**ITT-307 Lab Assessment**

Professor: Juan Gonzalez

Course: ITT-307

Student: Matt Sievers

Date: 08/06/2019

Title: Windows VM – Anti-virus/malware installation

Directions:

# Overview: To provide detailed instructions on how to setup a virtual machine running windows. We were then to install a free anti-virus, perform a scan and then disable the windows firewall in an attempt to see if anything would get through. After 24 hours we were to run the scan again and document the differences. This is in an effort to show that just being connected to the internet makes you vulnerable.

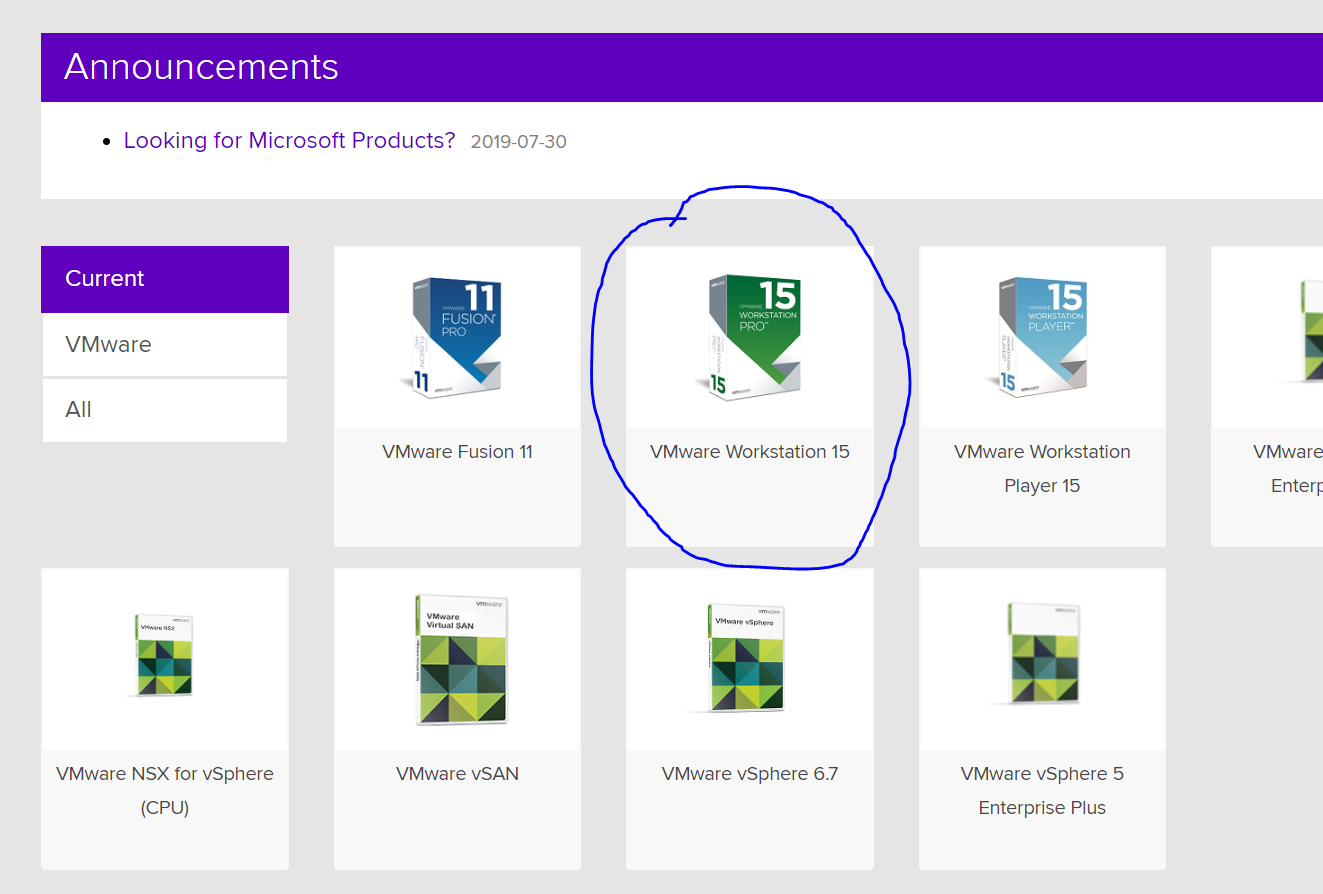
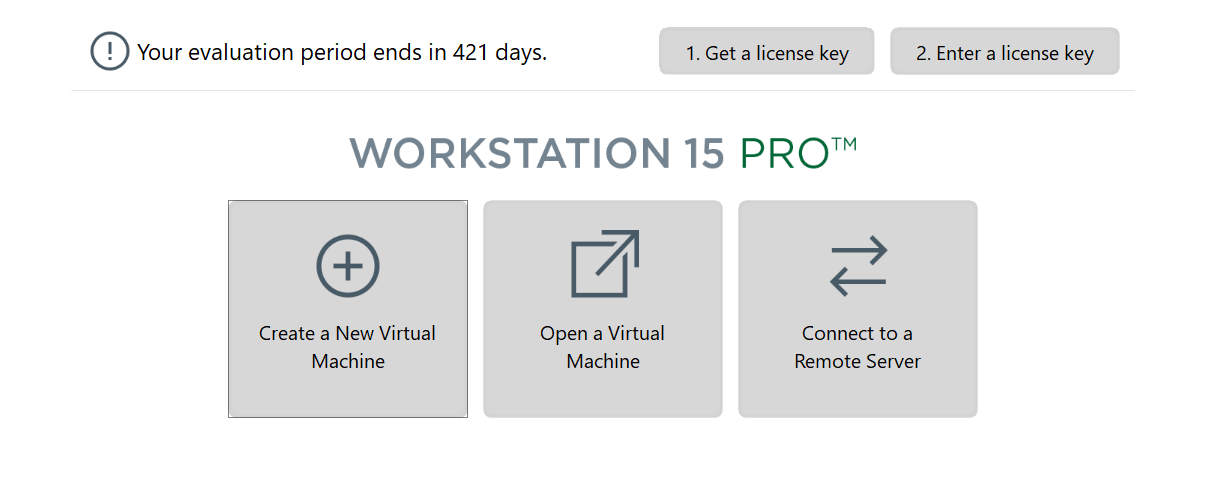
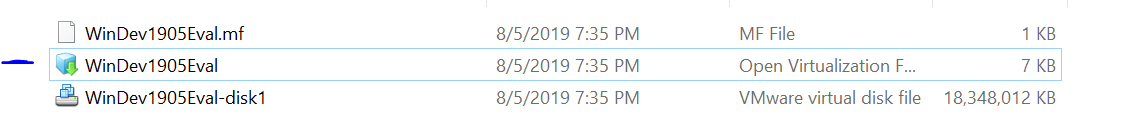
# Details:

*Assumptions: User has requested access to VM toolset from GCU, if not, follow the how to setup documentation found under coarse material.*

Setting up a virtual machine.

1. Start by navigating to the following link to gain access to the VM software available to you.

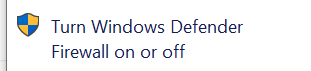
<https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?ws=9c07565e-a326-e711-9427-b8ca3a5db7a1&vsro=8>

1. Sign in using your GCU email and password (this is the same you use to login into the online student portal).
2. For windows users click on the VMWare Workstation 15. 
3. Accept and download the software. Take note of the license/serial number that is provided as you will need this to install software.
4. Navigate to <https://developer.microsoft.com/en-us/windows/downloads/virtual-machines> to locate the ISO required for a windows based VM. Click on the VMWare download link. Be aware, this download is in access of 20GB and will take a while to complete.
5. While image is downloading, install VMWare workstation 15, using all the default settings. Once again ensure that the disk you install it on has enough space (around 20GB HD space per VM).
6. Update as needed/if prompted.
7. Once image is complete, unzip the file.
8. Open VM ware and you will have a landing screen that looks similar to this: 
9. Click create new virtual machine, clicking typical installation on the next part of the wizard.
10. On the next screen you will have the ability to navigate to the folder where you unzipped the image. You should have three files, you want to select the .ovf (Open Virtualization Format Package) file indicated below: 
11. The wizard will install windows 10 on your new VM, process will take about 30 mins or less depending on your system.

Installation of Anti-Virus software.

