Nessus Vulnerability Scanner Project Steps

Purpose: Compare 4 scans to one another and try to remediate by installing updates and uninstalling deprecated software

- □ Step 1| Download VMware Workstation

- □ Step 2 | Download Windows 10 ISO or Windows 10 VHDX (for ARM)

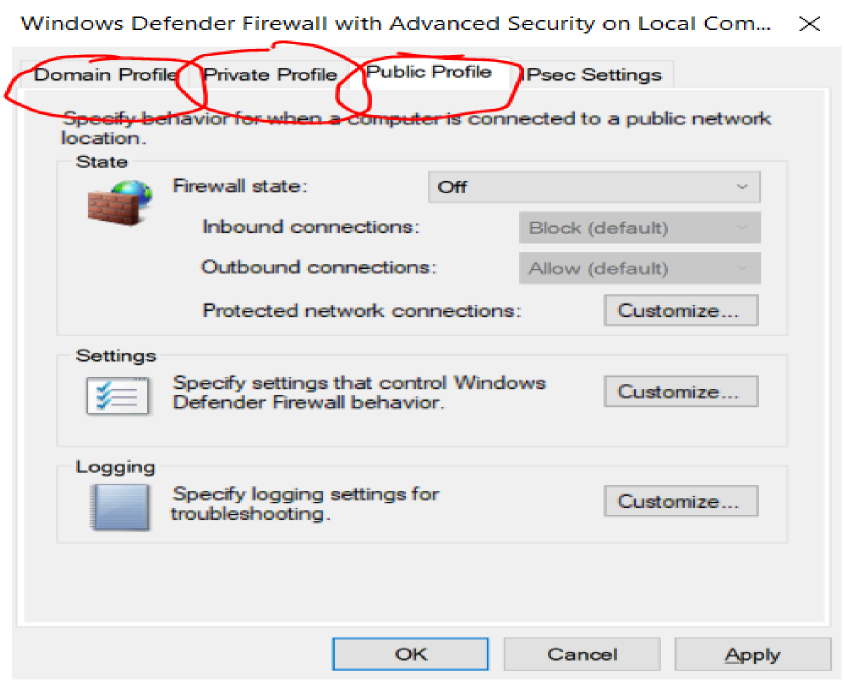
- □ Step 3 | Download Nessus Essentials
    - it will ask you for your name and email and Tenable will email you an access code which will be used later

- □ Step 4 | Copy web address just in case
    - Click Open SSL (and it will initialize for some time)

- □ Step 5 | Set up Nessus Essentials | the plugins may take a while to install, in some cases hrs so just be patient and wait and you will be good to go

- □ Step 6 | Set up Vm and make sure network connection is set up as bridged| Once you set up VM, get the IP address from it by opening up the command line and putting ***ipconfig*** and look at the IPv4 address
    - test ip by using ping command (i.e ***ping 10.0.0.1 -t*** (if there is a timeout request you have to disable firewall)

- □ Step 7 | Disable firewall by typing ***Windows Defender Firewall*** into search bar in VM then click ***Advanced Settings*** and then ***Windows Defender Firewall Properties*** and change Firewall State to Off for all tabs



Specify behavior for when a computer is connected to a public network location.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections:

Settings

Specify settings that control Windows Defender Firewall behavior.

Logging

Specify logging settings for troubleshooting.

□ Step 8 | Go into Nessus web app and click ***New Scan*** | select Basic Network Scan and then add a name and copy the IP address from your VM | once that is all set up click the play button and let the scan run

□ Step 9 | Set up for credentialed scan | go back to ***services.msc*** and select Remote Registry to enable

- 1st type ***share*** into Windows search to enable printer/file sharing
- 2nd type ***user account control*** into Windows search to set notify to ***never notify***
- finally go to start and type regedit then go to ***Local Machine*** → ***Software*** → ***Microsoft*** → ***Windows*** → ***CurrentVersion*** → ***Policies*** → ***System*** | then right click on empty space and select ***DWORD (32-bit) Value*** and name it ***LocalAccountTokenFilterPolicy*** and then set the value to 1
- Now just restart Vm to finalize changes

□ Step 10 | Run credentialed scan and compare it to non-credentialed scan

□ Step 11 | Install deprecated software and run another credentialed scan (MAKE SURE TO DO IT INSIDE VM) https://ftp.mozilla.org/pub/firefox/releases/3.6.12/win32/en-US/

□ Step 12 | Remediate | uninstall Firefox and keep running windows updates until there isn't anymore and then see how many vulnerabilities are remediated (run one last scan)