**Vulnerability Management with Nessus (LAB)**

**Objective:** The purpose of this lab is to implement vulnerability scanning and vulnerability remediation on a sandbox windows 10 host and network. Vulnerability scanning and vulnerability remediation are the two main steps in the Vulnerability Management Lifecycle, this lab will cover the configuration of Nessus Essentials to scan local VMs hosted on VMware (player) workstation in other to run non-credential scans to start as well as credentialed scans to discover vulnerabilities, remediate some of the vulnerabilities, then perform a rescan to verify remediation.

**Tools**: Nessus Essentials, VMware Player, Windows 10 ISO, old software versions.

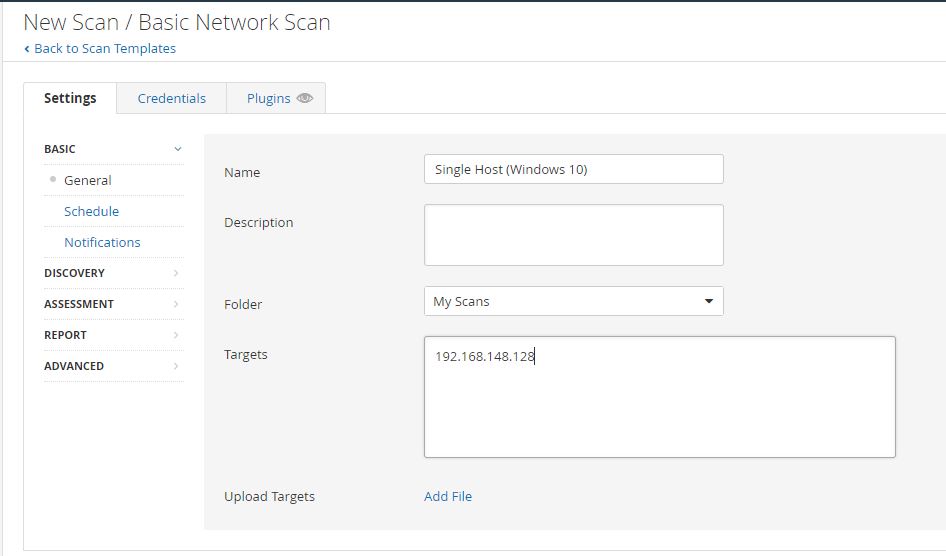
**Virtual Machine Configuration**

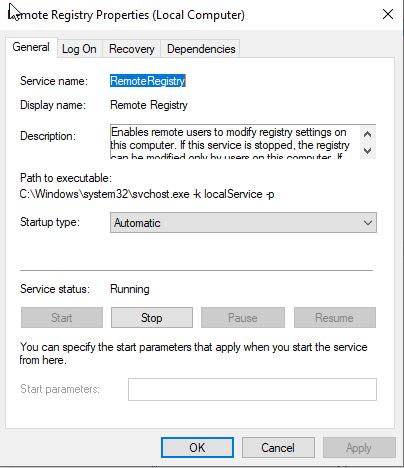
Ping request
Using VMware Player, a virtual machine will be configured with windows 10 ISO to mount/install the windows operating system, which is going to be scanned by Nessus for vulnerabilities. To have the ability to scan the VM using Nessus scanner; ipconfig command will be executed to grab the IPv4 address associated to the VM, to ping from the local machine (not the VM).

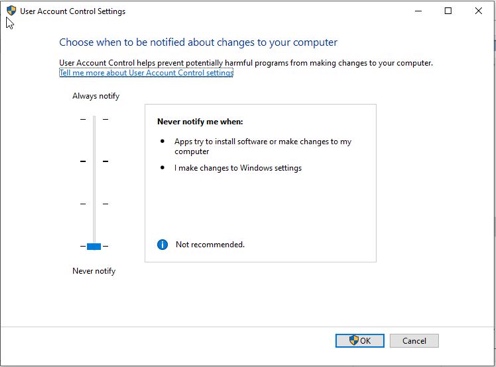
As you can see from the screenshot above the ping requests times out, which means the VM is unreachable. To fix this, windows firewall on the VM will need to be disabled; yes, this is not ideal in a production environment, but to demonstrate the use of Nessus scanner, windows Domain profile, Private profile, and Public profile will be disabled. After disabling the Firewall on the VM, we can notice the ping going through on the local computer.

