As we begin phase three of our penetration procedures, we will be scanning all devices, software and firewalls. As mentioned via the client, they are wanting to phase out Cisco Firewall and use Fortinet instead, but we will still complete a vulnerability scan on the Cisco Firewall. Client has provided internal IP ranges 10.1.1.01/24, 10.2.1.01/24,10.3.1.01/24.,10.4.1.01/24 and 10.5.1.01/24

First we will begin testing the firewalls Cisco, Fortinet, Palo Alto and F5-Big IP. With Cisco Firewall, we can use nessus but first we have to make sure the configuration of nessus has the privilege level for users, if not we would have to escalate privileges for cisco in SSH. With Palo Alto we would perform a compliance scan, but make sure we have the proper credentials. F5-Big IP can also be scanned against nessus, but has to be configured as well. We would configure the nessus scanner to use a BIG-IP user account, that has the auditor role. There are several advantages of using nessus for scanning such as high speed-asset discovery, configuration auditing, malware detection and sensitive data discovery. With these advantages, it can carry drawbacks such as no guarantees that all vulnerabilities would be seen and only 16 targets scanned at one time max.

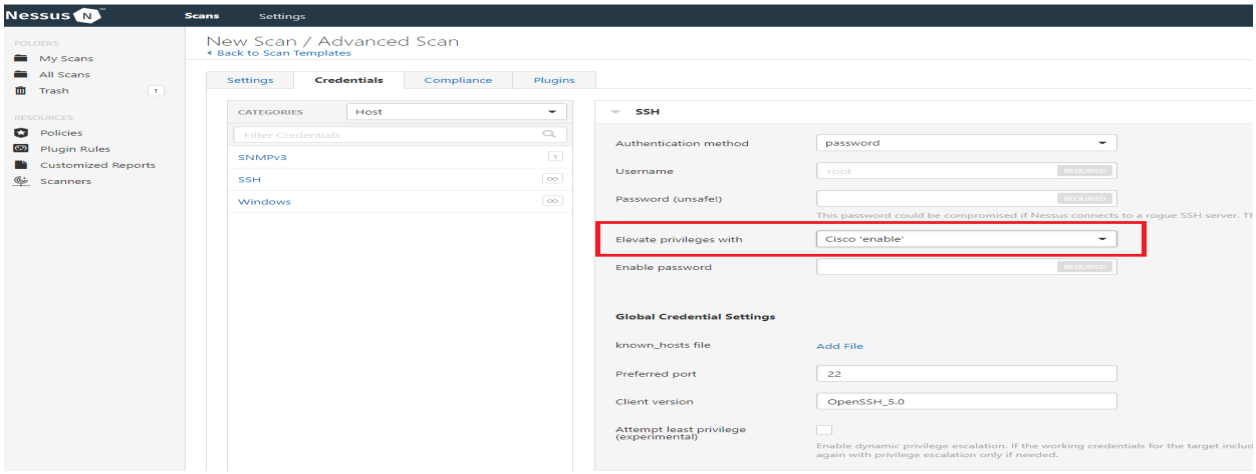
We can use Nmap to scan for additional data of the firewalls. With Nmap we would identify the open ports, services used and more detailed information on the vulnerabilities that we find.We can also use the OpenVas vulnerability scanner. The benefits of Nmap and OpenVas are more comprehensive as it allows us to see

everything that is connected and we are able to use several scanning techniques such as TCP connect and TCP SYN. OpenVas can detect high level web threats such as cross site scripting.