1. Navigate to [www.avg.com](http://www.avg.com) and click on the “Free” green download button. 
2. Follow the instructions on the installation wizard and keep all configurations set to default. Accept and finish installation.
3. Once sofware is installed click the scan system button. 
4. Step through the three different scan options. Make sure to take screenshots of the status report of each scan for later annylsis.
5. Do not fix any issues at this time, leave as is. We want to compare the results post firewall termination.

Turn off Windows Defender

1. Click your windows button on your keyboard or click the start button in the bottom right. Type in Windows Defender. Select Windows Defender Firewall when it comes up.
2. Click on the button that allows the defender to be turned off or on: 
3. Select the option to turn off the firewall for both public and private networks.
4. To turn these back on simply follow steps 1-3 and choose to turn the service back on.

Rerun anti-virus

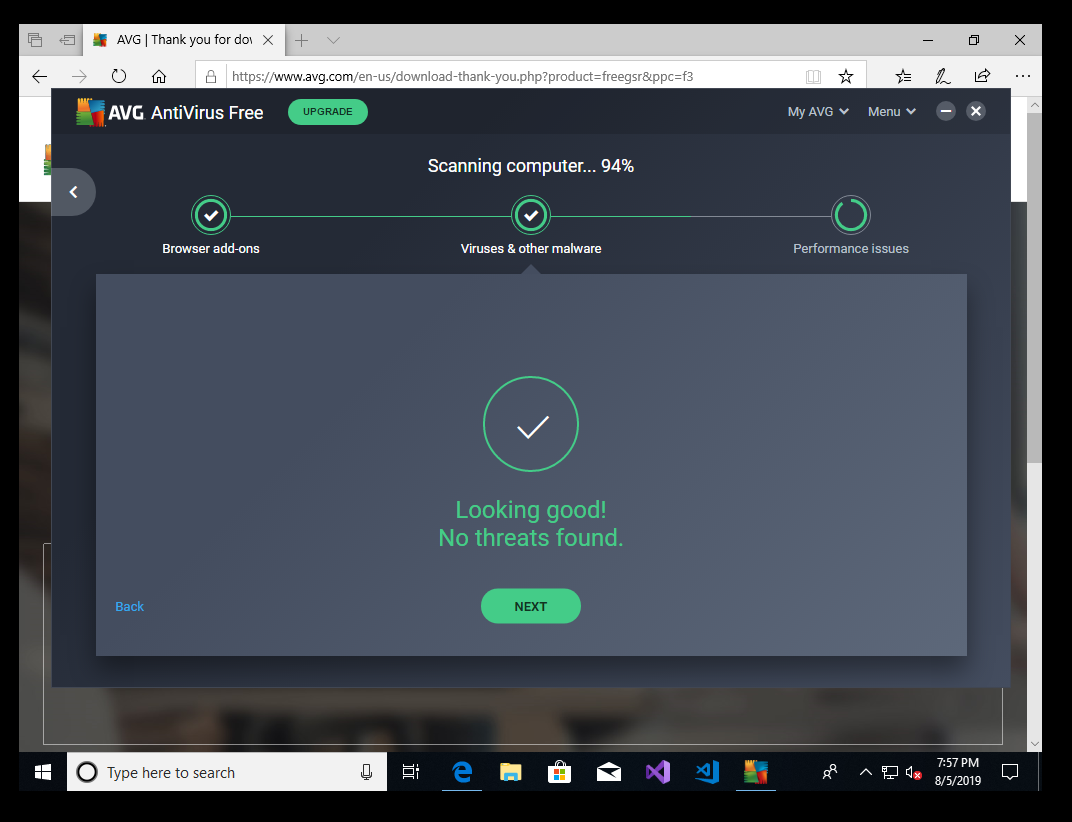
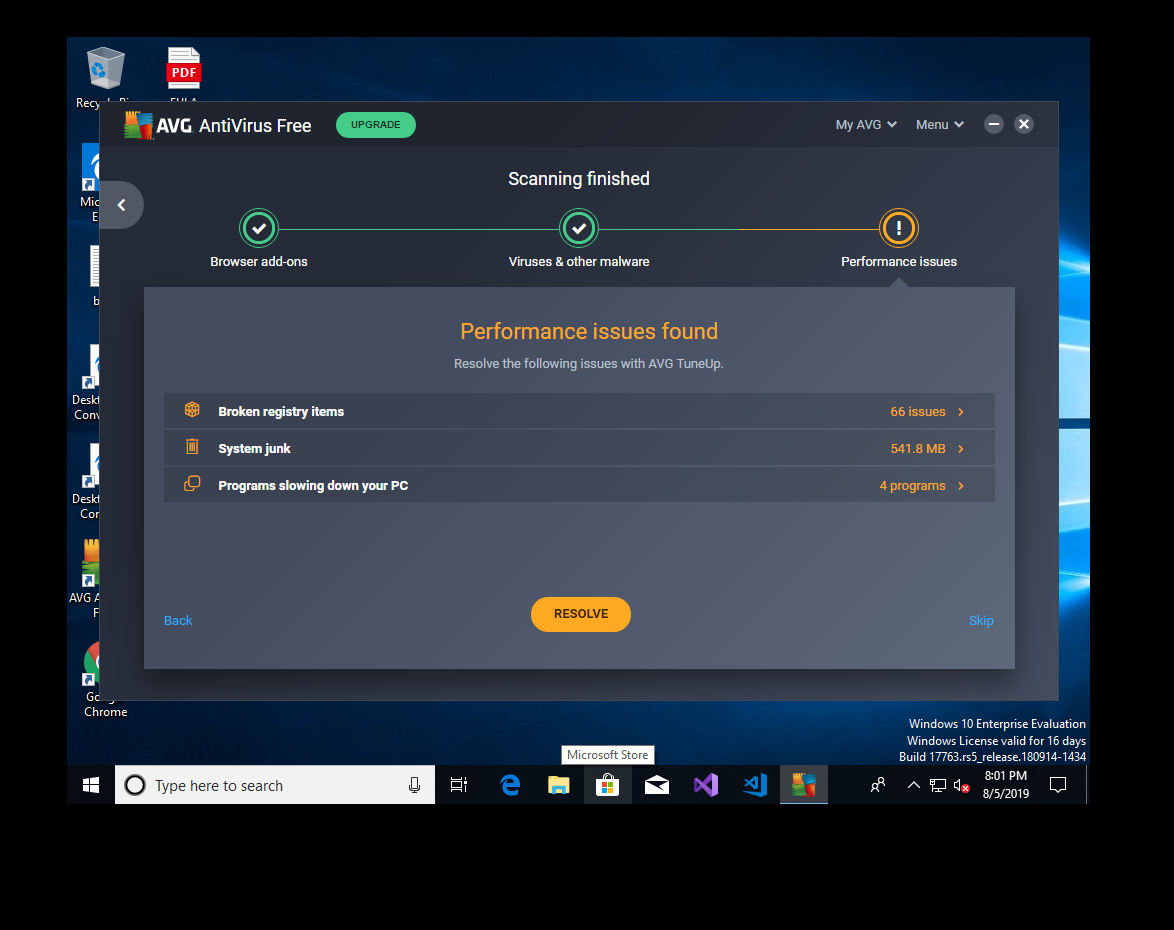
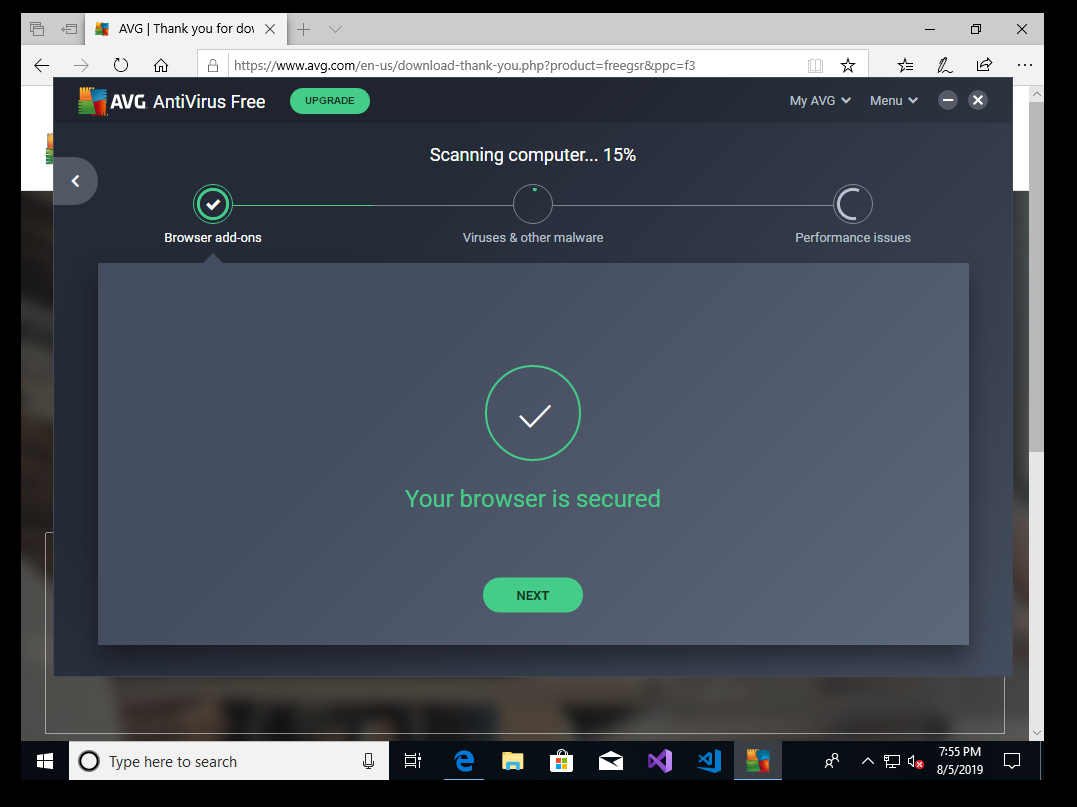
1. Wait for 24 hours with the VM up and connected to the internet.
2. Follow steps 3-5 on the anti-virus installation steps.