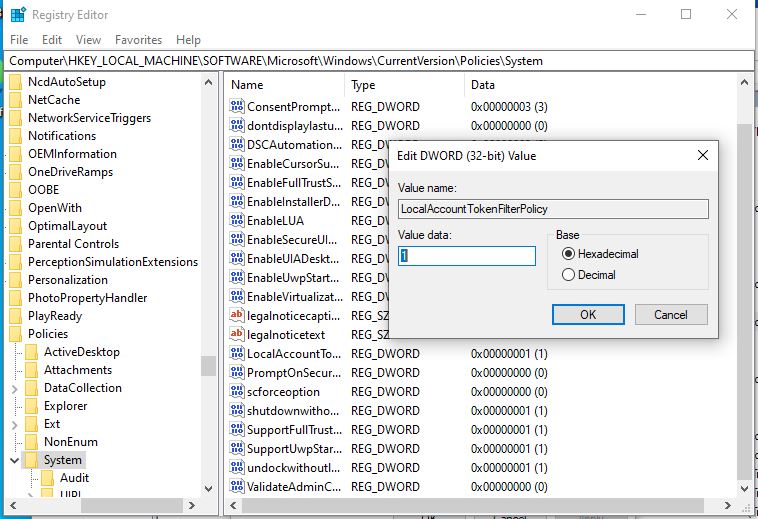
**Nessus Configuration**

After the installation and initialization of Nessus Essentials, the configuration of a basic network scan will be done.



A screenshot of a computer

Description automatically generatedThe first scan execution will be a non-credentialed scan, which is a basic network port scan, to make sure we can scan the VM to get some results (the credential tab of our new scan will not be configured for this section). For credentialed scans, the credentials tab as seen in the image will be configured with an addition of the windows username and password. Because the host is not on a domain, some not so ideal hacks will be done to enable the scan for Nessus; First remote registry will be enabled to allow the scanner to connect to the VM’s registry to crawl through and identify insecure configurations, next network discovery file and printer sharing will be turned on, user account control settings will be 

modified, lastly a key (DWORD) will be added to the computer’s registry; **LocalAccountTokenFilterPolicy** key, which further disables user account control for the remote account so the remote used to connect can connect to VM.

The key will be added to HKEY\_Local\_Machine\Software\Microsoft\Windows\CurrentVersion\Policies\System. Also, old versions of Firefox and Google Chrome will be installed to test if they get picked up by Nessus. After all configurations are complete, we can run some scans!

**Non-Credential Scan Results**

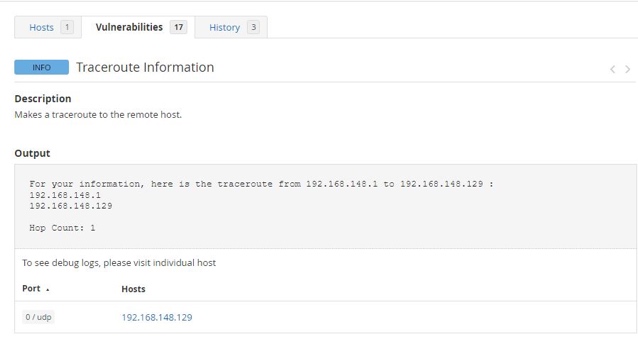
Non-Credential Scan
A screenshot of a computer

Description automatically generated  
As you can see from the screenshot above, the non-credential scan did not produce as much when it comes to Critical and High vulnerabilities. 96% of the scan are informational, while 6% are Medium for a total of 17 vulnerabilities detected on the host machine.

A screenshot of a computer

Description automatically generated

To provide a deeper look into the highest vulnerability on the non-credential scan; from the screenshot the name of the vulnerability is provided, a description, and solution. To the left more information like plugin details, risk information, and vulnerability information.

The non-credential scan had a lot more vulnerabilities listed as “Info”; which could not necessarily be a vulnerability but just information you should be aware of, for example, traceroute information, OS Identification, ICMP Timestamp Request etc. A screenshot of a computer error

