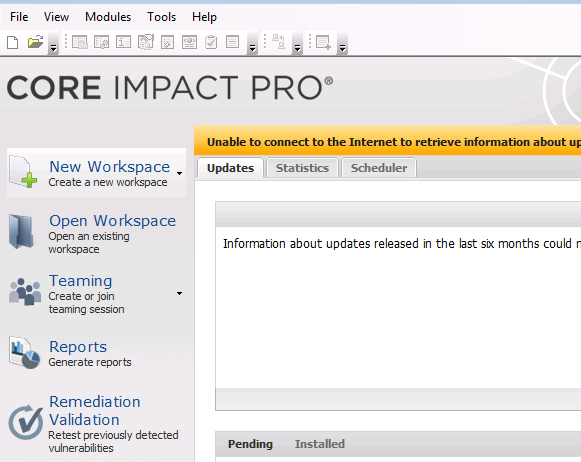
**Set-up, configuring a Vulnerability scanner (Core Impact)**

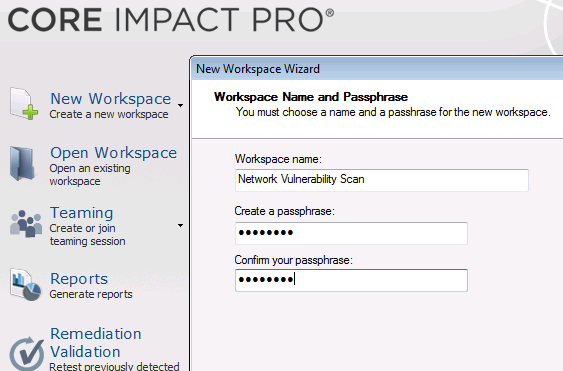
**Core Impact**

Launching the software

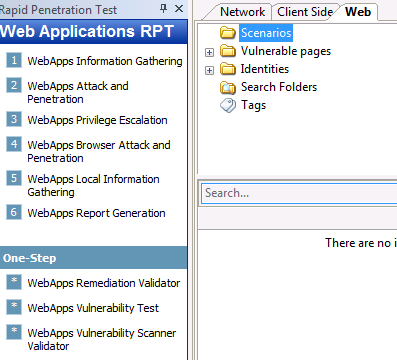
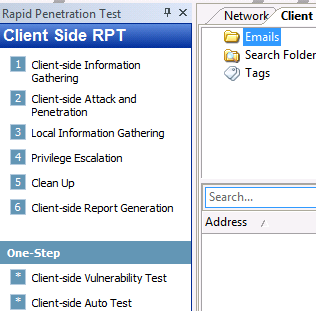
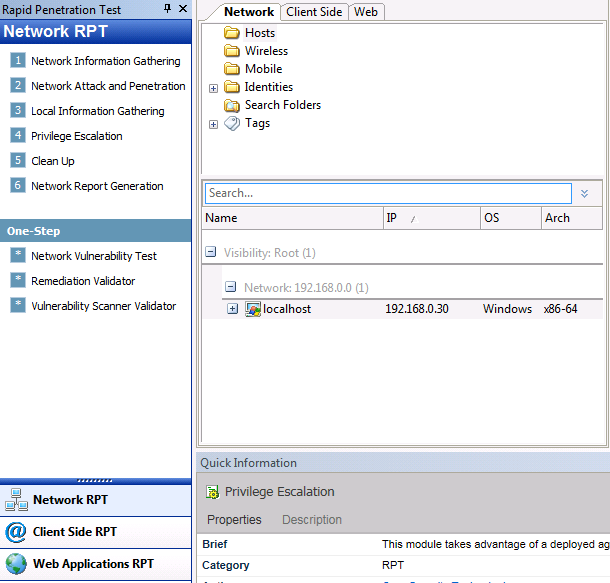
****



Creating a Blank Workspace

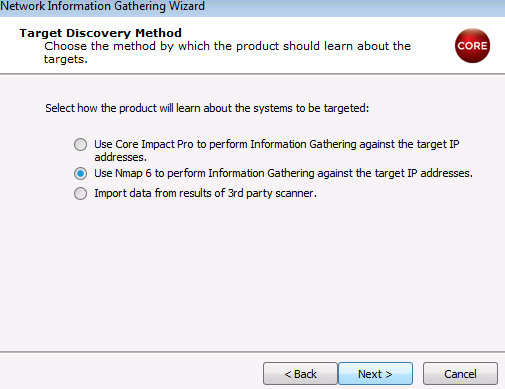


Before a vulnerability scan can take place, it is important to ensure that all of the computers on the network are identified.