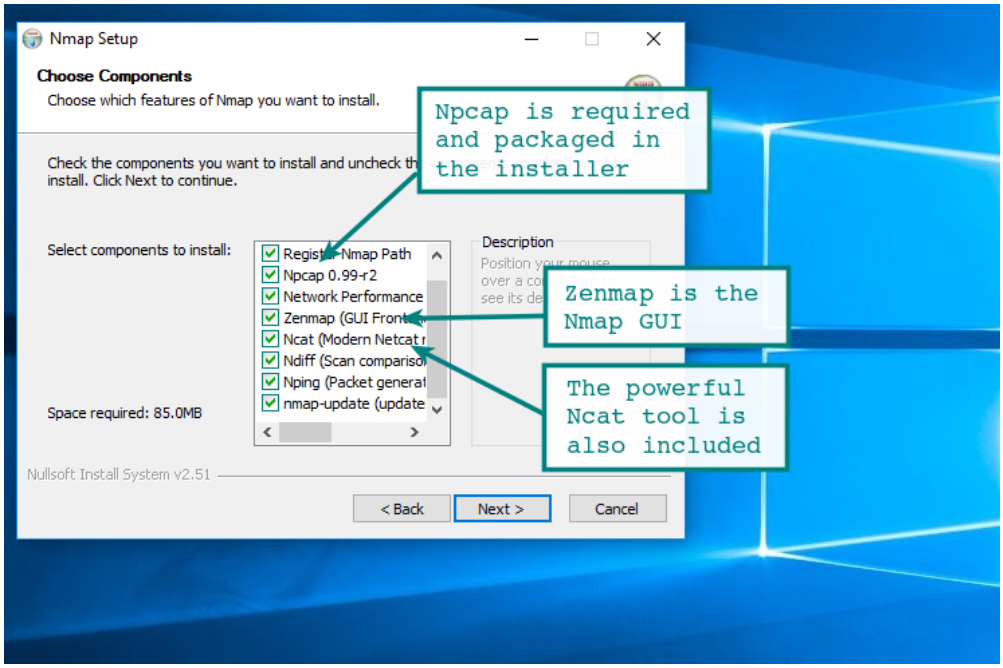
For web applications, such as Zsclar we can run Zscaler Cloud performance test tool or Wireshark, to check for vulnerabilities and to measure performance. We can check to see if traffic is going to the service by checking the connectivity via ip.zscaler.com. We can also enable the Zsclar client connector, which allows traffic to be captured specifically to the device. With wireshark we can also capture traffic, but we may not be able to see all traffic. With wireshark, we can also trace connections and view the contents of suspicious network transactions. A drawback of wireshark is that if there is an intrusion, notifications will not make it evident.

We can test the Amazon Web Services,which houses most of the servers and applications with the amazon inspector tool. This tool is offered via Amazon, automated and can detect software vulnerabilities. Advantages of this tool is that it scans quickly and a disadvantage is that there are a variety of systems used, which can be a challenge to implement. Burp suite can also be used as a scanning tool, for our web applications. This tool runs automated scans on our targets, covers initial mapping and analysis of information found. This tool is more advanced and will require more comprehensive knowledge. Estimated timeframe to complete identifying vulnerabilities, will take 2 to 3 days.

