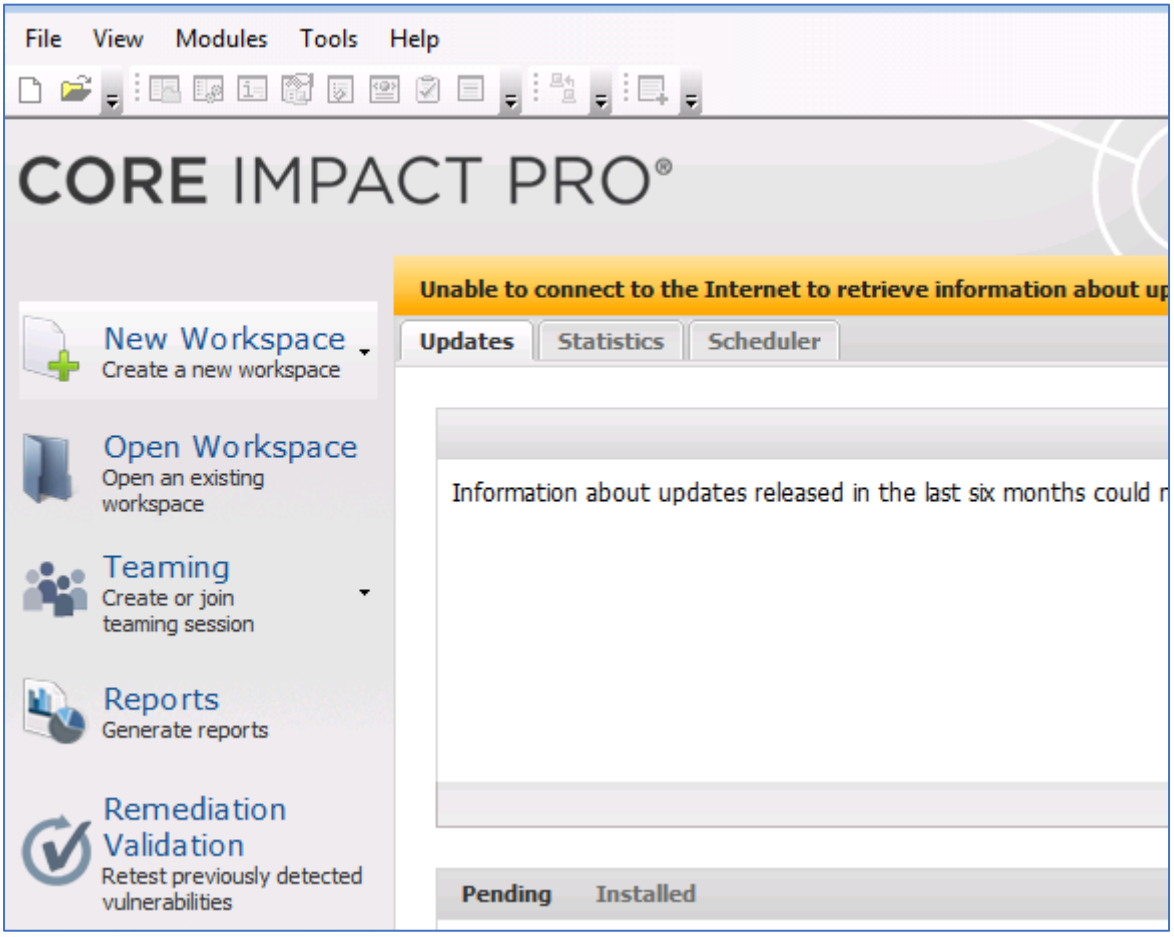
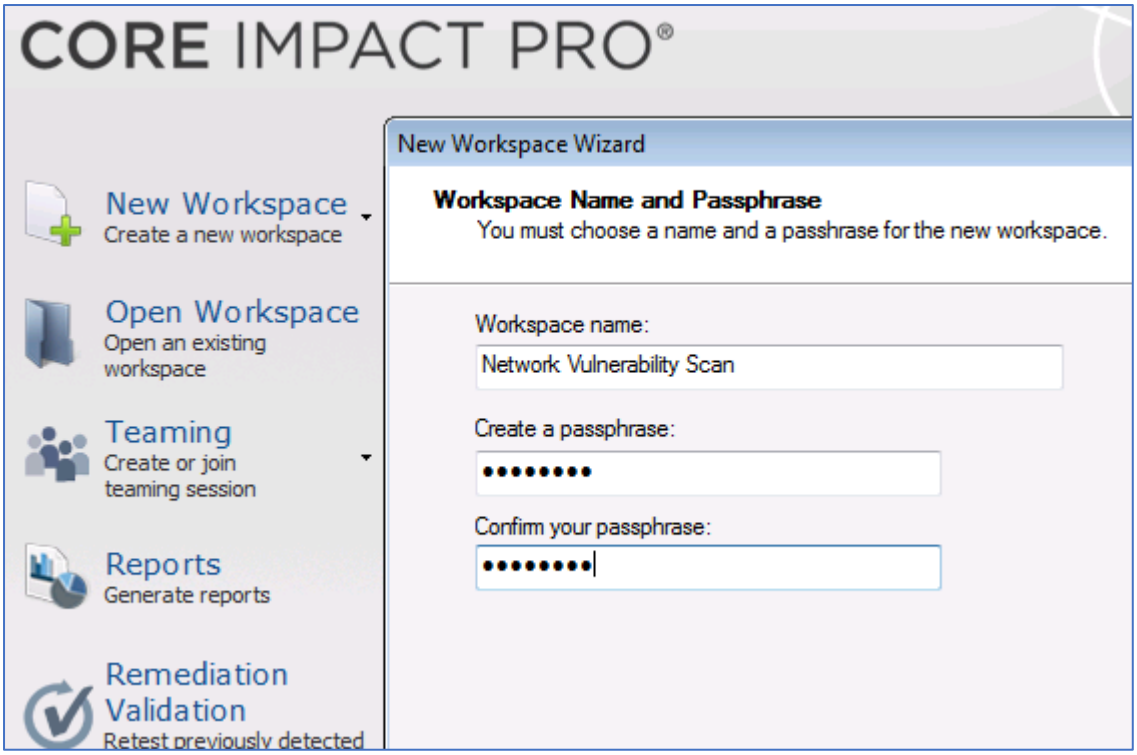
Set-up, configuring a Vulnerability scanner (Core Impact)