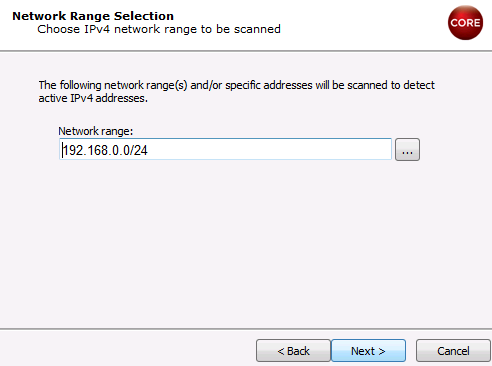


I select the **Network Information Gathering** in the left-hand corner of the screen to open the Network Information Gathering wizard.

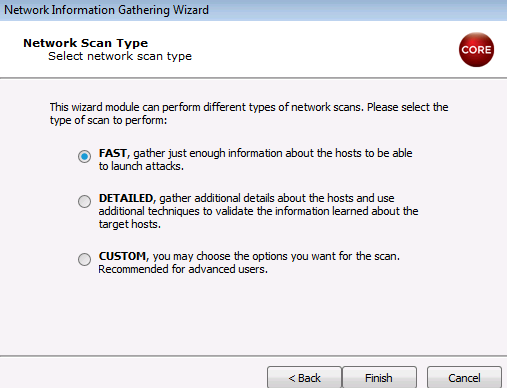


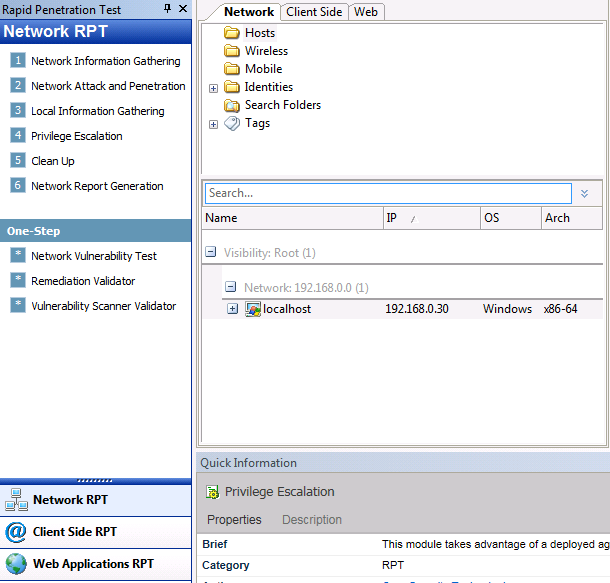


The network range we are targeting is 192.168.0.0/24

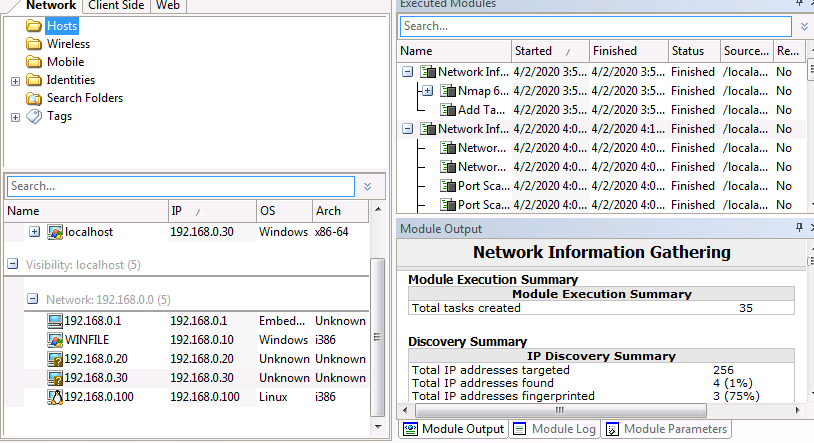


During the enumeration phase, gathering as much information as possible is crucial but in this case I am choosing fast scan to get just enough information on the network target.

