Nessus Tutorial for Beginners: Vulnerability Management

Based on Video Created By: Josh Madakor
Blog Created By: Jose Romero

Lab Overview:
In this vulnerability management lab, the focus is on strengthening the understanding of the vulnerability management processes. Vulnerability management is the continuous process of assessing assets, identifying vulnerabilities, remedying them to an acceptable risk level, and repeating the cycle to maintain a low or acceptable level of risk within an organization's security framework. The key objectives include the installation of Nessus Essentials and VMware Workstation Player, followed by the setup of a Windows 10 virtual machine. Within this VM, aged and deprecated software will intentionally be installed to simulate a potentially vulnerable environment.

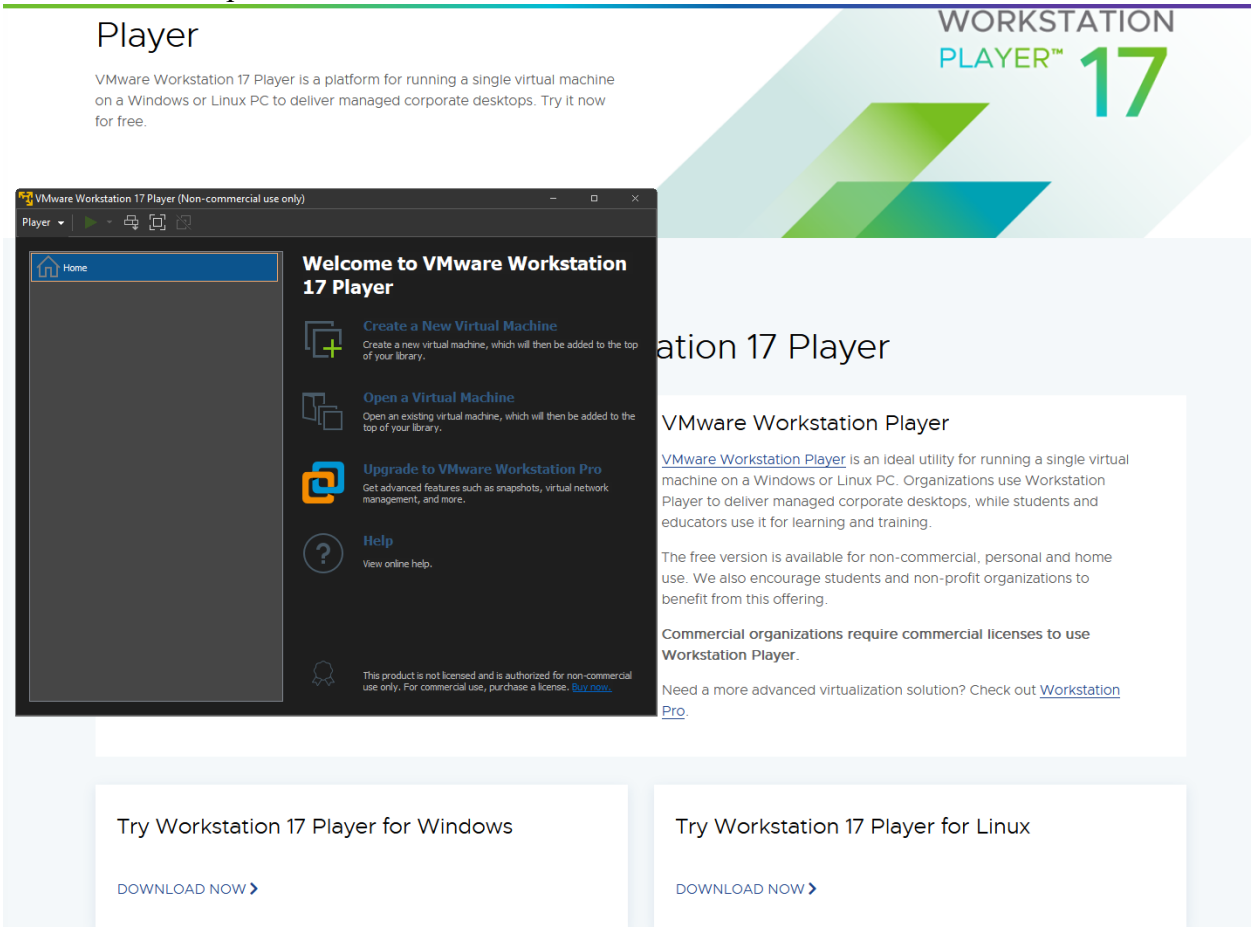
Subsequently, vulnerability scans will be conducted on the virtual machine using Nessus. These scans aim to reveal existing vulnerabilities within the system, offering valuable insights into the security posture of the environment. Following the identification of these vulnerabilities, the next step involves remediating the vulnerabilities. This practical remediation process provides a unique opportunity to observe the effects of addressing security flaws and to gain a deeper understanding of the practical aspects of enhancing system security.

Technologies Used:

1. **Nessus Essentials** - Nessus Essentials is a widely used vulnerability scanner and assessment tool that helps identify security weaknesses in computer systems, networks, and applications.
2. **VMware Workstation Player** - VMware Workstation Player is a virtualization software that enables users to create and run virtual machines on their desktop computers, making it easier to test and manage different operating systems and software configurations.
3. **Windows 10 ISO Virtual Machine** - A Windows 10 virtual machine is a virtualized instance of the Windows 10 operating system, allowing users to run Windows 10 on their computers without the need for a separate physical system.
4. **Deprecated Firefox (3.6.12)** - Deprecated Firefox refers to an older or no longer supported version of the Firefox web browser, which may not receive security updates or feature enhancements, making it potentially vulnerable to security risks.

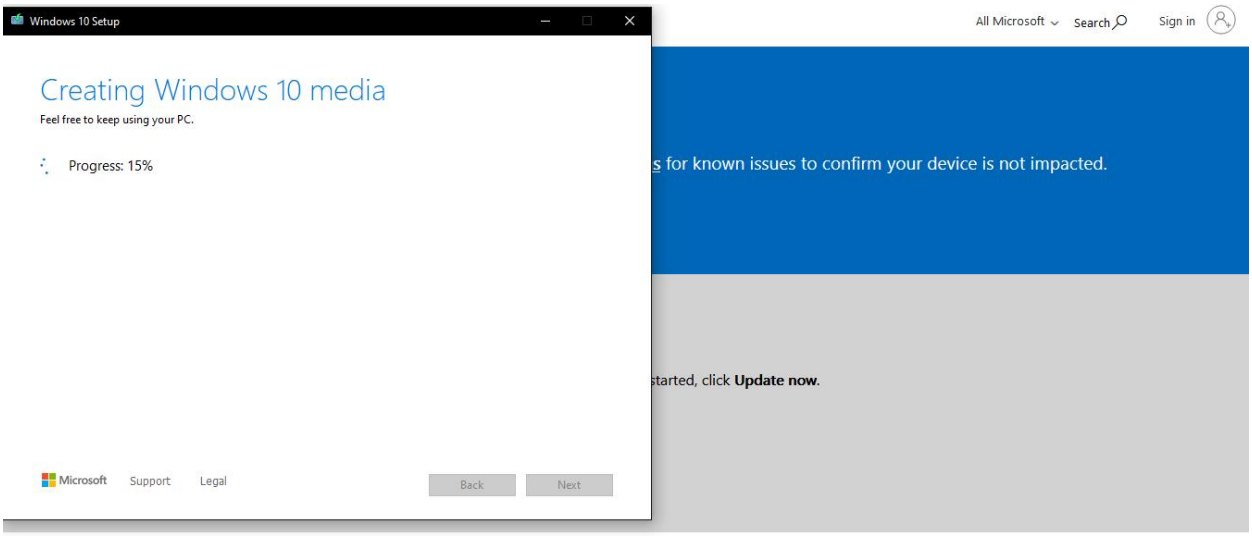
Step 1: Download VMware Workstation Player

