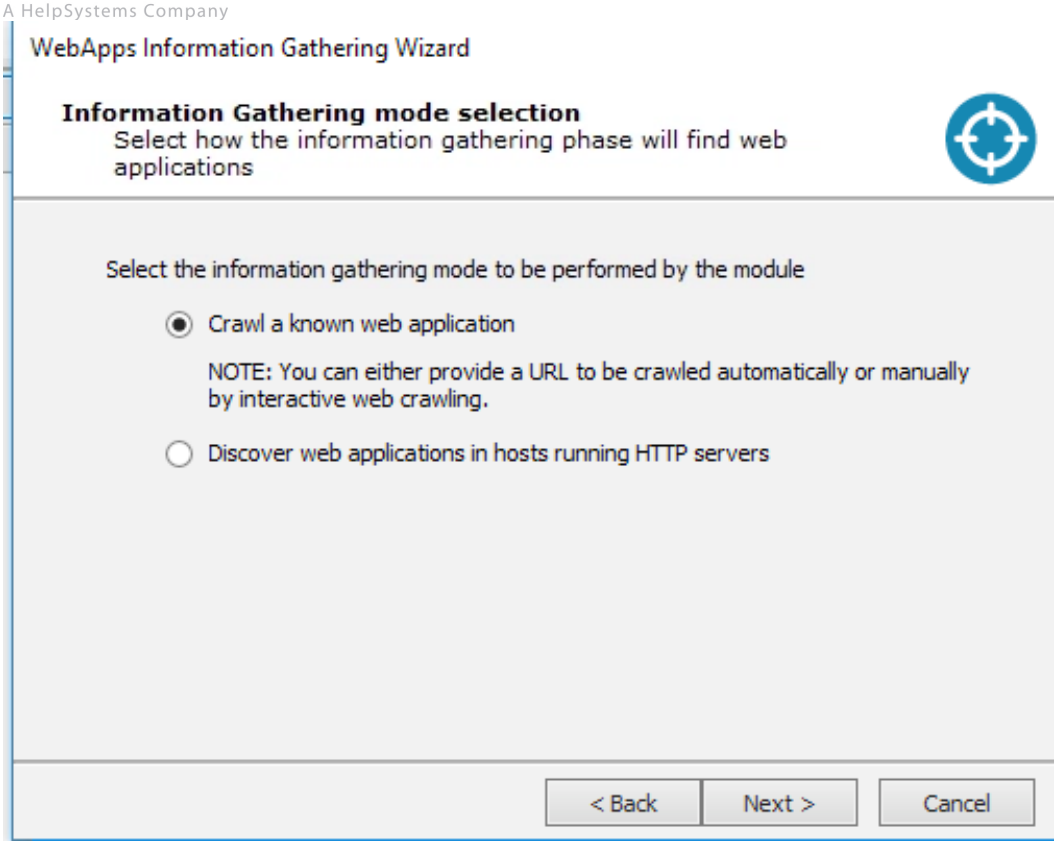
Core IMPACT AWS lab allows for testing a custom web application identified as http://www.mycorp.com/mutillidae

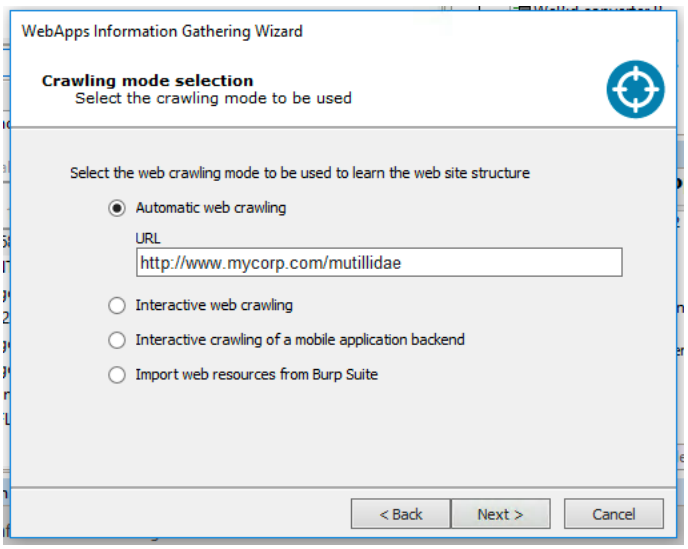
You will be required to switch to the Web Applications RPT tab as indicated below.

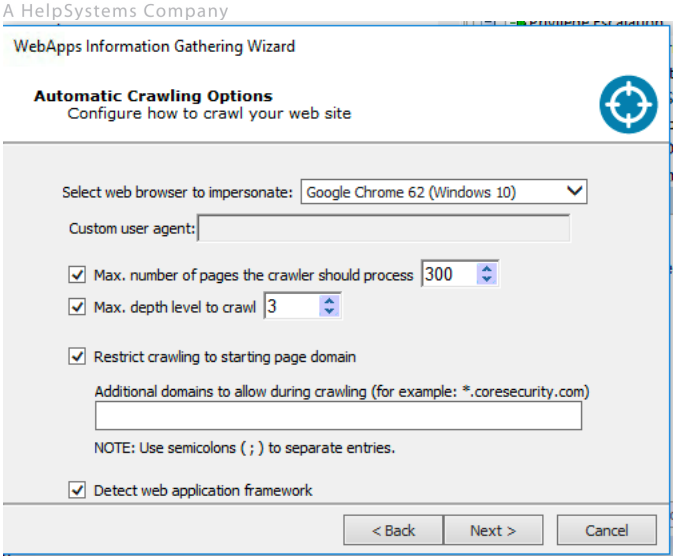


Once in the Web Attack Vector you can start by running the Web Apps Information Gathering in Step #1 of the RPT. Create a scenario called “MUTILLIDAE” and accept all defaults. Under Automatic web crawling, please enter following URL : http://www.mycorp.com/mutillidae

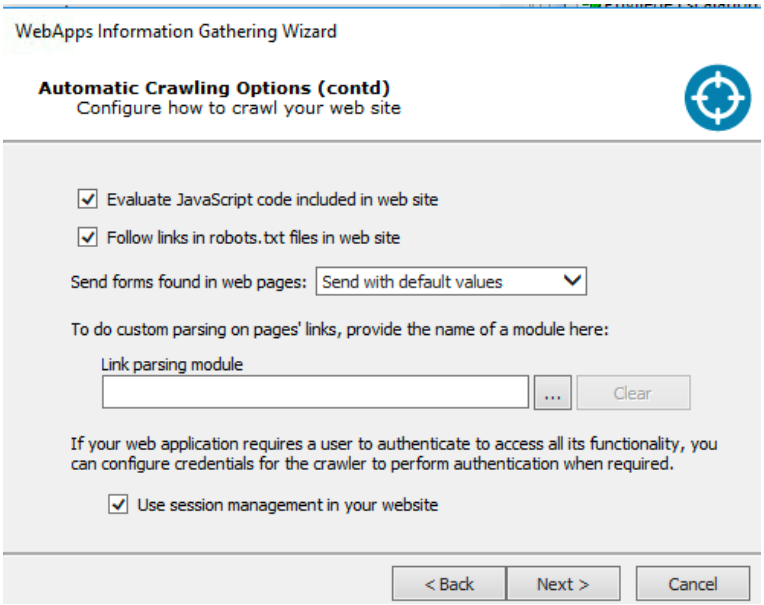
CORE SECURITY
A HelpSystems Company



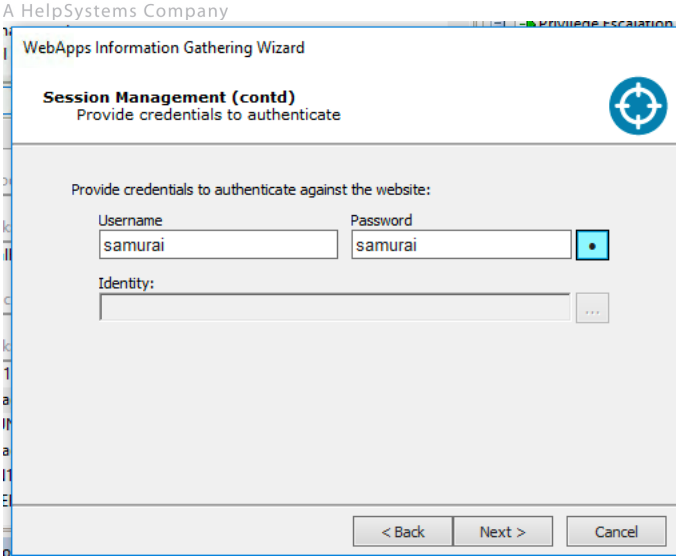




Check “use session management in your website” under Automatic Crawling options.

