# **Qualys Essentials Vulnerability Management Lab**

## **Description**

This is a walkthrough of how I created A Virtual Machine environment using VMWare ESXi. In this virtual environment, I created Windows 10 and Windows 7. I did this project to gain experience with Qualys and learn how to scan for vulnerabilities and remediate them. This project will showcase Some of the steps of the Vulnerability Management Lifecycle. I will use Qualys to scan local VMs hosted on VMWare ESXi to discover vulnerabilities, remediate some vulnerabilities, and then perform a rescan to verify remediation.

**Quick disclaimer.** PLEASE do NOT scan a network you do not have explicit permission to scan. Unauthorized activity like this can result in serious legal consequences. So, only scan your home network.

## **Utilities Used**

* Qualys Community Edition
* CMD

## **Environments Used**

* VMWare ESXi
* Windows 10 Pro Version 1709
* Windows 7 Ultimate (Service Pack 1)

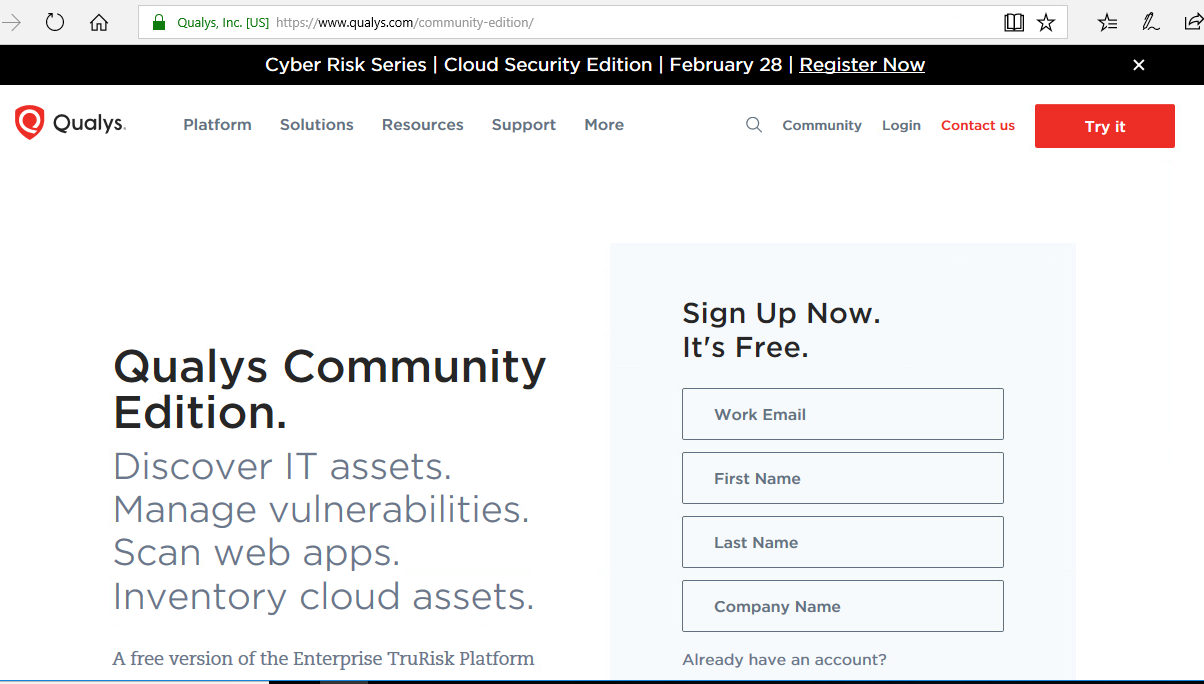
## **Links**

* Qualys Community Edition:
  + [Qualys Community Edition | Qualys](https://www.qualys.com/community-edition/)
* VMWare ESXi:
  + [Download the ESXi Installer (vmware.com)](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-016E39C1-E8DB-486A-A235-55CAB242C351.html)
* Windows 10 Installation:
  + <https://www.microsoft.com/en-us/software-download/windows10>
* Windows 7 Ultimate (Service Pack 1)
  + <https://support.microsoft.com/en-us/windows/install-windows-7-service-pack-1-sp1-b3da2c0f-cdb6-0572-8596-bab972897f61>
    - <https://www.catalog.update.microsoft.com/Search.aspx?q=KB976932>

## **Program walk-through**

The first thing I am going to do is Download and install VMware ESXi. Then download and install Windows 10 Pro and Windows 7.

Next, I am going to download and install Qualys Community Edition. You will need a work or school email to do so.

