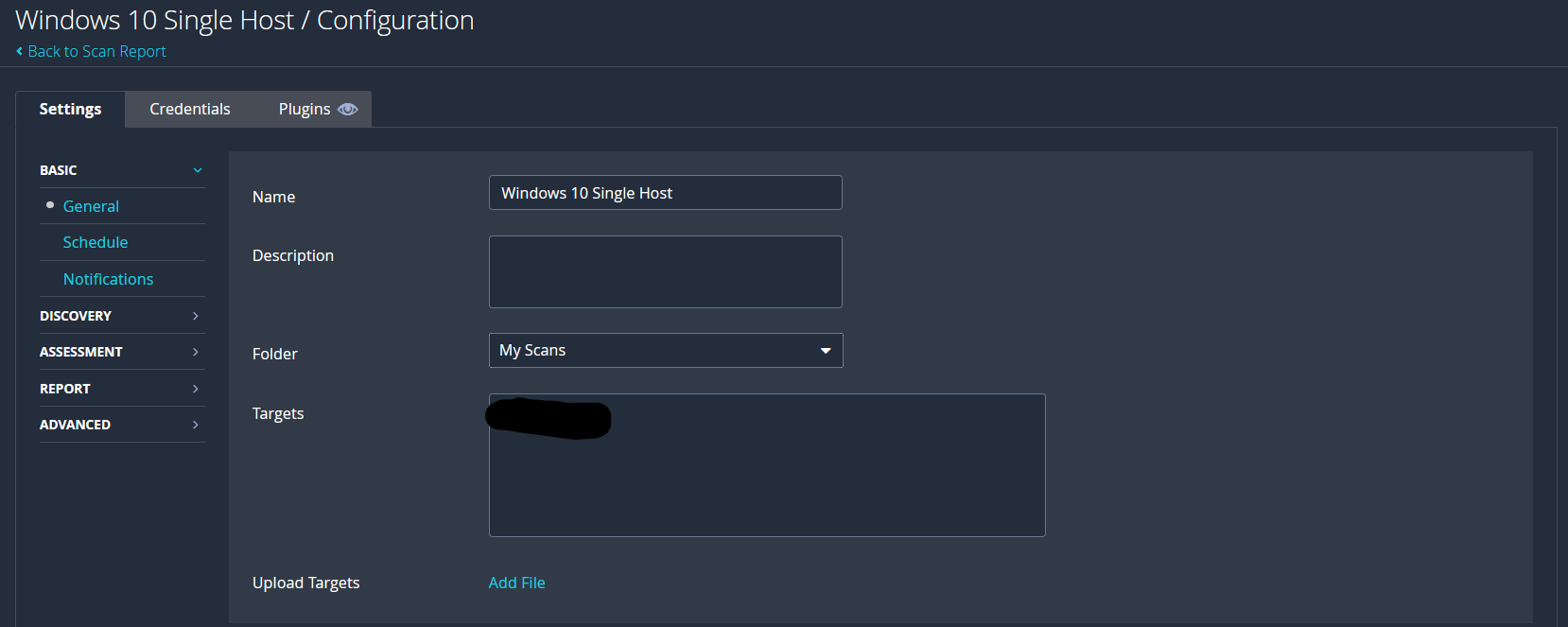
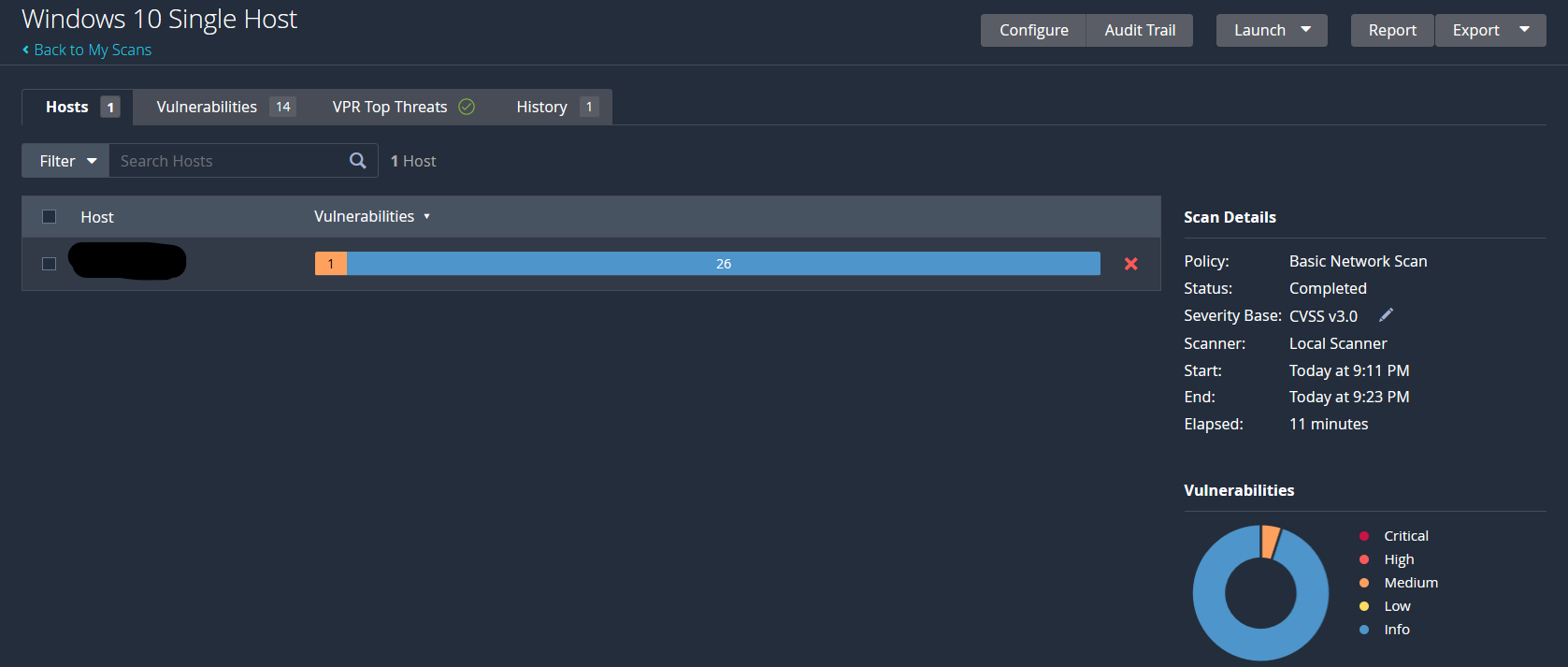
Vulnerabilty Management using Tenable Nessus LAB