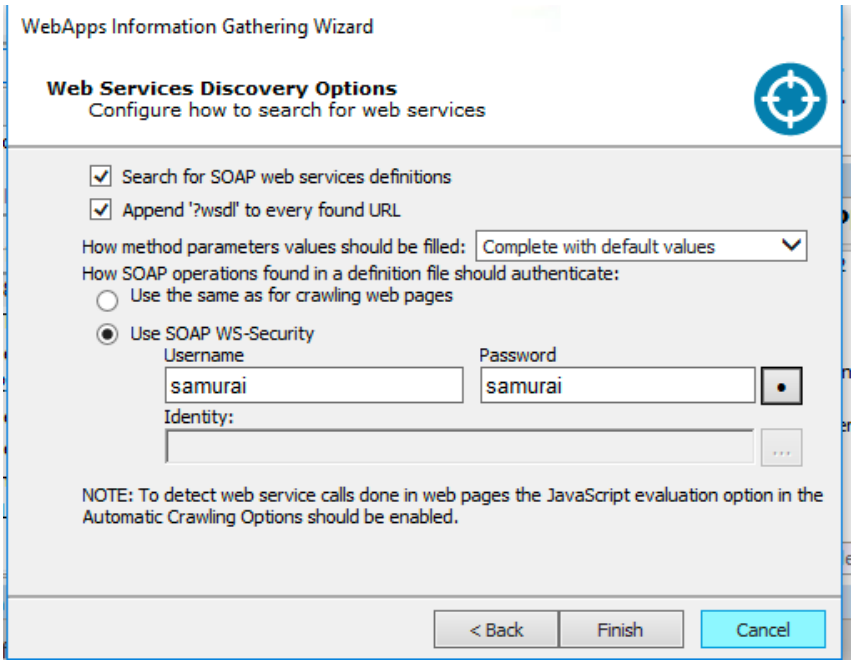


Select Form-based and enter username/password which are samurai/samurai

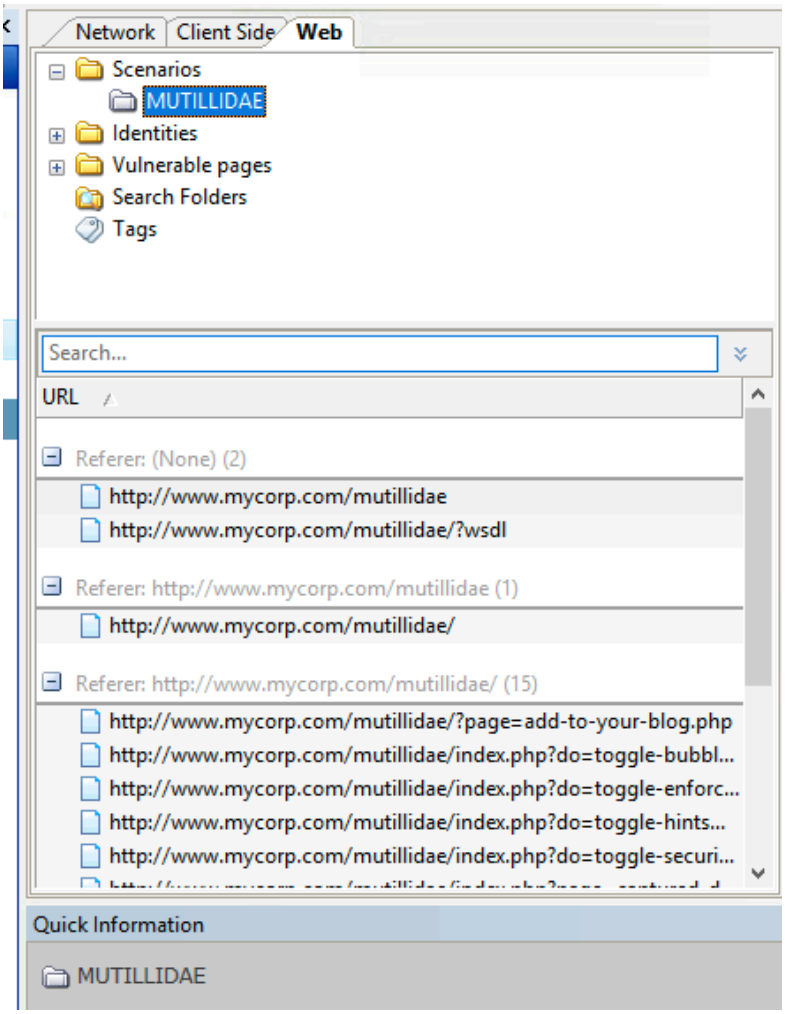


Click Next until Web Services Discovery Options.

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



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 referrer 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.

CORE SECURITY
A HelpSystems Company

WebApps Attack and Penetration Wizard

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

- [x] A1 - Injection
  - [x] Look for SQL Injection vulnerabilities
  - [x] Look for OS Command Injection vulnerabilities
- [ ] A2 - Broken Authentication
- [ ] A3 - Sensitive Data Exposure
  - [x] Look for Sensitive Information in documents
  - [x] 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

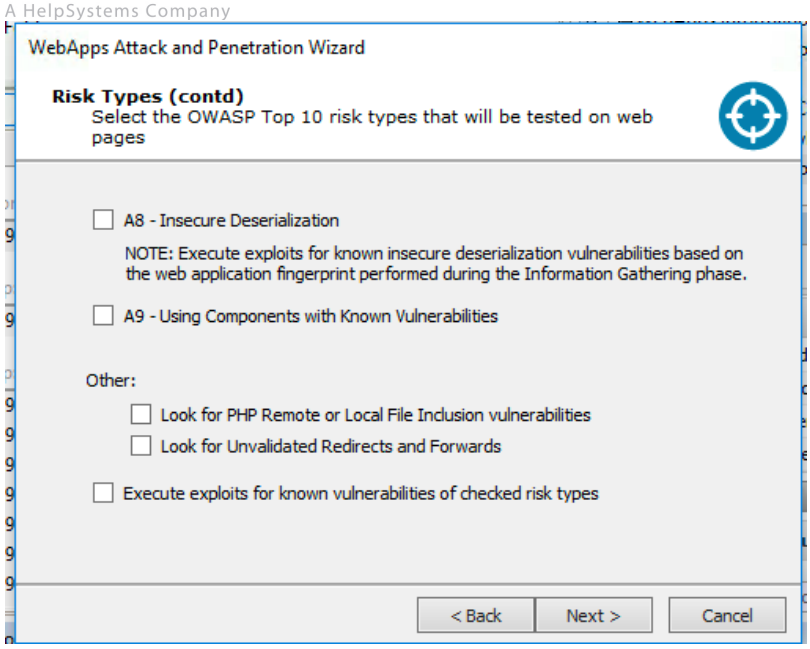
Risk Types (contd)
Select the OWASP Top 10 risk types that will be tested on web pages