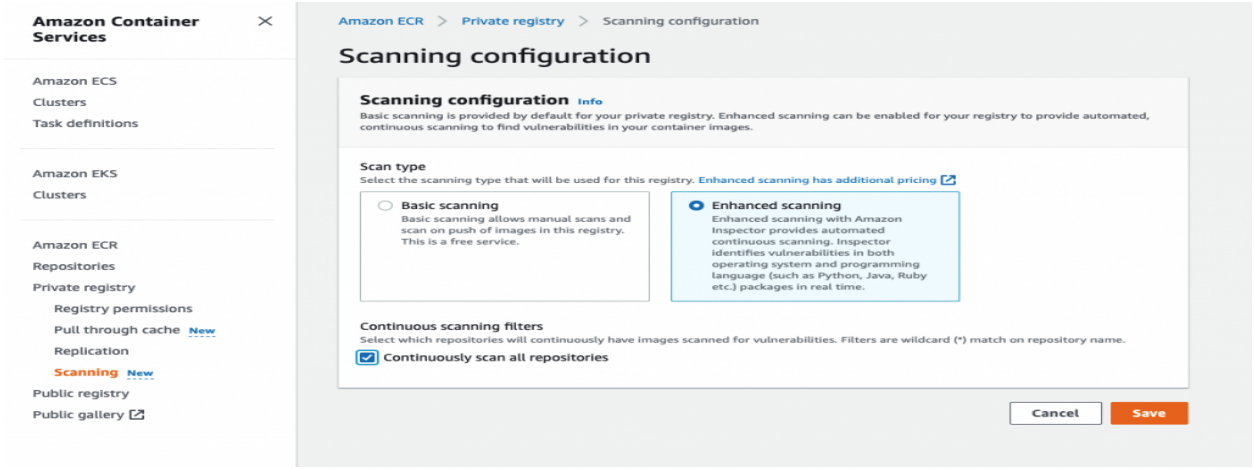
1. Cisco Configuration



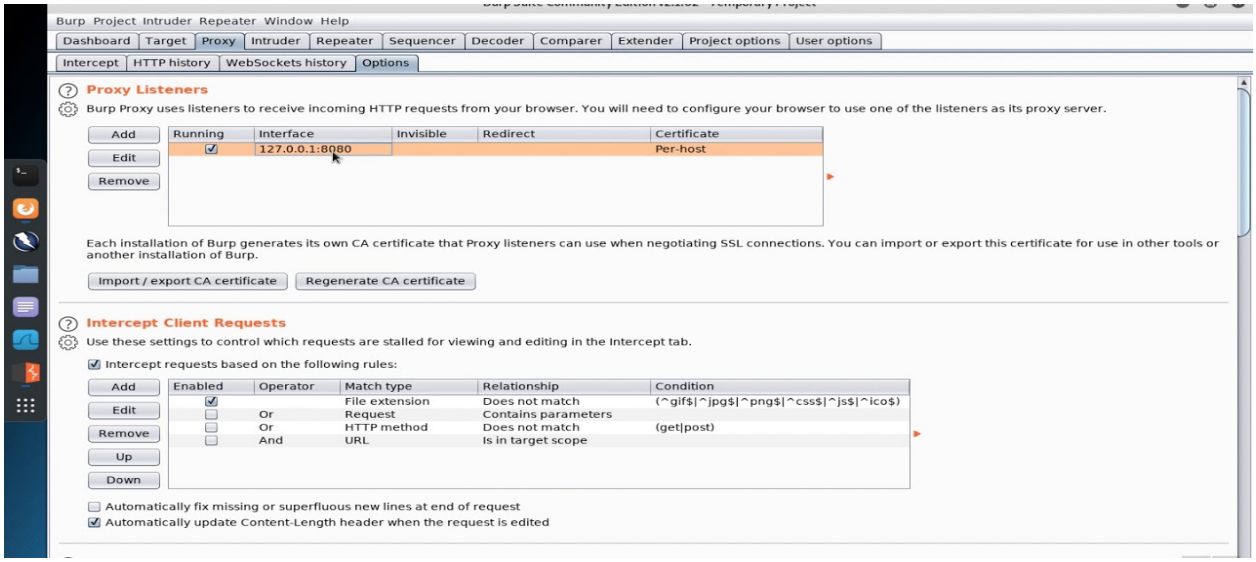
2.Nmap Configuration



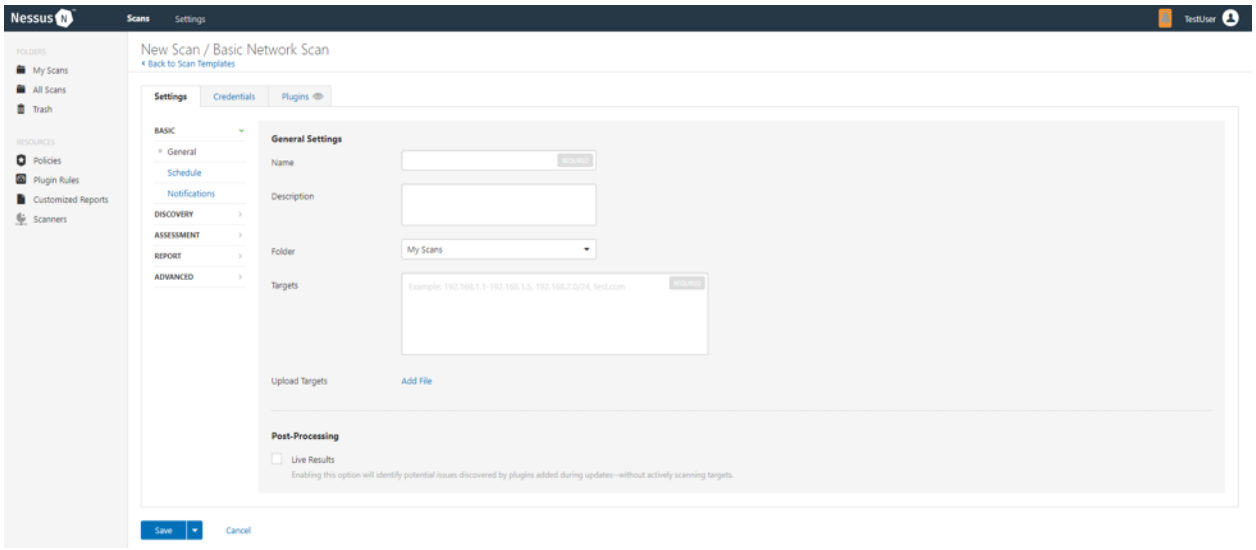
3.AWS Configuration



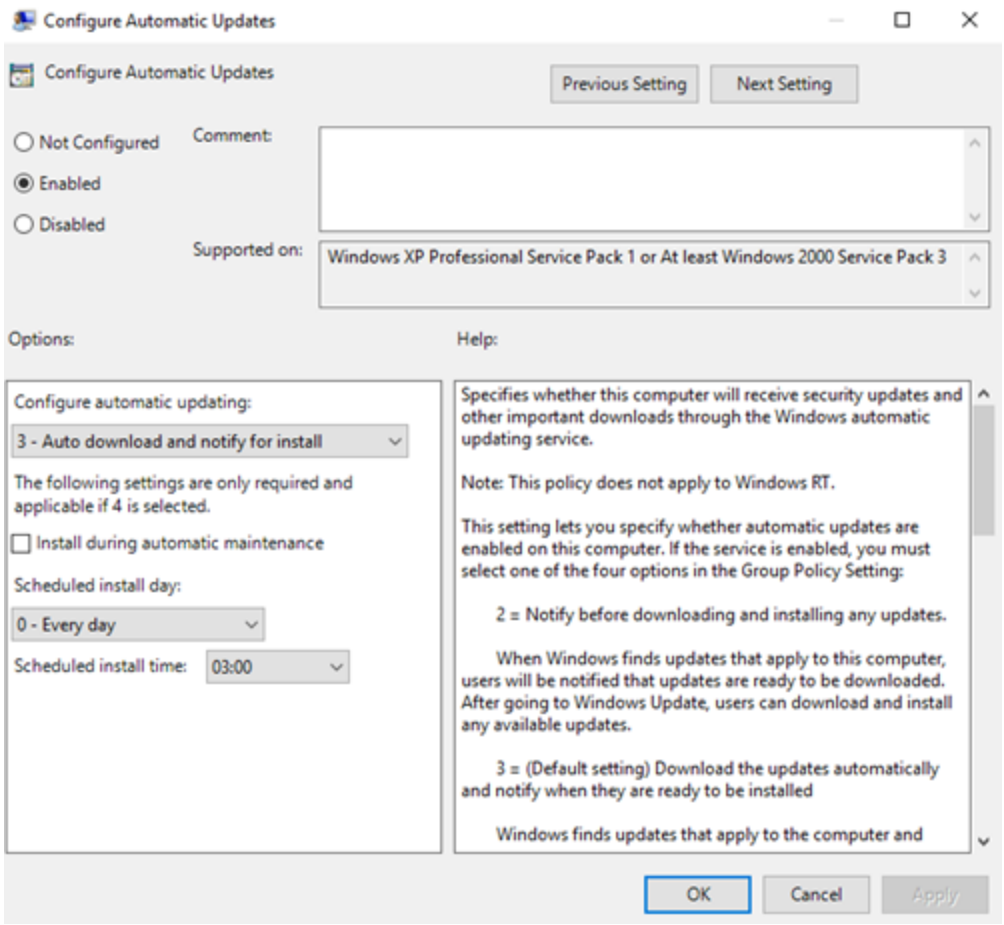
4. BurpSuite



5. Nessus Configuration



6. Windows Server


Configure Automatic Updates
Configure Automatic Updates
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3
Options:
Help:
Configure automatic updating:
3 - Auto download and notify for install
The following settings are only required and applicable if 4 is selected.
Install during automatic maintenance
Scheduled install day:
0 - Every day
Scheduled install time:
03:00
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.
Note: This policy does not apply to Windows RT.
This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:
2 = Notify before downloading and installing any updates.
When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.
3 = (Default setting) Download the updates automatically and notify when they are ready to be installed
Windows finds updates that apply to the computer and
OK
Cancel
Apply