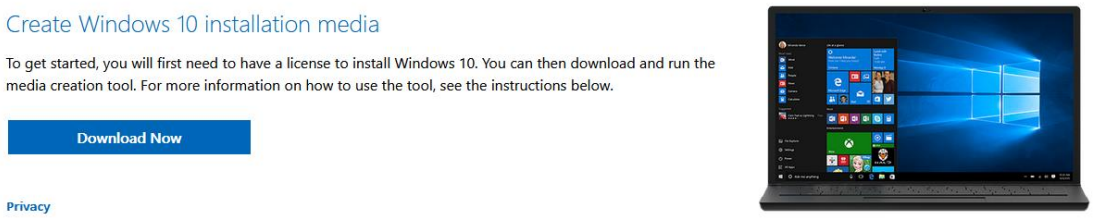
1. Go to this link and click download now under try workstation 17 player for windows
2. Once the player setup opens click next then I accept then next then next then check desktop then next then install then finish once installation has completed
3. Press start button and search VMware to open VMware Workstation 17 Player
4. Once open choose “use VMware for free” then continue then finish
5. Leave it open



Step 2: Download Windows 10 ISO

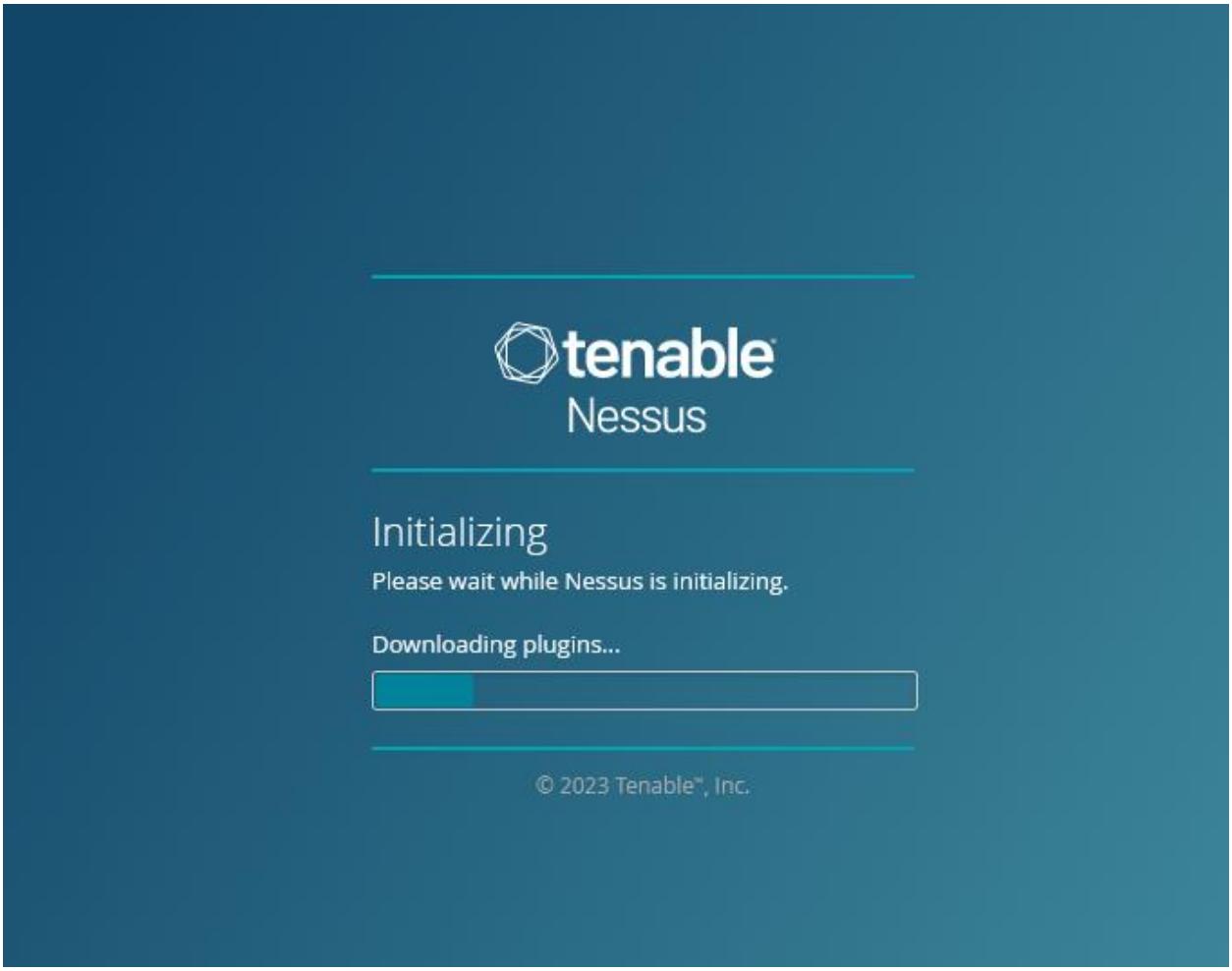
1. Create folder on desktop named ISOs
2. Go to this link and click download now under create windows 10 installation media
3. Once open click accept then create installation media then next then next then choose ISO file then next then place it into the folder ISOs that was just created
4. Wait till creation reaches 100% progress then click finish