- [x] A4 - XML External Entities
- [ ] A5 - Broken Access Control

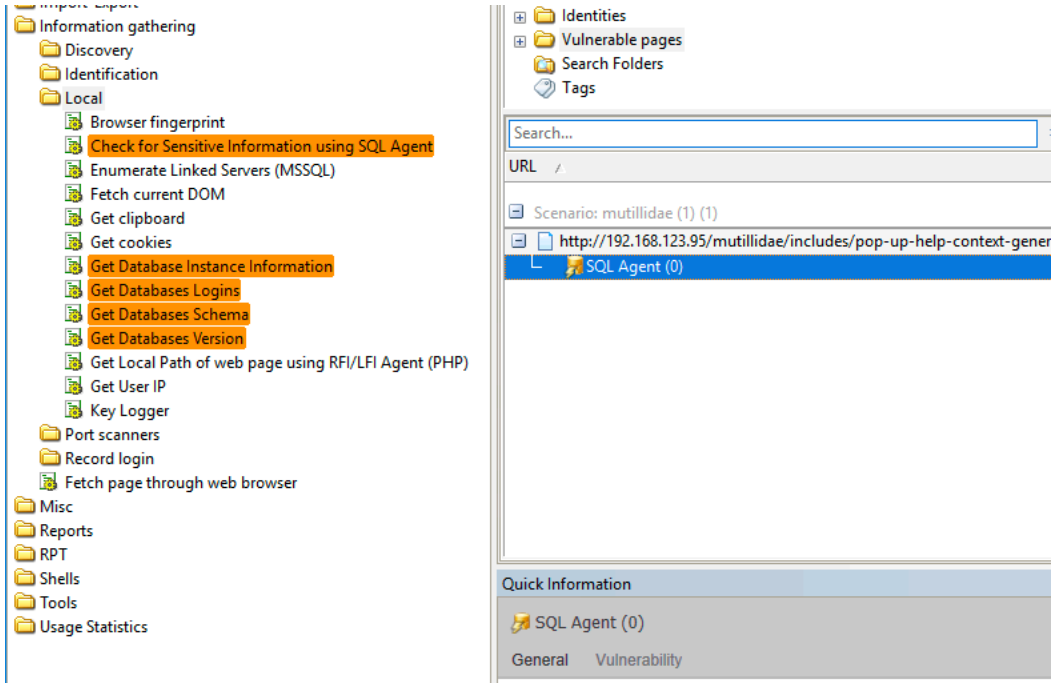
NOTE: Broken access control detection need user interaction to obtain session cookies. It can be performed running the Broken Access Control Analyzer module that have a separate wizard to guide the test configuration.

- [ ] A6 - Security Misconfiguration
  - [x] Look for known security misconfiguration issues
  - [x] Look for WebDAV vulnerabilities
  - [x] Look for default host credentials
- [x] A7 - Cross Site Scripting (XSS)

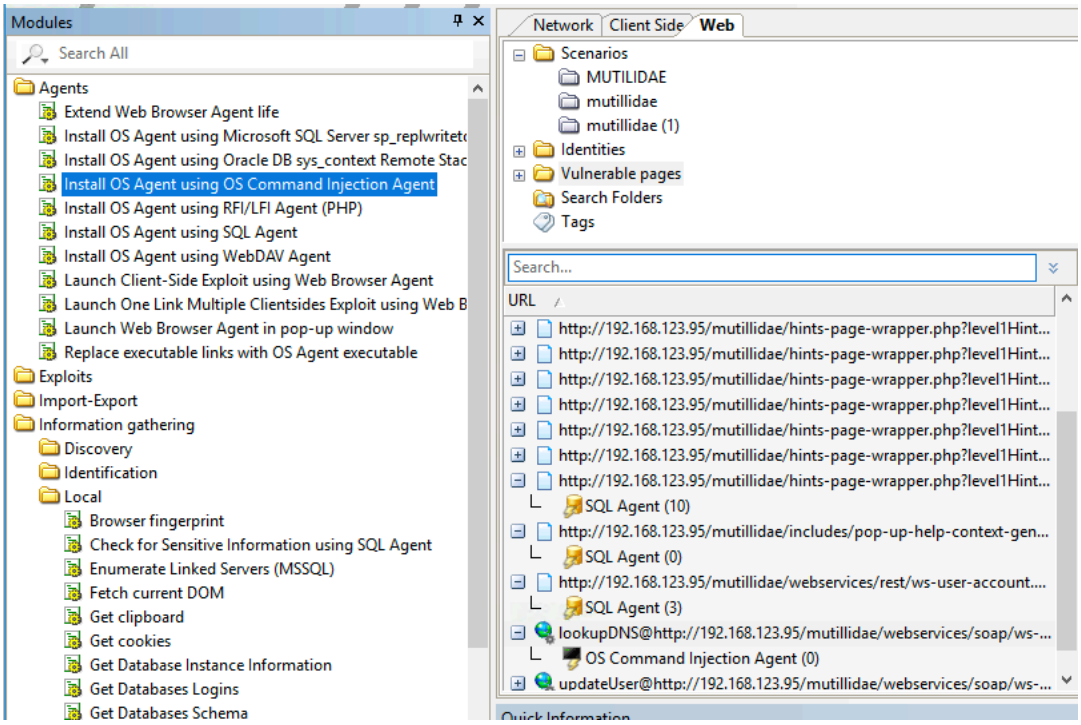
< Back | Next > | Cancel



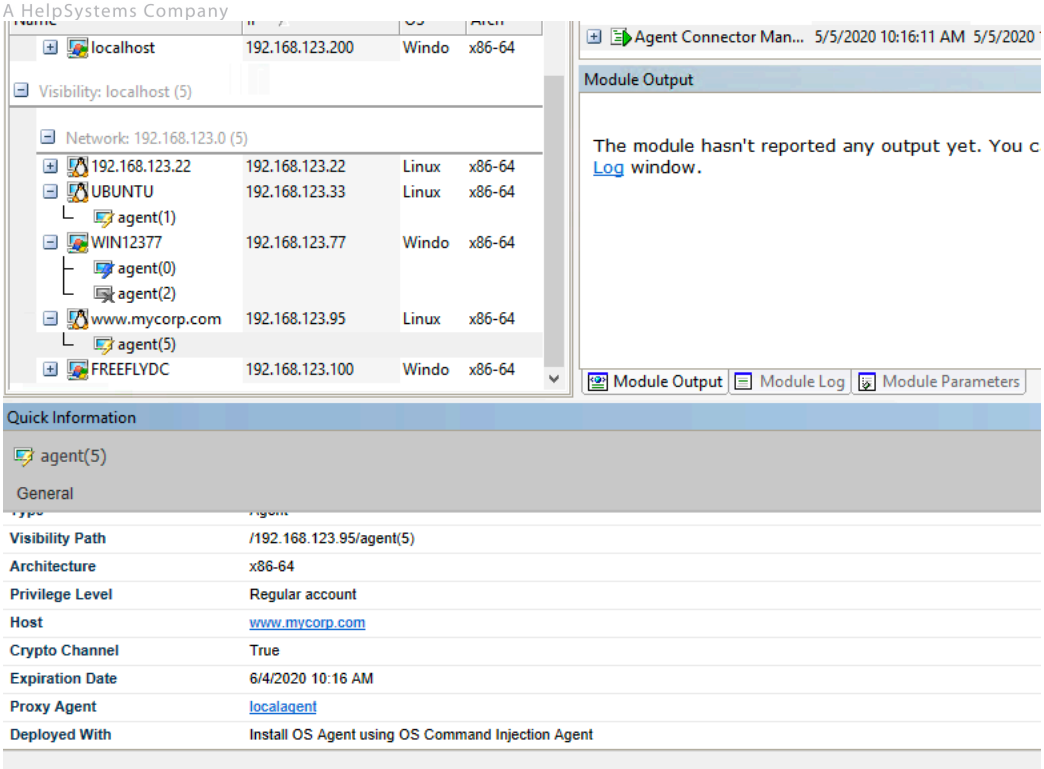
All of the above agents can be leveraged to gain additional information such as getting the DB schema, Logins or DB version. Simply “drag and drop” the highlighted module onto the logical agent



You now have the ability to leverage that vulnerability and challenge the Web Application Firewall (WAF) by attempting to deploy and 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.