Core Impact

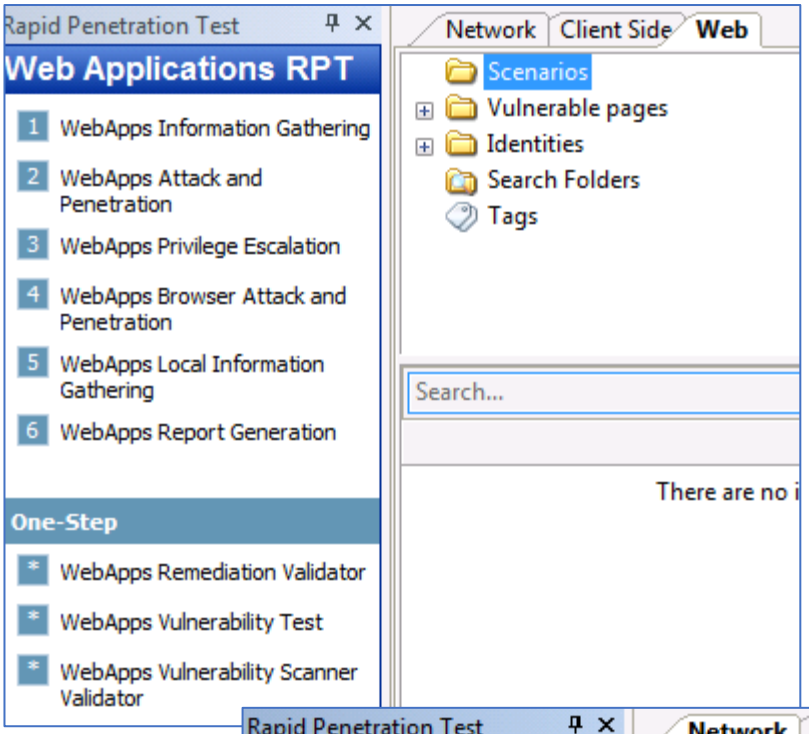
Launching the software

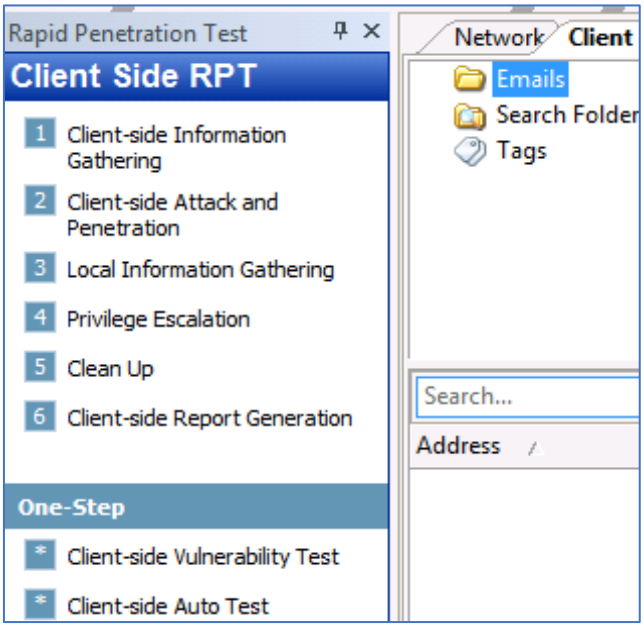


Creating a Blank Workspace

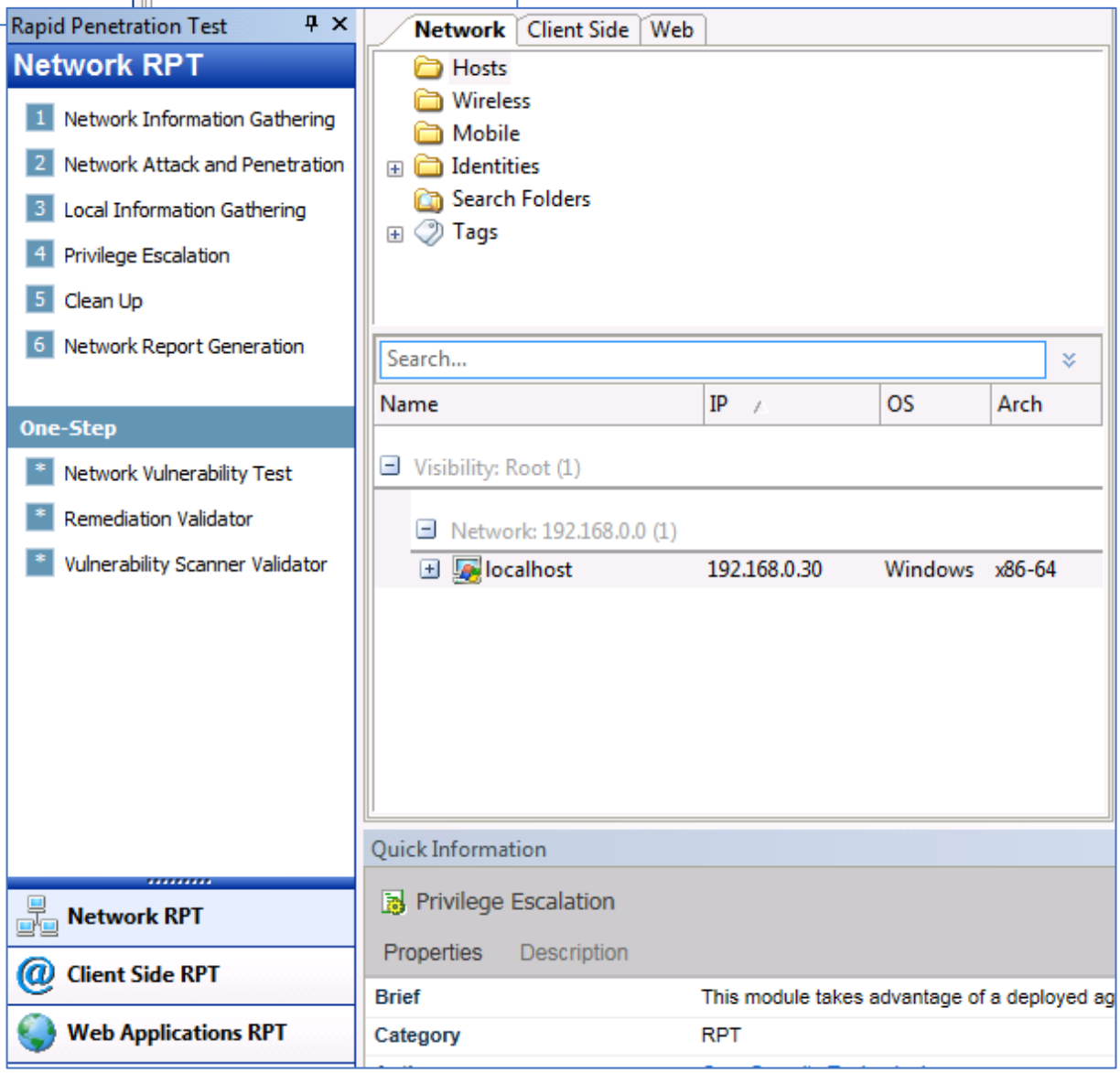


Before a vulnerability scan can take place, it is important to ensure that all of the computers on the network are identified.

