**VULNERABILITY ASSESSMENT LAB**

This project is all about Vulnerability assessment, in this project the use of VMware workstation with Windows 10 VM, finally Nessus a well-known vulnerability scanner will be used conduct the vulnerability scan. This portfolio will give a step-by-step process on how the windows system was made vulnerable and how the scan was conducted, what was found during the scan and the remediation strategy that was in place to ma kth system secure.

**SETTING UP THE NETWORK**

**STEP 1:** After logging in to Nessus Vulnerability scanner find the

**A screenshot of a login form

Description automatically generated**

Figure 1

A screenshot of a computer

Description automatically generated

Figure 2

A screenshot of a computer

Description automatically generated

Figure 3

**STEP 2**: Log into the windows VM figure out the IP Address and ping the IP with the host where Nessus reside to confirm they are communicating and on the same network.

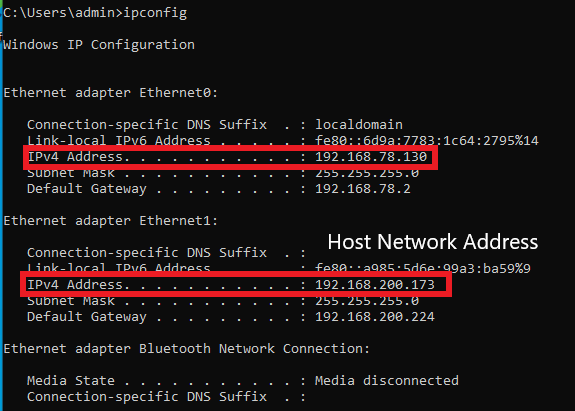


Figure 4

Using ICMPto confirm thy can both communicate with each other see figure 5.

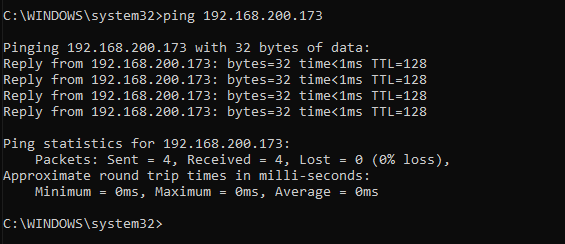


Figure 5

**CONDUCTING THE FIRST SCAN**

**STEP 3:** Now we can perform ICMP successfully, we will go ahead to perform our first scan.

On NESSUS. In figure 6 the details of the target machine are set which include name and IP Address

A screenshot of a computer

Description automatically generated

Figure 6

After the first scan was conducted here is the result, we got in figure 7. We can see the vulnerability is low, there are no serious vulnerabilities attached.

A screenshot of a computer

Description automatically generated

Figure 7

**MAKING THE WINDOWS VM VULNERABLE**

**STEP 4:** To make the windows VM vulnerable we need to ensure some services are disabled. Here are the services that were disabled to allow access to the windows VM.

A screenshot of a computer

Description automatically generated

Figure 8

First, we disable remote registry following these services. **Service > Remote registry > setup type (Automatic).**

A screenshot of a computer

Description automatically generated

Figure 9

Secondly, user access control was disabled to ensure that the user is not notified when a software is installed on the device.

A screenshot of a computer

Description automatically generated

Figure 10

In addition to make the windows VM vulnerable a registry a file is created on ***Computer\HKEY\_LOCAL\_MACHIN\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System*** called ***LocalAccountTokenFilterPolicy*** with the value Data of ***1.*** This policy in place makes the system more vulnerable.

Next a legacy software is installed, the software is an old firefox outdated software which has a lot of vulnerabilities se figure 11 and 12 on the download and installation of the software.

A close-up of a computer

Description automatically generated

Figure 11

A screenshot of a computer

Description automatically generated

Figure 12

After installation w are inform of the vulnerability associated with the installed software. This shows that the certificate is expired which makes it vulnerable to attacks.see figure 13

A screenshot of a computer

Description automatically generated

Figure 13

**SCANNING OF THE VULNERABLE DEVICE**

**STEP 5:** Moving back to Nessus a Credential scan has been setup to scan the Windows VM. Se Figure 14. In the credential scan setup, the username and password of the windows PC is added.

A screenshot of a computer

Description automatically generated

Figure 14

In figure 15 the result of the credential scan is shown which include 93 critical, 114 High and 24 medium vulnerabilities. This is a lot of vulnerabilities found by Nessus, to resolve this this Nessus already suggested possible remediation see figure 16.

A screenshot of a video

Description automatically generated

Figure 15

A screenshot of a computer

Description automatically generated

Figure 16

In figure 16 the suggested remediations says that Firefox needed upgrade and installation of patches is required. In figure 17 we can see the windows VM needs update

A screenshot of a computer error

Description automatically generated

Figure 17

**REMEDIATION STAGE**

A screenshot of a computer error

Description automatically generated

Figure 18

A blue screen with white text

Description automatically generated

Figure 19

In figure 20 we are informed that our windows is up to date

A screenshot of a computer error

Description automatically generated

Figure 20

To resolve the issues with Firefox which was the first remediation suggested by Nessus in figure 16. I decided to uninstall Firefox which resolve the issues with Firefox completely. A new scan is taken by Nessus to see the overall result. In the new scan there are no vulnerabilities discovered.