|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: NISHCHAL SREEVATHSA |  |  |  |  |

Scanning The Network on The Lan

Ethical Hacking & Lab 2

Table of Contents

1. [Executive Summary 2](#_Toc409378035)

[Highlights](#_Toc409378036)

[Objectives](#_Toc409378037)

1. [Lab Description Details 2](#_Toc409378038)

[Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives](#_Toc409378039)

1. [Supporting Evidence 12](#_Toc409378040)
2. [Conclusion & Wrap-Up 13](#_Toc409378041)

[Summary with observations, Success & Failures, Challenges](#_Toc409378042)

# Executive Summary

## Highlights

|  |  |
| --- | --- |
|  | 1. Nmap/Zenmap: The IP addresses of the computers on the LAN will be discovered using nmap's ping scan. We will also do a scan using nmap/Zenmap in order to determine the various Transmission Control Protocol (TCP) ports that are open for a variety of devices on the LAN. 2. Metasploit and Armitage: In order to take the exploitation of the system's vulnerabilities. |

## Objectives

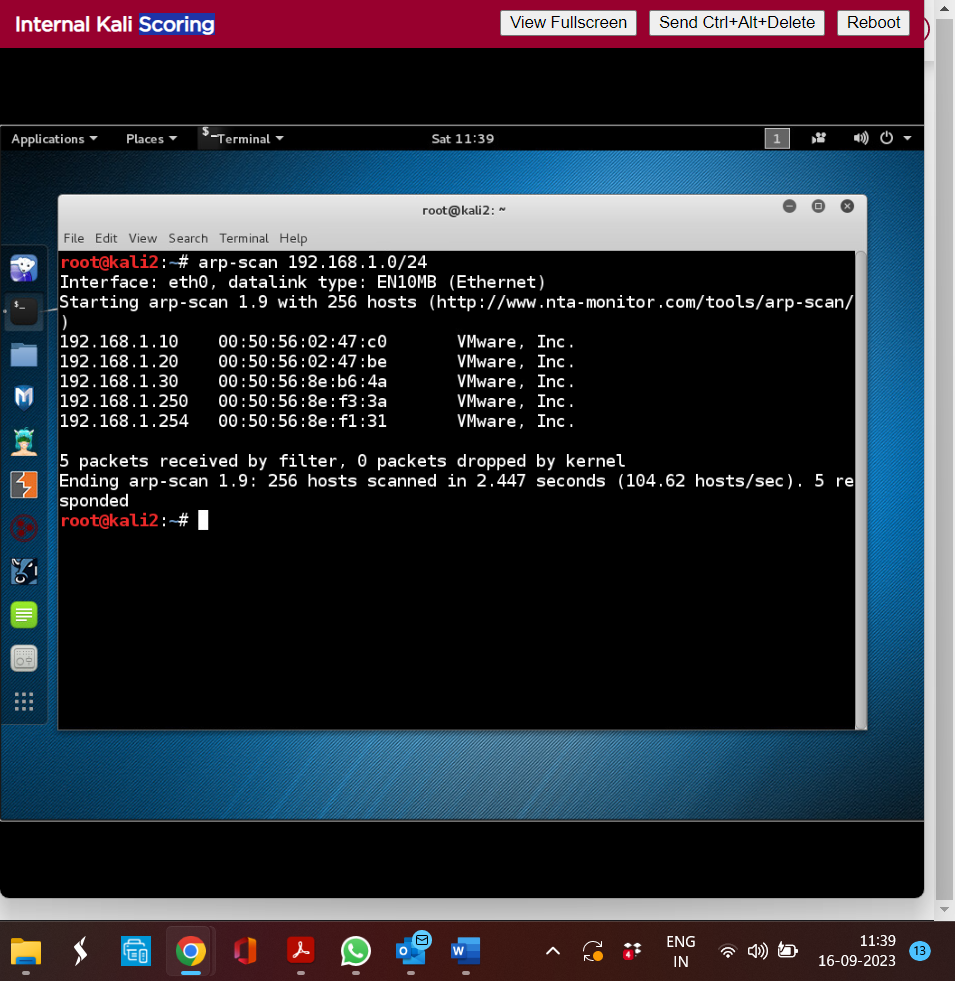
|  |  |
| --- | --- |
|  | The primary objective of this lab is to scan the various Windows hosts connected to the same Local Area Network (LAN) using the Linux distribution Kali. To exploit a weak system, we will also use Armitage and Metasploit. |

# Lab Description Details

**Step 1:** Accessed the internal Kali Linux2 machine on the topology and entered **root** as username and **toor** as password.

**Step 2:** After opening the terminal, Scan the network using the following command to find out how many hosts are there: **arp-search 192.168.1.0/24.**

ARP packets are sent to hosts on the local network by arp-scan, which then displays any responses it receives.