Objective: Used Nessus Essentials to scan local VMs in Windows 10 hosted on Oracle Virtualbox to run different scans such as basic and credentialed/authenticated to discover vulnerabilities, remediate some of the vulnerabilities, then perform a rescan to verify remediation.

1. Downloaded and Installed Virtualbox, Windows 10 ISO, and Tenable Nessus Essentials

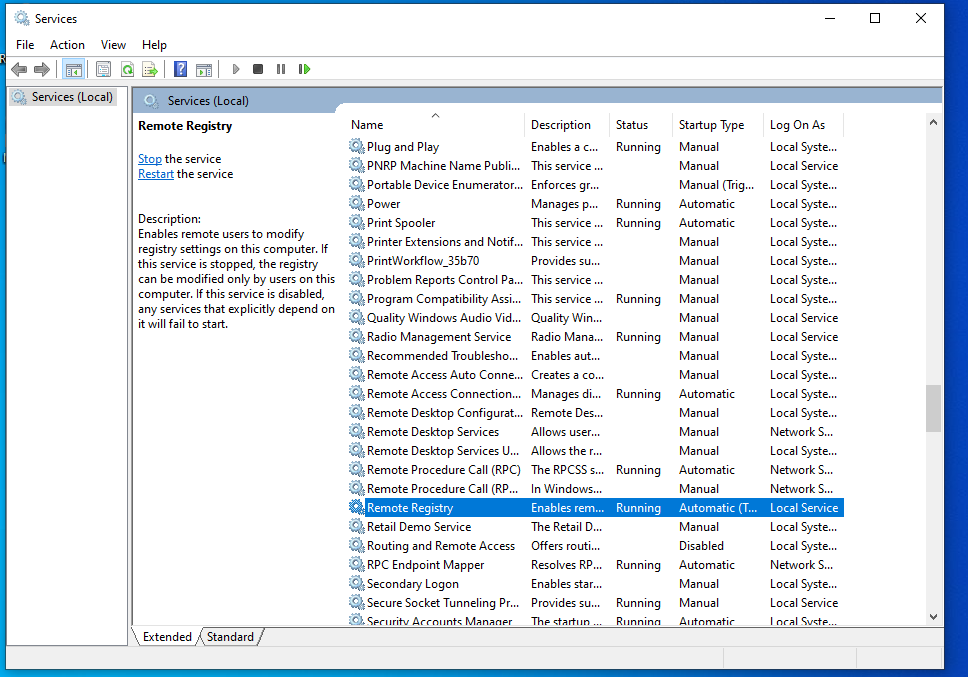


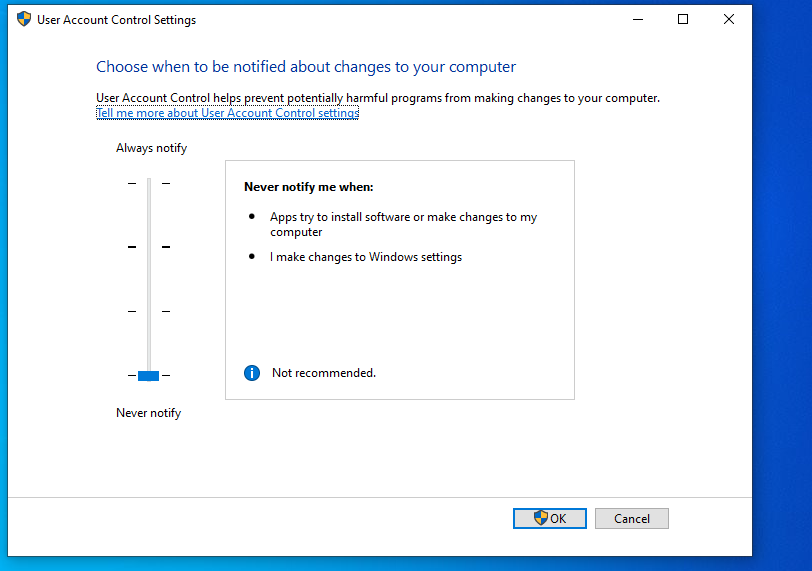
Creating my first basic scan into Tenable searching vulnerabilities of the my windows 10 single host.



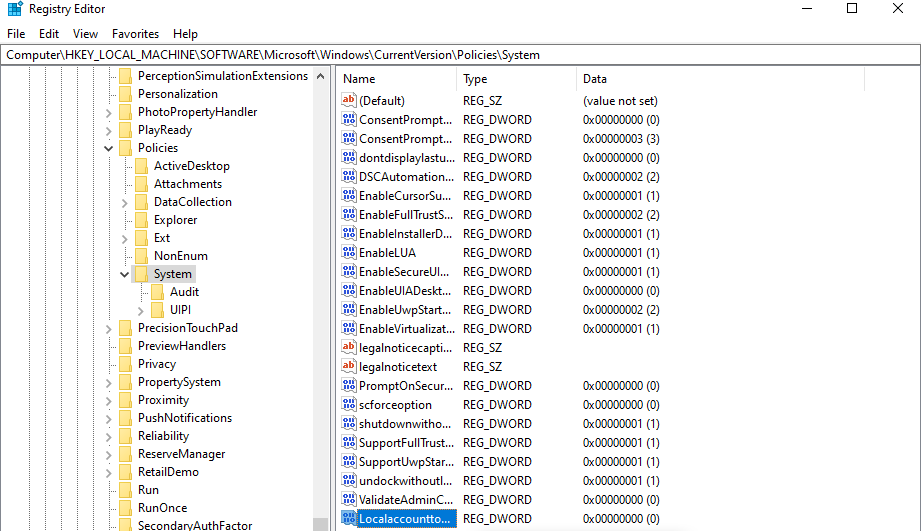
Running my first basic scan to see what kind of vulnerabilities this VM test box has. Analyzing the completed scan I see that I have 14 vulnerabilities and one that could be a mid concern being a serverity of medium.

If i recieved any high or criticals I would be presented with a remediation tab where it will tell or guide me into how to correct the issues. For example, if It was a out-of-date software and I updated that software, restarted my system then ran a new scan That entry should no longer be there.