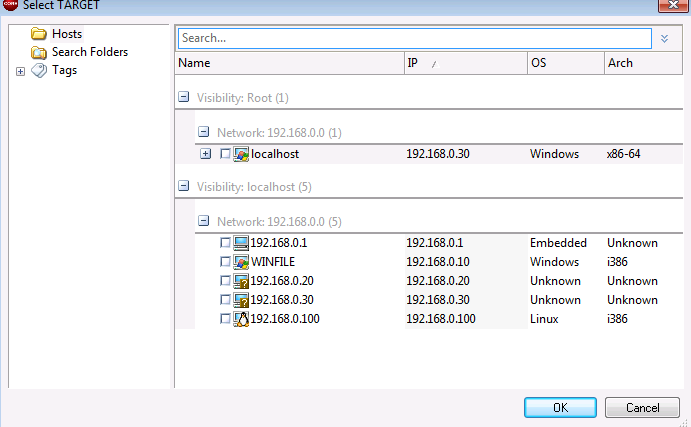




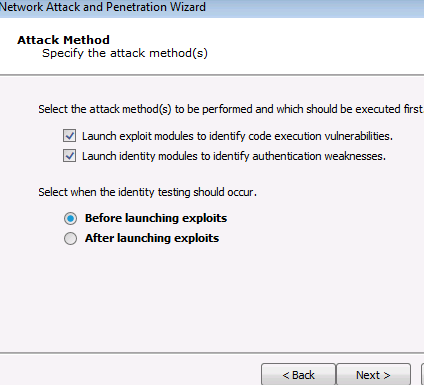
Since the scan was not effective enough, I launched a detailed scan instead

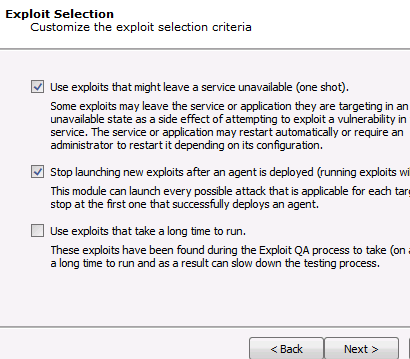


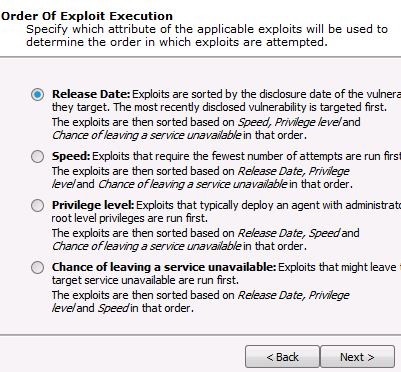
Moving to the next attack phase (Network Attack and Penetration) I select a target

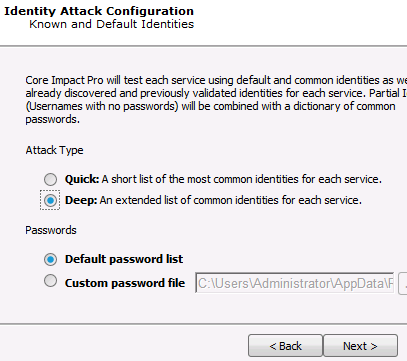


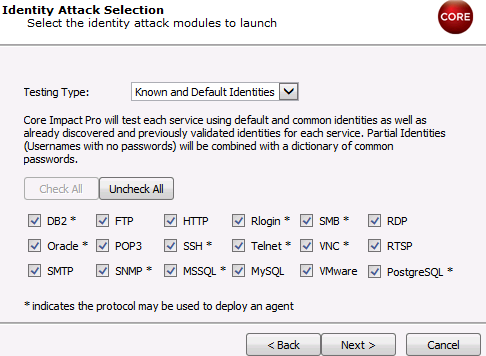
Many options regarding the exploits execution are given including password attacks



