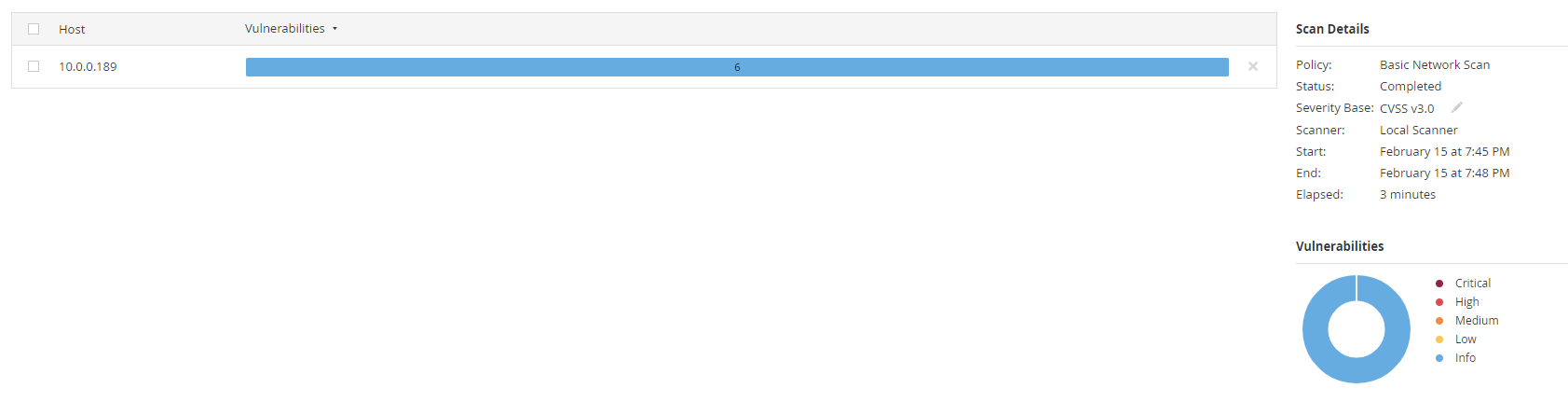
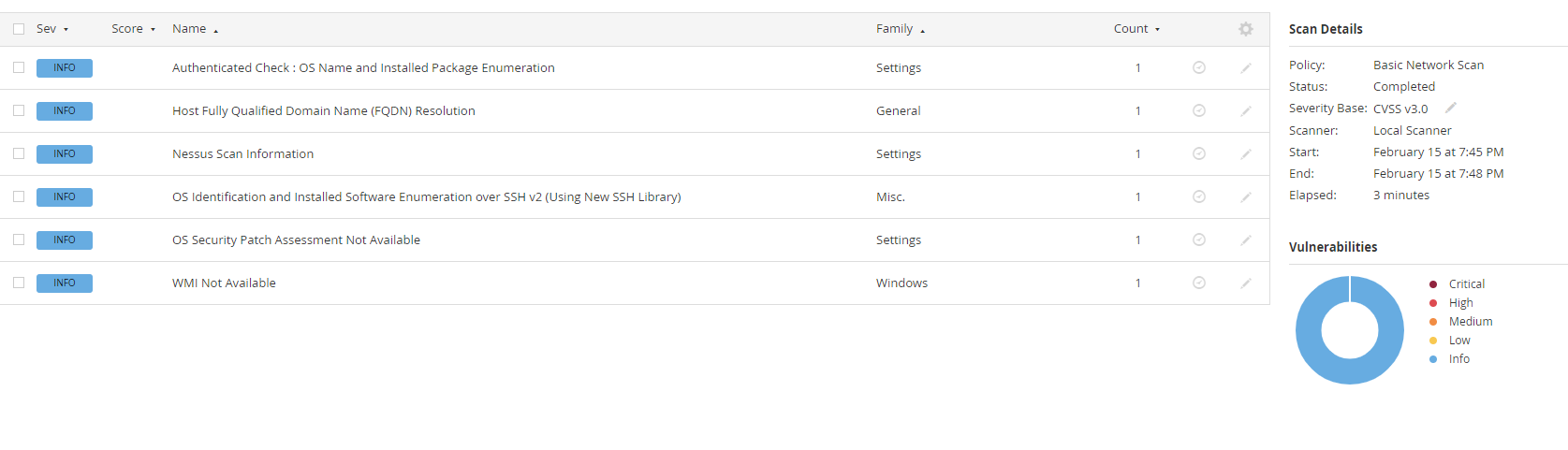
To get some further experience implementing vulnerability scanning within my own home environment, I installed Nessus Essentials to my local machine. After installing Nessus Essentials, I installed VMWare Player and a .ISO file of windows 10 from Microsoft’s website.