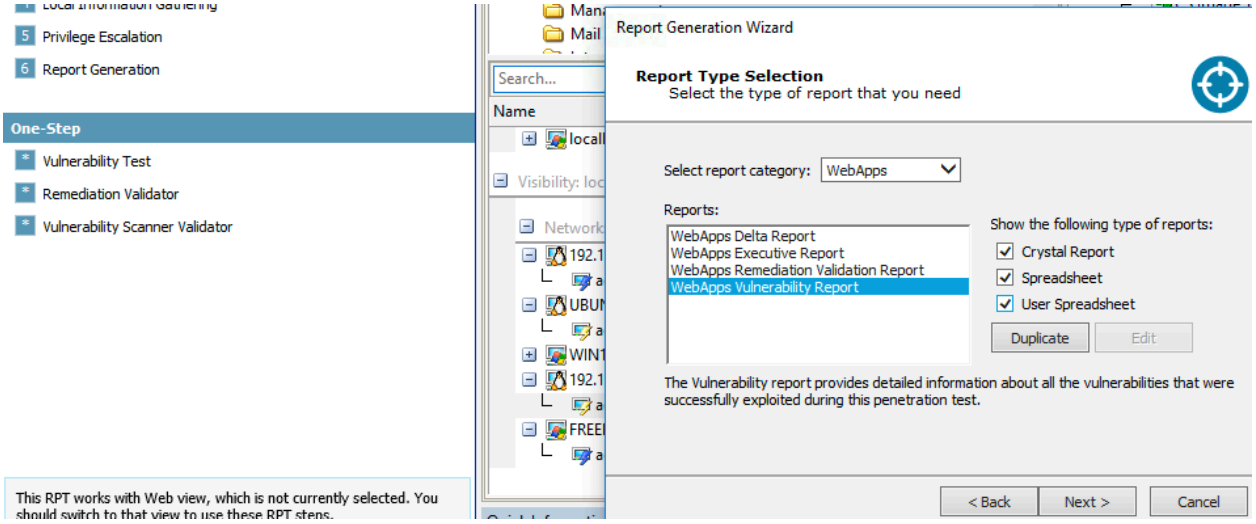


The result will be as shown an OS agent deployed from the OS Command Injection agent and we end up back onto the network with the OS deployed onto the windows server hosting the web application



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.



CORE SECURITY
A HelpSystems Company

CORE Impact

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.

CORE SECURITY
A HelpSystems Company

CORE Impact

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

CORE Impact

A1. SQL injection - vulnerabilities

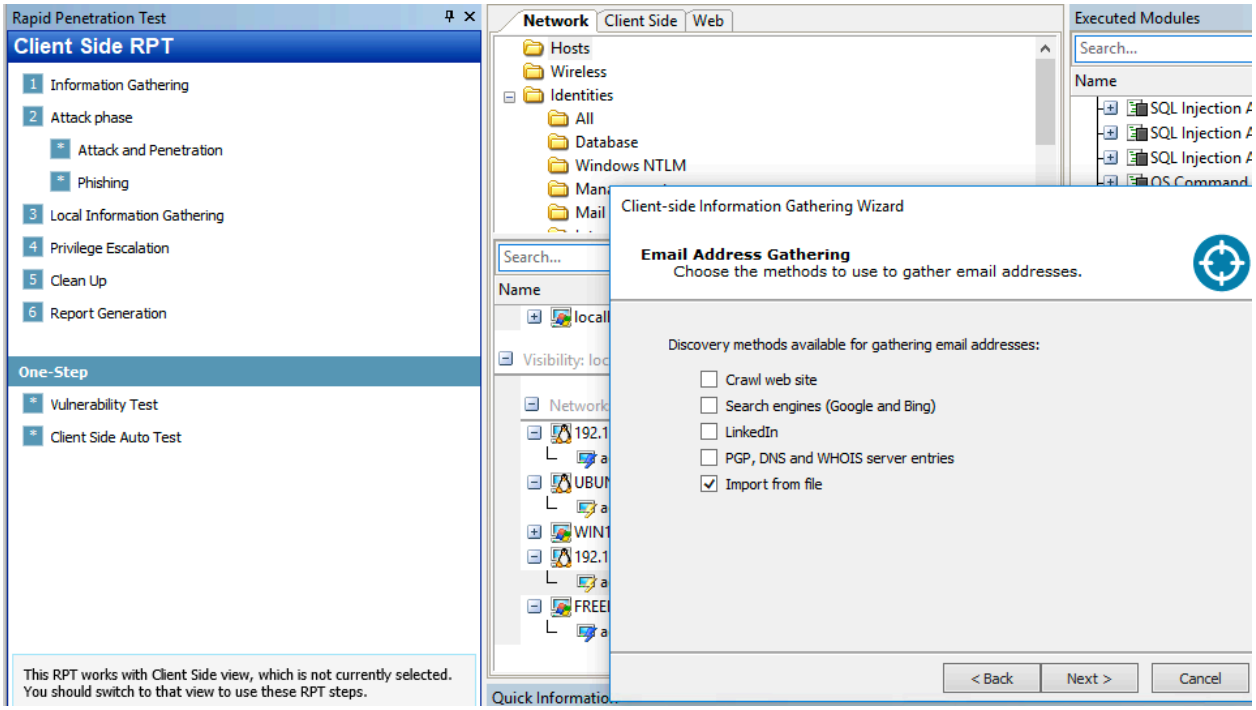
Workspace	Scenario	Web Page	Vuln Id	Documentation	Basic Information
cj-test2	mutillidae (1)	http://192.168.123.95/mutillidae/hints-page-wrapper.php?level1HintIncludeFile=62	1	Description The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization. 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", "@"