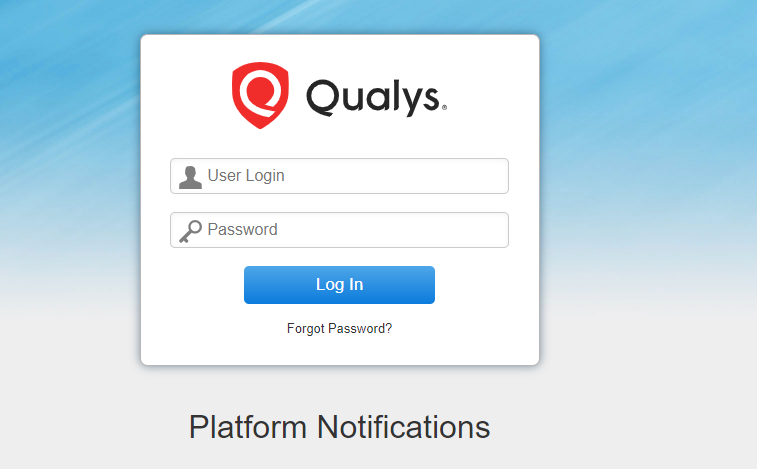


Notes About this Edition

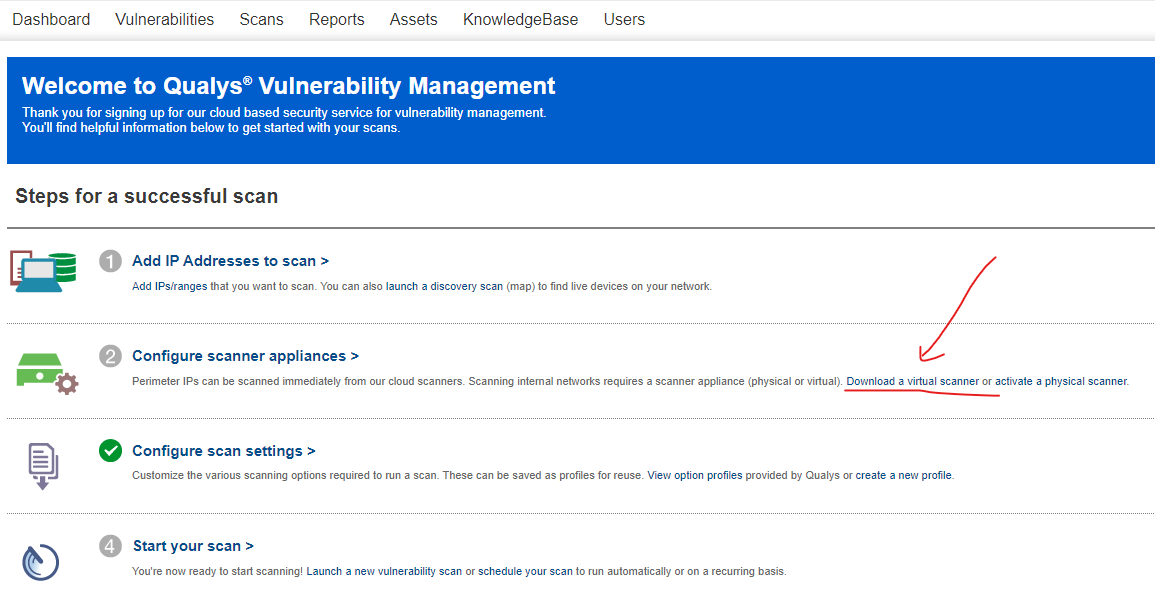
Qualys Community Edition gives you these great capabilities at no cost:

* Monitor up to 16 assets with Qualys Cloud Agent
* Scan up to 16 internal and 3 external IPs with Vulnerability Management
* Scan 1 URL with Web Application Scanning.
* Deploy a Virtual Scanner Appliance within your internal network.
* Gain visibility within your cloud environments.
* Generate reports and assess results quickly and easily.

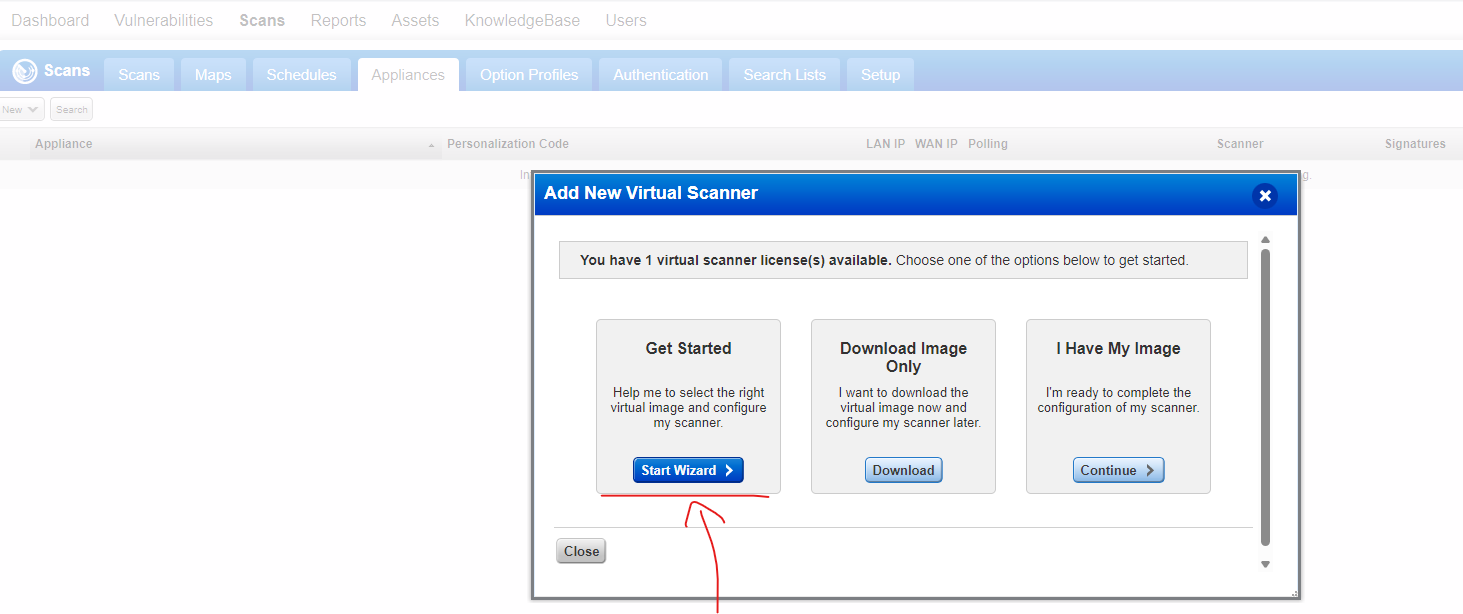
If you follow the instructions properly you will receive a URL link to the Qualys Cloud Dashboard with credentials and instructions on how to access it.

