

Vulnerability Management 101

Key Contributors: Garrett Stokes



4/26/2022

EXECUTIVE SUMMARY

Vulnerability assessment and remediation plays a huge role in the cyber world today, and it is my goal within this project to become better acquainted with this concept. There are numerous vulnerability scanning applications, as well as numerous ways to minimize and reduce vulnerability. In this project, I will be using the vulnerability scanner Nessus. Using virtual machines set up on a Nat network, I will run vulnerability scans and remediations of those vulnerabilities. This project is aimed to increase my scope of knowledge in the field, by increasing my skill level using Nessus essentials on a deprecated virtual machine to assess and remediate vulnerabilities within it. I will be able to resorb this information as I graduate and enter the working field, being able to bring this kind of knowledge to those who need it.

Project Milestones:

1. Setup network, Install Nessus essentials, configure target VM's for scanning
2. Perform uncredentialed and credentialed scans on a target Windows 10 and Windows XP
3. Assess vulnerabilities and remediate them

Deliverables:

1. Setup for uncredentialed/credentialed scans
2. Uncredentialed/credentialed scan results
3. Vulnerability remediation

Professional Accomplishments:

1. Vulnerability assessment / remediation
2. Develop Virtual machine expertise
3. Develop Nessus essentials expertise

REASONING FOR CHOSEN VMS AND SCANNING SOFTWARE

I chose to use Nessus as a scanning software, as it is extremely popular and efficient, and covers a very wide range of vulnerabilities in comparison to other scanners such as OpenVAS. It is one of the most deployed vulnerability assessment solutions across the cyber industry. Because of this, practicing with it

and using it for this project would prove to be a worthwhile skill set to develop for the sake of my future career in cyber.

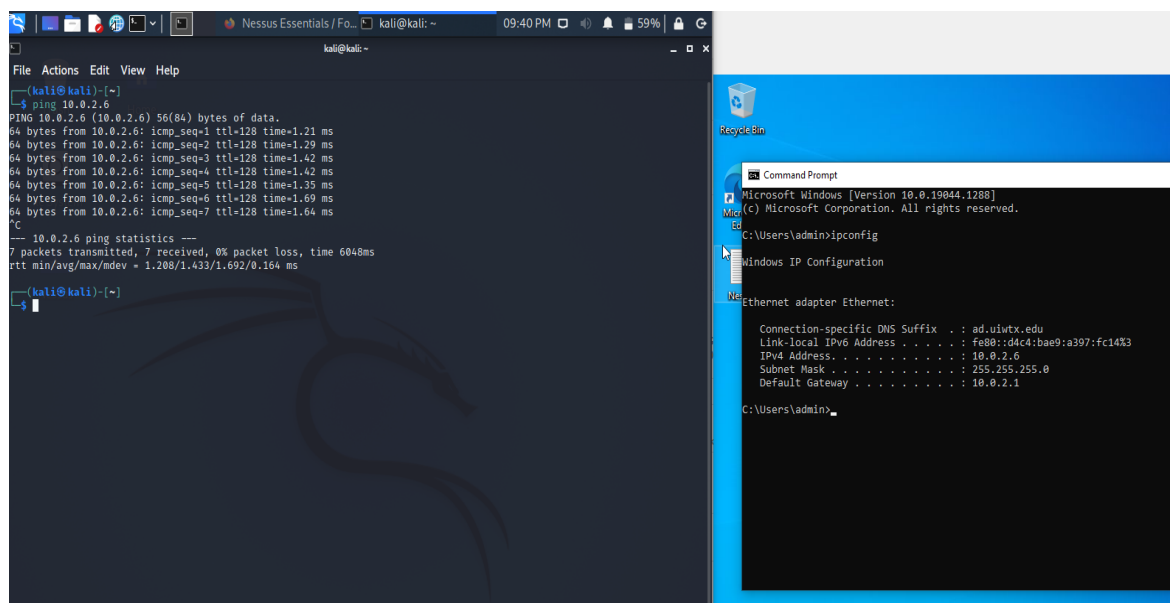
Windows 10 is a very popular OS today and is used primarily by companies in the United States. Because of this, scanning and remediating vulnerabilities within a newer OS like Windows 10 is relevant, since it is so popular. That also goes without saying that seeing the number of vulnerabilities and newer OS like this can have is quite eye-opening.

Windows XP is a legacy OS and is currently unsupported. Seeing that some still use older systems like this, it is worthwhile to look at the vulnerabilities and possible remediations it might present. It also is important in showing the constantly growing field of cyber, as it has many more vulnerabilities since it is an older unsupported system, but in 10 to 15 years, Windows 10 will look much like Windows XP looks now.

PROJECT SETUP

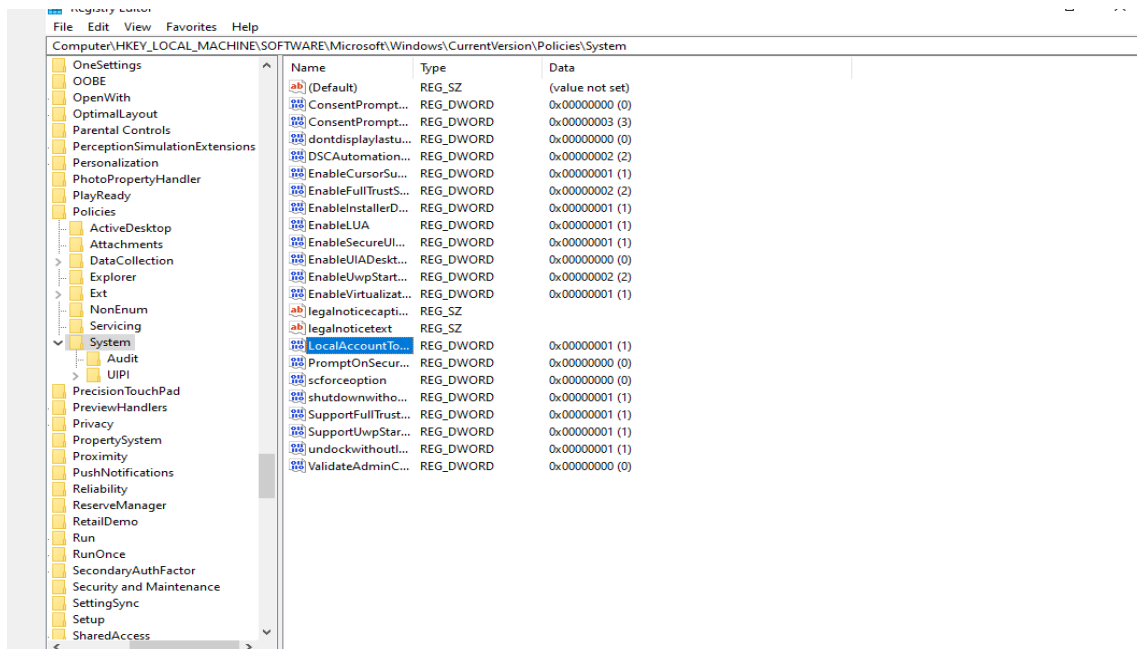
The setup portion for this project consisted of the installation of the target VMs, Windows 10 and Windows XP, as well as the Kali-Linux VM which was used to conduct the scans using a pre-installed Nessus Essentials application. All of the VM's were connected to a virtualbox NAT network, allowing the virtual machines to communicate. At this point, all that had to be done was the scan creation of the target VM's on the Nessus application. Credentialed scans required some configuration of registry values on Windows 10 VM, as well as some configuration of the registry files, sharing settings, and permissions on the Windows XP VM.