# Summary:

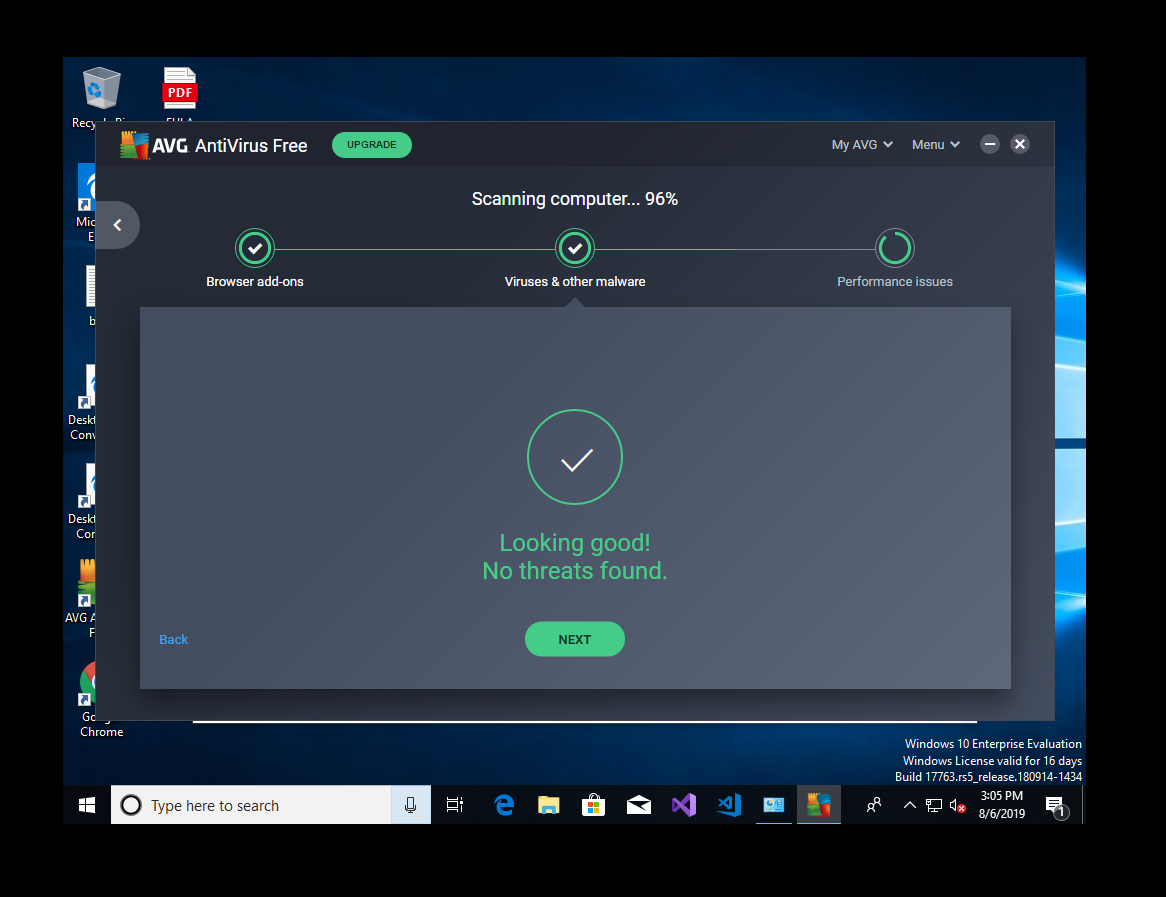
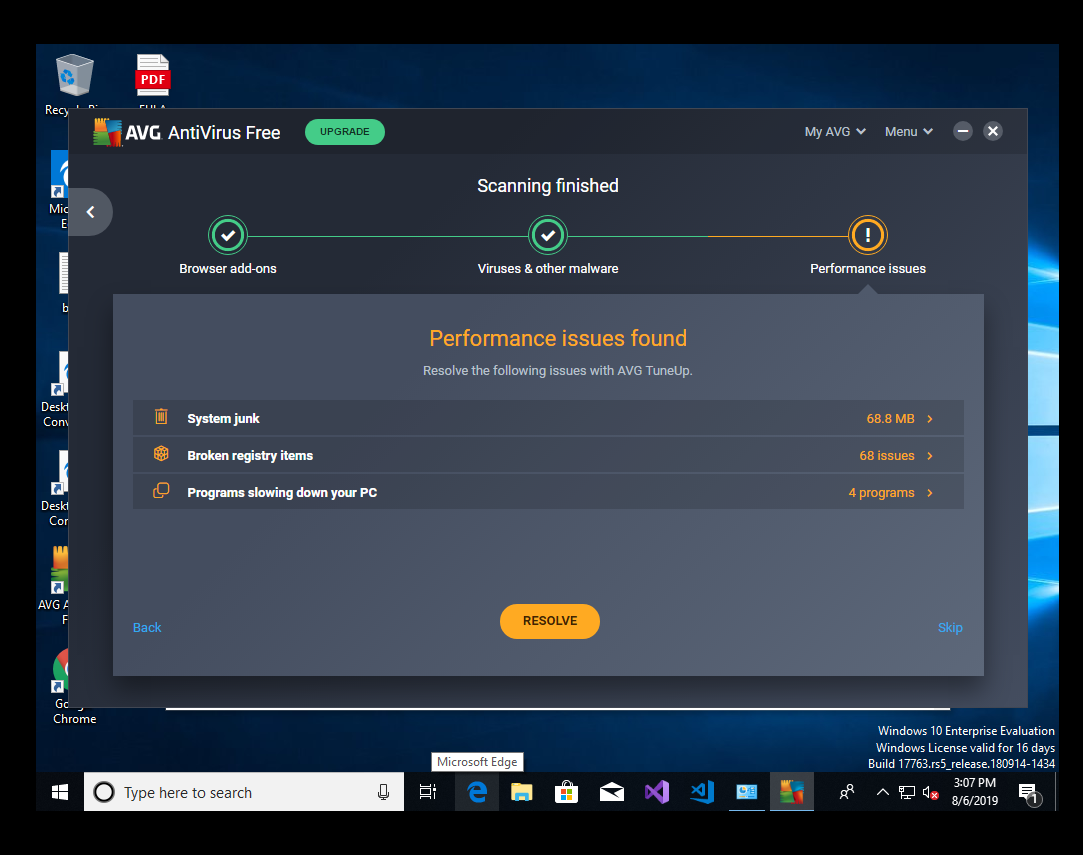
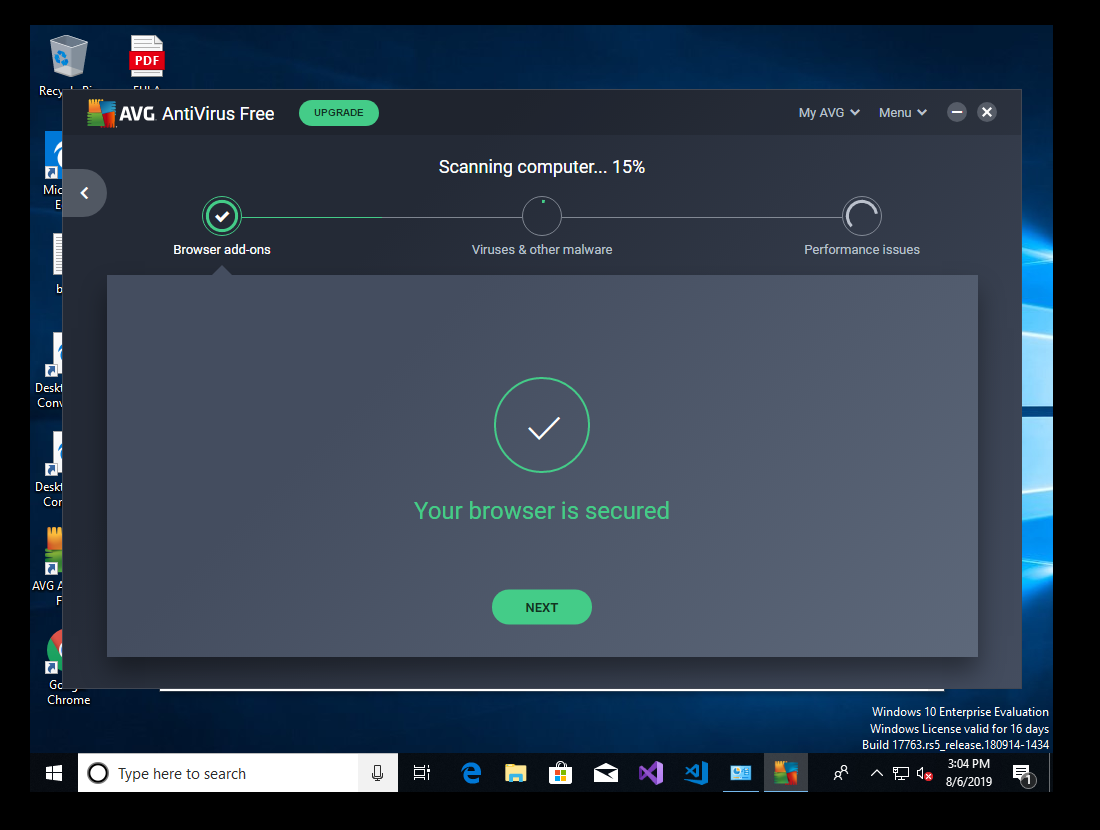
System was up and running for 24 hours. No noticeable issues were brought up. Some performance issues were noted but no change was seen between the scans. After doing some research the current vulnerability that is noted on the AVG website is that of one called BlueKeep. NSA has advised all users to ensure their windows updates are current to avoid being infected.