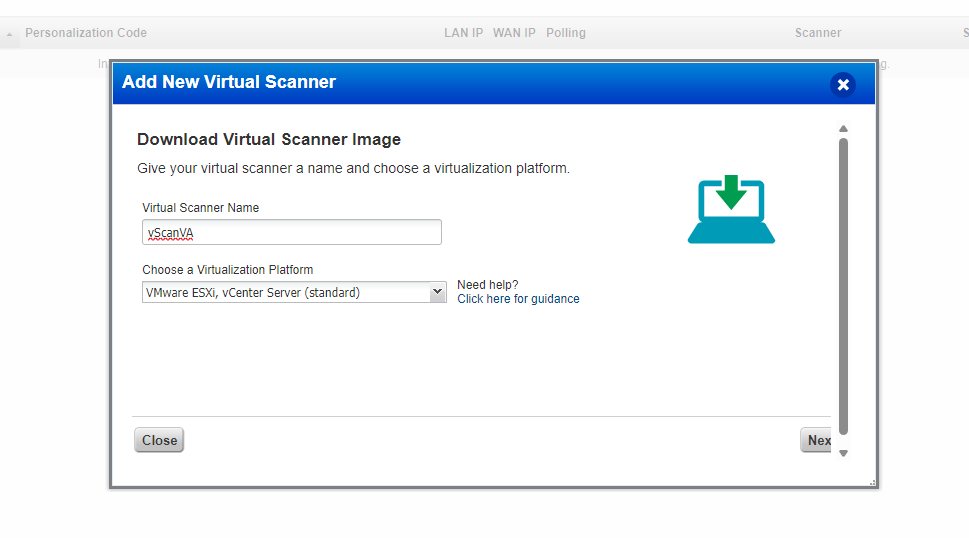


Once you get to the page below, configure and download the virtual appliance



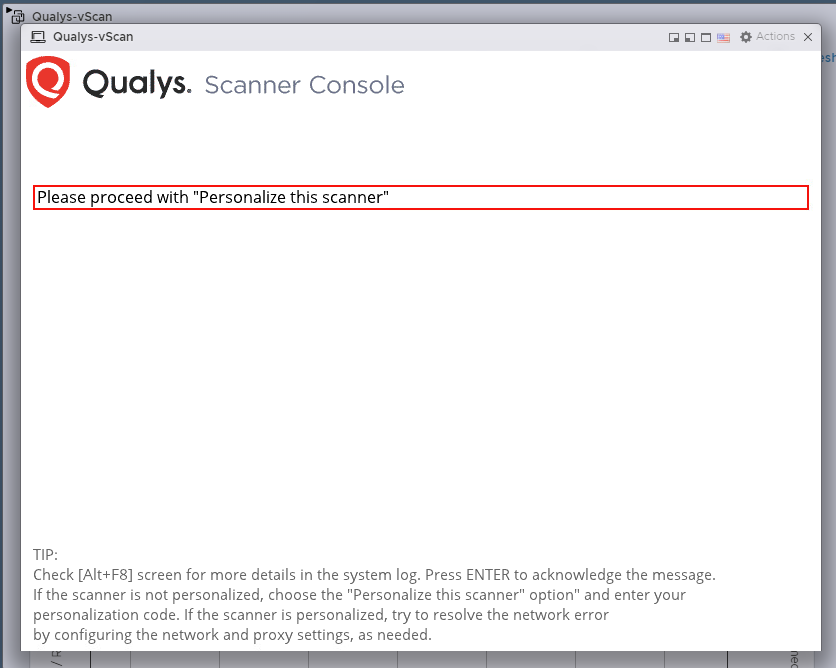
Next, click on **Start Wizard** and follow the instructions



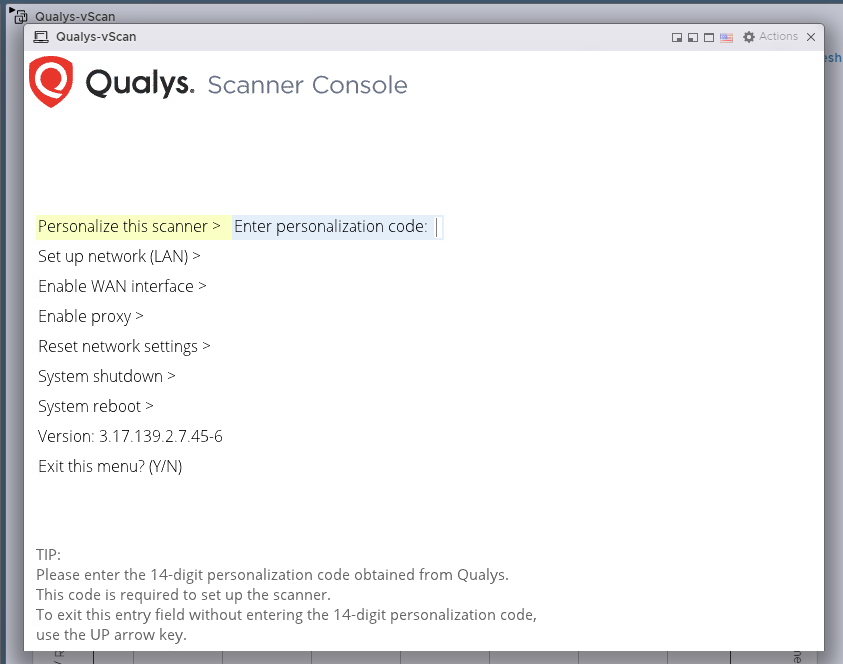


Click next and follow the instructions. Make sure to copy and save your Personalization Code. Configure your scanner and activate it using the personalization code.

Once you are done installing the Virtual Appliance in VMware ESXi, launch it. The main screen should ask for the **Personalization Code**.

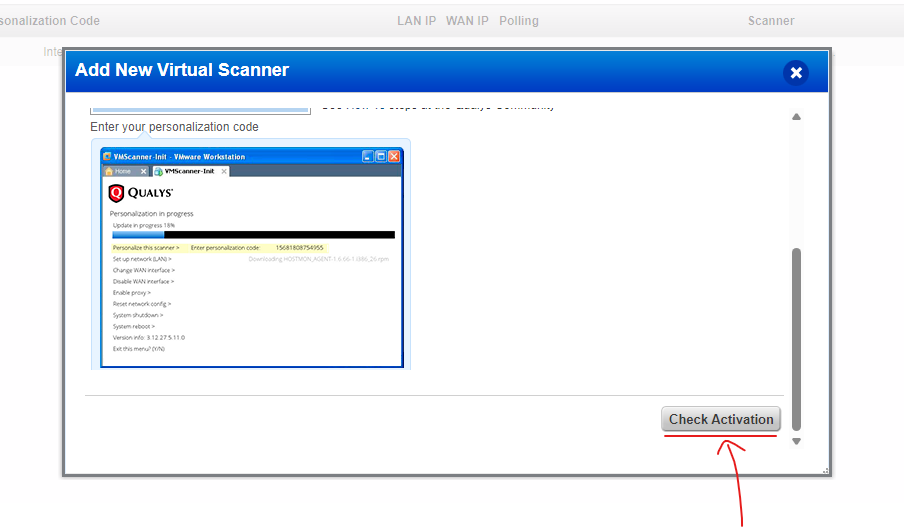


Once you see the screen above, hit enter to get to the page where you need to enter the code. Use the up and down arrow to navigate the menu

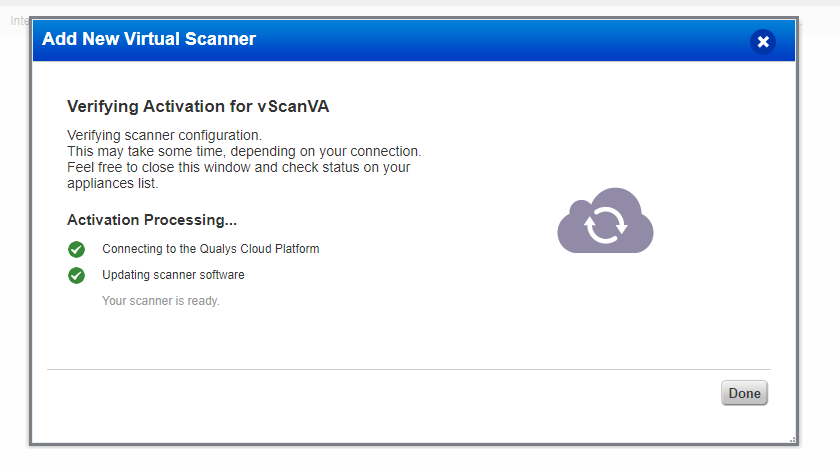


Once it finishes installing you will see the display of the private IP the Virtual appliance will use.