I booted up VMWare Player and loaded the .ISO file into VMWare player. From there, I was able to open a VM of Windows 10, making sure to set up the VM with the network adapter to be bridged, to ensure it’s part of my home’s network. I pinged the machine from outside of the VM, after turning off the firewall, to ensure the VM could be properly scanned.

From there, I ran the first scan and had this as a result



After checking the Vulnerabilities tab, I found more information regarding the information level vulnerabilities



After running the noncredentialed scan, I set up the VM to ensure that it would allow for a credentialed scan by enabling remote registry, permit file and printer sharing in the network and sharing center settings of control panel.

I also created a LocalAccountTokenFilePolicy Dword set to 1 in regedit \HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System.

I then ran a credentialed scan on the computer and had the following results:



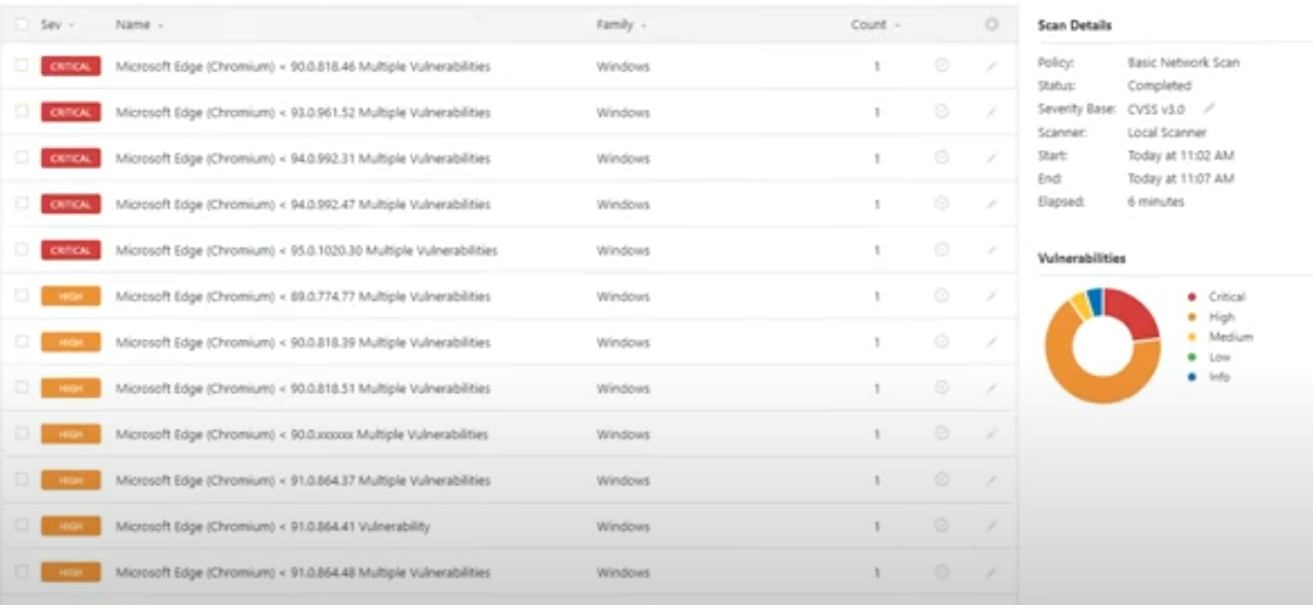
More vulnerabilities are shown this time, showing that while one can scan a network, most critical vulnerabilities won’t be shown outside of a credentialed scan.

I proceeded to then install some legacy software (old iterations of Edge and Firefox), and ran another scan.

The following scan was done after installing legacy firefox onto the VM, and running a scan.



And the final scan I did was after installing a legacy installation of MS Edge, results are as follows:



To conclude, major vulnerabilities can be found in legacy/out of date patches of software. Having a patch maintenance system is vital, especially for networks with a large amount of threat vectors.

It is imperative that a patching process is in place, so as to not interfere with workflow by pushing downloads. It’s also a good note to ensure patches are safe and do not have vulnerabilities that are easily exploitable. A balance must be made with patching, of course, but as you can see, patching and vulnerability scanning for said patches is necessary.