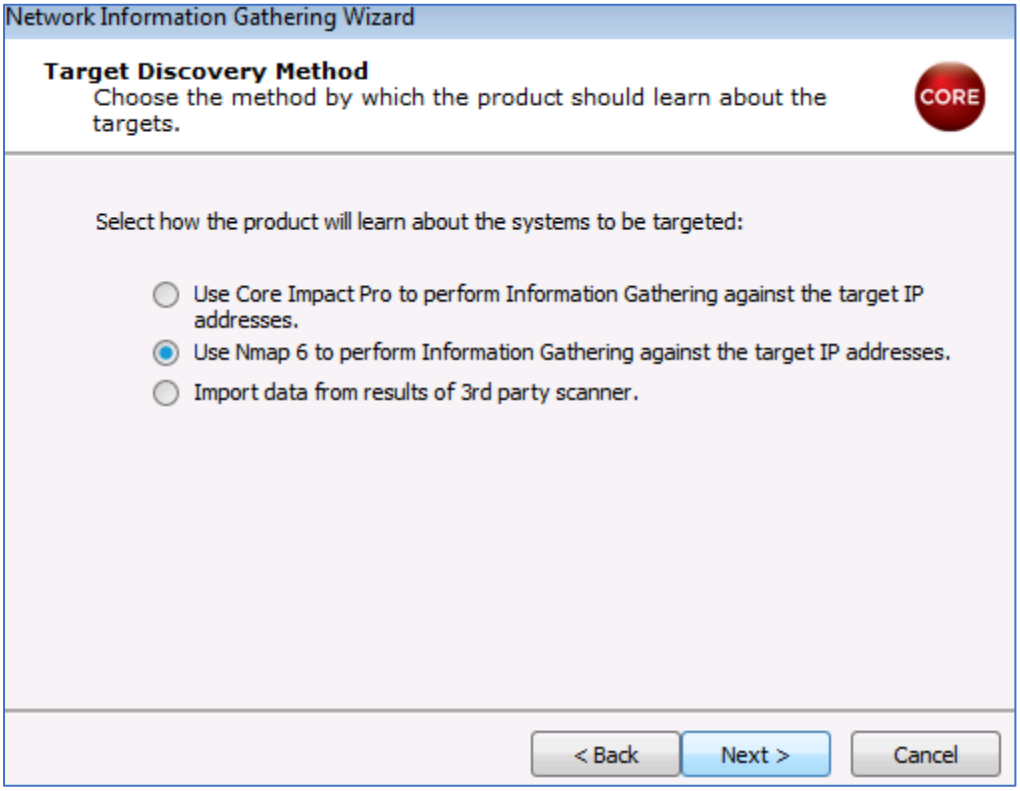




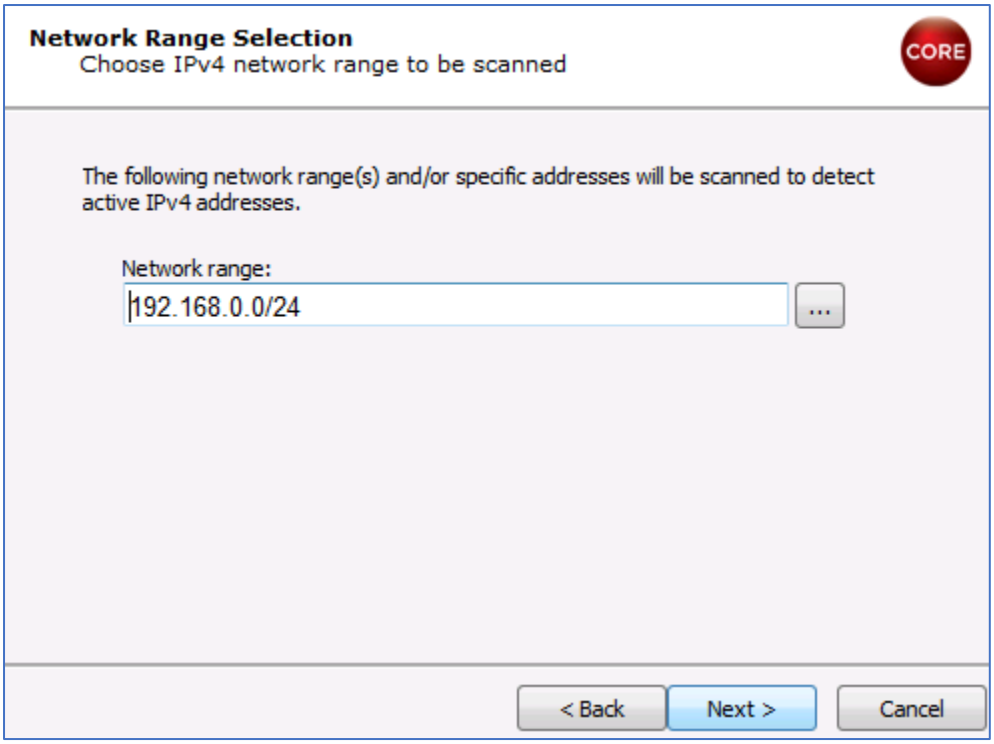
I select



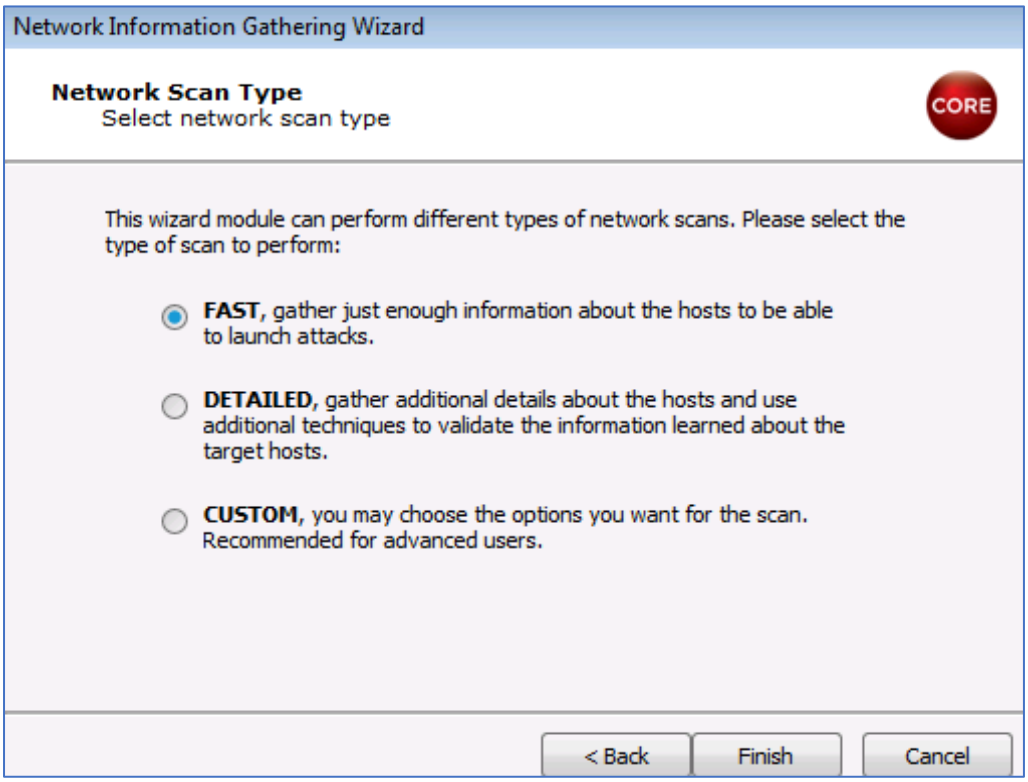
the **Network Information Gathering** in the left-hand corner of the screen to open the Network Information Gathering wizard.