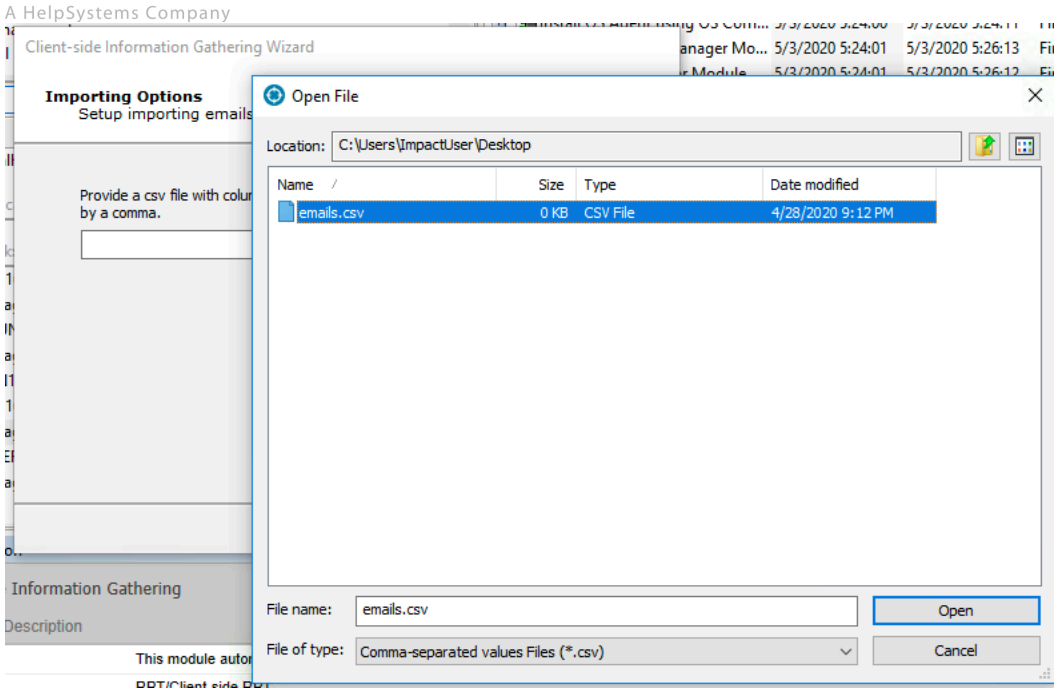
CORE SECURITY
A HelpSystems Company

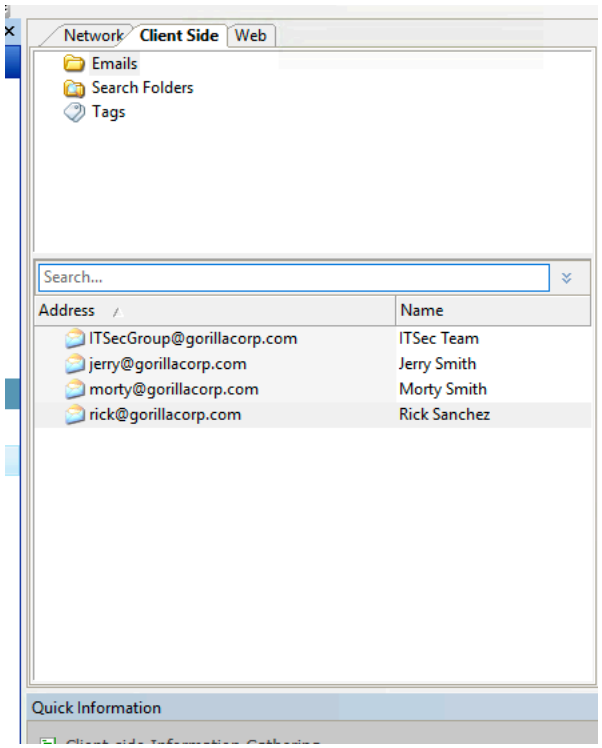
Client Side Penetration Testing

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

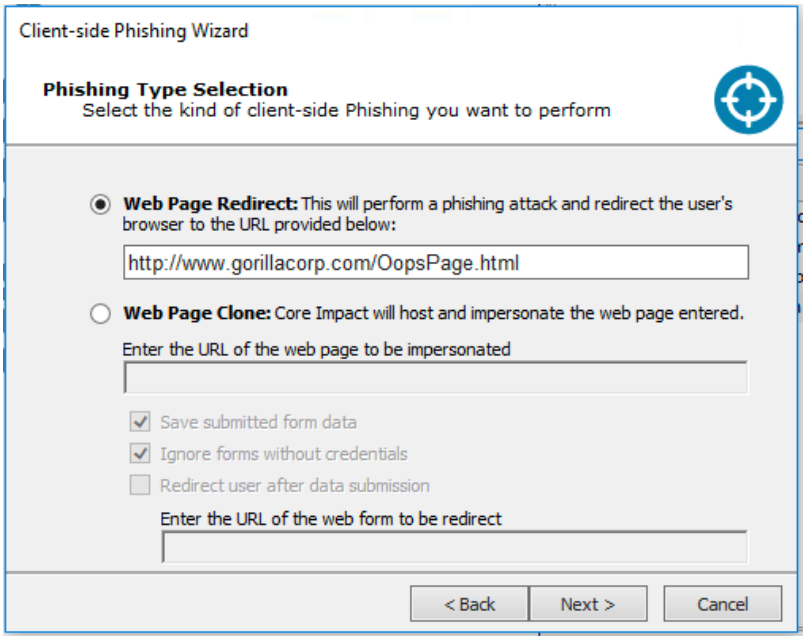




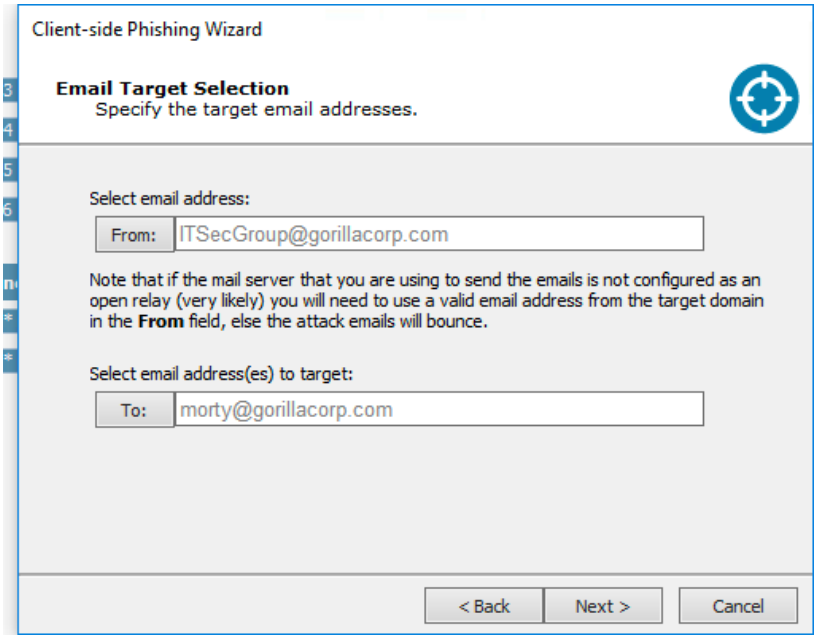


Under Step 2 – attack phase, select Phishing, under Web Page Redirect, type http://www.gorillacorp.com/OopsPage.html .This can be a security awareness website whereby users will be redirected to a site that notify users that they had been phished and will received an email soon to attend security awareness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

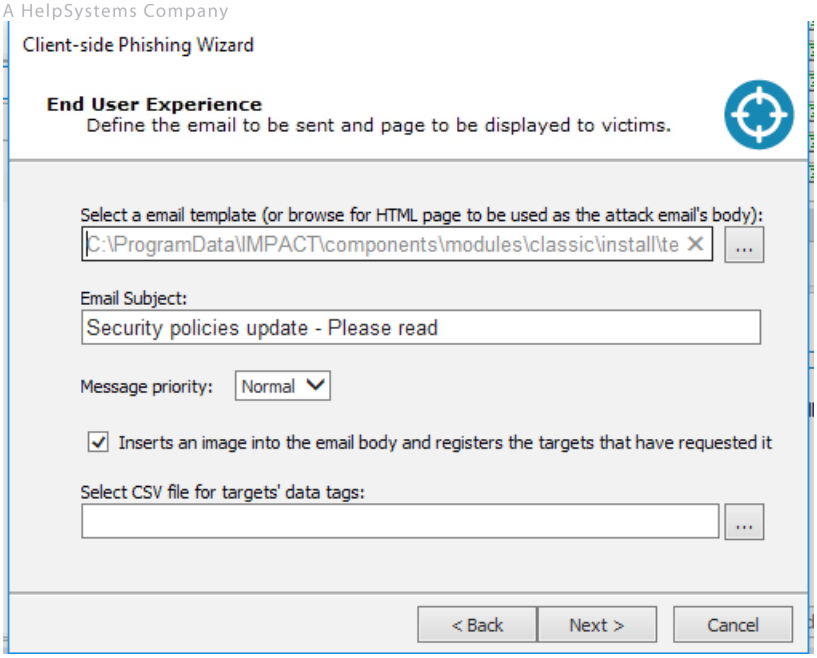
Impact will host and impersonate the web page entered, customer submitted form data including username & password can be captured by Core Impact under this cloned web page



