1. Create a NAT network in VirtualBox.

NAT network was created and assigned to Network adapter for both machines

Graphical user interface, application

Description automatically generated

2. Deploy a VM using each of the provided images.

3. Connect the first interface of each VM to the NAT network. Present a simple diagram of the network topology you just created.

Diagram

Description automatically generated

4. Access the Kali Linux Image, open a terminal, and ping the IP address assigned to the Metasploitable 2 VM. This step is just required to make sure there is communication between the two VMs. Provide screenshots and explain thoroughly each step.

Step 1:

Use ifconfig command in Metasploitable to identify IP address for metasplotable

Text

Description automatically generated

Step 2:

Open Kali Linux terminal and use command “ping “ to check for a connection from metasploitable our target machine

Text, calendar

Description automatically generated

5. Perform a scan using Armitage on the target VM (Metasploitable 2) to**~~identify the OS, open ports~~, and applications running** in this target. Provide screenshots and explain thoroughly each step.

Step1 . Use terminal to Open Armitage via sudo. Armitage is run through the account msfrpcd so it must have route privileges in order to run Nmap and other root restricted operations

Text

Description automatically generated

Step 2.Sellect yes option

Graphical user interface, text, application

Description automatically generated

Step 3. Wait for initialization

Graphical user interface, text, application

Description automatically generated

Step 4. Hosts🡪Nmap Scan🡪Quick Scan (OS detect)

Graphical user interface, text, application

Description automatically generated

Step 5. Input target OS Ip address and select OK

Graphical user interface, text, application

Description automatically generated

Step 6. Nmap scan is performed giving us port and application information on Metasploit

Text

Description automatically generated

6. Open the Nessus application in the Kali Linux VM.

7. Perform a scan with Nessus on the target VM. Provide screenshots and explain thoroughly each step.

Step 7. Selected Basic Network Scan

Graphical user interface, application, email, website

Description automatically generated

Step 8. Name the target OS. Make a description of target. Input target IP address into “Targets”. Save the scan

Graphical user interface, application

Description automatically generated

Step 9. Find scan that was created and select the play button to launch scan. This will tell Nessus to start the scan on the target OS(Metasploitable)

Graphical user interface, application

Description automatically generated

Step 10. Wait for scan to complete

Graphical user interface, text, application, email

Description automatically generated

Step 11. Click on file created to view the progress of scan while it is finding vulnerabilities

Graphical user interface, application

Description automatically generated

Step 12. Select the vulnerabilities tab to view vulnerabilities found

Graphical user interface, text, application, email

Description automatically generated

8. Download the generated report from Nessus and select 2 vulnerabilities that you would like to exploit.

Step 1. Select Report🡪PDF and then generate with the default Executive summary selected

Graphical user interface, text, application, email

Description automatically generated

Step 2. Once Report completes save as a file🡪Go to downloads at top right of screen

A screenshot of a computer

Description automatically generated with medium confidence

Step 2. Open a cloud storage server to store downloaded report into. In theis case we will be using google drive

Step 3.Access drive and select the “New” icon

Graphical user interface, text, application

Description automatically generated

Step 4. Select File upload and

Graphical user interface, application

Description automatically generated

Step 5. Navigate to downloads and select Metaspliot or Report PDF that was downloaded from nessus page

A screenshot of a computer screen

Description automatically generated with medium confidence

Step 6. Select open at bottom right of the screen

Graphical user interface, text, application

Description automatically generated

Step 7.

Go to Host computer(Computer that is hosting virtual machines and environment). Access cloud storage services that PDF was stored through. In this case, we visited our google drive and downloaded the Report PDF we had uploaded to the cloud within the virtual machine.