Below will be attached screenshots which will highlight the setup for this project.



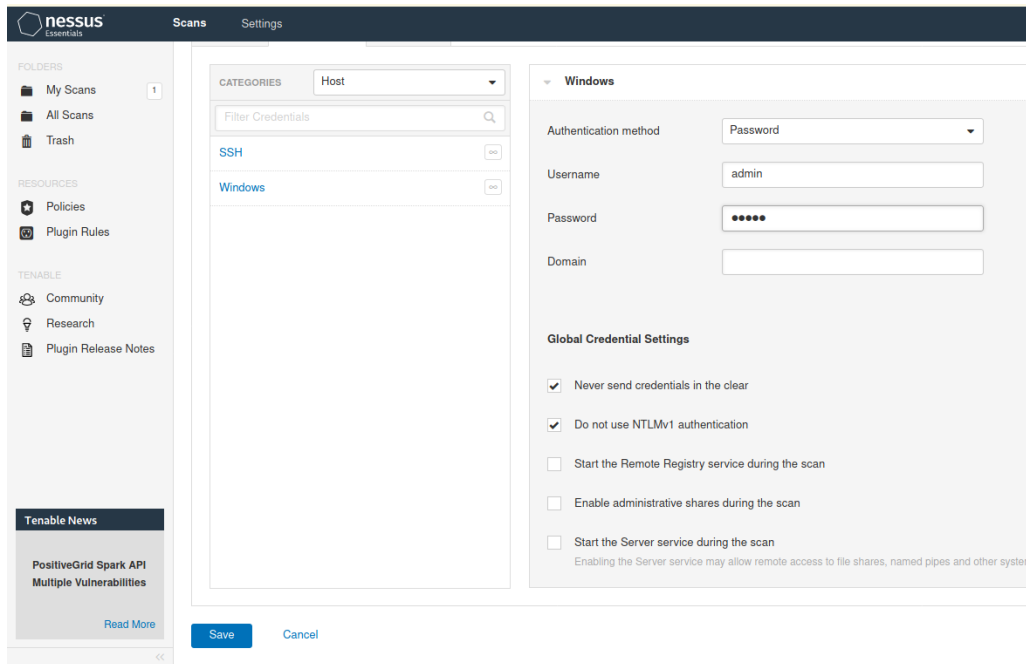
Ensuring connectivity of Kali VM to Windows 10 VM

This was phase one. In the left pane, we have the Kali-Linux machine with Nessus preinstalled, pinging the Windows 10 virtual machine seen on the right pane.



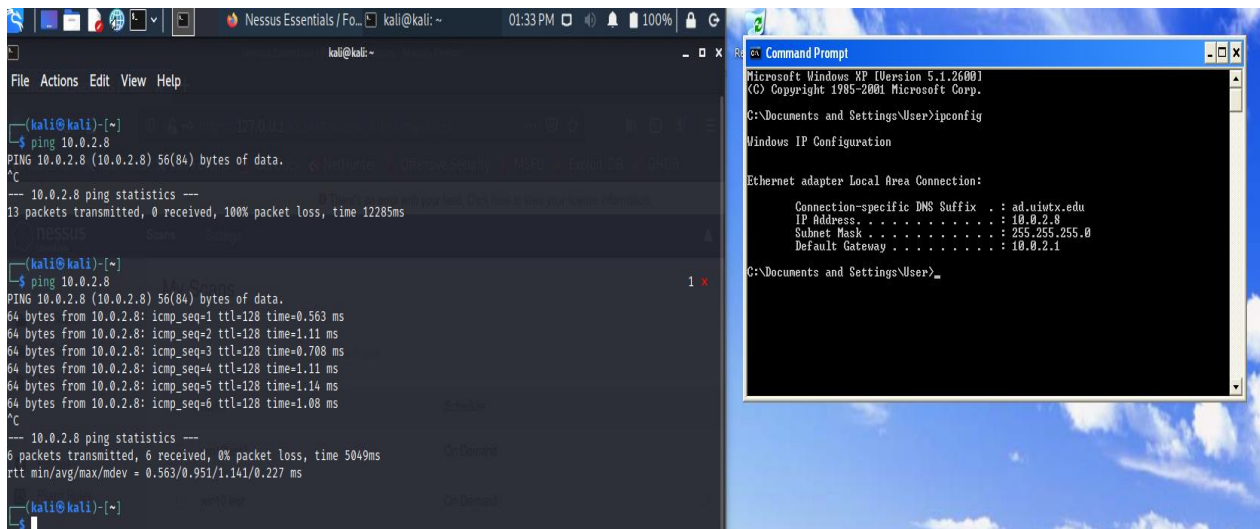
Editing LocalAccountTokenFilterPolicy registry value dword to allow for credentialed scanning on Windows 10 VM

Here I am in the Windows 10 registry, editing the dword value of the LocalAccountTokenFilterPolicy in the windows registry, which will allow for remote access to the virtual machine. This allows us to credential scan the target VM from our remote host, Kali-Linux.