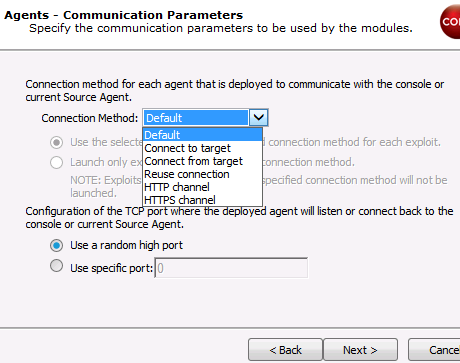


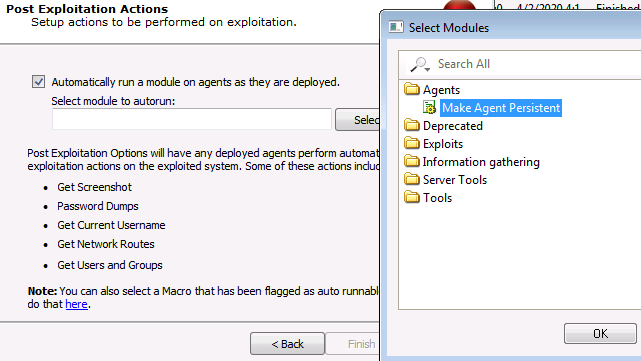




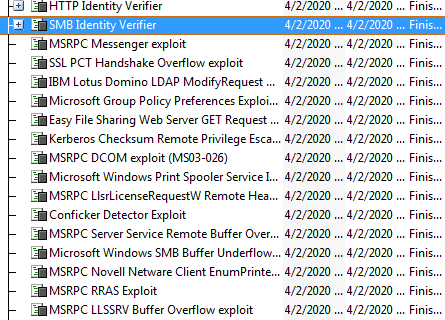


Checking all the protocols boxes

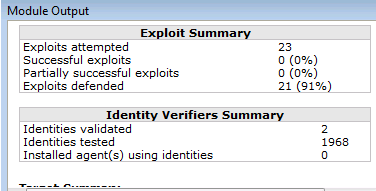




I choose and post exploitation actions like persistence on the targets.

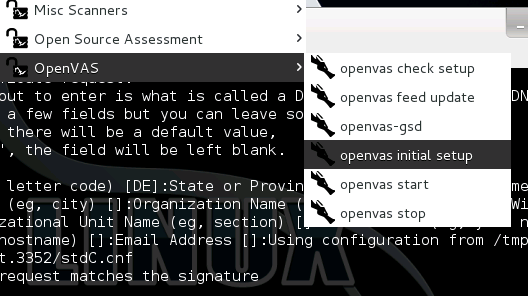


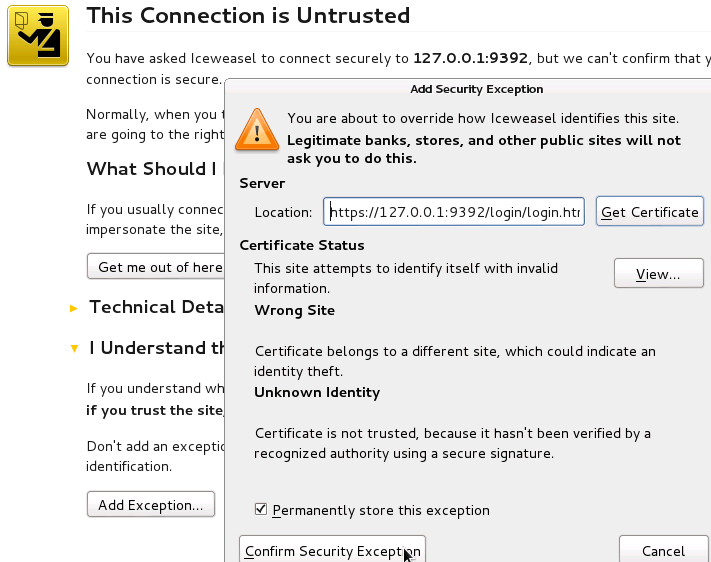
When the **Network Attack and Penetration** wizard closes, I can see that many modules are launched to analyze and auto exploit whenever possible. Since the targeted machines are fully updated and patched, the network attack failed for now.