Summary Screenshots Pre/Post scan:

Pre:



Post:



Basic Secure Design Fundamentals:

When designing a test environment that would be required to detonate malicious software there are some basic fundamentals that are required. In this assignment, we were required to create a new windows VM to establish our test environment. This covered a few of the basic design principles of Separation and Isolation. By doing so we ensured that at least the operating system was segregated away from the main environment and could be tore down with ease.

In this basic design, there were no other requirement needed for the setup of this system. We could use security practices like limiting the privileges to access this system to just a few or at most one. Having an admin account is both helpful and hurtful. If multiple people have access to the account it adds a layer of anonymity to who’s logging in as it cannot be personalized. The installation of the system was pre-determined by Microsoft in this case as to what their image included. Going forward for our test environments, it would be strongly encouraged to make our own images to break down and minimized the amount of software that is installed.

A basic installation installs a bunch of un needed services that will need to be manually turned off. Creating a custom image can help mitigate that setup should a new VM be required. Services that are up and running all offer a point of vulnerability to the system Limiting what is up and available helps cut down on those open spots that attackers could take advantage of.

Lastly, update or ensure you have the latest updates available should your system not be connected to the internet at first. Make sure both your anti-virus software and the OS software has the latest updates for security related issues. This will ensure you have the latest threats covered before you attach your system to the network.