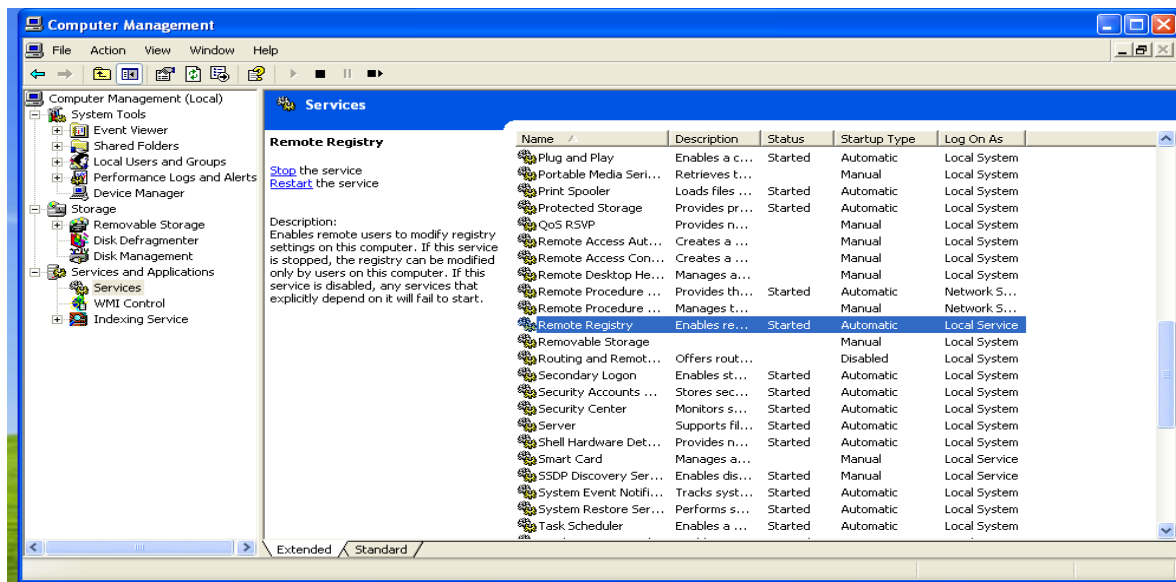
Configuring Nessus for Credentialed scan on Windows 10 VM (same process was applied for Windows XP Credentialed scan).

Nessus must be configured to run a credentialed scan, which is what is depicted here. All that must be done is provide the username and password of the target VM, and the credentialed scan is ready to be run if the proper setup was achieved on that target VM. I achieved this setup in the prior steps.

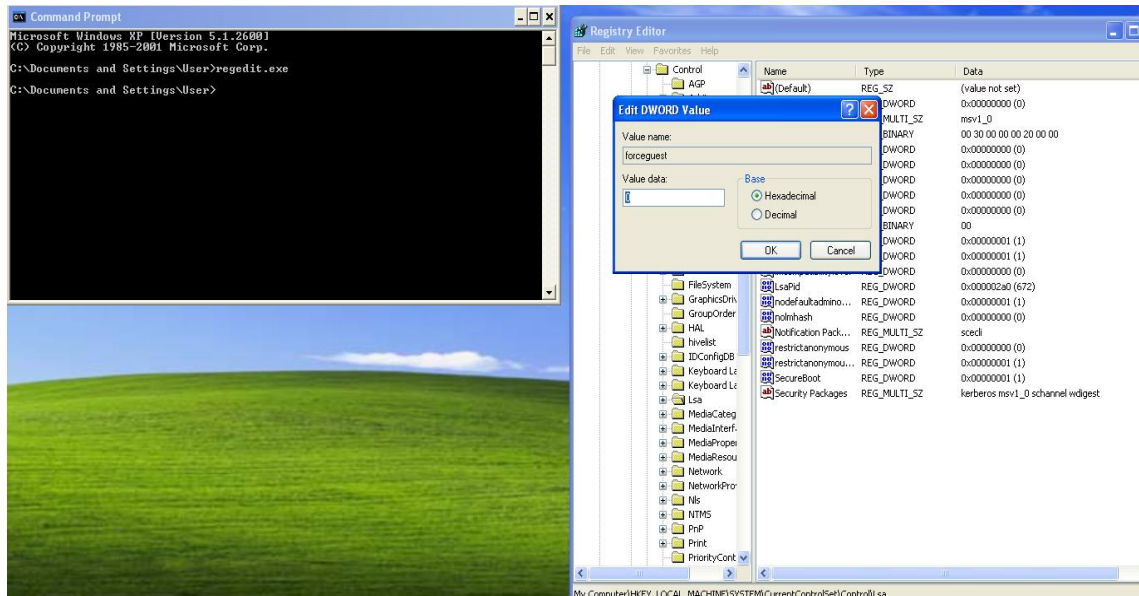


Ensuring connectivity of Kali VM to Windows XP VM

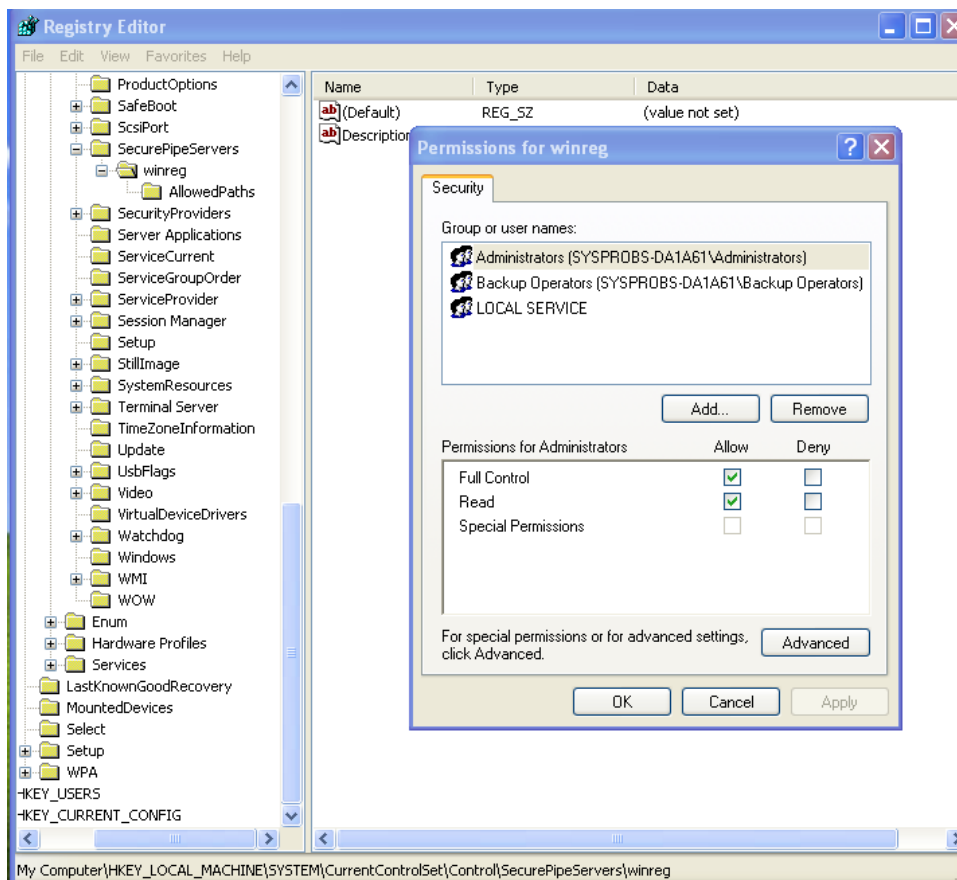
Here I ensure connectivity between the Kali-Linux VM and the Windows XP VM. This process was the same as the Kali – Win 10 setup.