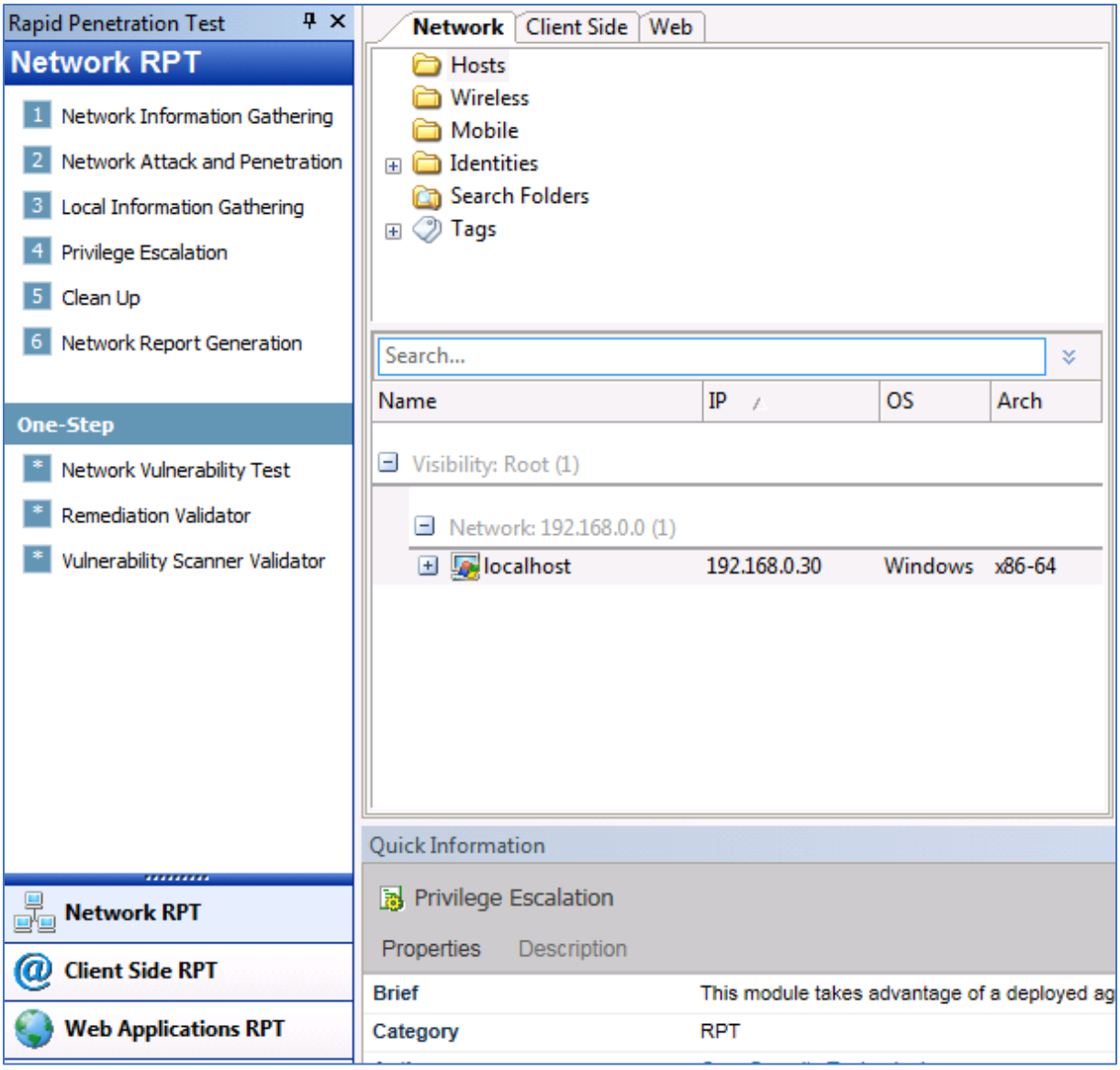


The network range we are targeting is 192.168.0.0/24

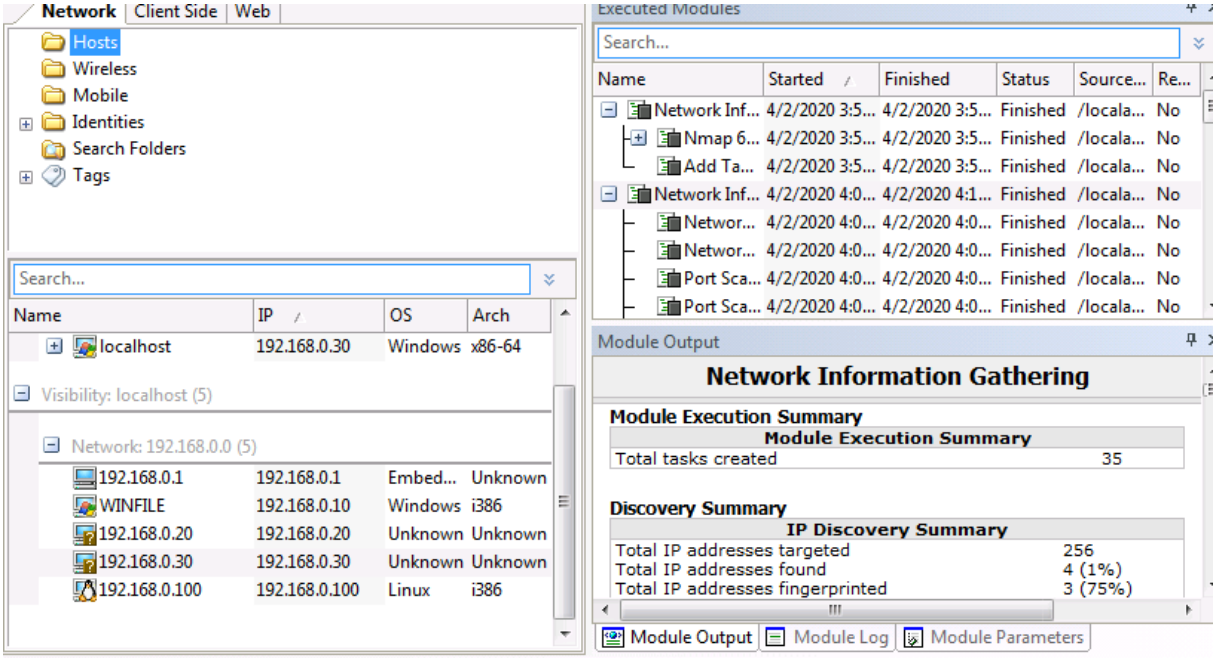


During the enumeration phase, gathering as much information as possible is crucial but in this case I am choosing fast scan to get just enough information on the network target.