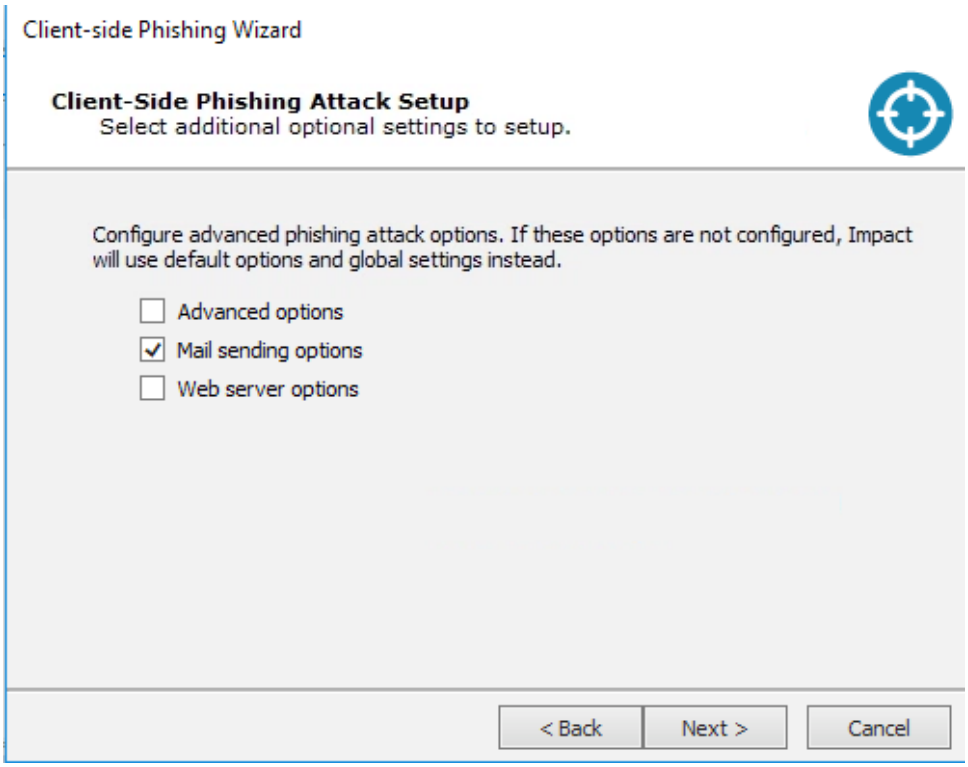
For the From: column email, choose itsecgroup@gorillacorp.com For the To: column email, choose morty@gorillacorp.com

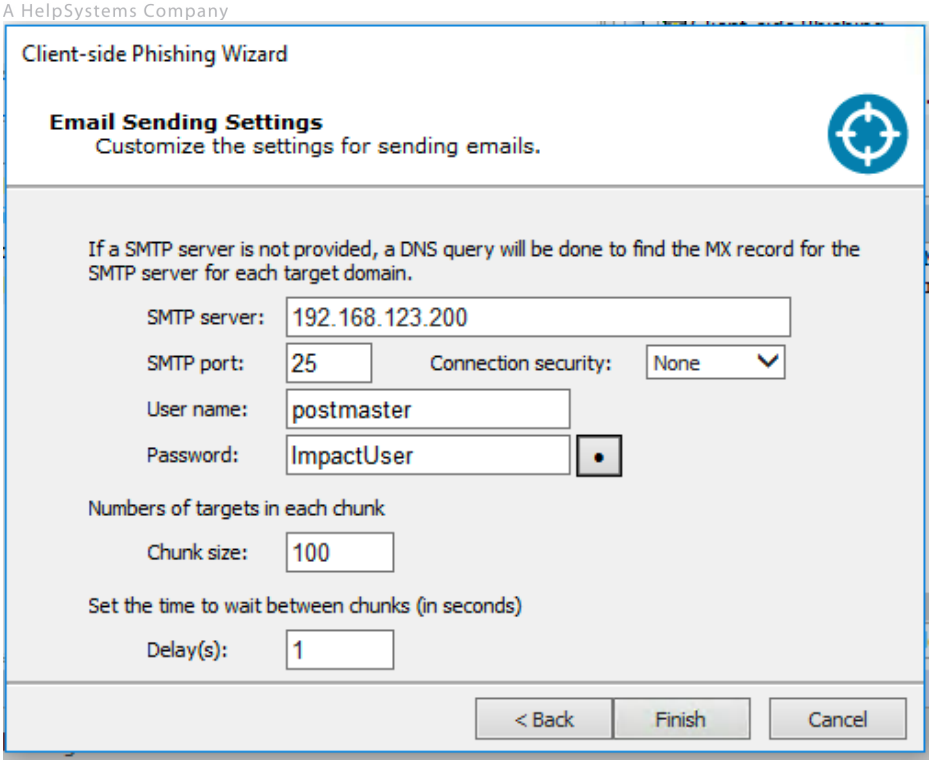


You can choose the email template or upload your own email template

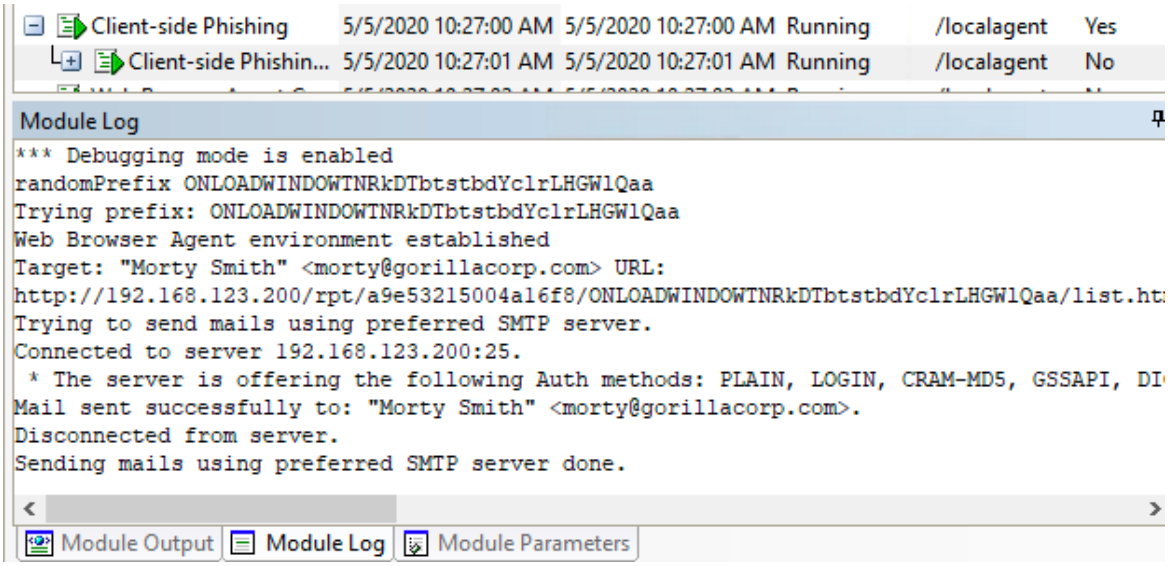


1. Select mail sending options and put 192.168.123.200 as the smtp server. User as postmaster, password is ImpactUser

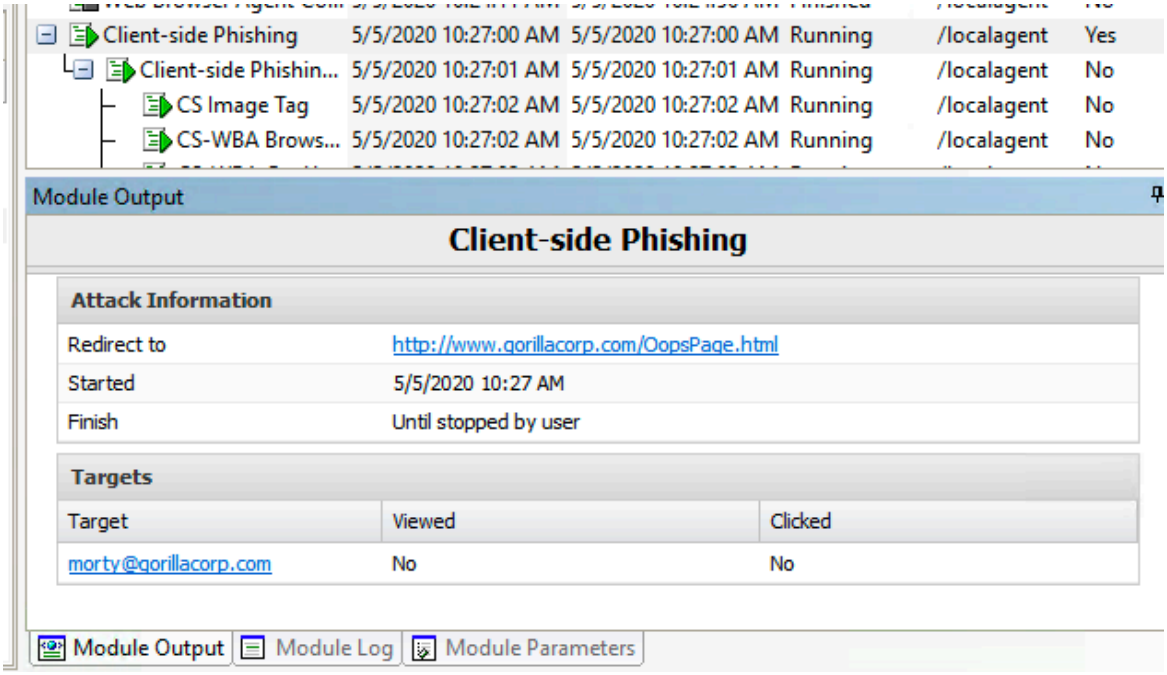




Checked Executed Modules log to make sure email was successfully sent



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



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.gorillacorp.com/OopsPage.html
Started	5/5/2020 10:27 AM
Finish	Until stopped by user