Enabling remote registry...



Enabling WMI by changing DWORD value...



Altering registry access configuration of permissions to User...

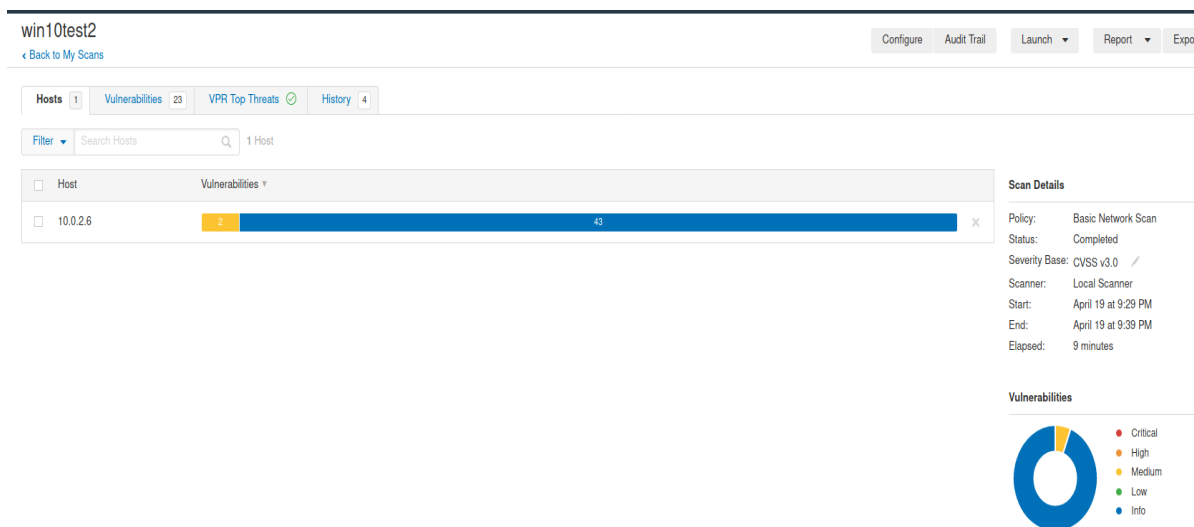
Above are the three individual steps I took on the Windows XP to allow for remote scanning. First, was the enabling of the remote registry, which allows a remote system to view and modify the registry of the Windows XP VM. Next is the enabling of the Windows Management Instrumentation, with the purpose to help administrators manage different Windows operational environments, including remote systems. Finally, is the WinReg edit that allows correct permissions for remote access. The user must have correct permissions for me to perform a credentialed scan using user credentials.

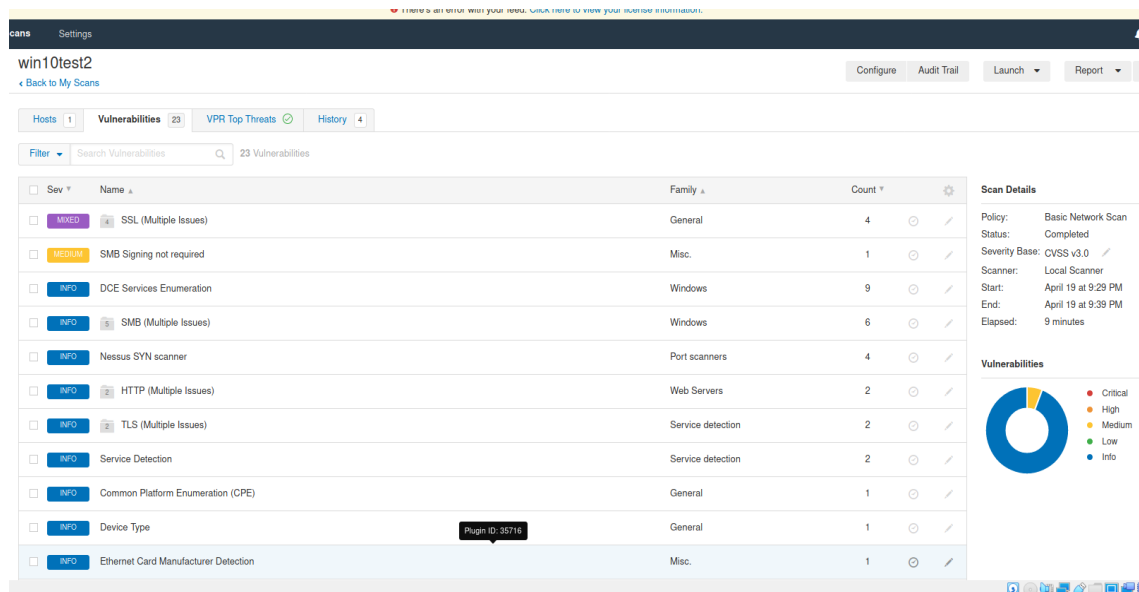
SCANNING RESULTS

To begin scanning, I started with the Windows 10 VM. First, I ran an uncredentialed scan on the stock OS, to see what it was looking like from an outside perspective. A few vulnerabilities came back, but nothing shocking. Of course, after this, I moved on to the credentialed scan, and not surprisingly many vulnerabilities were uncovered in comparison to the uncredentialed scan. This still was not enough for me, however, so I installed a really old version of Firefox and ran the scan back. This time there was many more vulnerabilities than the first credentialed scan. After remediation, I ran another scan to make sure the same vulnerabilities were not still present.

For Windows XP, the process was the same. I began with an uncredentialed scan, but just from this there were already many vulnerabilities found, large in part since Windows XP is such an outdated and vulnerable system. After I performed the credentialed scan. This uncovered a sickeningly large number of vulnerabilities, not surprisingly. Like the Windows 10 scan process, I ran a scan after remediation, and downsized the amount of vulnerabilities substantially.