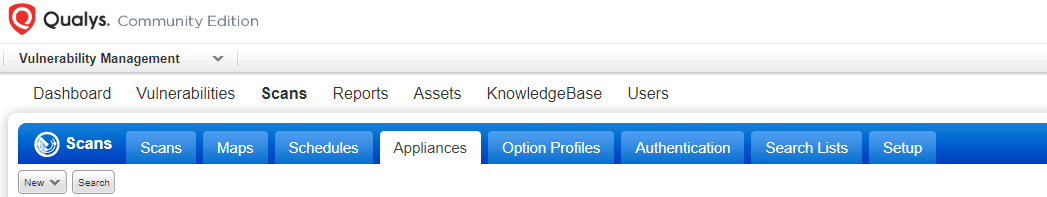
Then go back to the page where you got your personalization code and click on **Check Activation.**



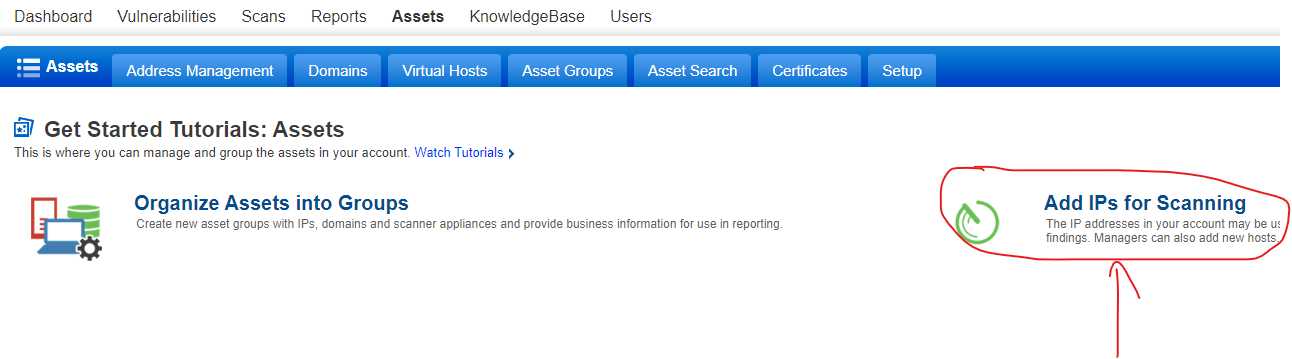
Here is it going to verify that your appliance is active and running.



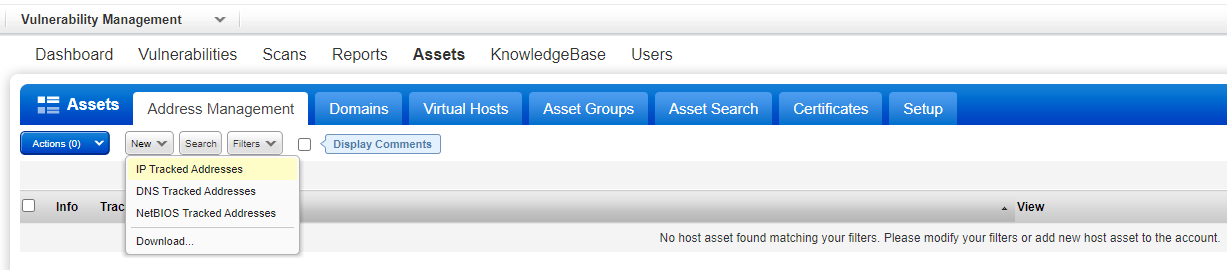
If it is successfully set up and connected, you will see your appliance under the **Appliances** tab in the Qualys Web Dashboard.



Next, We need to select the IP range that Qualys will be scanning. While in the Qualys Cloud Dashboard, click on Assets and then on **Add IPs for Scanning**



Next, click on New then click on IP Tracked Addresses

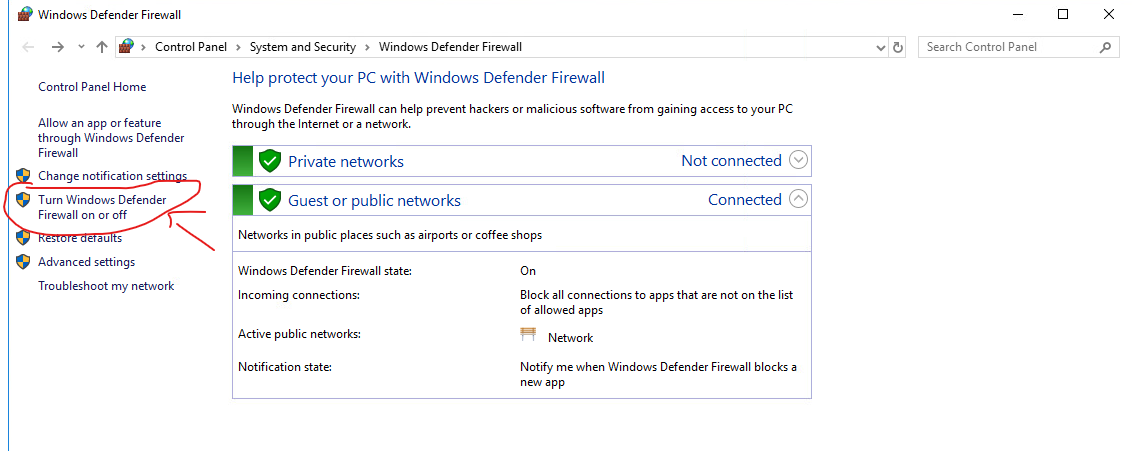


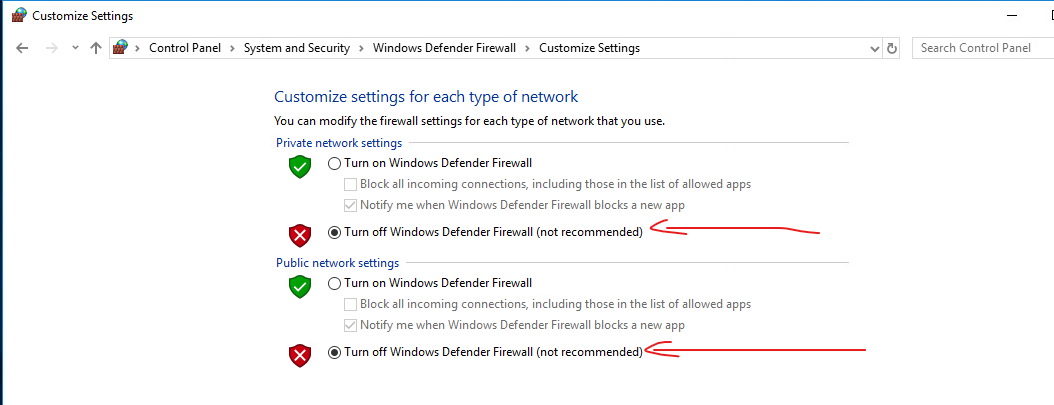
Next, go to subscription IPs and enter the IPs range you want to scan.