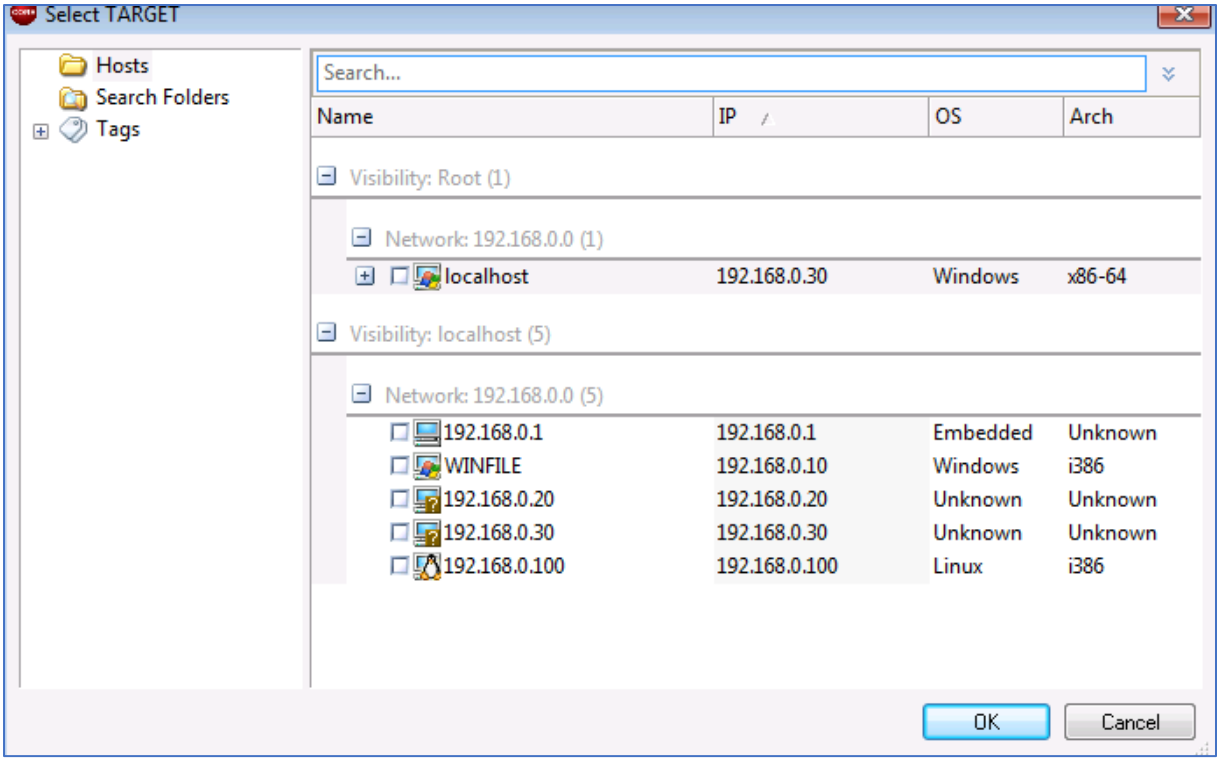




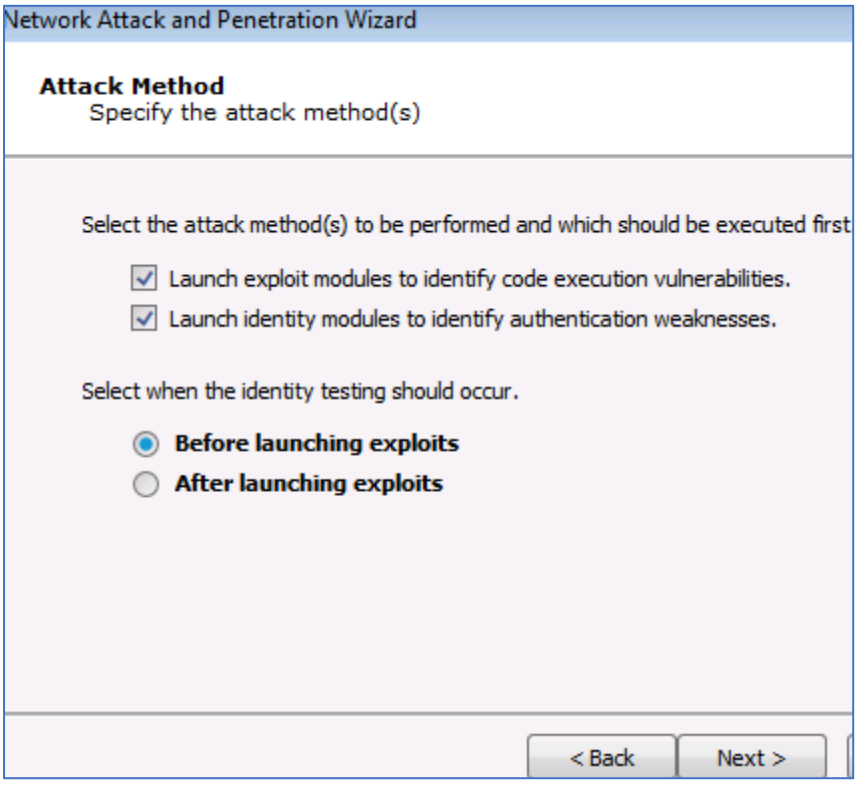
Since the scan was not effective enough, I launched a detailed scan instead



Moving to the next attack phase (Network Attack and Penetration) I select a target



Many options regarding the exploits execution are given including password attacks



Exploit Selection
Customize the exploit selection criteria

- [x] Use exploits that might leave a service unavailable (one shot).

  Some exploits may leave the service or application they are targeting in an unavailable state as a side effect of attempting to exploit a vulnerability in service. The service or application may restart automatically or require an administrator to restart it depending on its configuration.

- [x] Stop launching new exploits after an agent is deployed (running exploits wi

  This module can launch every possible attack that is applicable for each tar stop at the first one that successfully deploys an agent.

- [ ] Use exploits that take a long time to run.

  These exploits have been found during the Exploit QA process to take (on a long time to run and as a result can slow down the testing process.

< Back | Next >

Order Of Exploit Execution
Specify which attribute of the applicable exploits will be used to determine the order in which exploits are attempted.

- (●) **Release Date:** Exploits are sorted by the disclosure date of the vulnera they target. The most recently disclosed vulnerability is targeted first.
  The exploits are then sorted based on *Speed, Privilege level* and *Chance of leaving a service unavailable* in that order.
- ( ) **Speed:** Exploits that require the fewest number of attempts are run first
  The exploits are then sorted based on *Release Date, Privilege level* and *Chance of leaving a service unavailable* in that order.
- ( ) **Privilege level:** Exploits that typically deploy an agent with administrat root level privileges are run first.
  The exploits are then sorted based on *Release Date, Speed* and *Chance of leaving a service unavailable* in that order.
- ( ) **Chance of leaving a service unavailable:** Exploits that might leave target service unavailable are run first.
  The exploits are then sorted based on *Release Date, Privilege level* and *Speed* in that order.

< Back | Next >

Identity Attack Configuration
Known and Default Identities

Core Impact Pro will test each service using default and common identities as we
already discovered and previously validated identities for each service. Partial I
(Usernames with no passwords) will be combined with a dictionary of common
passwords.

Attack Type

- ○ **Quick:** A short list of the most common identities for each service.
- ◉ **Deep:** An extended list of common identities for each service.

Passwords

- ◉ **Default password list**
- ○ **Custom password file** C:\Users\Administrator\AppData\F

< Back | Next >

Identity Attack Selection
Select the identity attack modules to launch

CORE

Testing Type: Known and Default Identities

Core Impact Pro will test each service using default and common identities as well as
already discovered and previously validated identities for each service. Partial Identities
(Usernames with no passwords) will be combined with a dictionary of common
passwords.