Description automatically generatedA screenshot of a email

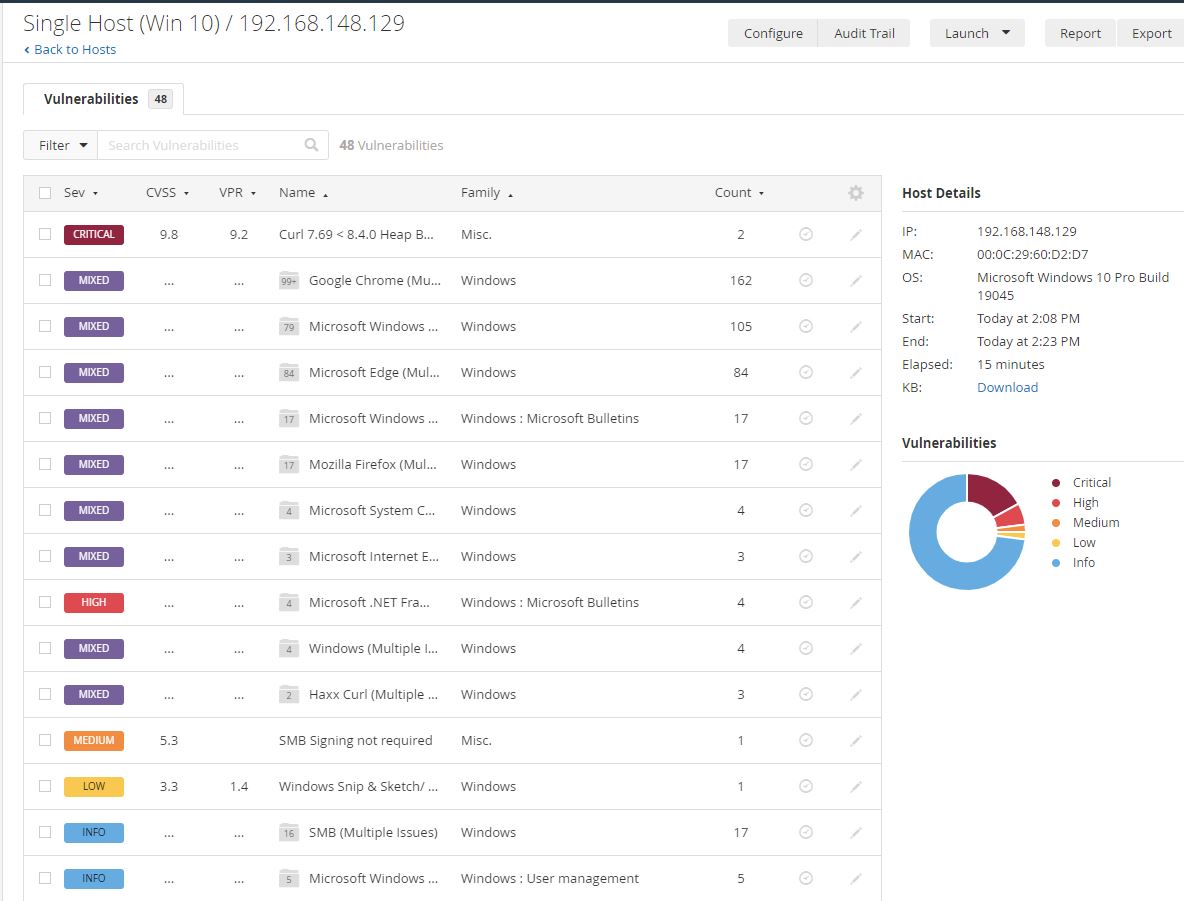
Description automatically generated

All Info vulnerabilities might not be dangerous, but they can be used by attackers to gain passive reconnaissance on an environment.