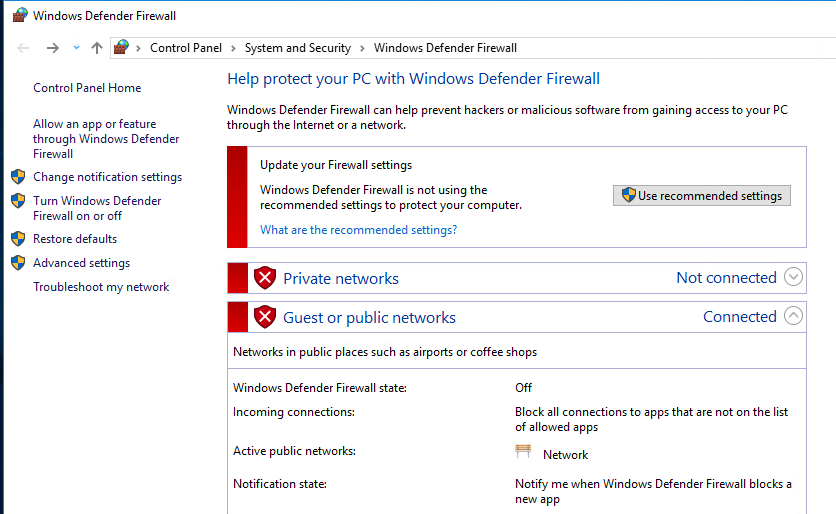
Ensure the Windows 10 Pro host is within the scanning range initially configured. Otherwise, you can manually assign a static IP to the machine within the scanning range. ( Window 10 Pro —> Network and Internet —> Network and Sharing Center —> Ethernet —> Properties —> Internet Protocol Version 4 (TCP/IPv4)) —> Properties —> Use the following IP address:) [You can ping the host from your main computer to make sure the IP assigned is working ]

While you are on a Windows 10 Pro machine, make sure the firewall is not going to block the scanner's IP. Since it is a built-in device firewall, I would simply just turn it off for this lab. ( We are disabling the firewall mainly for this lab. Otherwise, in a professional environment, this would not be recommended)

Window 10 —> Search and click on: Windows Defender Firewall —> Turn Window Defender Firewall On or Off —> OK

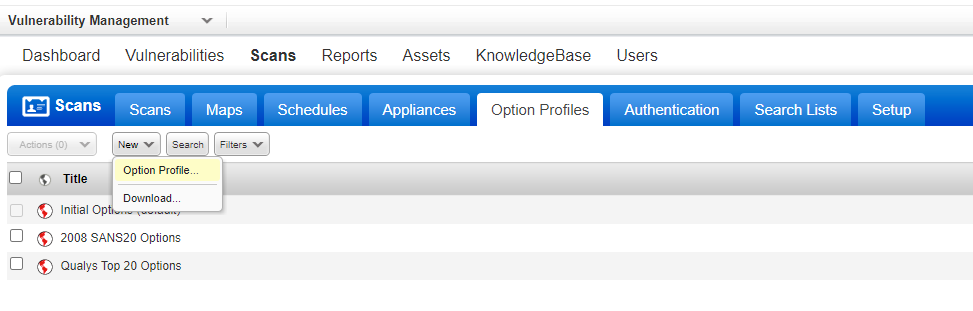






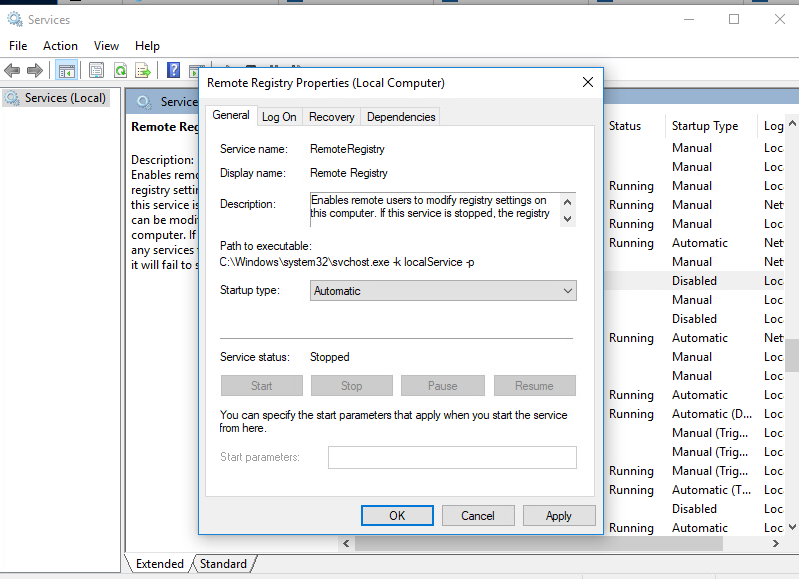
Turn off the built-in Firewall on Windows 7 as well.

Now we are ready to scan the host. Go back to Qualys Cloud Dashboard, click on **Scans**, then on **Option Profiles** then select **New and Option Profile**. Provide a name to the scan



On the same page click on Scan below Option Profile Title. Next, let’s set up authentication for the scan. To make sure our scanner can access the registry, we need to make some adjustments on our Windows machines.

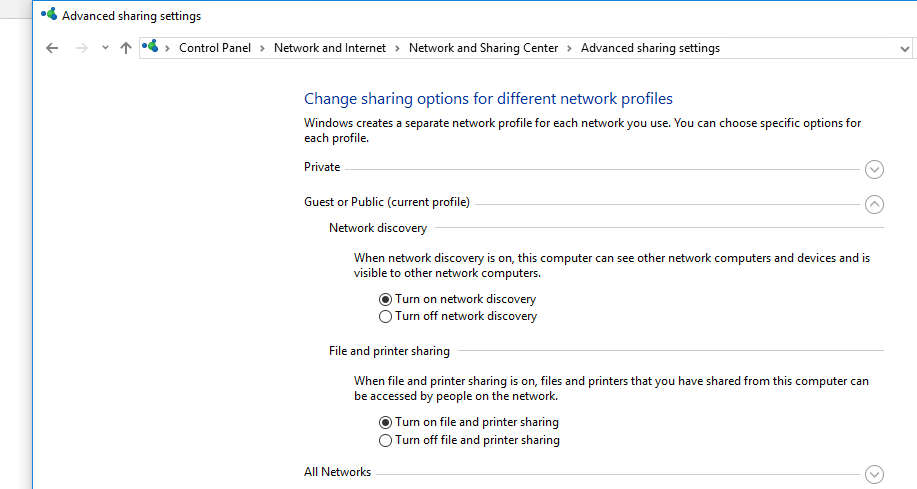
On Windows, go to **Services —> Remote Registry —-> Properties —> Startup Type = Automatic —> Apply → Ok.**