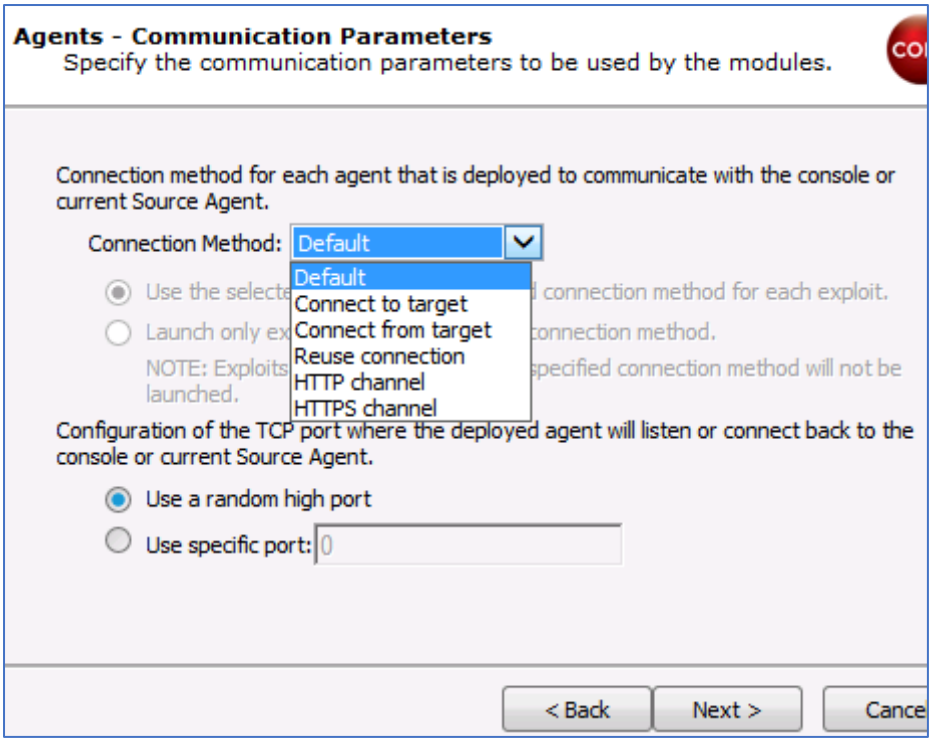
Check All | Uncheck All

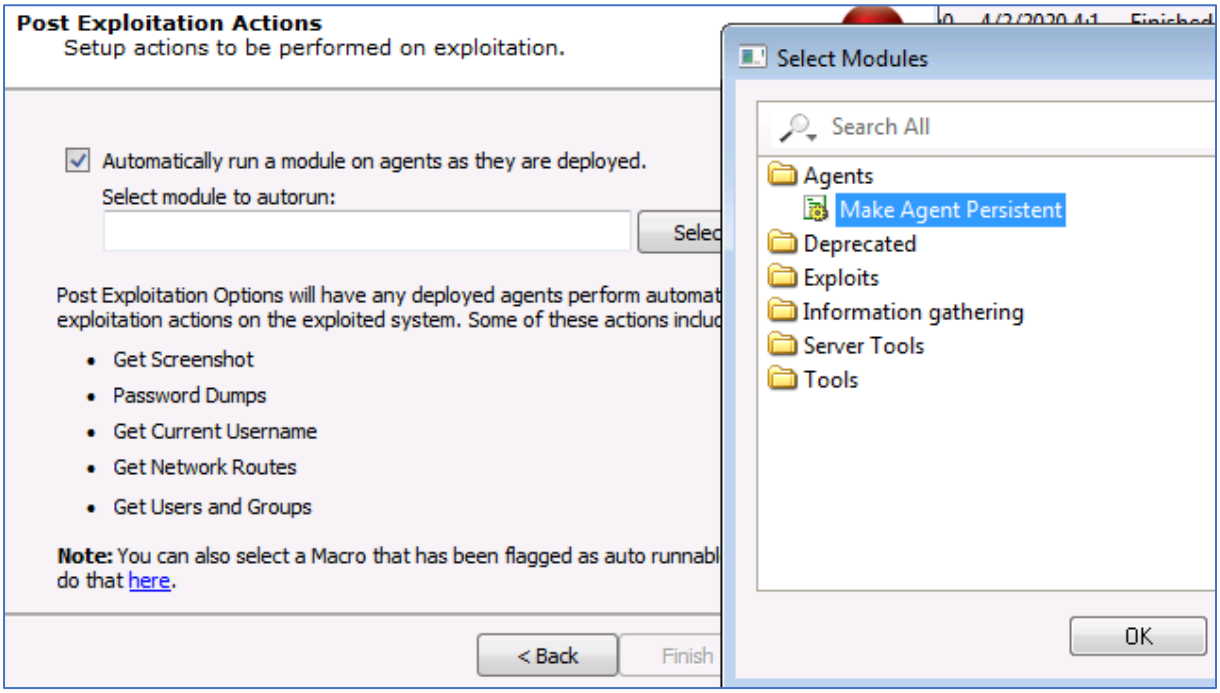
☑ DB2 *	☑ FTP	☑ HTTP	☑ Rlogin *	☑ SMB *	☑ RDP
☑ Oracle *	☑ POP3	☑ SSH *	☑ Telnet *	☑ VNC *	☑ RTSP
☑ SMTP	☑ SNMP *	☑ MSSQL *	☑ MySQL	☑ VMware	☑ PostgreSQL *

* indicates the protocol may be used to deploy an agent

< Back | Next > | Cancel

Checking all the protocols boxes





I choose and post exploitation actions like persistence on the targets.

HTTP Identity Verifier	4/2/2020 ...	4/2/2020 ... Finis...
SMB Identity Verifier	4/2/2020 ...	4/2/2020 ... Finis...
MSRPC Messenger exploit	4/2/2020 ...	4/2/2020 ... Finis...
SSL PCT Handshake Overflow exploit	4/2/2020 ...	4/2/2020 ... Finis...
IBM Lotus Domino LDAP ModifyRequest ...	4/2/2020 ...	4/2/2020 ... Finis...
Microsoft Group Policy Preferences Exploi...	4/2/2020 ...	4/2/2020 ... Finis...
Easy File Sharing Web Server GET Request ...	4/2/2020 ...	4/2/2020 ... Finis...
Kerberos Checksum Remote Privilege Esca...	4/2/2020 ...	4/2/2020 ... Finis...
MSRPC DCOM exploit (MS03-026)	4/2/2020 ...	4/2/2020 ... Finis...
Microsoft Windows Print Spooler Service I...	4/2/2020 ...	4/2/2020 ... Finis...
MSRPC LlsrLicenseRequestW Remote Hea...	4/2/2020 ...	4/2/2020 ... Finis...
Conficker Detector Exploit	4/2/2020 ...	4/2/2020 ... Finis...
MSRPC Server Service Remote Buffer Over...	4/2/2020 ...	4/2/2020 ... Finis...
Microsoft Windows SMB Buffer Underflow...	4/2/2020 ...	4/2/2020 ... Finis...
MSRPC Novell Netware Client EnumPrinte...	4/2/2020 ...	4/2/2020 ... Finis...
MSRPC RRAS Exploit	4/2/2020 ...	4/2/2020 ... Finis...
MSRPC LLSSRV Buffer Overflow exploit	4/2/2020 ...	4/2/2020 ... Finis...

When the **Network Attack and Penetration** wizard closes, I can see that many modules are launched to analyze and auto exploit whenever possible. Since the targeted machines are fully updated and patched, the network attack failed for now.