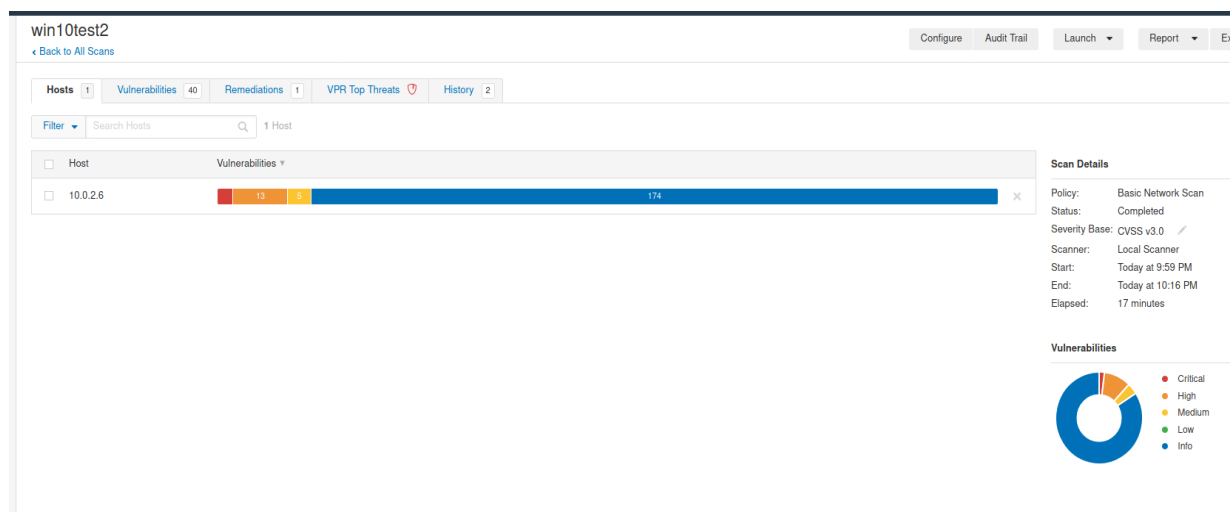
Below will be attached photos and descriptions of the scanning process (not including remediation scans)





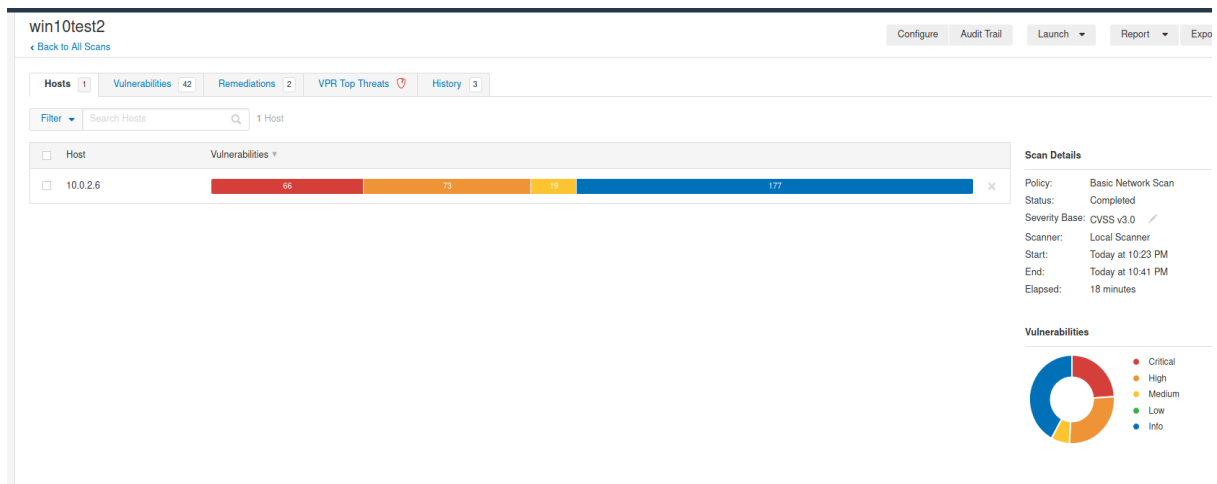
Windows 10 VM uncredentialed scan highlights and vulnerabilities list

Here I completed the first scan of the Windows 10 VM, performing an uncredentialed scan. As seen in the picture, not many vulnerabilities were found. This is regular as an uncredentialed scan is not nearly as effective as a credentialed scan. Imagine a thief planning to perform a robbery. If the thief does a quick scan looking at the target house from the outside, they will not actually know what will be within the house, they can only judge the value of what will be inside by the look of the house from outside. This is like an uncredentialed scan. Now imagine the thief had access to the house they were going to rob. They can see the most valuable items within the house and will have a much better understanding of what they are going to rob. This is like a credentialed scan.



Windows 10 VM credentialed scan highlights

Here I did a credentialed scan of the Windows 10 VM and uncovered a good amount more vulnerabilities than I did in the uncredentialed scan. This however was still not enough vulnerabilities for me to be satisfied.



win10test2

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 42 Remediations 2 VPR Top Threats History 4


Filter Search Vulnerabilities 42 Vulnerabilities

Sev	Name	Family	Count
MED	Mozilla Firefox (Multiple Issues)	Windows	148
MED	Microsoft Windows (Multiple Issues)	Windows : Microsoft Bulletins	6
MED	Microsoft Windows (Multiple Issues)	Windows	79
MED	SSL (Multiple Issues)	General	4
MEDIUM	SMB Signing not required	Misc.	1
INFO	Netstat Portscanner (WMI)	Port scanners	28
INFO	SMB (Multiple Issues)	Windows	16
INFO	DCE Services Enumeration	Windows	9
INFO	Microsoft Windows (Multiple Issues)	Windows : User management	5
INFO	Service Detection	Service detection	3
INFO	HTTP (Multiple Issues)	Web Servers	2
INFO	SMB (Multiple Issues)	Windows : User management	2