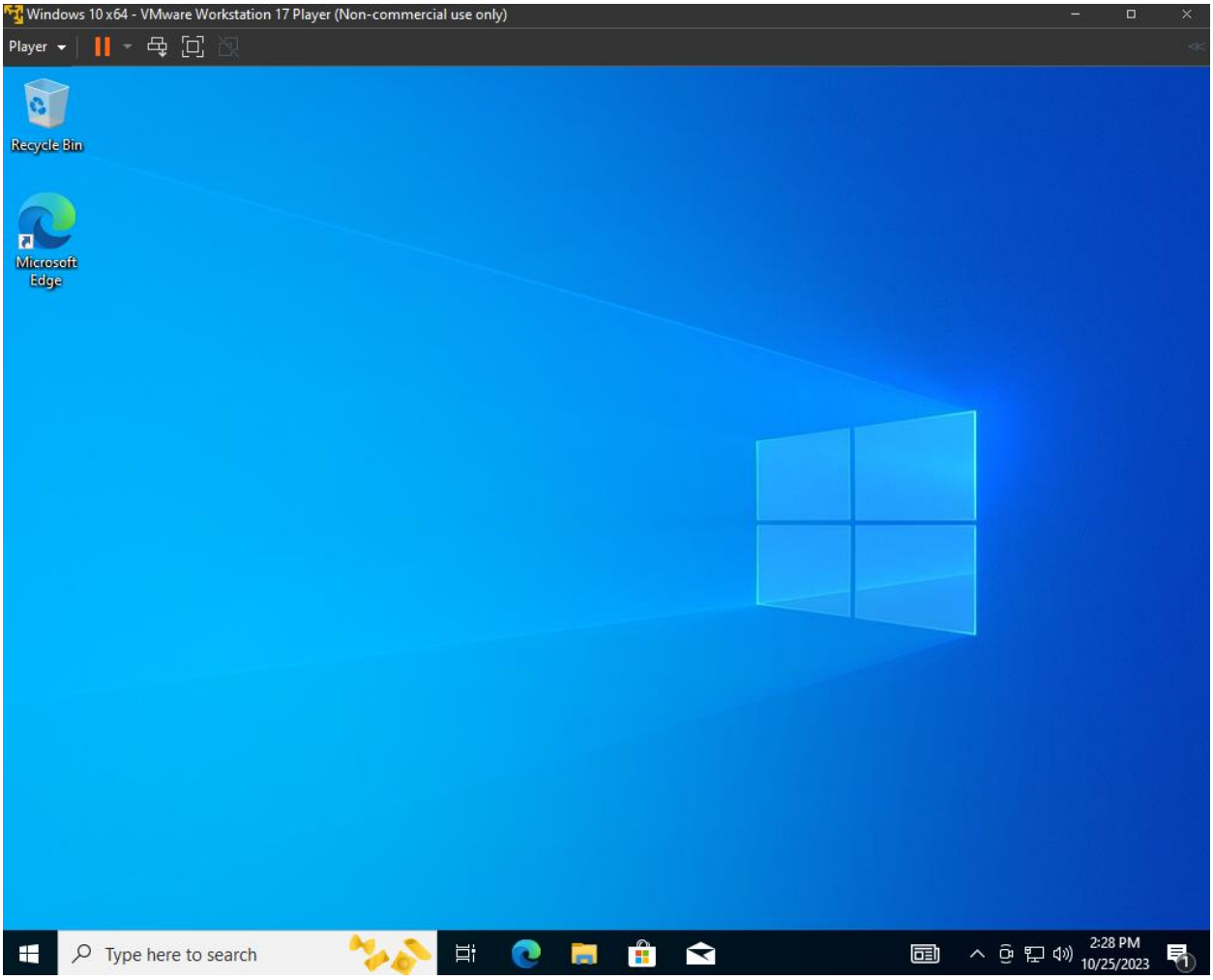
Step 3: Download Nessus Essentials Vulnerability Scanner

1. Go to this link and insert information under register for an activation code the click get started
2. Check email for key and copy it then click red button in email to download Nessus
3. The button takes you to a website where you click view downloads for Tenable Nessus
4. Now under platform choose your current platform on host machine (Usually Windows – x86_64)
5. Click download then I agree
6. When install wizard opens up click next then I accept then next then next then install then finish
7. Once finished a website should open up in browser with a URL like shown: http://localhost:0000/WelcomeToNessus-Install/welcome
8. Click connect via SSL then advanced then accept the risk and continue then continue then register for Nessus Essentials then continue then skip then type in key from previous email then continue then continue then create username and password then click submit
9. Wait for Nessus to initialize