**Step 3:** To find open ports, a TCP scan is run on a number of IP addresses. To find hosts and open ports/services, utilize the free and open-source network vulnerability scanner Nmap.

Commands:

**nmap -sT 192.168.1.10**

**nmap -sT 192.168.1.20**

**nmap -sT 192.168.1.30**

**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatednmap -sT 192.168.1.254**

**A screenshot of a computer

Description automatically generated**A computer screen shot of a black screen

Description automatically generatedNote: Captured the Challenge flag number of **Flag 2: 717993 and Flag 3: 554422** when TCP scanning was performed on IP address 192.168.1.10.

Note: Captured the Challenge flag number of **Flag 4: 232441** when TCP scanning was performed on IP address 192.168.1.30.

**Step 4:** We must run an OS scan for various IP addresses in order to identify the Operating System of various hosts.

Command:

**nmap –O 192.168.1.10 | tail**

**nmap –O 192.168.1.20 | tail**

**nmap –O 192.168.1.30 | tail**

**nmap –O 192.168.1.254 | tail**

A screenshot of a computer

Description automatically generatedA computer screen shot of a computer screen

Description automatically generatedA screenshot of a computer

Description automatically generated

**Step 5:** Use the command "**zenmap**" to launch the zenmap GUI application. Zenmap, a GUI application for viewing ports and information, is now being used to scan the networks. We type in the target IP hosts (192.168.1.\*) and press scan. By clicking on the Ports/Hosts of each IP address, we can see all the open ports and the related banner messages.

A screenshot of a computer

Description automatically generated

**Step 6:** Use Armitage and Metasploit for conducting a Scan. Make sure that the PostgreSQL service is active before executing a scan.

Command: **service postgresql start**

to list all files and directories, the command used is **ls**.

To Switch to the Armitage Directory the command used is **cd armitage**.

to go to the Metasploit interface the command used is **msfconsole**

Note: Captured the Challenge flag number of **sampleflag:999818 and Flag 6: 929211**

**A screenshot of a computer

Description automatically generated**A screenshot of a computer

Description automatically generated

**Step 7:** Start a database nmap scan, run it, and then put the results in the database.

Command: **msf > db\_nmap 192.168.1.\***

**A screenshot of a computer

Description automatically generated**

**Step 8:** Launch Armitage and click the connect button after entering the host, username, password, and port number. After connecting, a GUI containing five hosts, among them the Kali system from the nmap scan, emerges.

**A computer screen shot of a computer

Description automatically generated**Command: **msf>./Armitage**

**A screenshot of a computer

Description automatically generated**

**Step 9:** Run a scan on each host. Right-click on the host and choose "Scan it."Operating System for Host is what we see.

**A computer screen shot of a computer

Description automatically generated**

**Step 10:** Make an attack against machines utilizing Java\_rmi, in which we use Java to access objects located in another virtual machine. We are now attacking the hosts from the menu bar of Armitage.

**A screenshot of a computer

Description automatically generatedA computer screen shot of a computer program

Description automatically generated**Click on Find Attacks and clicked on ok button for the message Attack Analysis Complete that popped-out. The right clicked on 192.168.1.30 and selected Attack->misc->java\_rmi\_server. Attack 192.168.1.30 window opens and click on launch and the host got compromise .

**A screenshot of a computer

Description automatically generated**

**Step 11:** After the Host 192.168.1.30 got compromised, right click on 192.168.1.30 and select meterpreter 1-> Interact -> Command Shell.To see the hashes in a shadow file enter the command: **$ tail /etc/shadow** and was able to find the hashes at the last entry of shadow file, copy the hash and create a new text file called pass.txt using the command: **# leafpad pass.txt** and save the file.

**A computer screen shot of a computer

Description automatically generated**

**Step 12:** Enter the following command to decrypt the hash of pass.txt.

Command: **# John pass.txt**

**A screenshot of a computer

Description automatically generated**

**Step 13:** Choose the host 192.168.1.10 – choose login and set up a telnet connection, enter the user and pass and click on launch, the machine then gets compromised.

A screenshot of a computer

Description automatically generated

**A screenshot of a computer

Description automatically generatedStep 14:** Choose the host 192.168.1.20 – choose login and then click on psexec and then type user (administrator) and pass(P@ssw0rd) and then check mark the use reverse connection and then click on launch, this machine also gets compromised.

**Step 15:** Choose the machine 192.168.1.254 and click on Login and select ssh and enter the user as admin and pass as pfsense and click on launch, this machine also gets compromised.

**A computer screen shot of a computer

Description automatically generated**

# Supporting Evidence

**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedScreenshots, Research, Etc.**

**A screenshot of a computer

Description automatically generated**

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

Gathering network data and identifying network vulnerabilities are both aided by scanning the LAN network. Through network scanning, we may take the necessary precautions to guard against security threats, vulnerable assaults, and data breaches.