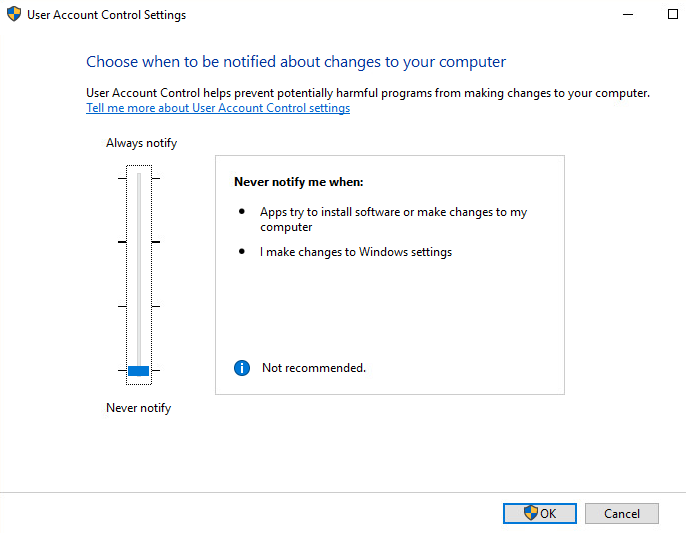
**Remote Registry —> Right-click → Start**

After that, within Services still: **Server —> Properties —> Startup Type = Automatic —> Apply → OK.** Then start it as well

**Next go to Control Panel —> Network and Internet —> Network and Sharing Center —> Advanced sharing settings**. Make sure **“Turn on network discovery”** and **“Turn on file and printer sharing”** are selected.



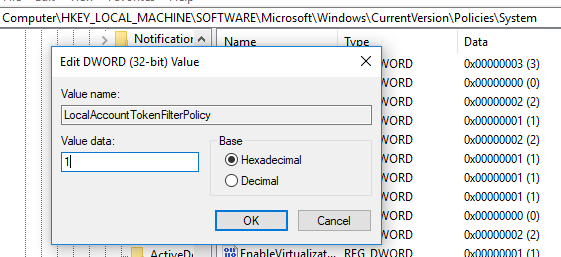
Go to User Account Control Settings and change it to never notify



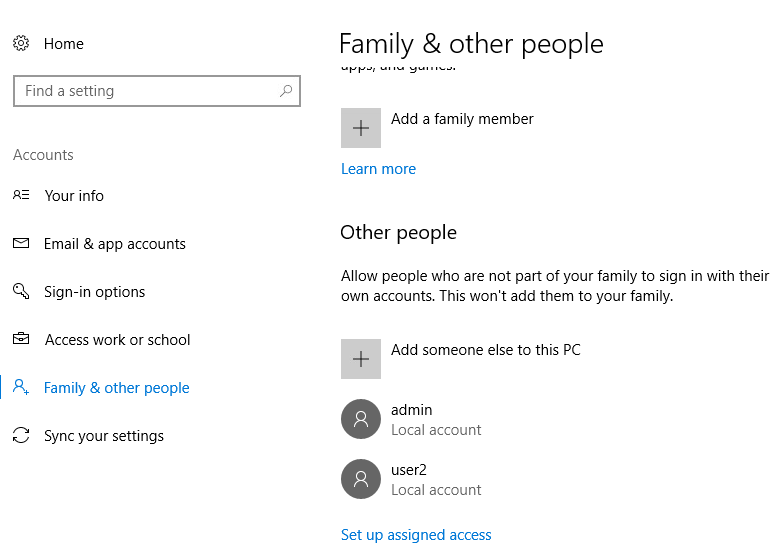
Make these changes in Registry Editor:

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Then right-click → New → Key → DWORD (32-bit) value. Value name = FilterPolicy TokenLocalAccount. Value data = 1

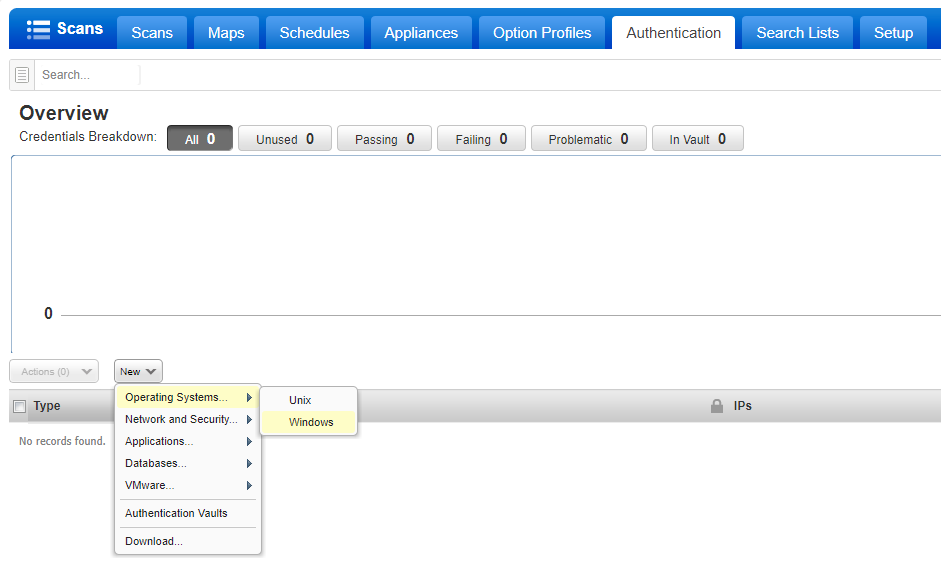


Make sure you have some user profile created in the machine that we will use for the authentication scan. For this lab, I have created 2 users (admin and user1) with simple passwords.