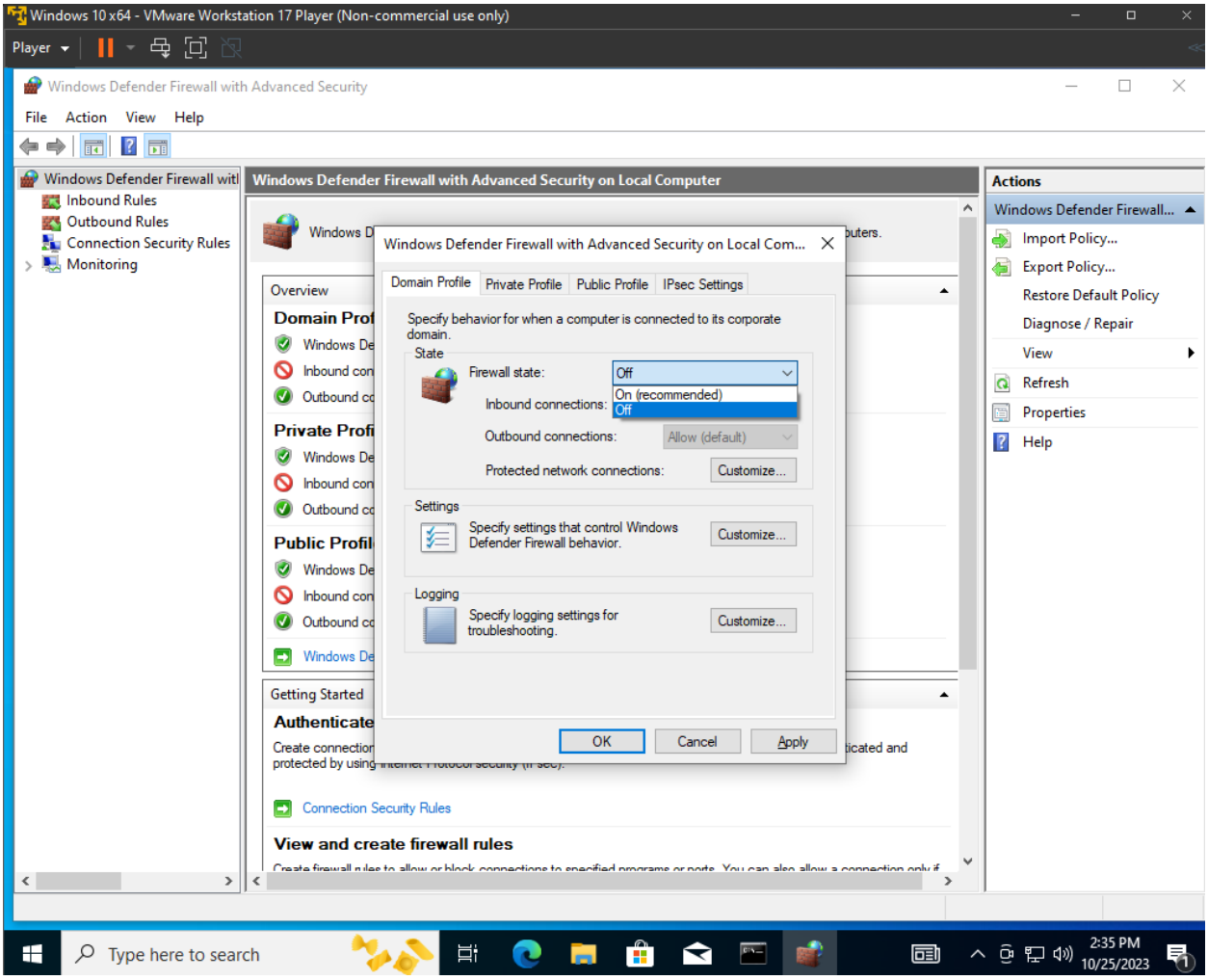
Step 4: Setup Windows Virtual Machine

1. Open up VMware workstation player then open up the player dropdown menu then click file then new virtual machine
2. Once in new virtual machine wizard under install form choose installer disc image file (iso) then click browse and find ISOs file that was made in step 2 then click next then next then use recommended size for windows 10 then next then customize hardware then under memory choose 4Gb for a better user experience then under network adapter under network connection choose bridged then close then check power on this virtual machine after creation
3. Once VMware opens click any key to boot into the ISO then hit next then install then I don't have a product key then windows 10 pro then next then accept then next then choose custom installation choose blank hard drive then wait till finish install
4. Once in windows choose United States then yes then yes then skip then setup for personal use then next then offline account then limited experience then name virtual machine admin then make a password then next then confirm password then make security questions then say no to privacy settings then skip then not now then wait until windows home screen shows up



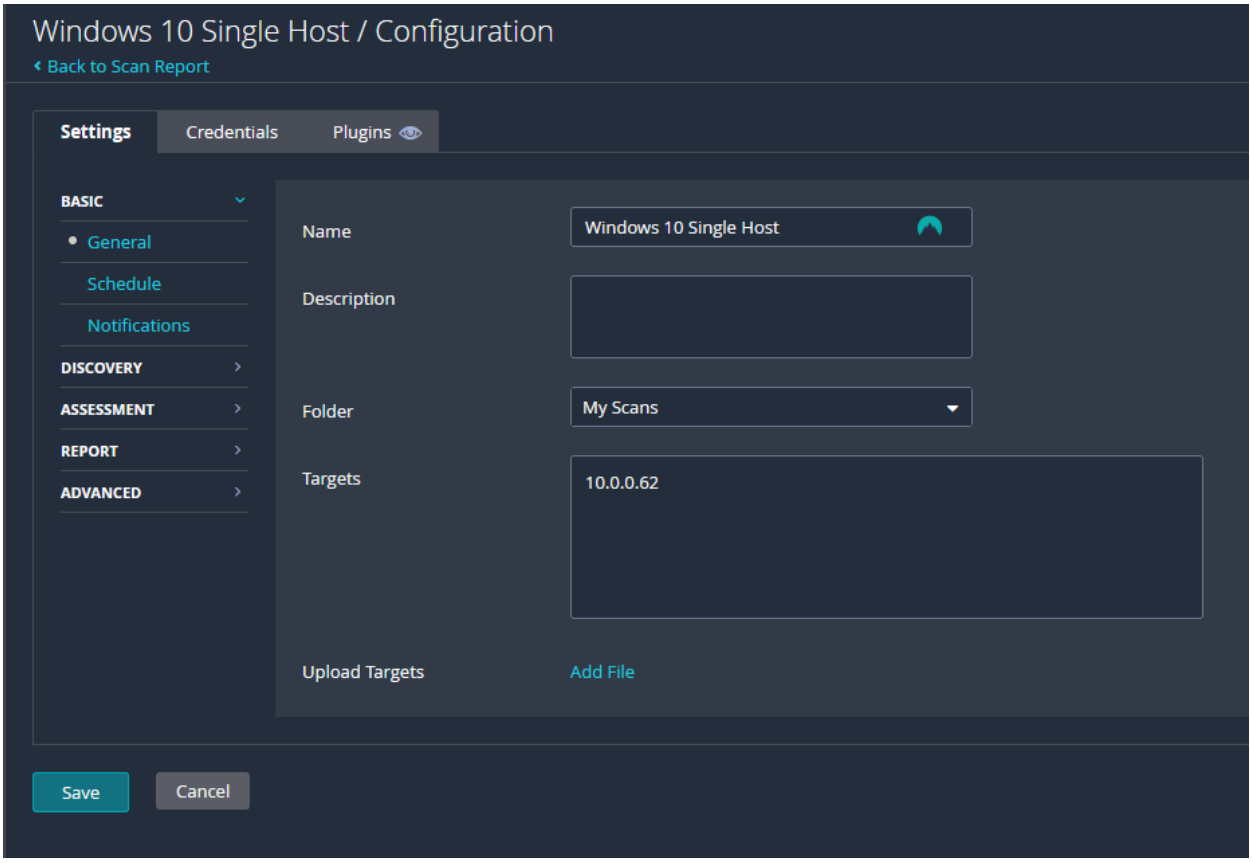
Step 5: Turn Firewall off on virtual machine

1. In virtual machine press windows start button then search cmd to open command prompt then type in ipconfig to obtain the IP address
2. In the host machine press windows start button then search cmd to open command prompt then type in ping “IP address virtual machine”. This shouldn’t work yet and give request times out.
3. In virtual machine press windows start button then search wf.msc and open it then click defender firewall properties then turn off firewall state for domain profile, private profile, and public profile
4. Now try pinging the virtual machine from host machine again it should say reply from virtual machine IP address



