**NESSUS – VULNERABILITY MANAGEMENT**

Vulnerability management is a continuous and proactive task that scans our network and the different end devices in it to discover, assess, and remediate various vulnerabilities caused due to outdated software or bad patches. This is often an automated job and it helps in keeping the systems and networks safe from attacks. There are various tools available in the market to perform vulnerability scans and one of the most popular ones is NESSUS.

This project aims to install and configure Nessus to scan for vulnerabilities in Windows 10 machines hosted on a virtualization platform like VMWare or Virtual Box. For this particular project, we will be using VMWare Workstation Player 17.

* Step 1 is to download VMWare workstation Player 17, Windows 10 ISO, and Nessus software.
* Then we install the VMWare hypervisor and the Nessus software on the host machine and configure Windows 10 hosts on the VMWare with a Bridged adaptor such that the VM and the host system can communicate as if they are in the same network.
  + Setting up Bridged Adapter
    - Choose bridged Adaptor from the network setting and click on advanced configurations.
    - Deselect all the optios except the host machines NIC.
    - Restart the VM and It should be connected to the host machine and receive and IP from the router DHCP.
* Since this is a lab environment we can disable the domain, public, and private profile settings under the Windows Defender firewall properties to allow communication between the host and the VM

A screenshot of a computer

Description automatically generated

* We can see that the host machine and the VM are able to communicate as if they were on the same network

**Install NESSUS**

* Go to the Nessus website and fill out the form to receive the product key via email. After that download the software.
* Install the Nessus software on the host machine.
* Choose Nessus Essentials as the installation version.
* Create a username and password and complete the installation.

A screenshot of a computer

Description automatically generated

Test the Nessus installation by scanning the Windows 10 machine.

* To do this locate the IP address of the Windows 10 VM using ipconfig command.
* We already have tested the communication between the host system and the VM

Go to Nessus and set up a standard scan.

* Click on the new scan option on the Nessus home page.

A screenshot of a computer

Description automatically generated

* This provides us with various options for different types of scans some of which are
  + Host discovery
  + Basic network scan
  + Advanced scan
  + Advanced dynamic scan

A screenshot of a computer

Description automatically generated

* Click on host discovery to see if we can locate the VM (192.168.26.128) on the network

A screenshot of a computer

Description automatically generated

* The scan details are as follows

A screenshot of a computer

Description automatically generated

* Upon scanning the VM we can see that there is a medium vulnerability in the VM. There are no other software installed on the system other than the OS.
* Next let us try a network scan on the network 192.168.26.0/24

A screenshot of a computer

Description automatically generated

* We can see that the scan has discovered 2 hosts on the network. One is the VM (192.168.26.128) , the other is the host machine (192.168.26.1) and the third one is the DHCP server (192.168.26.254) for the network.

**Performing a Credential Scan**

To perform a credentialed scan on a system outside of a domain we have to first configure the VM using the following steps.

* Go to the VM and open Services.msc

A screenshot of a computer

Description automatically generated

* We can see that the remote registry is disabled, this will allow Nessus scanner to connect to the VM’s registry and scan it for insecure configurations and deprecated settings. We will proceed and enable it. Click on remote registry and the dialog box that opens up choose the Automatic option.

A screenshot of a computer

Description automatically generated

* Next we need to enable file and printer sharing. These settings can be found in the control panel and turn on network discovery and file and printer sharing.
* Since the VM is not on the domain we also need to disable use account control. Search for user accounts in the start bar and pull the scrollbar all the way down.

A screenshot of a computer

Description automatically generated

* *This is not a good control to turn off on a system connected to a domain. But in this Home Lab setup the VM is not connected to any domain and for the credential scan to work we need to be off*
* Open the registry and add a key that will allow the scanner to connect in through the remote access. Go to the registery editor app and follow the path: Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.
* Create a new DWORD in it by right clicking and selecting DWORD from the new>> dropdown list. Name the new DWORD as LocalAccountTokenFilterPolicy and set its value as 1 and then restart the VM.

A screenshot of a computer

Description automatically generated

* After the restart go to Nessus on the host machine and start a new scan, provide the name, description and the IP address of the target (192.168.0.58). Then go to the credentials tab, choose windows and provide the username and password.

A screenshot of a computer

Description automatically generated

* Save and launch the scan. Once completed we can see that the credential scan has revealed several high and medium priority issues with the VM

A screenshot of a computer

Description automatically generated

* Clicking on each of the vulnerabilities will give us the information about what it is and how it can be remediated. For instance the critical IE vulnerability can be fixed by updating the browser

A screenshot of a computer error message

Description automatically generated

**Running Nessus on Windows Server 2019 against a system joined to a Domain**

* Install Nessus on the Windows server Domain controller.
* Launch the client machine connected to the domain. The IP address of the client machine is 172.16.0.100

A computer screen with white text

Description automatically generated

* Go to Nessus on the Domain Controller and create a new scan. First, perform a network scan to check if all the clients are discoverable.
* We can see that the following hosts have been discovered.

A screenshot of a computer

Description automatically generated

* Now we perform an advanced credential scan on the client machine. Since this machine is part of a domain we will first attempt the scan without making any changes to the registry or user account control.
* We are able to launch the scan without issues

A screenshot of a computer

Description automatically generated

* But this has revealed only information items. Try enabling the registry so that the scanner can go deeper. Run the scan again after the configuration changes
* We can see that multiple new vulnerabilities have been revealed, some of which are under the critical and high priority categories.

A screenshot of a computer

Description automatically generated

**Resolving a vulnerability identified by Nessus**

For demonstration purposes we will choose the vulnerability associated with the current version of Internet Explorer (IE) installed on the client system

A screenshot of a computer

Description automatically generated

We will proceed with the critical vulnerability that says the version of Internet Explorer installed on the client is no longer supported.

A screenshot of a computer

Description automatically generated

The Solution provided by Nessus is that we can either upgrade the version of IE or disable it altogether. We will upgrade the version and run the scan once again to verify whether the vulnerability have been resolved. We will run a windows update to try and resolve all outdated version issue of IE and other Windows issues revealed in the vulnerability scan.