Targets

Target	Viewed	Clicked
morty@gorillacorp.com	No	No

Module Output | Module Log | Module Parameters

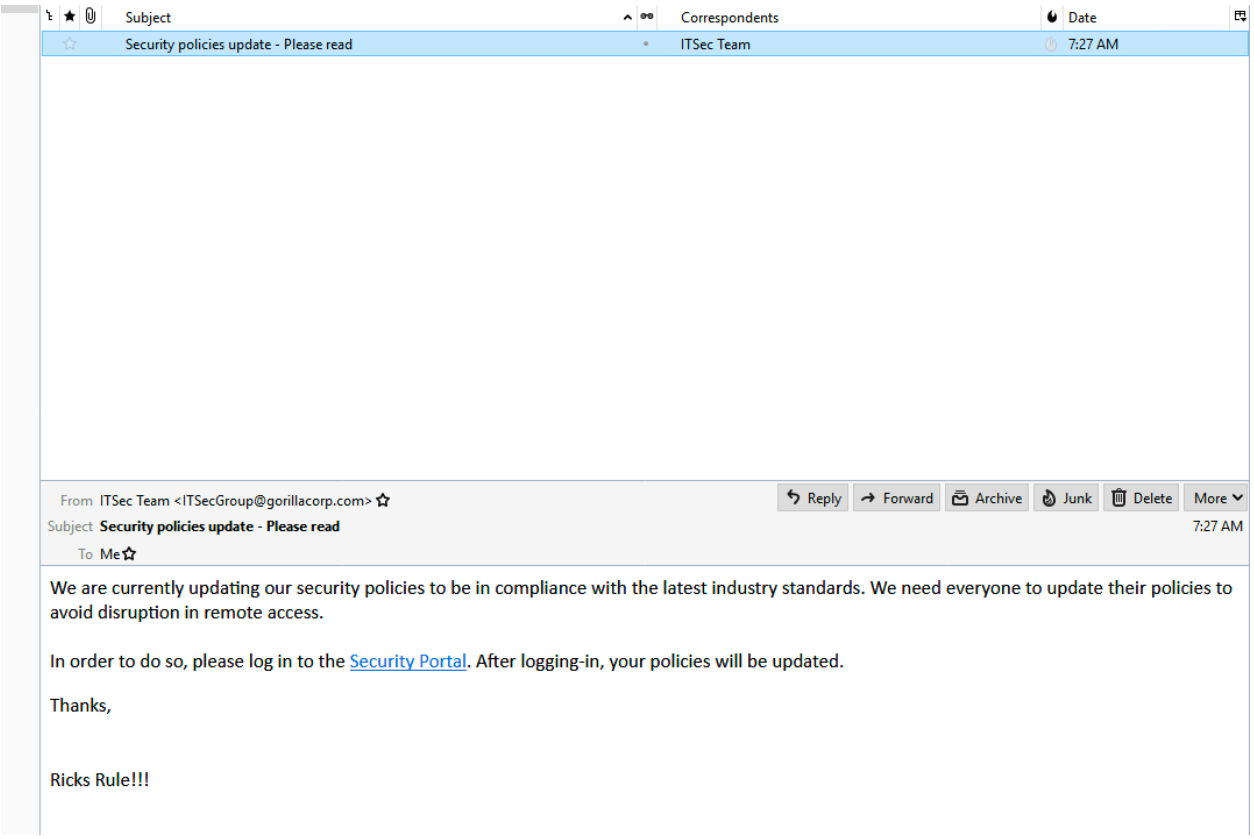
Go to Email Client to test phishing email.

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

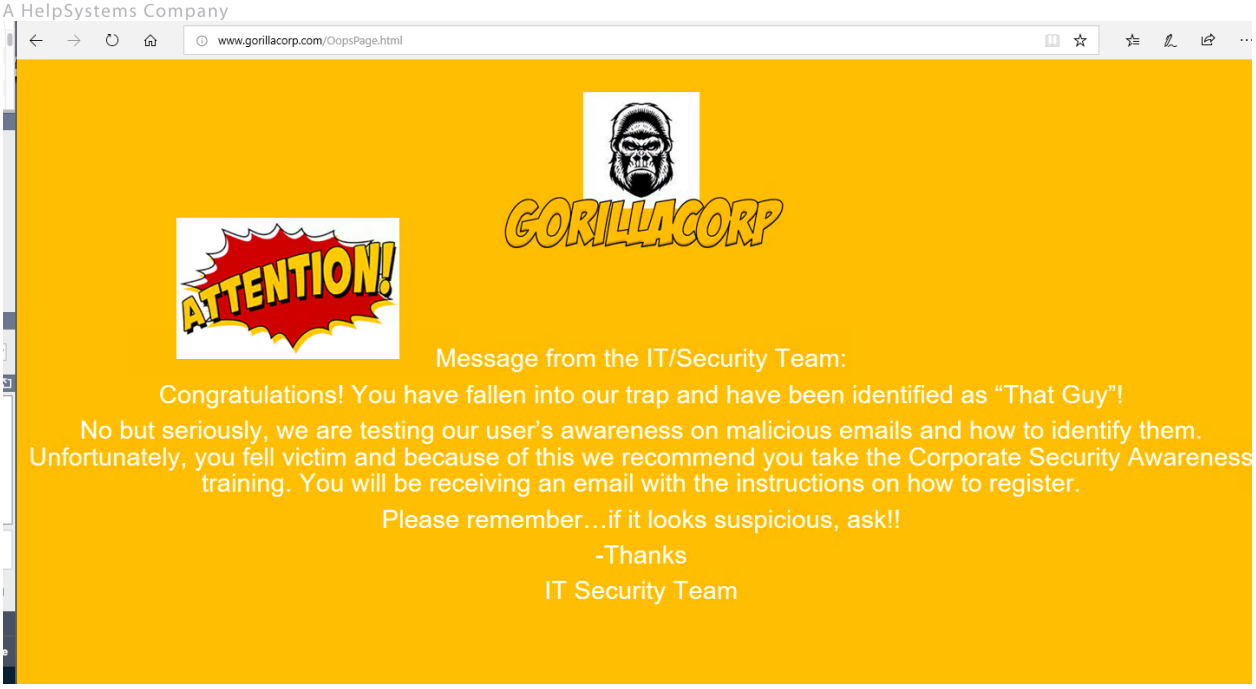
Username : morty
Password :P1ckl3R1ck!