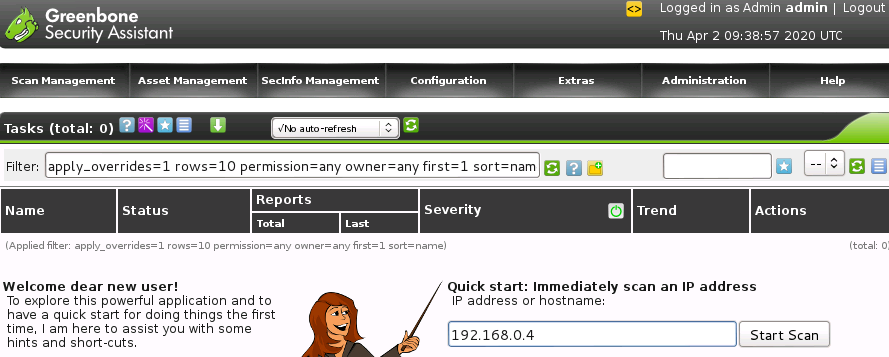
OpenVAS ( Scanning a network range and interpreting the security report)

Initial setup





This is the login panel

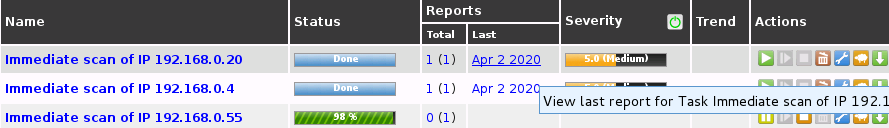


**Entered the 192.168.0.4 IP address and requested to scan other networks**

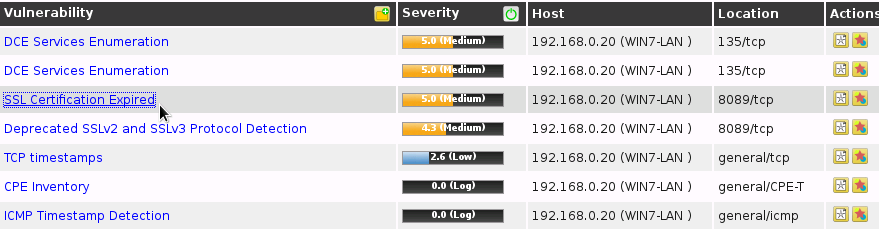
**192.168.0.20**  
**192.168.0.55**



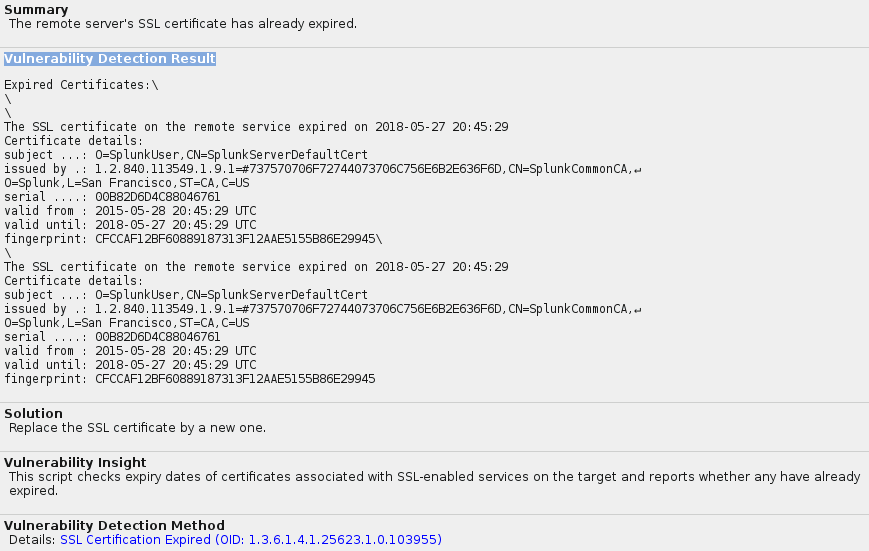
Once some of the scan done, the report are available. Let’s check the 192.168.0.20’s security report.



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

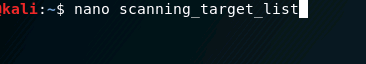


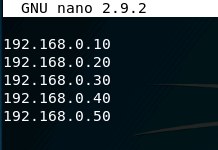
We can view the vulnerability and take note of what the vulnerability is, why it is a security risk, and the solution to this vulnerability.



**Scan alternative:**

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





Launching OpenVAS with command-lines