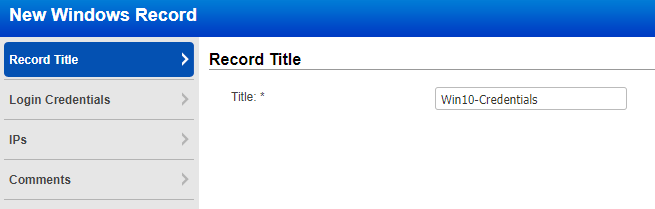


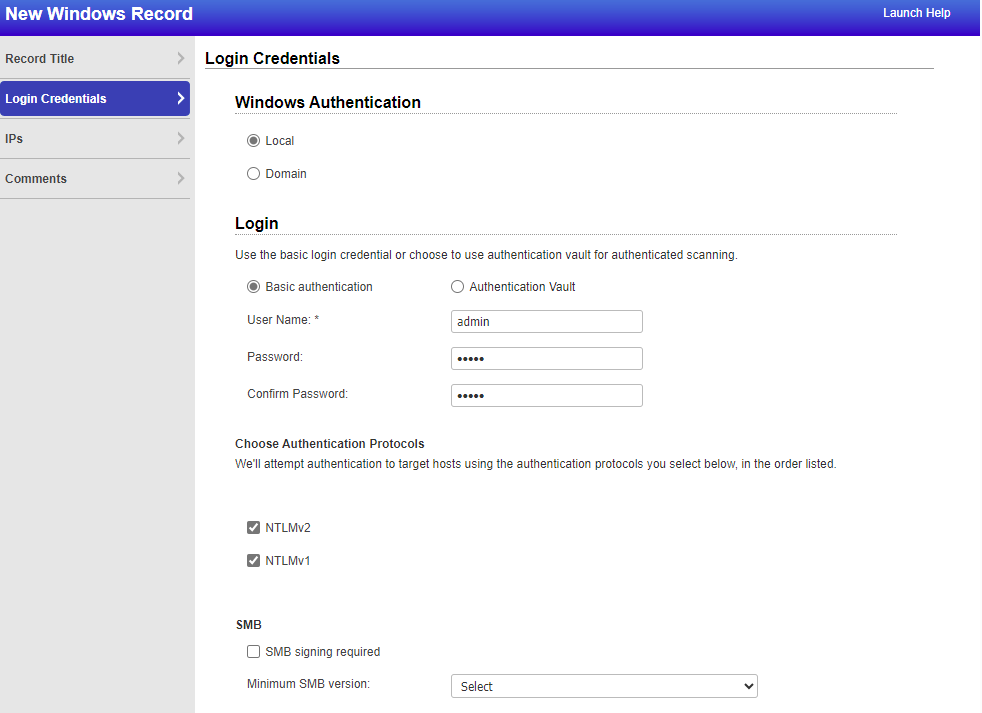
**The machines are now ready for scan.**

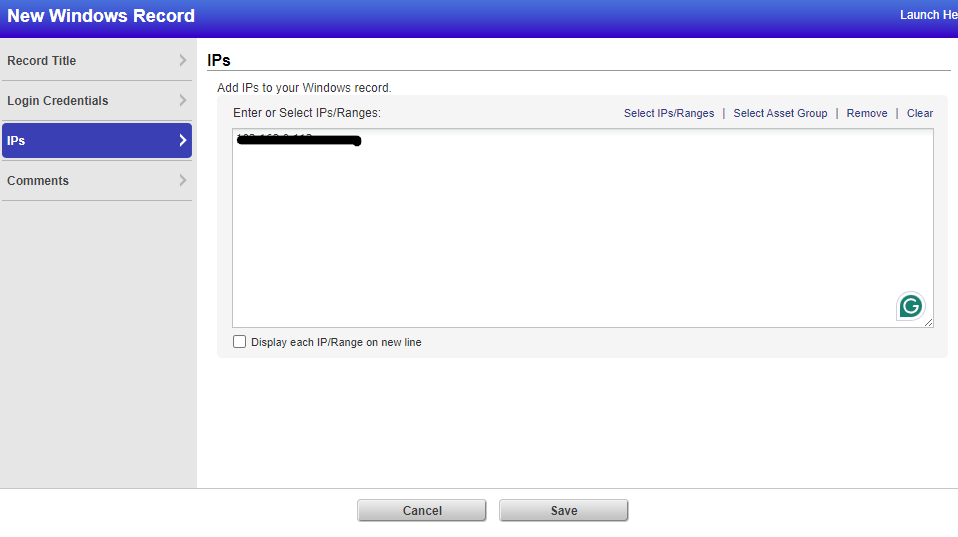
Go back to Qualys and click on **Authentication → New —> Operating System → Windows**



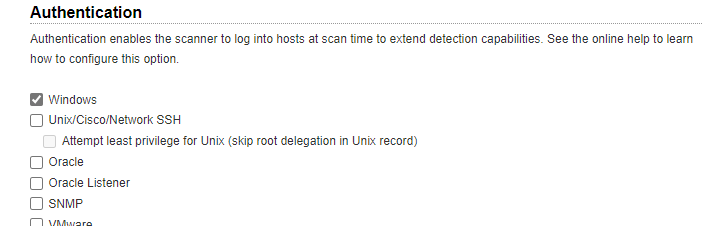
Provide a name and login Credentials and the host IP you are running a credential scan against.

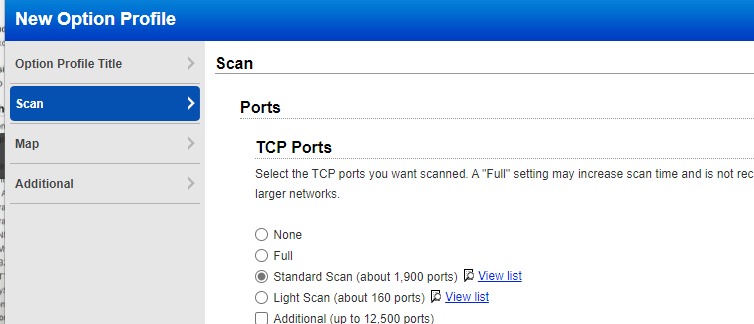




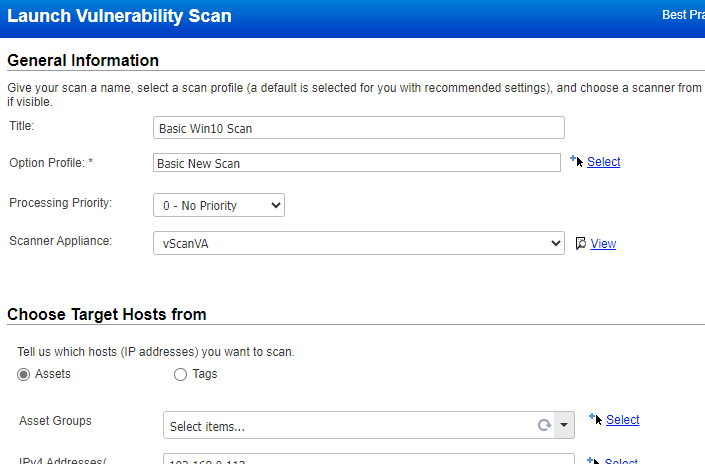


Now go back to Option Profiles in Qualys, click on the profile you created earlier, and make sure “Windows” is selected under Authentication. Hit Save.