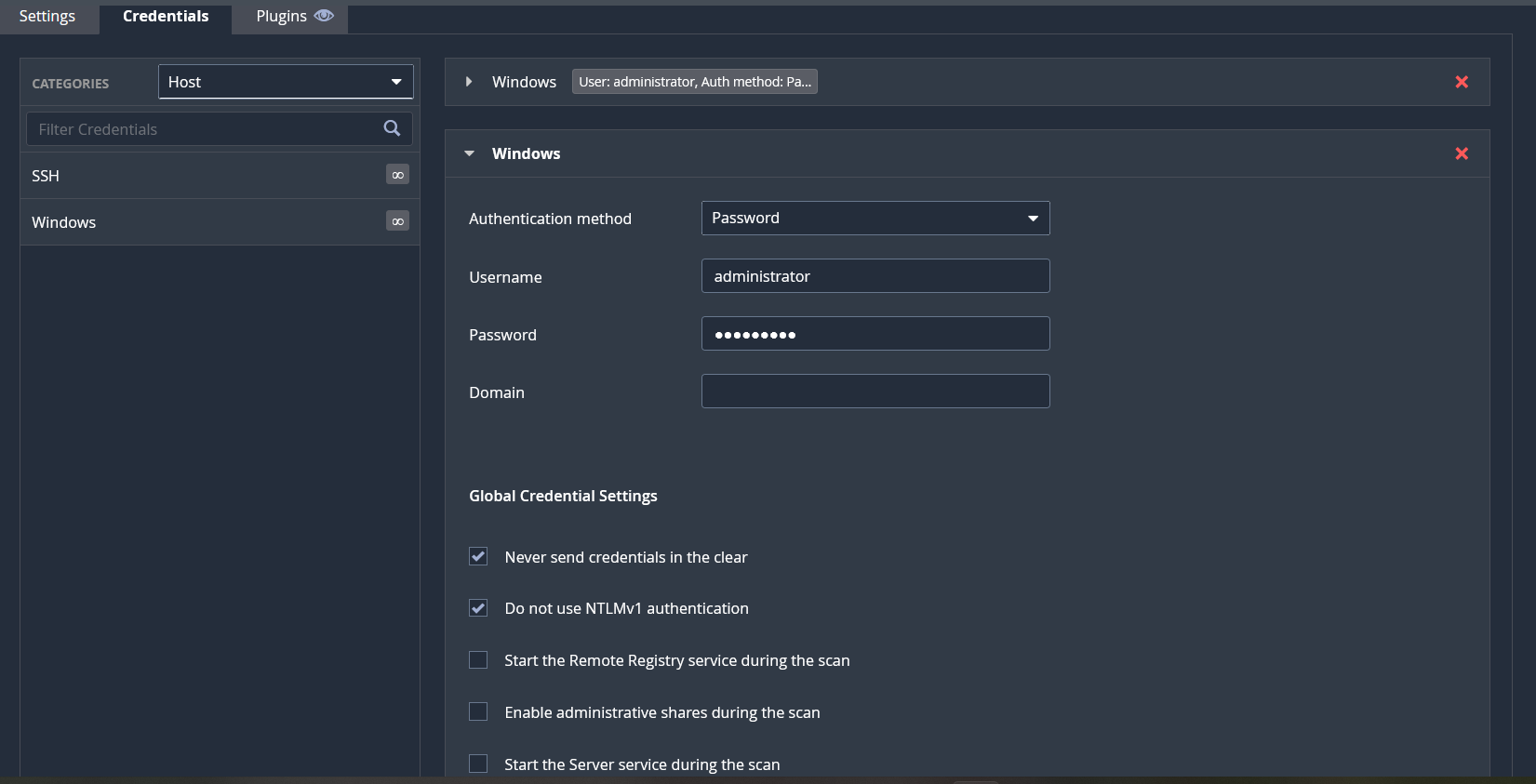
Enabling Remote Registry so scanning can dive deeper into the machine’s system. The scan is going to crawl the registry, ram, boot files , applications and services in search of vulnerabilities that aren’t showing up on a regular basic scan. 

Modifying User account control settings in the vm in to disregard notifiying when there is applications or services attempting to install or if changes are being made to the user account. This is for testing and training purposes and would never apply this to a production environment because you will not be able to detect malware or other attacks.



Path to get here is go to registery editor --> local Machine --> Software --> Microsoft --> Windows --> Current Version --> Policies --> System. Once under the system you want to make a dword policy which I have created above named Localaccounttokenfilterpolicy, and set the value data to 1 by double clicking on the policy name.

5. Restart VM so changes can go into effect



I edited my initial scan to do a credential/ Authenticated scan. This is going to provide a deeper insight of my VM system. The scan is going to use the provided Credentials to log into my VM and application in hopes of providing a list of required patches and showing misconfigurations.

Other things it looks for is evaluating password policies, enumerating usb devices, and checking anti-virus/malware software configurations.

Result: For some reason, my result didnt change from my regular basic scan. after troubleshooting, I still havent been able to figure out why I didnt get any new vulnerabilities.



Downloading a Depreciated version of firefox for the next vulnerability testing scan.

Running the scan knowing that i have a out of date software application my results still didnt change when it certainly should have. As mentioned prior in this lab write up I should have recieved a high or critical alert which would present me with a remediation tab. Knowing that I had a out of date browser I immeditaly new how to correct the issue which installing the new version.

Issues in this lab:

I checked my VMs configuration and nothing seems misconfigured. I verified the IP my machine was receiving was on the same subnet as my network and it was. I then verified that I could ping my VM machine from my laptop and it was a success. I finally checked to see if I could get out to the internet using my VM and that was also a success.

I verified that I did enable print sharing allowing my VM to be discoverable. I then check the firewall policies ensuring that file sharing was enable there for TCP/UDP. It was initially disabled. After enabling those two policies I again attempted to run a scan to see if there would be any changes in the completed scan and there wasn’t.

I verified that Tenable was working properly by running a quick scan on my laptop. The results came out as working scans. Yet, after fixing a issues that I was alerted to by my scan, I still was recieving the same scan output which should be different as I fixed an Issue.