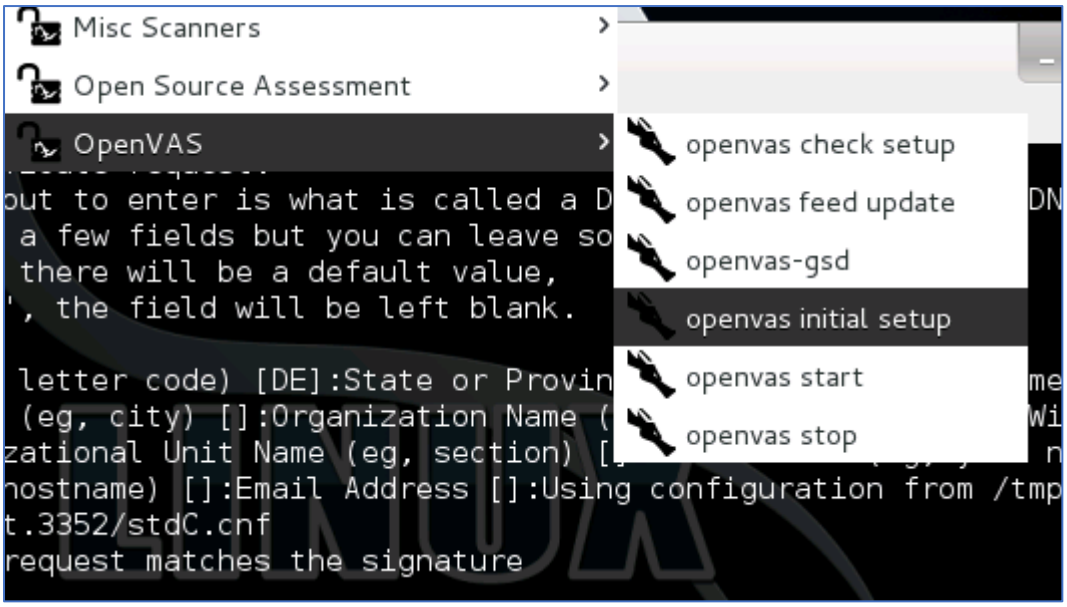
Module Output

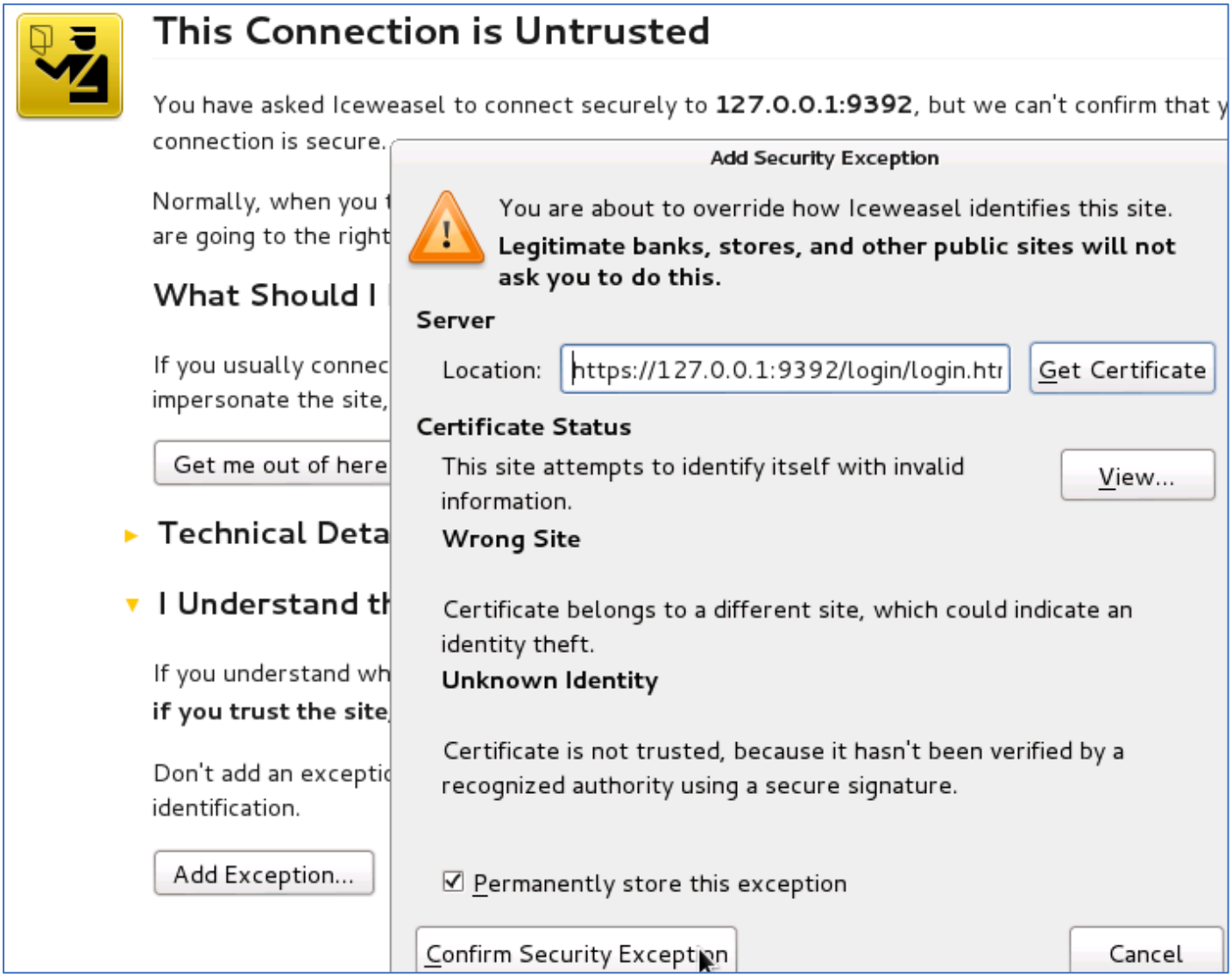
Exploit Summary	
Exploits attempted	23
Successful exploits	0 (0%)
Partially successful exploits	0 (0%)
Exploits defended	21 (91%)

Identity Verifiers Summary	
Identities validated	2
Identities tested	1968
Installed agent(s) using identities	0

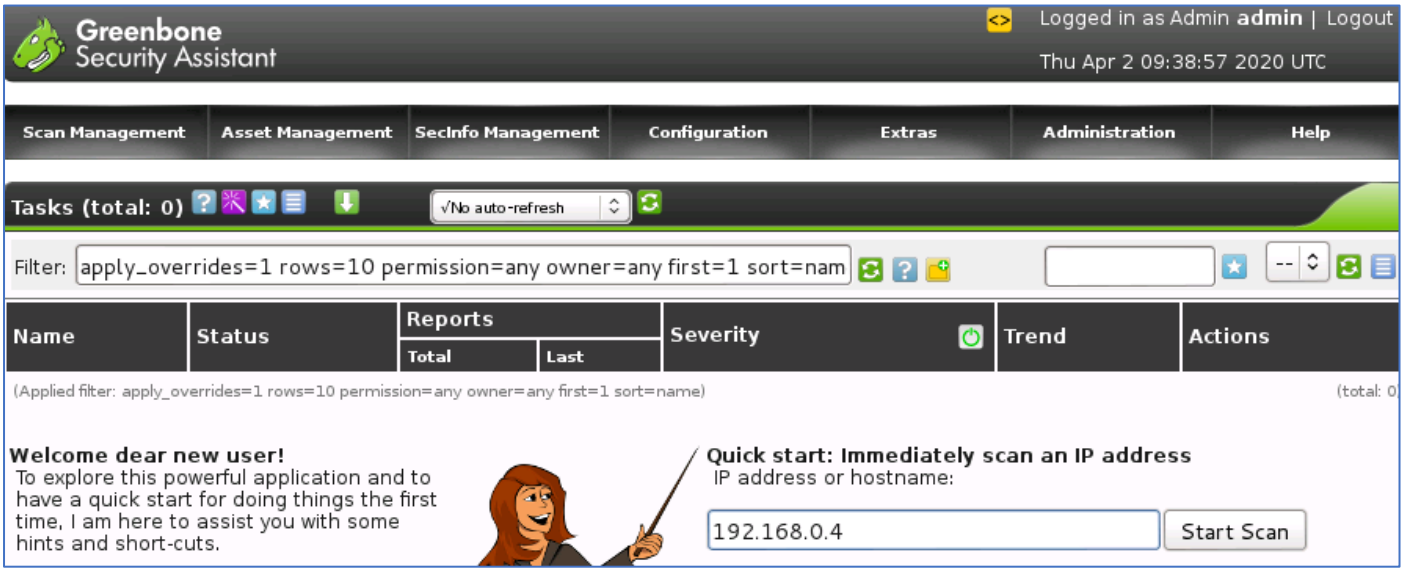
OpenVAS (Scanning a network range and interpreting the security report)