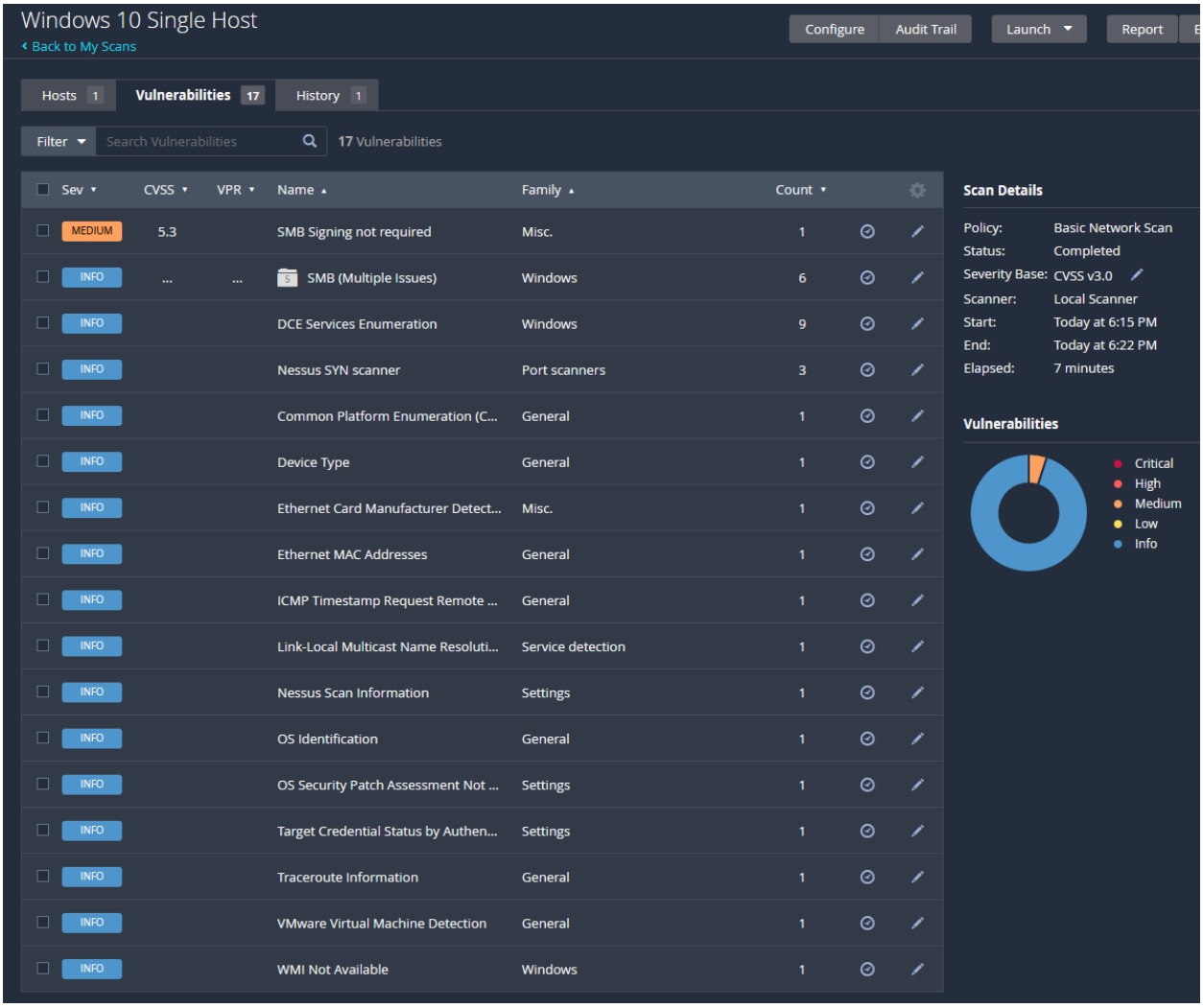
Step 6A: Run first scan on virtual machine

1. Open Nessus Essentials on host machine browser and click create a new scan then click basic network scan then type in virtual machine IP address under targets section then click blue save button
2. In name section name it Windows 10 Single Host
3. In my scans section find Windows 10 Single Host and click the launch button to the right
4. Wait for checkmark confirmation of completion



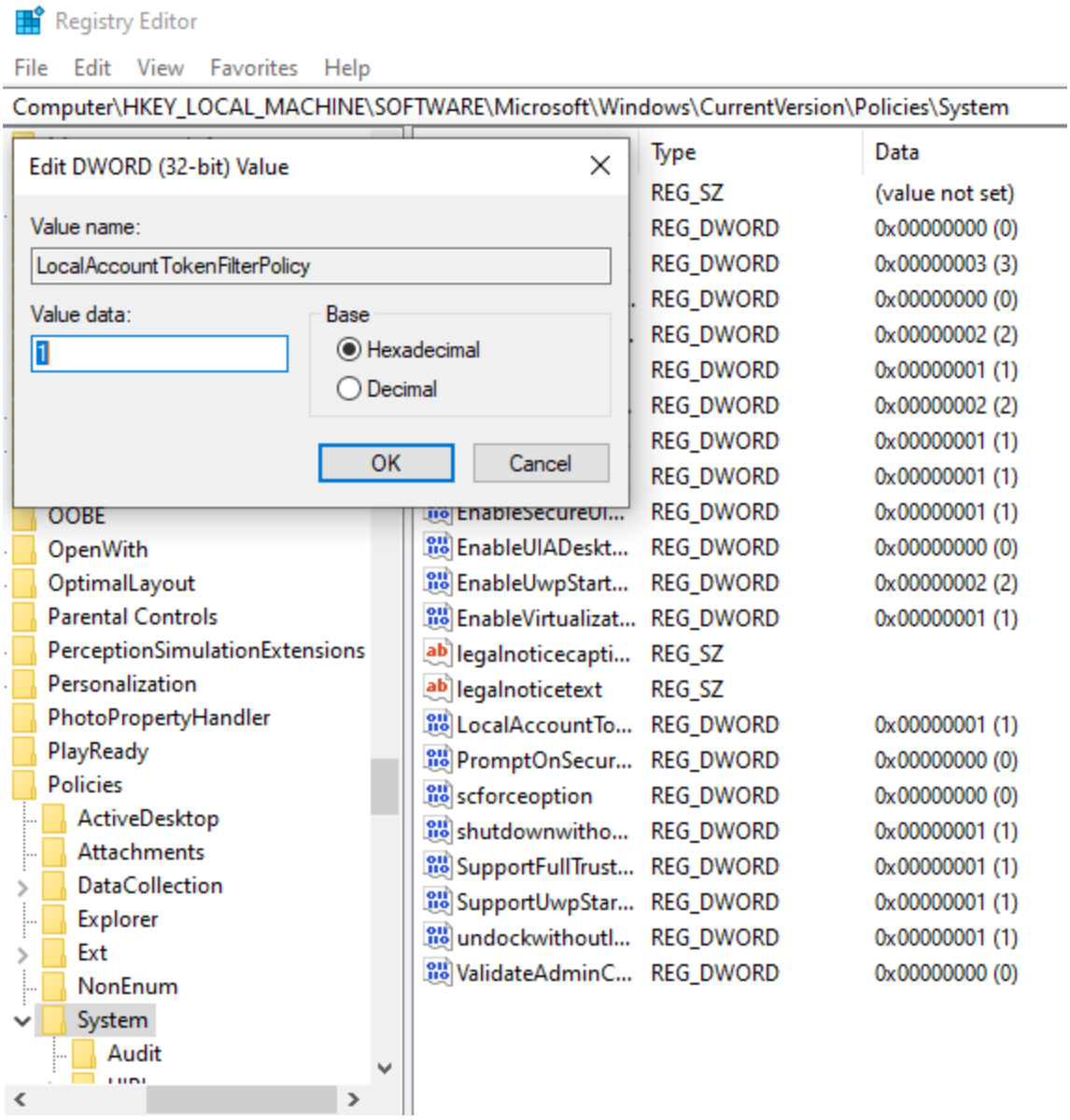
Step 6B: Inspect first scan on virtual machine (Without Credentials)

