|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: Nishchal Sreevathsa |  |  |  |  |

Enumerating Hosts Using Wireshark, Windows, and Linux Commands

Ethical Hacking & Lab 4

Table of Contents

1. [Executive Summary 2](#_Toc409378035)

[Highlights](#_Toc409378036)

[Objectives](#_Toc409378037)

1. [Lab Description Details 3](#_Toc409378038)

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

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

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

# Executive Summary

## Highlights

|  |  |
| --- | --- |
|  | With the help of the tool Wireshark, we do a passive scan for users to record network traffic, and with the aid of the Windows user interface and the application Armitage, we perform an active scan. Use the Windows command-line tool nbtstat to look into NetBIOS name resolution. Nbt stands for NetBIOS over Transmission Control Protocol/Internet Protocol (TCP/IP). NetBIOS provides communication services across networks.  Wireshark: A user can record network traffic or examine a capture file using a free and open-source protocol analyzer.  PostgreSQL: is an object-relational database management system that is open-source. Its main job as a database server is to safely store data.  Nbtstat: To investigate NetBIOS name resolution, use the nbtstat Windows command-line utility. NetBIOS over Transmission Control Protocol/Internet Protocol (TCP/IP) is referred to as Nbt. Over networks, NetBIOS offers communication services.  net Command: To check NetBIOS name resolution, use the Windows command-line utility nbtstat. NetBIOS over Transmission Control Protocol / Internet Protocol (Nbt) is the technical name for this protocol. Network communication services are offered by NetBIOS. |

## Objectives

|  |  |
| --- | --- |
|  | Run a network scan using Armitage 1.  To list or enumerate resources on a target system, use system commands. |

# Lab Description Details

## Performing Passive Scanning

## Step 1: Starting with passive scanning, we click on Kali 2 Linux machine with IP address 192.168.1.101, once the machine starts, enter the username as root and password as toor and login to the system.

## Step 2: Launch the terminal and find the system IP address using the command: ifconfig and then save the IP address configuration using the command: ifconfig > ip1.txt

## 

A screenshot of a computer

Description automatically generated

**Step 3:** Viewed the Ip address configuration of the file ip1.txt, ip2.txt and ip3.txt using the command:

**Cat ip1.txt**

**Cat ip2.txt**

**Cat ip3.txt**

**Note:** Found the Sample flag for ip2.txt and the flag number is **999818**, also captured the flag for ip3.txt and **flag number** is **123457**.

A screenshot of a computer

Description automatically generatedA computer screen shot of a black screen

Description automatically generated

**Step 4:** Ipv4 will not be mentioned for eth0 because the system doesn't have an IP address, for this to take place input the command: **ipconfig eth0 0.0.0.0 up** and then to cross verify whether the IP address is not showing enter the command: **ifconfig**

A computer screen shot of a black screen

Description automatically generated

**Step 5:** The Wireshark application then launches once you type that word in the terminal. Check the eth0 box, then choose Interfaces from Capture, and then push Start. The packet list displays packets. The packet contained the IP addresses **192.168.1.10, 192.168.1.20, and 192.168.1.254**. These IP addresses were found without the use of any active scanning equipment. After analyzing the packets close the Wireshark without saving the file.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Step 6:** **Ifconfig eth0 192.168.1.101 netmask 255.255.255.0** is the command to use to set Kali's IP address and subnet mask. Then use the following command to configure the gateway: **route add default gw 192.168.1.254**

A screenshot of a computer

Description automatically generated

**Step 7:** Backup the current resolv configuration file using the command: **cp /etc/resolv.conf /etc/resolv.conf.backup1**

Then See the system's IP configuration using the command: **cat /etc/resolv.conf.backup1**

**Note: Found the Challenge 2 flag in the backup 2 file: cat /etc/resolv.conf.backup2**

**A screenshot of a computer

Description automatically generated**

**Step 8:** Configure the DNS Server for the Windows Server with Ip address: 192.168.1.10 using the command:

**echo nameserver 192.168.1.10 > /etc/resolv.conf**

Viewed the content of the file resolve using command: **cat /etc/resolv.conf**

**Note:** Found the Challenge 3 flag with number **888999** using command: **cat /etc/resolv.flag**

A computer screen shot of a computer screen

Description automatically generated

**Performing Active Scanning using Commands**

**Step 9:** Select a Windows 10 Machine with IP address 192.168.1.20. Enter the provided login information into the Windows 10 icon and the command prompt as administrator.

**Step 10:** Using the net view command, enumerate the information (data) pertaining to domains.

Commands used are**: net view**

**net view /domain**

**net view /domain: campus**

**net view /domain:workgroup**

# A screenshot of a computer Description automatically generated

**Step 11:** Use the command: **net view \\server** to try to enumerate the shares on the machine. Use the command **net view \\metasploitable** to list the shares on the machine with the name metasploitable.

A computer screen with white text

Description automatically generated

**Step 12:** Found the flag for Challenge 4 and challenge 5 in localhost machine using the command:

**net view \\localhost**

**Challenge 4: Flag5 – 571444**

**Challenge 5: Flag6 - 333459**

A screenshot of a computer

Description automatically generated

**Step 13:** Run the following command to enumerate the IP and MAC Address of the device known as server: **nbtstat -a server**

Then Run the following command to enumerate the IP and MAC Address of the device named metasploitable:  **nbtstat -a METASPLOITABLE**

A computer screen shot of a black screen

Description automatically generated

A computer screen shot of a computer

Description automatically generated

**Performing Active Scanning using the Tools**

**Step 14:** Select Internal Kali 2 Linux with IP address 192.168.1.101 and start the postgresql service in terminal using the command: **service postgresql start**

Then change the directory to Armitage by the command: **cd armitage** then launch the Metasploit using the command: **msfconsole**

A screen shot of a computer

Description automatically generated

**Step 15:** Scan the hosts by entering the following command**: msf > db\_nmap -T4 -A -v 192.168.1.\***

A computer screen with white text

Description automatically generated

**Step 16:** See every host that has been found by entering following command: **msf > hosts**

then launch the armitage which then will start Metasploit RPC server and then scan the **192.168.1.254**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

# Supporting Evidence

**Screenshots, Research, Etc.**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

In the lab, we looked into system enumeration on both Linux and Windows operating systems using a variety of command-line tools such db\_nmap, net, nbtstat, and ifconfig. Wireshark and Armitage were two more graphical user interface (GUI) tools we used. In the lab, we learned about both active and passive scanning—active scanning can be seen on the network while passive scanning cannot.

Through this activity, we learned the critical need of identifying and safeguarding things discovered throughout the enumeration process. By aggressively probing the network, potential vulnerabilities, open ports, and service information were found; if these problems weren't resolved, attackers might take advantage of them. The importance of monitoring network traffic for questionable activities was again highlighted through passive scanning, underlining the need for robust security measures.

In order to prevent threats and preserve the integrity and confidentiality of important assets, proactive network security is critical, with an emphasis on the need to protect and rectify discovered vulnerabilities.

I faced an issue when I tried to view the IP Address configuration in the backup 2 file and couldn’t the challenge2 flag number because when entered the command that was mentioned, the flag number didn’t show up only, I tried rebooting the system and trying the command again but that also didn’t work out and I had to stop the machine and redo it again after some time in which I got the flag number captured for challenge 2.