Scan Details

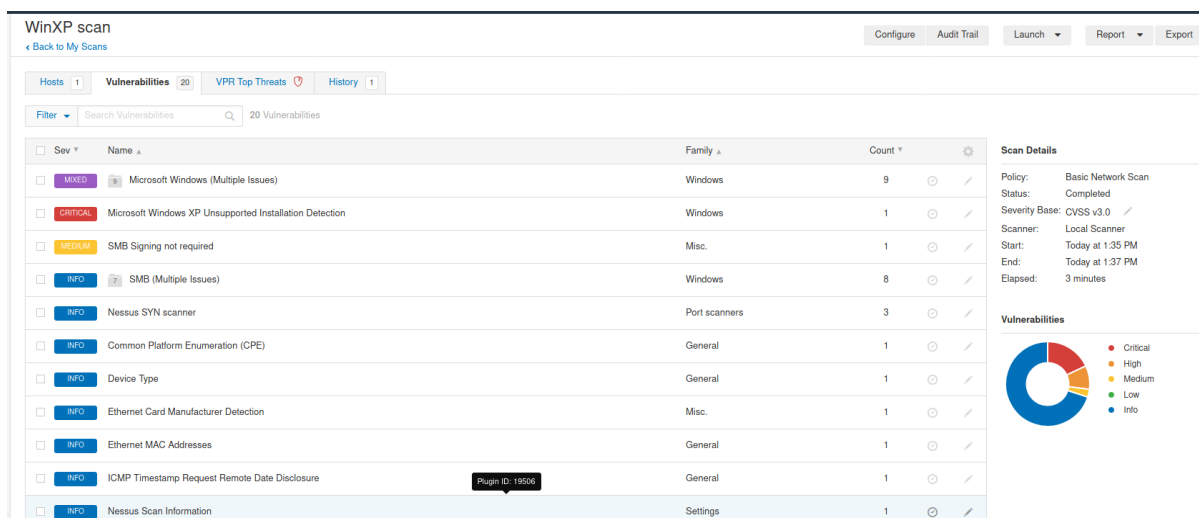
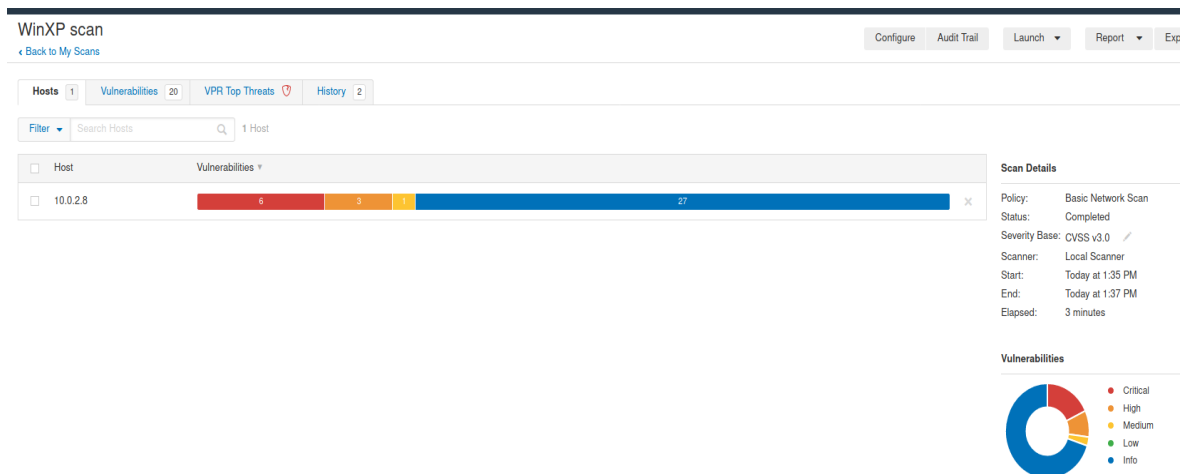
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: April 20 at 10:23 PM
End: April 20 at 10:41 PM
Elapsed: 18 minutes

Vulnerabilities



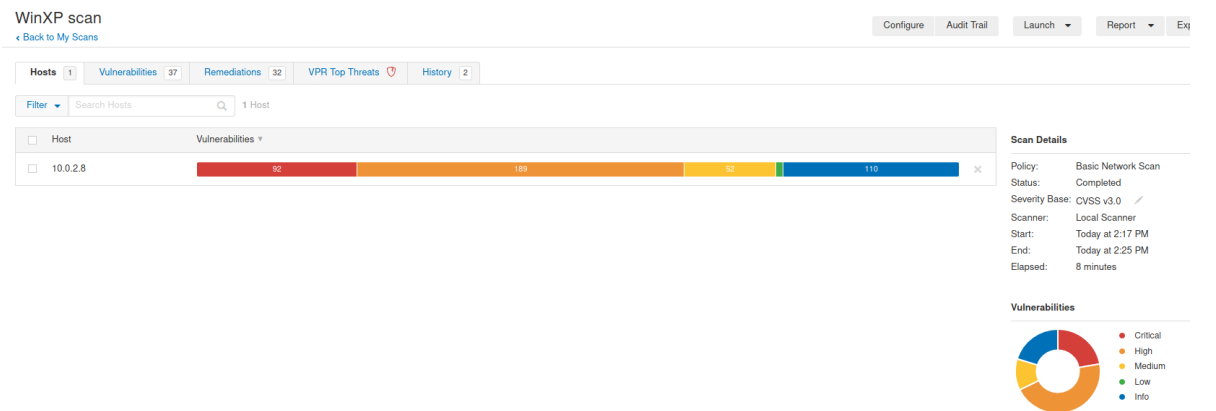
Windows 10 VM deprecated credentialed scan highlights and vulnerabilities list

After installing a deprecated Firefox in the Windows 10 VM, I ran another credentialed scan, and this time the vulnerability list was greatly increased. This is because the deprecated Firefox browser is extremely old and unsafe, and it contains many vulnerabilities, making the entire system vulnerable.



Windows XP VM uncredentialed scan highlights and vulnerabilities list

Moving on to Windows XP, I started with an uncredentialed scan just as I did with Windows 10 VM. This time, with Windows XP, there is many more vulnerabilities than there is with Windows 10, even with an uncredentialed scan. This is because Windows XP is an old and outdated system, that is not even in support anymore by Microsoft.



WinXP scan

← Back to My Scans

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 37 Remediations 32 VPR Top Threats 0 History 2

Filter Search Vulnerabilities 37 Vulnerabilities

Sev	Name	Family	Count	Details
MIXED	Microsoft Windows (Multiple Issues)	Windows : Microsoft Bulletins	203	Details
MIXED	Adobe Flash Player (Multiple Issues)	Windows	98	Details
MIXED	Microsoft Windows (Multiple Issues)	Windows	77	Details
MIXED	Microsoft Internet Explorer (Multiple Issues)	Windows	2	Details
CRITICAL	Microsoft Windows XP Unsupported Installation Detection	Windows	1	Details
CRITICAL	Microsoft XML Parser (MSXML) and XML Core Services Unsupported	Windows	1	Details
HIGH	Microsoft XML Core Services (Multiple Issues)	Windows : Microsoft Bulletins	2	Details
HIGH	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	Windows : Microsoft Bulletins	1	Details
MEDIUM	Macrovision SafeDisc seedrv.sys Crafted METHOD_NEITHER IOCTL Local Overflow	Windows	1	Details

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:17 PM
End: Today at 2:25 PM
Elapsed: 8 minutes

Vulnerabilities

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Green), Info (Blue)

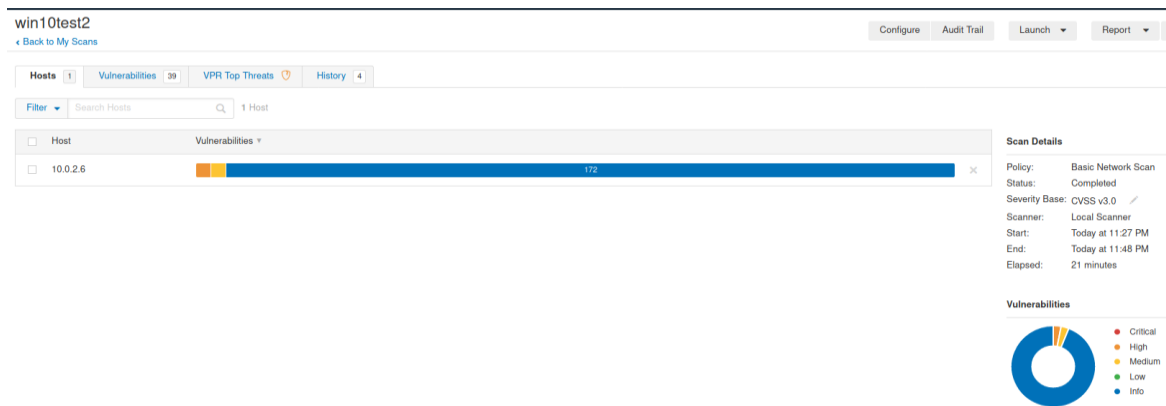
Windows XP VM credentialed scan highlights and vulnerabilities list

Here is the credentialed scan of Windows XP, which is filled to the brim with vulnerabilities. Already full of vulnerabilities with an uncredentialed scan, a credentialed scan unlocks even more vulnerabilities in this weak system of windows XP.