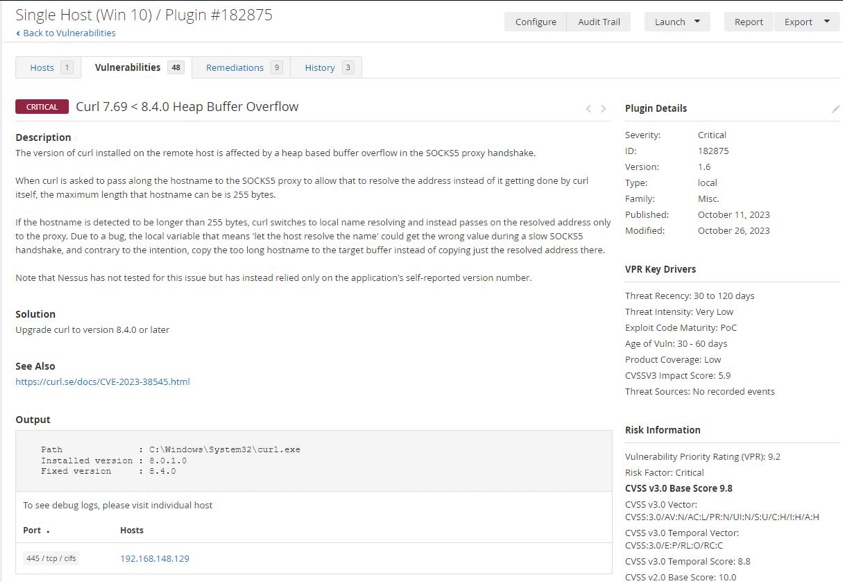
**Credentialed Scan Results**

A screenshot of a computer

Description automatically generated



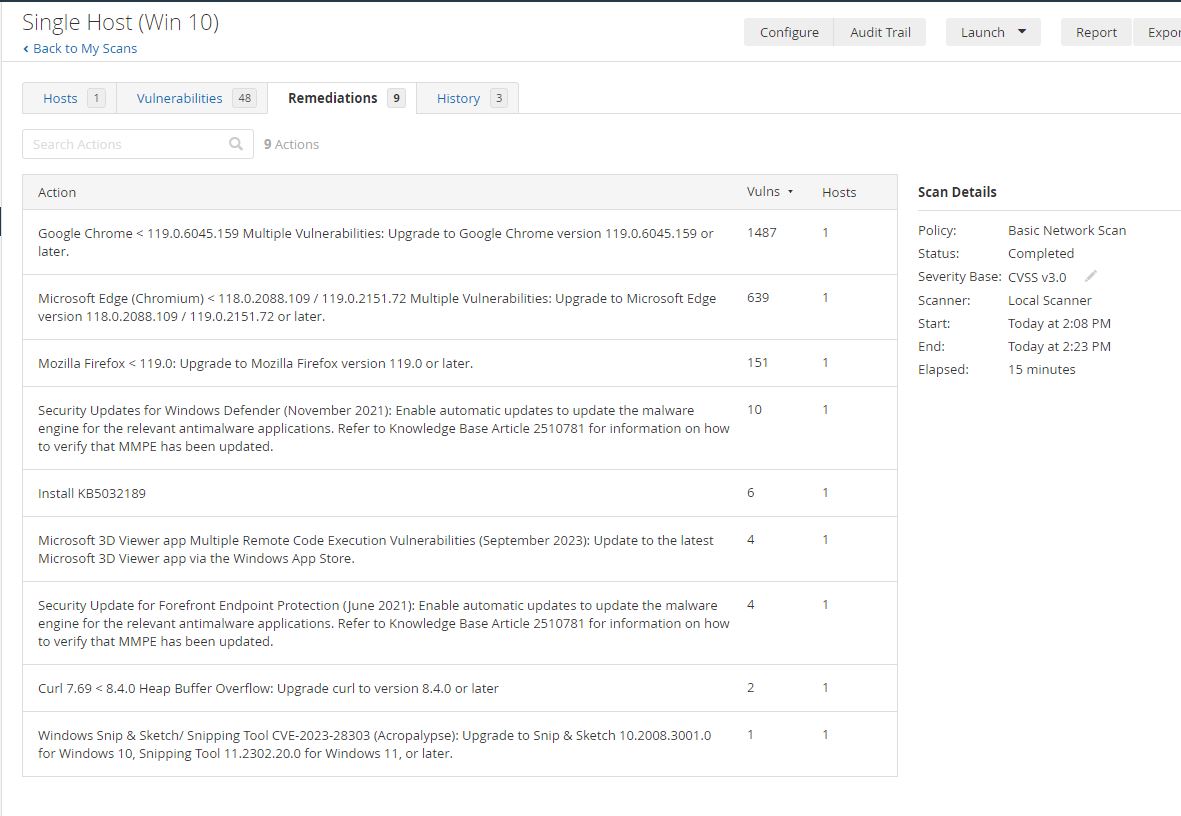
A screenshot of a computer

Description automatically generated****A screenshot of a computer

Description automatically generatedA screenshot of a computer

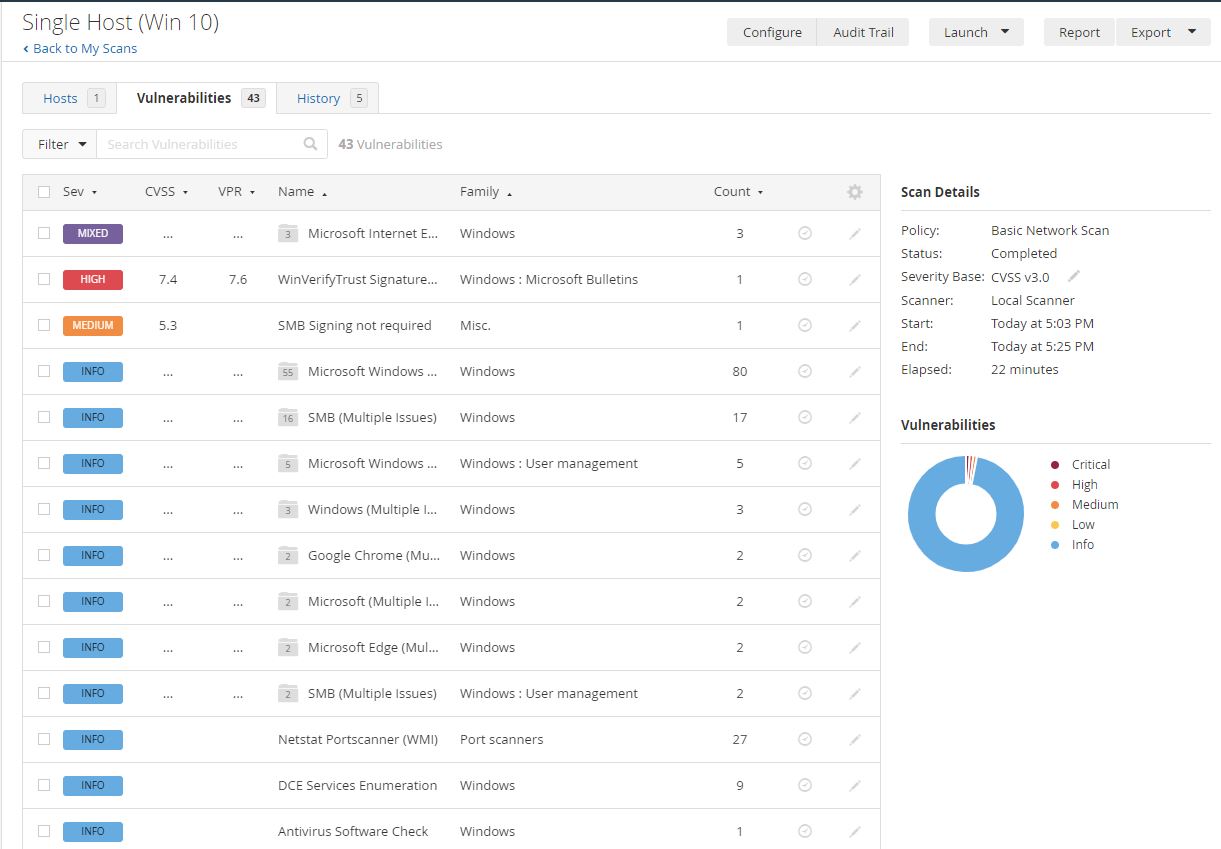
Description automatically generatedAs you can see from the screenshot above, the credentialed scan produced a lot more vulnerabilities; 18% critical, 50% high, 4% medium, 28% info. We can detect vulnerabilities caused by the installation of the older versions of Chrome (162 vulnerabilities majority are critical) and Firefox (17 vulnerabilities half are critical), vulnerabilities caused by the lack of windows security updates can be detected, which could be the remediation for most of the windows and Edge vulnerabilities detected by the scanner, one vulnerability caused by an older version of curl, which came standard with the VM.

**Remediation**

****

Looking at the Remediation tab of the last scan, we can see recommendations to update Google Chrome, Microsoft Edge, Firefox to the latest versions. Security updates that can be remediated by executing windows updates. If this was done in an organization, first step will be to have an automated third-party patching and windows operating software patching tested and deployed to executes in regular intervals to remediate vulnerabilities that can be easily fixed by automated patching. For the lab, to remediate most of the critical vulnerabilities, Firefox, chrome and edge will be updated to the latest versions, windows updates will be executed, and a third a final scan will be done to show the results.

A screenshot of a computer

Description automatically generated

After remediation of the critical vulnerabilities discovered from the previous scan, we can see from the screenshot above the amount of critical and high vulnerabilities have been reduced to a low significant amount.

**Conclusion**

The objective of the lab was to display what Vulnerability management is, the core components being scanning an environment, endpoint, or network for vulnerabilities and remediating those vulnerabilities to have low possibilities of an attacker gaining access to the environment. Yes, a lot more goes into Vulnerability managements, in a big organization there will be standards, policies, and procedures created for the process, also meetings will be held to bring all participating departments to work with individual groups, to get credentials for all individual resources or the use of a domain account will be utilized to scan the environment. It could get complicated in a real-world scenario, but this lab shows the guts of vulnerability managements, which is to scan and essentially remediate vulnerabilities. Automation can or will need to be used to update third party apps and windows/system updates. The use of automation brings the fact that secure build standards must be tested and checked for remediation to secure the environment enough before deployment into the production environment.