1. Open Windows 10 Single Host after checkmark shows up and click vulnerabilities to see what vulnerabilities the virtual has
2. Click on some of the vulnerabilities to explore and learn (Should only show a few vulnerabilities)



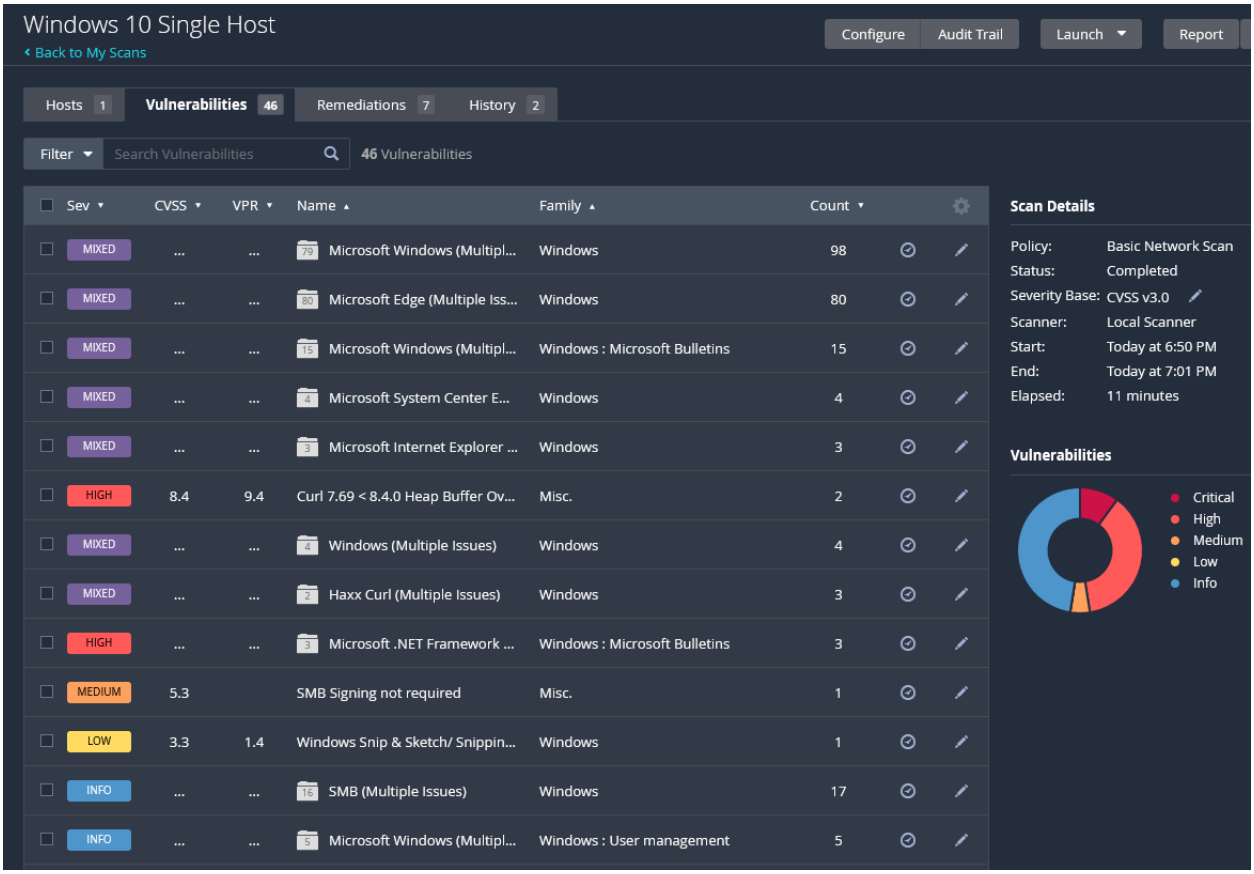
Step 7A: Configuring virtual machine for credentialed scan

1. Back on the virtual machine open up services.msc by pressing the start button then searching
2. Find remote registry and under startup type choose automatic then apply then start then ok now exit out
3. Press start button then search advanced sharing settings under network discovery then under file and printer sharing click turn on
4. Press start button and search user account control and slide the bar to never notify then click ok
5. Press start button and search registry editor and open it then click HKEY_LOCAL_MACHINE then SOFTWARE then MICROSOFT then Windows then CurrentVerion then policies then system then right click under name, type, and data to click new DWORD (32-bit) Value then name it LocalAccountTokenFilterPolicy press enter then click on LocalAccountTokenFilterPolicy and set value date to 1
6. Restart virtual machine
7. Log in



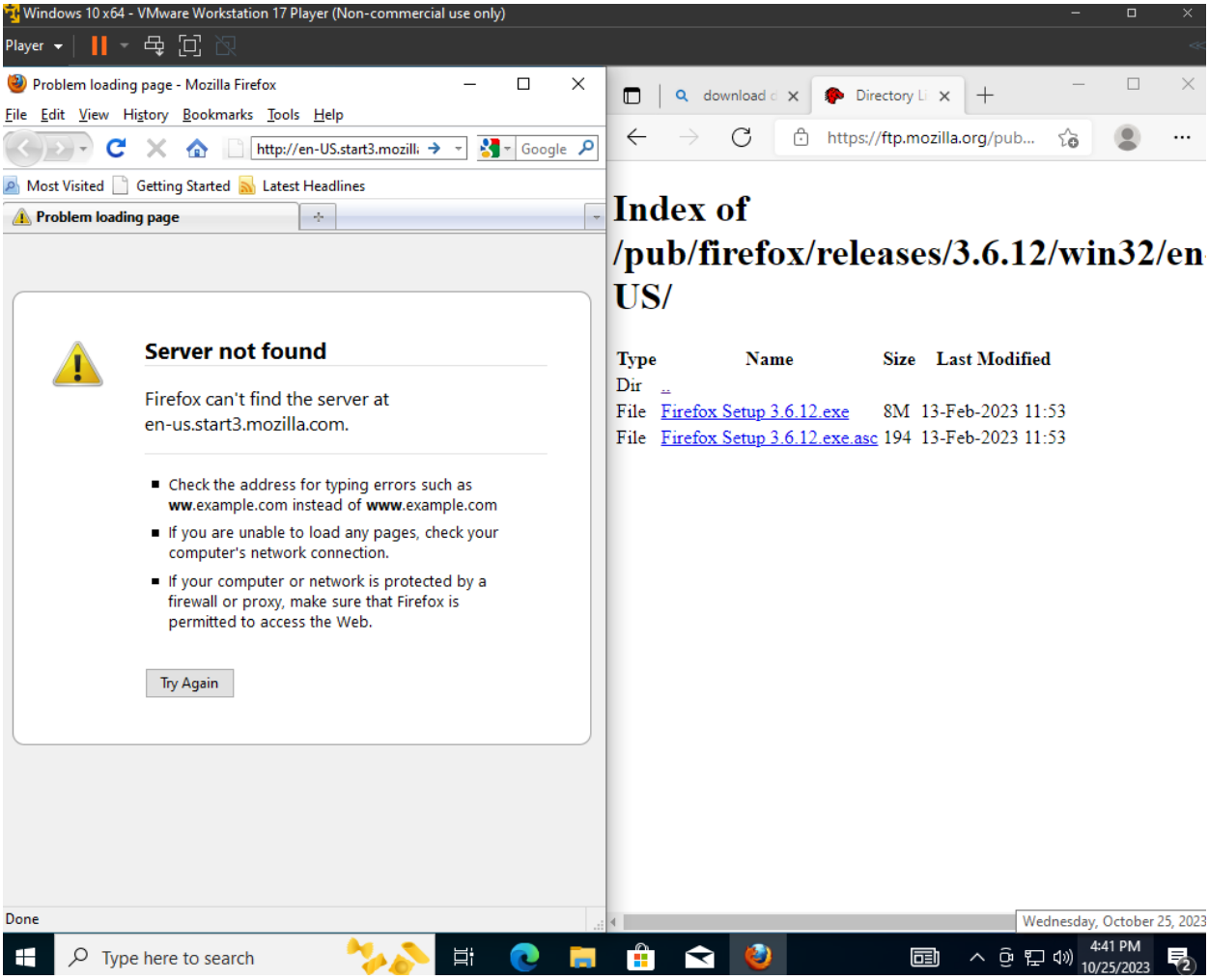
Step 7B: Configure, run, and inspect second scan on virtual machine (With Credentials)