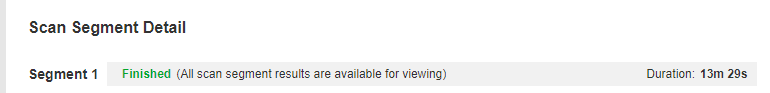




Click Save, go to Scans, and then click New and Scan. Give it a title of your choice. In Option Profile, select the one we created previously. In Processing Priority, leave it unchanged (0 - No Priority). Scanner Appliance, select the appliance (virtual scanner) initially created. Under IPv4 Addresses/Ranges, you can provide the IP of the devices you want to scan. Then hit Launch

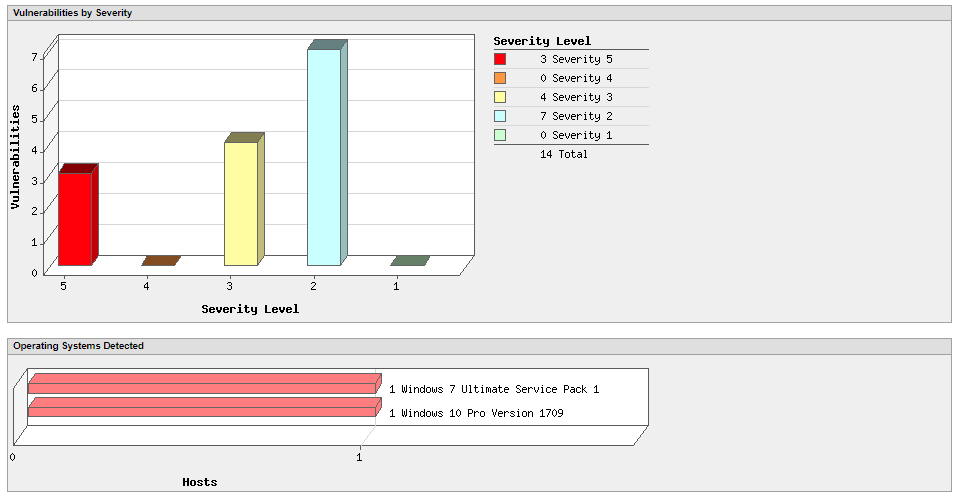


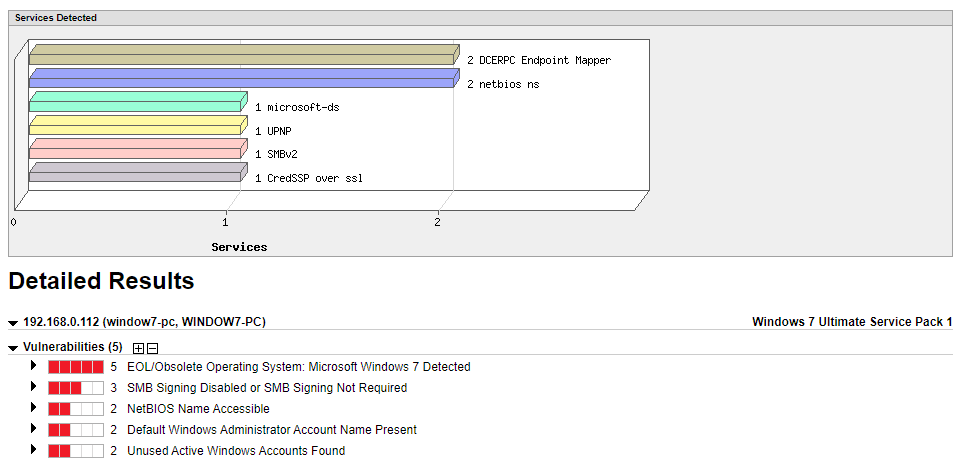
We now just have to wait for the scan to complete.

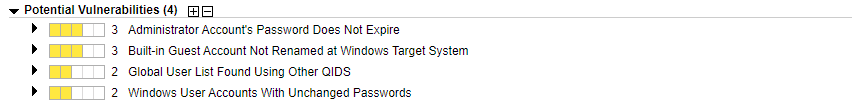


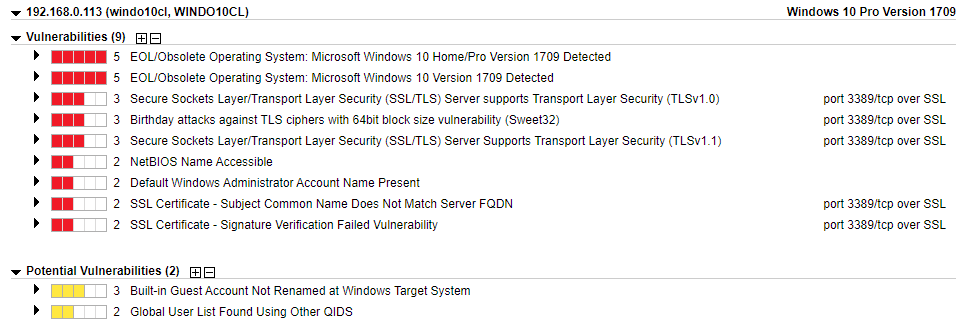
Scan results:





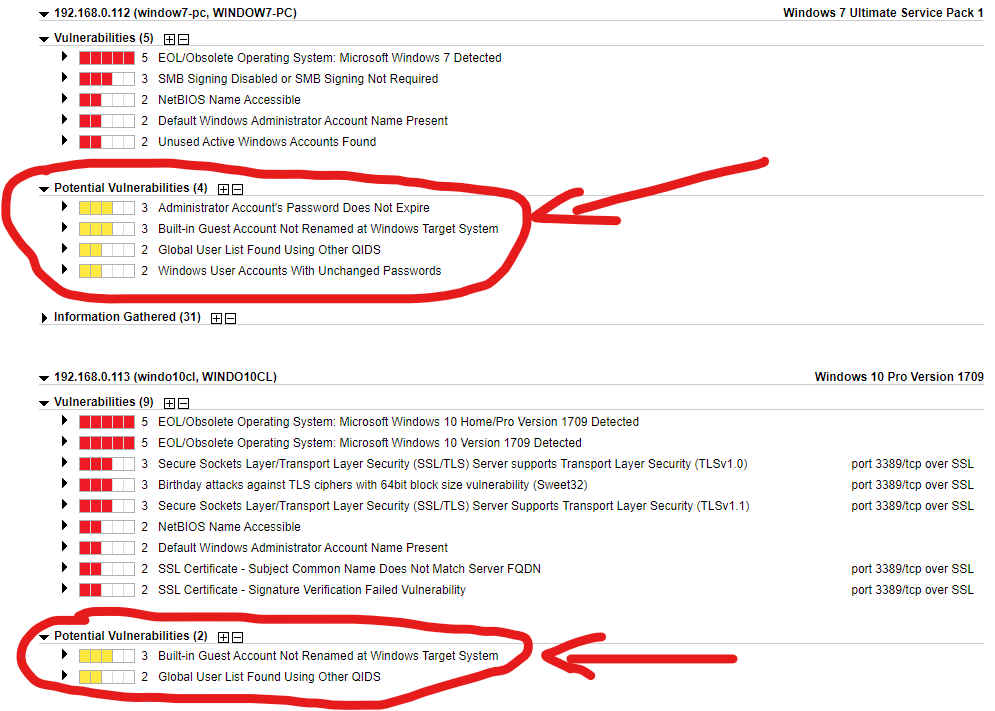






**Remediation of few vulnerabilities:**

On both devices, let’s resolve some vulnerabilities including the one circled in red in the screenshot below.



**Let’s rescan the host after remediation.**

You can see from the result below that some of the vulnerabilities detected previously are no longer showing up on the hosts after being rescanned. We went from **93** vulnerabilities to **61** after mitigation and rescan.