Open Mozilla Thunderbird email application in Desktop after login

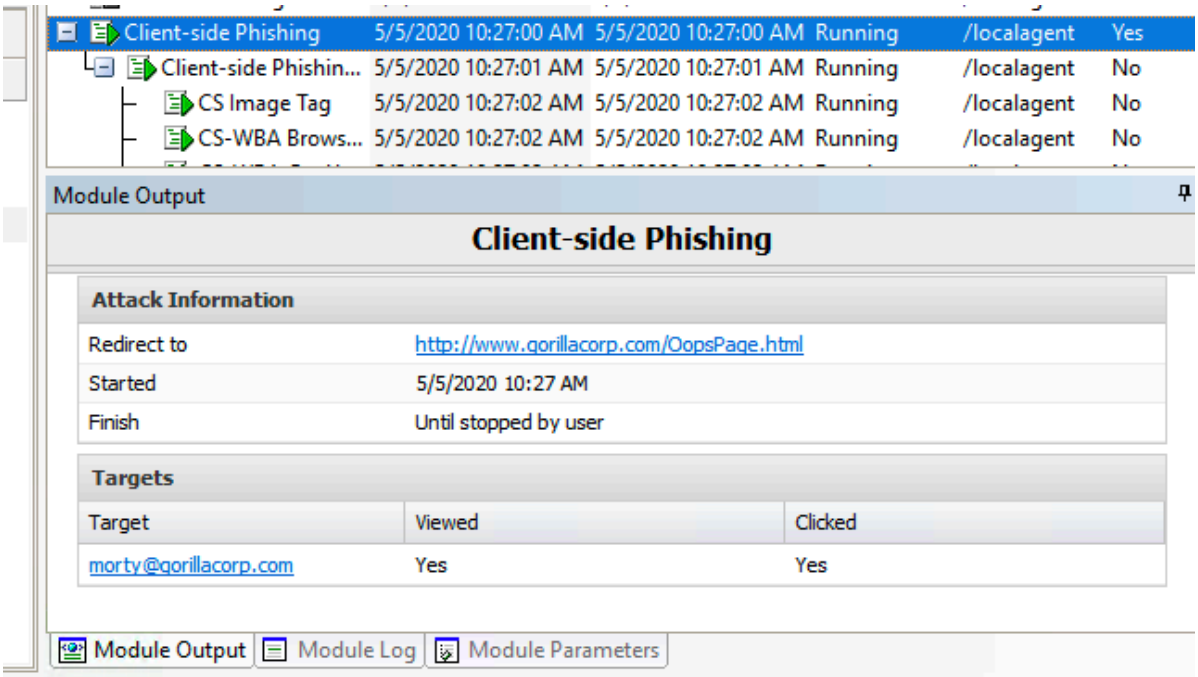


When the email has arrived open it and take a look at an email borne attack through the eyes of a victim.

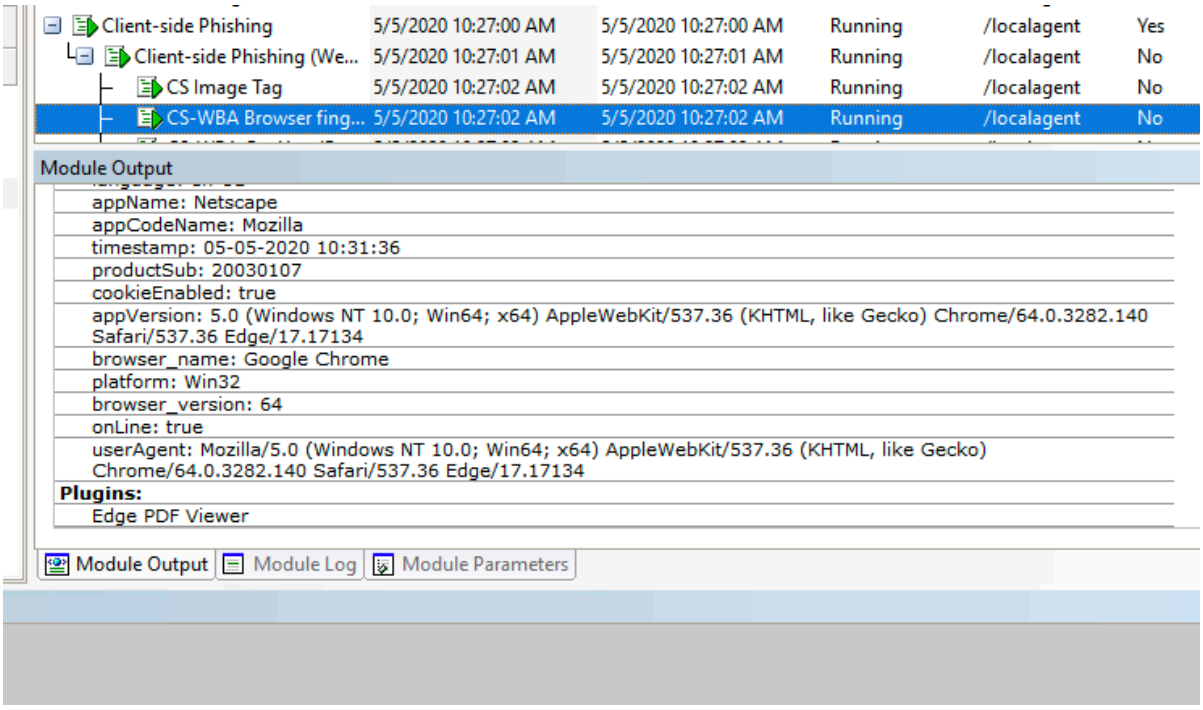
1. You will notice there is an email with a link in it, click on it. A browser will open and redirect to an IT Security Team warning site.



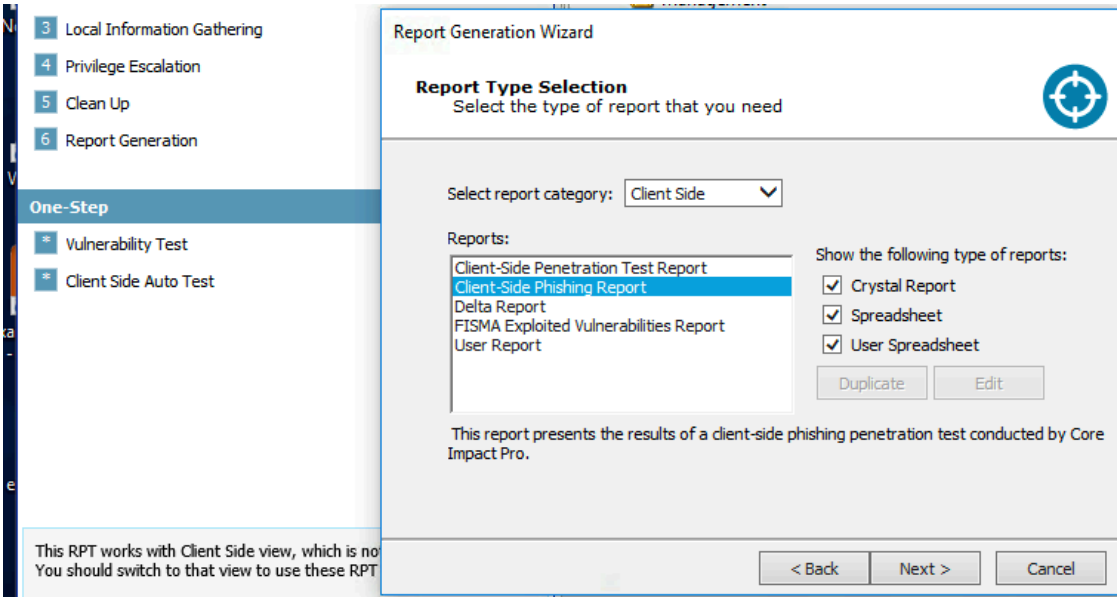
2. After clicking on the link, refer back to your IMPACT console. The executed modules pane will display if phishing is successful.



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.



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



Impact CORE

Tuesday, May 5, 2020

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 em 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*).

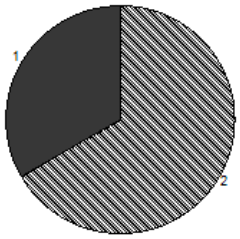
The goal of the *Web Page Clone* attack is to learn recipients' credentials (or other sensitive information) for a particular servi requiring the end user to enter such information. Although control of hosts is not directly obtained, credentials gathered coul be used to further abuse the service being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

CORE SECURITY
A HelpSystems Company

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%
Total:	100.0%

(*) 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

CORE SECURITY
A HelpSystems Company

Client Side Phishing Report

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.