1. In Nessus Essentials on host machine find Windows 10 Single Host check the box to the left and click the new more button then click configure
2. Go to credentials section then click windows then type in the same username and password used for the virtual machine then click save
3. In my scans section find Windows 10 Single Host and click the launch button to the right
4. Wait for checkmark confirmation of completion
5. Open Windows 10 Single Host after checkmark shows up and click vulnerabilities to see what vulnerabilities the virtual machine has
6. Click on some of the vulnerabilities to explore and learn (Should show more vulnerabilities)
7. Click on remediations and Nessus Essentials will show what actions to take to remediate the virtual machine



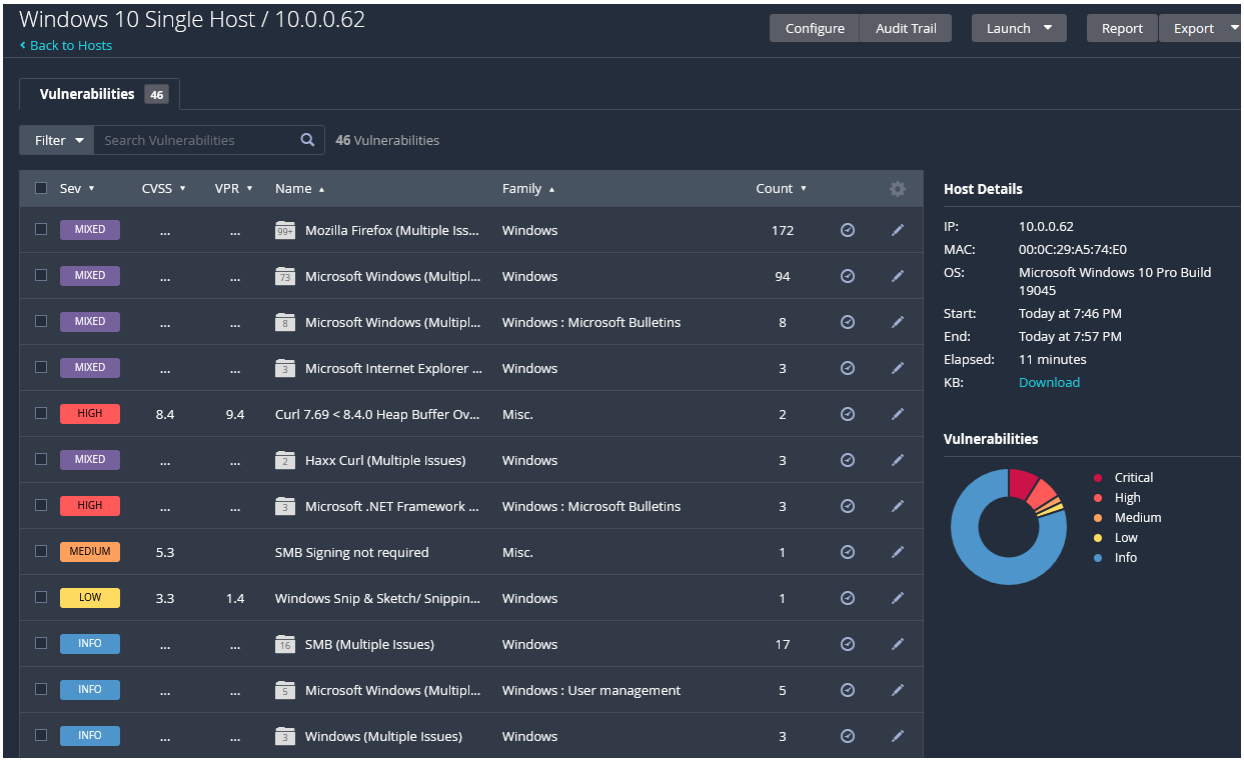
Step 8: Installing deprecated Firefox on virtual machine

1. Go to this link then find and click dir 3.6.12 then click win32/ then en-US then Firefox setup 3.6.12.exe
2. Open file then click next then standard and next then install then check launch Firefox now then finish then don't import anything