Initial setup



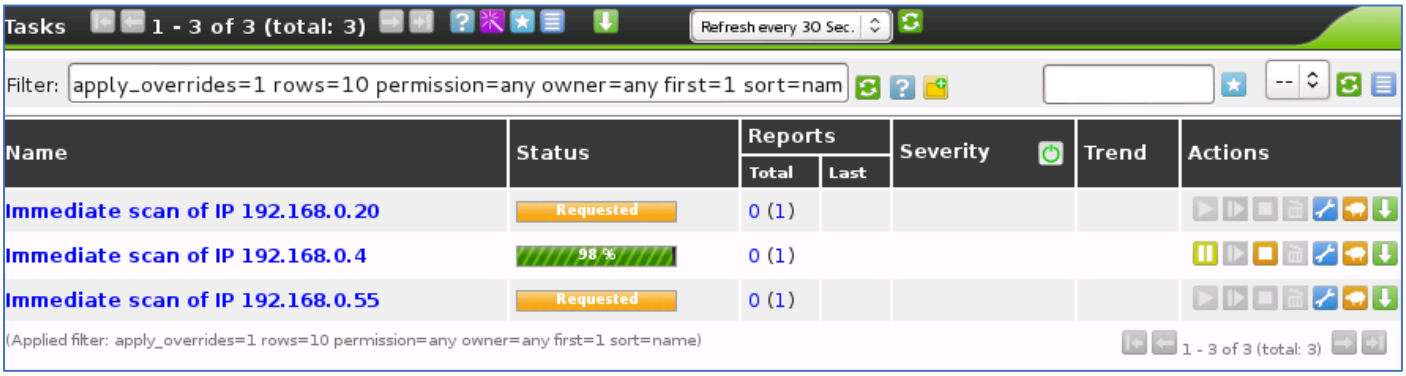


This is the login panel

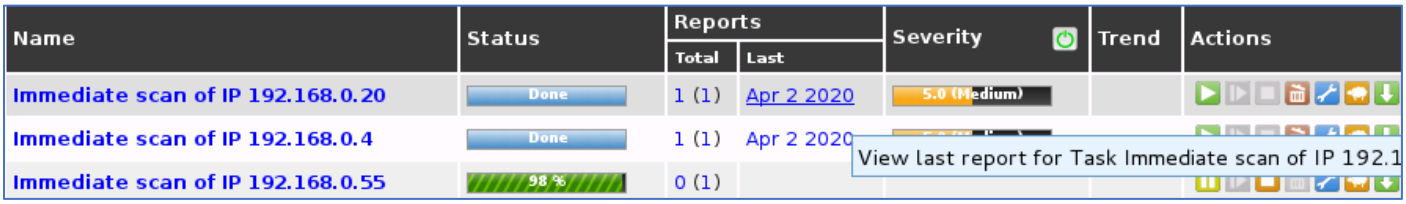


Entered the 192.168.0.4 IP address and requested to scan other networks

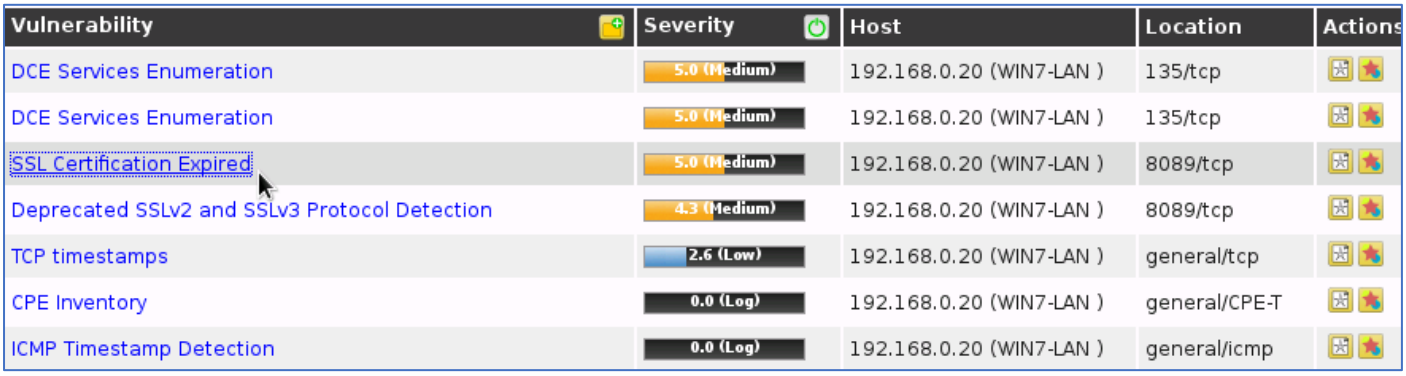
192.168.0.20
192.168.0.55



Once some of the scan done, the report are available. Let's check the 192.168.0.20's security report.



The security report shows a list of vulnerabilities. None are critical. I open the "SSL Certification Expired" to get more information.



Vulnerability	Severity	Host	Location	Actions
DCE Services Enumeration	5.0 (Medium)	192.168.0.20 (WIN7-LAN)	135/tcp	
DCE Services Enumeration	5.0 (Medium)	192.168.0.20 (WIN7-LAN)	135/tcp	
SSL Certification Expired	5.0 (Medium)	192.168.0.20 (WIN7-LAN)	8089/tcp	
Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	192.168.0.20 (WIN7-LAN)	8089/tcp	
TCP timestamps	2.6 (Low)	192.168.0.20 (WIN7-LAN)	general/tcp	
CPE Inventory	0.0 (Log)	192.168.0.20 (WIN7-LAN)	general/CPE-T	
ICMP Timestamp Detection	0.0 (Log)	192.168.0.20 (WIN7-LAN)	general/icmp	

We can view the vulnerability and take note of what the vulnerability is, why it is a security risk, and the solution to this vulnerability.

Summary
The remote server's SSL certificate has already expired.

Vulnerability Detection Result

```
Expired Certificates:\
\
\
The SSL certificate on the remote service expired on 2018-05-27 20:45:29
Certificate details:
subject ...: O=SplunkUser,CN=SplunkServerDefaultCert
issued by .: 1.2.840.113549.1.9.1=#737570706F72744073706C756E6B2E636F6D,CN=SplunkCommonCA,↵
O=Splunk,L=San Francisco,ST=CA,C=US
serial ....: 00B82D6D4C88046761
valid from : 2015-05-28 20:45:29 UTC
valid until: 2018-05-27 20:45:29 UTC
fingerprint: CFCCAF12BF60889187313F12AAE5155B86E29945\
\
The SSL certificate on the remote service expired on 2018-05-27 20:45:29
Certificate details:
subject ...: O=SplunkUser,CN=SplunkServerDefaultCert
issued by .: 1.2.840.113549.1.9.1=#737570706F72744073706C756E6B2E636F6D,CN=SplunkCommonCA,↵
O=Splunk,L=San Francisco,ST=CA,C=US
serial ....: 00B82D6D4C88046761
valid from : 2015-05-28 20:45:29 UTC
valid until: 2018-05-27 20:45:29 UTC
fingerprint: CFCCAF12BF60889187313F12AAE5155B86E29945
```

Solution
Replace the SSL certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: SSL Certification Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Scan alternative:

In this situation I create a new file and add ip address one by one

```
kali:~$ nano scanning_target_list
```

```
  GNU nano 2.9.2

192.168.0.10
192.168.0.20
192.168.0.30
192.168.0.40
192.168.0.50
```

Launching OpenVAS with command-lines

```
student@kali:~$ sudo openvas-start
[sudo] password for student:
[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```