VULNERABILITY REMEDIATION

After vulnerabilities were uncovered, Nessus provides a remediation tab. This tab basically gives you things you can do to get rid of the vulnerabilities present. For windows 10, this basically just consisted of removing the really old Firefox and installing Windows security updates. The process was easy and smooth. For Windows XP, the process was the same, but it was much more tedious and took hours to get figured out. For starters, Internet Explorer, which is the default browser used to install security updates on an XP system, was completely broken. Because of this, I had to install Firefox and install the updates manually, one by one. I also had to install the latest version of Adobe ActiveX supported by XP, which did fix most of the vulnerabilities that were present.

Below I will attach photos of final remediation results as well as describe the remediation process.



Windows 10 VM credentialed scan after remediation (All security updates installed, as well as removal of deprecated Firefox).

Here is the Nessus scan of the Windows 10 VM after remediation, which consisted simply of installing Windows security updates. This process was easy and straightforward, and remediation was complete as seen in the screenshot.

WindowsXP [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Microsoft Update Catalog

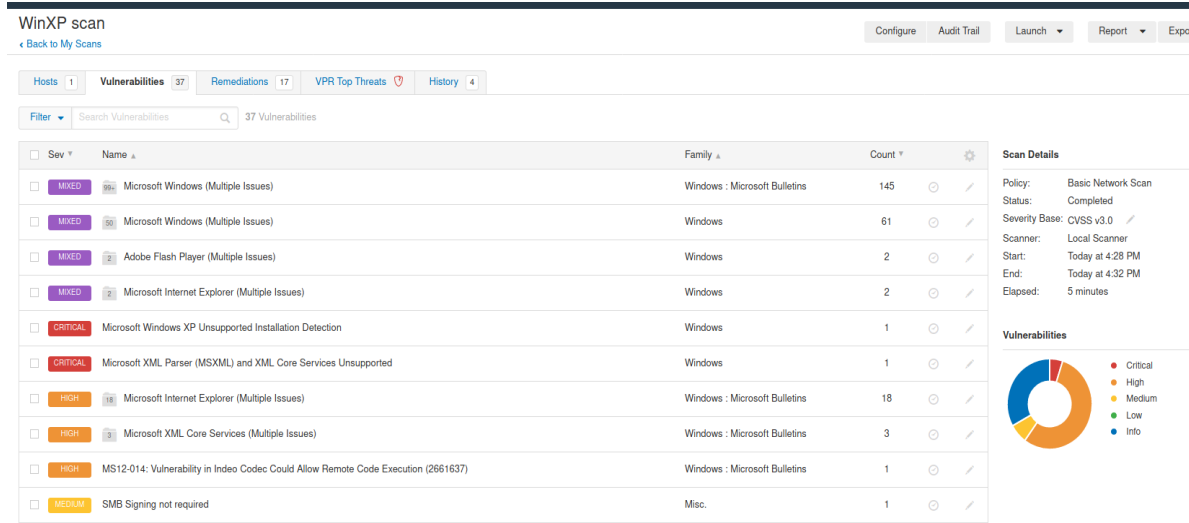
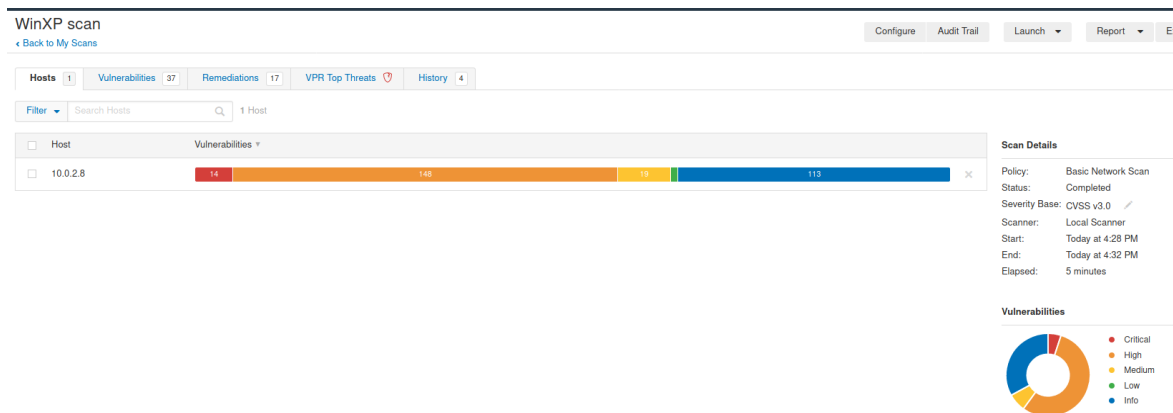
Search results for "SP3 XP"

Updates: 1 - 25 of 71 (page 1 of 3)