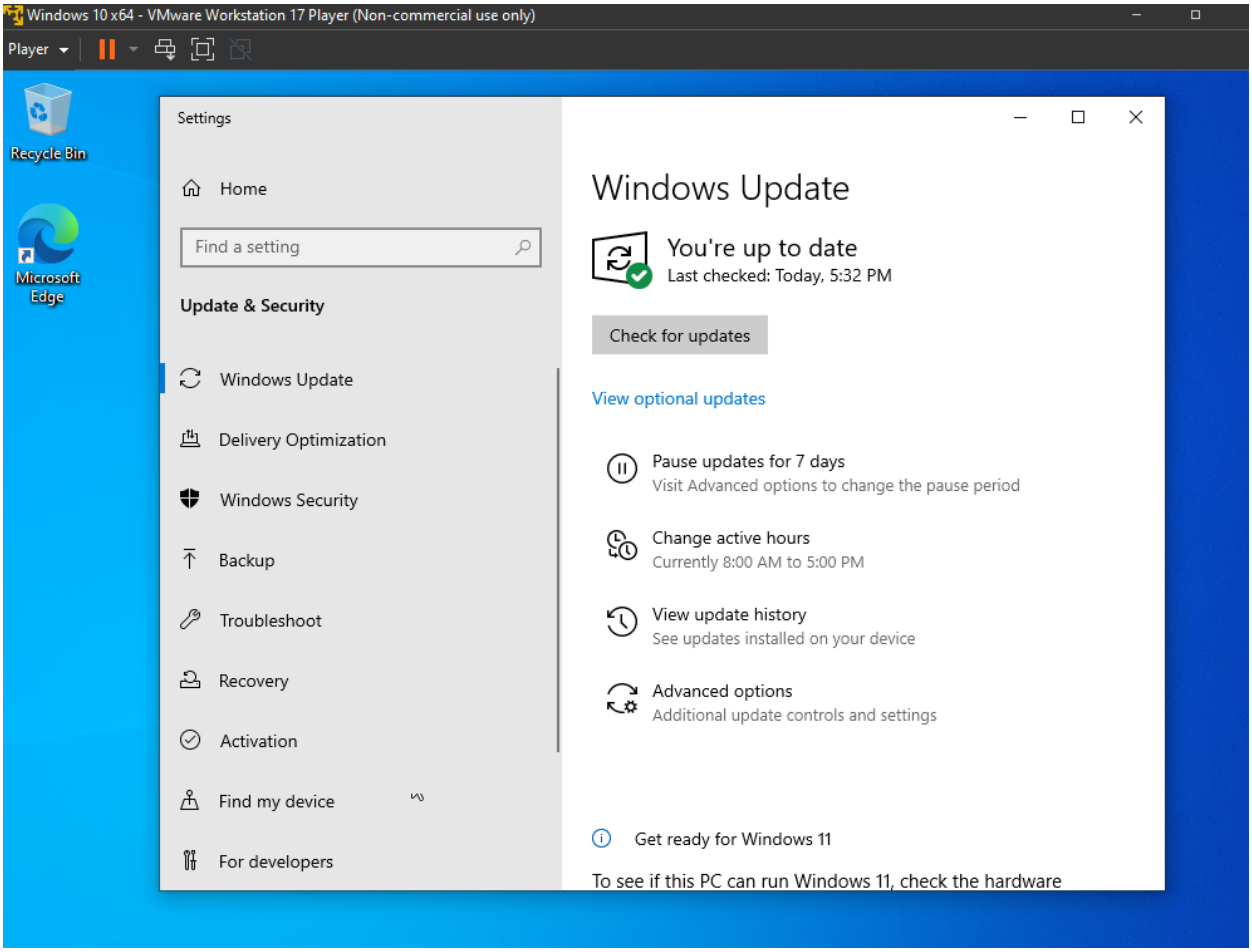
Step 9: Run and inspect third scan on virtual machine (With Credentials + Deprecated Firefox)

1. Back on Nessus Essentials on host machine under my scans section find Windows 10 Single Host and click the launch button to the right
2. Wait for checkmark confirmation of completion
3. Open Windows 10 Single Host after checkmark shows up and click vulnerabilities to see what vulnerabilities the virtual machine has
4. Click on some of the vulnerabilities to explore and learn (Should show many vulnerabilities)
5. Click on remediations and Nessus Essentials will show what actions to take to remediate the virtual machine



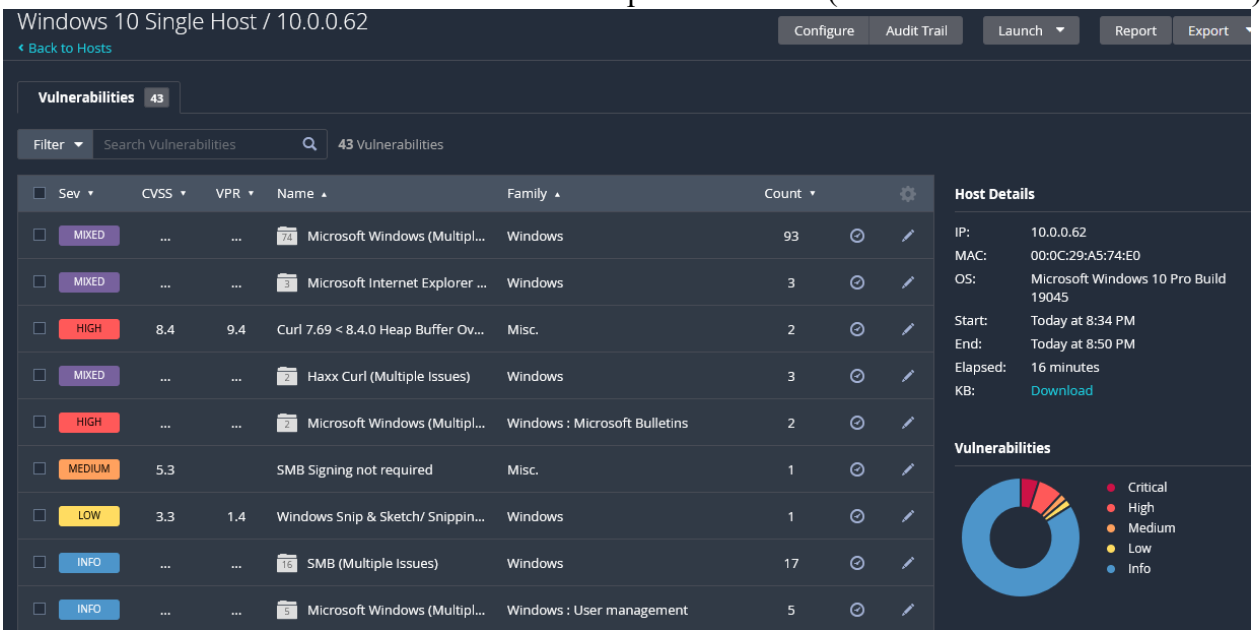
Step 10: Remediating Vulnerabilities

1. Back on the virtual machine press windows start button and search run then type appwiz.cpl then click on Firefox and click delete
2. Press windows start button again and search windows update then check for updates and update to most current version then restart and check for updates again until windows updates says it is up to date



Step 11: Run and inspect third scan on virtual machine (Remediated)

1. Back on Nessus Essentials on host machine under my scans section find Windows 10 Single Host and click the launch button to the right
2. Wait for checkmark confirmation of completion
3. Open Windows 10 Single Host after checkmark shows up and click vulnerabilities to see what vulnerabilities the virtual machine has
4. Click on some of the vulnerabilities to explore and learn (Should show less vulnerabilities)



Step 12: Compare all 4 scans on virtual machine

1. Click on the history tab the past 4 scans that have been completed should show up
2. Compare the 4 scans and try to remediate some more