Title	Products	Classification	Last Updated	Version	Size	Download
Windows XP Service Pack 3 (KB936929)	Windows XP	Service Packs	5/19/2009	n/a	316.4 MB	Download
Update for Windows XP (KB952287)	Windows XP	Critical Updates	8/11/2008	n/a	642 KB	Download
Update for Windows XP (KB953356)	Windows XP	Critical Updates	6/24/2008	n/a	498 KB	Download
Security Update for Windows XP SP3 (KB4500331)	Windows XP	Security Updates	5/9/2019	n/a	519 KB	Download
Security Update for Windows XP SP3 (KB4023218)	Windows XP	Security Updates	6/12/2017	n/a	518 KB	Download
Security Update for Windows XP SP3 (KB4024402)	Windows XP	Security Updates	6/9/2017	n/a	1.0 MB	Download
Security Update for Windows XP SP3 (KB4024323)	Windows XP	Security Updates	6/9/2017	n/a	846 KB	Download
Security Update for Windows XP SP3 (KB4022747)	Windows XP	Security Updates	6/9/2017	n/a	544 KB	Download
Security Update for Windows XP SP3 (KB4019204)	Windows XP	Security Updates	6/9/2017	n/a	1.4 MB	Download
Security Update for Windows XP SP3 (KB4018466)	Windows XP	Security Updates	6/9/2017	n/a	665 KB	Download
Security Update for Windows XP SP3 (KB4012598)	Windows XP	Security Updates	5/12/2017	n/a	665 KB	Download
Security Update for Windows Media Format Runtime 9.0.3.8.11 for Windows XP SP3 (KB978693)	Windows XP	Security Updates	6/7/2010	n/a	4.2 MB	Download
Security Update for Windows Media Player 9 for Windows XP SP3 (KB979402)	Windows XP	Security Updates	4/12/2010	n/a	2.2 MB	Download
Security Update for Windows XP SP3 for xPc (KB4500331)	Windows XP Embedded	Security Updates	5/9/2019	n/a	519 KB	Download
2018-02 Security Update for Windows XP Embedded SP3 for x86-based Systems (KB4074603)	Windows XP Embedded	Security Updates	2/12/2018	n/a	1.4 MB	Download
2018-02 Security Update for Windows XP Embedded SP3 for x86-based Systems (KB4027893)	Windows XP Embedded	Security Updates	2/12/2018	n/a	569 KB	Download
2018-02 Security Update for Windows XP Embedded SP3 for x86-based Systems (KB4024852)	Windows XP Embedded	Security Updates	2/12/2018	n/a	2.3 MB	Download
2018-01 Security Update for Windows XP Embedded SP3 for x86-based Systems (KB4055615)	Windows XP Embedded	Security Updates	1/4/2018	n/a	2.4 MB	Download
2018-01 Security Update for Windows XP Embedded SP3 for x86-based Systems (KB4055941)	Windows XP Embedded	Security Updates	1/4/2018	n/a	647 KB	Download
2017-12 Security Update for Windows XP Embedded SP3 for x86-based Systems (KB4052303)	Windows XP Embedded	Security Updates	12/12/2017	n/a	570 KB	Download
2017-11 Security Update for Windows XP Embedded SP3 for x86-based Systems (KB4048968)	Windows XP Embedded	Security Updates	11/10/2017	n/a	569 KB	Download
Security Update for Windows XP SP3 for xPc (KB4025218)	Windows XP Embedded	Security Updates	6/12/2017	n/a	518 KB	Download
Security Update for Windows XP SP3 for xPc (KB4024402)	Windows XP Embedded	Security Updates	6/9/2017	n/a	1.0 MB	Download
Security Update for Windows XP SP3 for xPc (KB4024323)	Windows XP Embedded	Security Updates	6/9/2017	n/a	846 KB	Download

Site used on Firefox within Windows XP VM to manually install Windows Security Updates (extremely tedious).

Here is the Microsoft Windows Update site I had to use to manually install updates, which was an extremely tedious process.

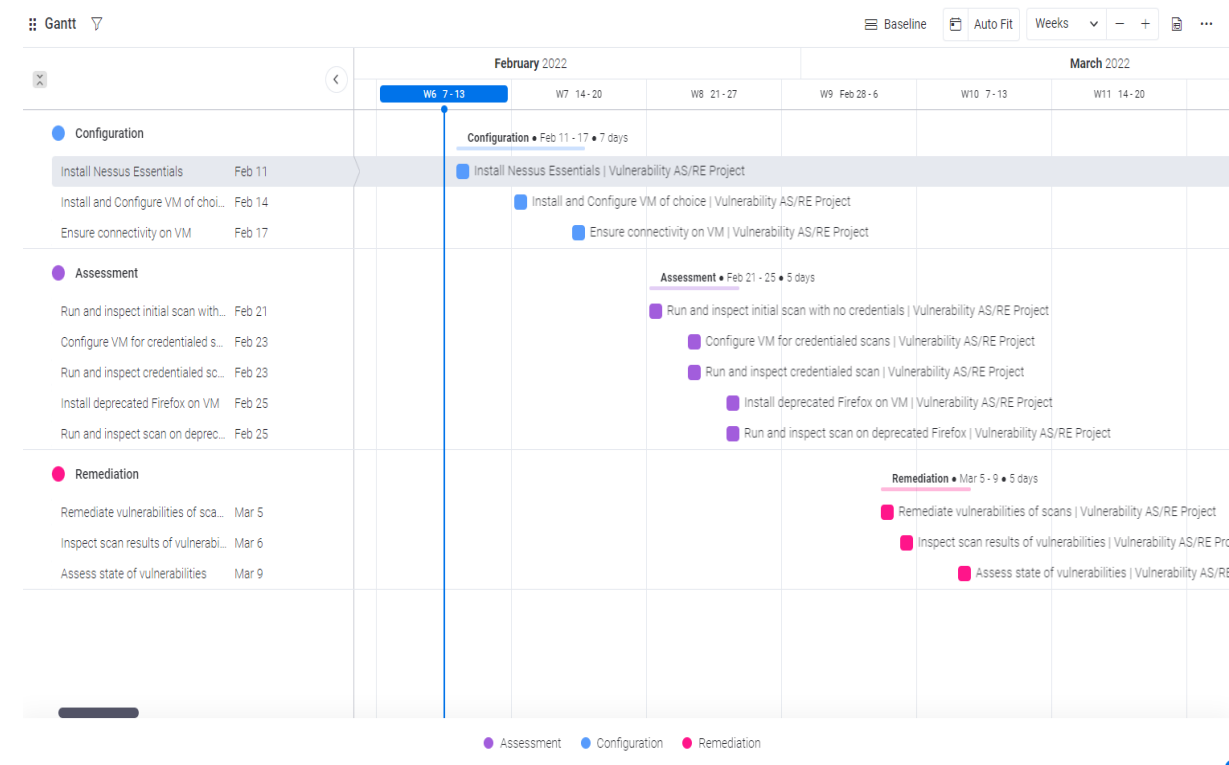


Windows XP VM credentialed scan after remediation highlights and further vulnerabilities (The vulnerability count was substantially decreased, although there still were further remediations, but for time's sake I decided to cut it here).

This was Windows XP after remediation. As said earlier, this process was quite difficult. This is because Internet Explorer, which is used by default by Windows XP to install Windows security updates, was utterly broken. No webpages could be loaded with Internet Explorer, in turn not allowing me to install security updates. Because of this, I had to install Mozilla Firefox, and install Windows security updates manually. This process was extremely slow and took hours upon hours to complete. In the screenshot, we can see Windows XP remediated, with vulnerabilities decreased dramatically.

PROJECT SCHEDULE MANAGEMENT

Gantt Chart



<https://github.com/stokesgarrett/Vulnerability-AS-RE-PRO.git>

<https://trello.com/b/D9jZMQTY/vulnerability-as-re>