Lab 2 - Port Scanning

LESSON TITLE:

WARNING:

Warning: Any use of penetration testing techniques on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have explicit permission to test its defenses.

Level:

☐ Beginner
☒ Intermediate
☐ Advanced

Audience: ☒ Instructor-led
☐ Self-taught

Lesson Learning Outcomes: Upon completion of this lesson, students will be able to:

- Demonstrate using advanced options with the nmap network scanning tool
- Demonstrate the use of Metasploit framework to gather and store information about systems on a network

Materials List:

- Computers with Internet connection
- Browsers: Firefox (preferred), Google Chrome, or Internet Explorer
- Intro to Ethical Hacking lab environment

Introduction

In this lab we will begin to explore the tools available in Kali Linux, including the Metasploit framework. We will discover different methods of port scanning a system on a network.

Follow the steps below and answer all question in your own words with as much detail as possible. Paste screen shots where requested. Turn in the entire document to your instructor. Include your username in the filename.

Systems/tools Used:

- Kali Linux *(u: root, p: toor)*
- Metasploitable2
- Power down all other systems on your network.

Module Activity Description:

Part One: Exploring Kali Linux

Look through the applications installed on your Kali Linux System.

1. **List and identify any tools that you recognize.**

Open the terminal application and look at the main page for nmap. Read through this page and do some independent research. Then answer the following questions:

Nikto, nmap, recon-ng, dmitry, sql injection and wireshark

2. **What tasks do system and network administrators use nmap for?**

**Administrators use it for tasks like network inventory,
managing service upgrade schedules and monitoring host or
service uptime**

3. **What option would you use to treat all hosts as online (skip host discovery)?**

Run nmap -Pn

4. **What option would you use to specify specific ports to scan?**

Run nmap -p(port number)

5. **What option would you use to determine service and version info on open ports?**

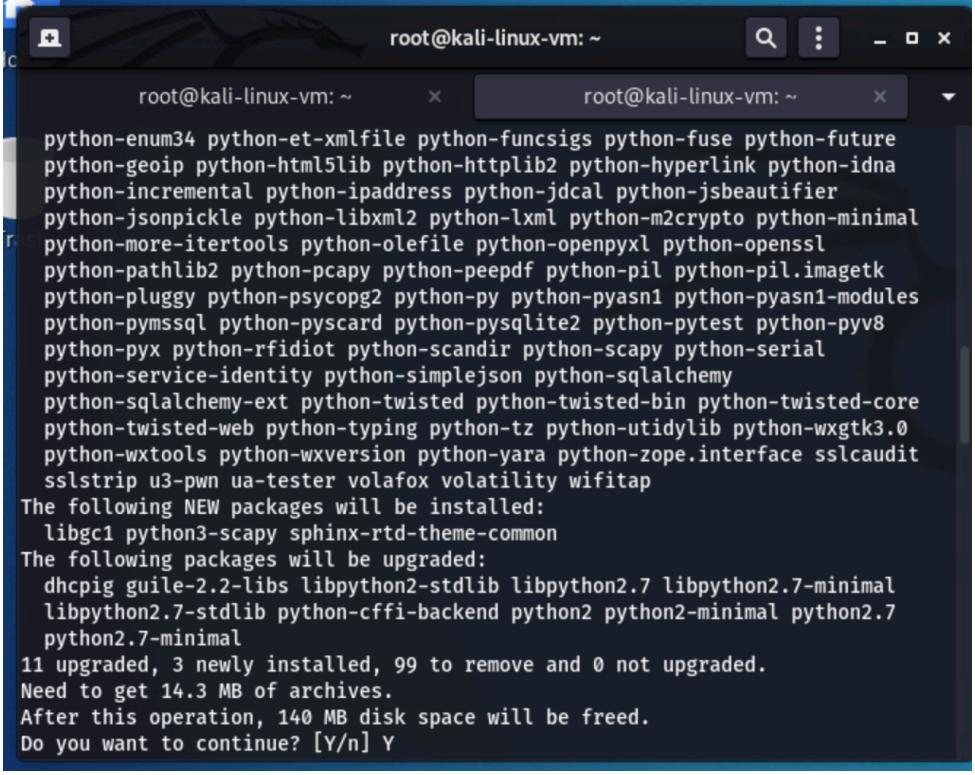
Run nmap -sV

6. **What option would you use to enable OS detection?**

Run nmap -O

Check to see if your Kali system is up to date. If not, install all updates.

7. **Paste a screen shot after updates are installed (or confirmed system is up to date.)**



8. **What distribution of Linux is Kali based on? (Hint: use the uname command)**

Linux Kali 4.15.0-kali2-amd64 #1 SMP Debiam 4.15.11-1kalil x86_64 GNU/Linux

Module Activity Description:

Part Two: Starting Metasploit Framework

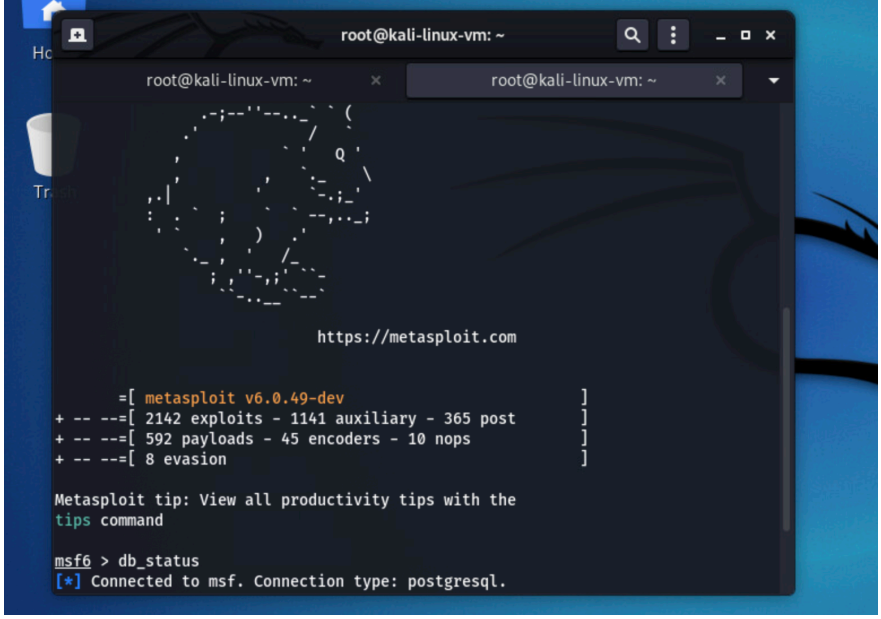
Use the Metasploit Unleashed site for help completing this portion of the lab.

9. **In your own words, explain what the Metasploit Framework is.**

Metasploit is a softward platform used for testing, executing exploits and developing. It used for security testing tools and to exploit modules and can be used to penetrate systems.

Start the postgresql, make sure the 'msfdb' is initialized, and open the msfconsole (see https://www.offensive-security.com/metasploit-unleashed/using-databases/).

10. **Paste a screen shot of each of the commands used to complete these steps**



Complete the rest of this section in the msfconsole. Hint: regular Linux commands will work here, and you can type help to find msf commands

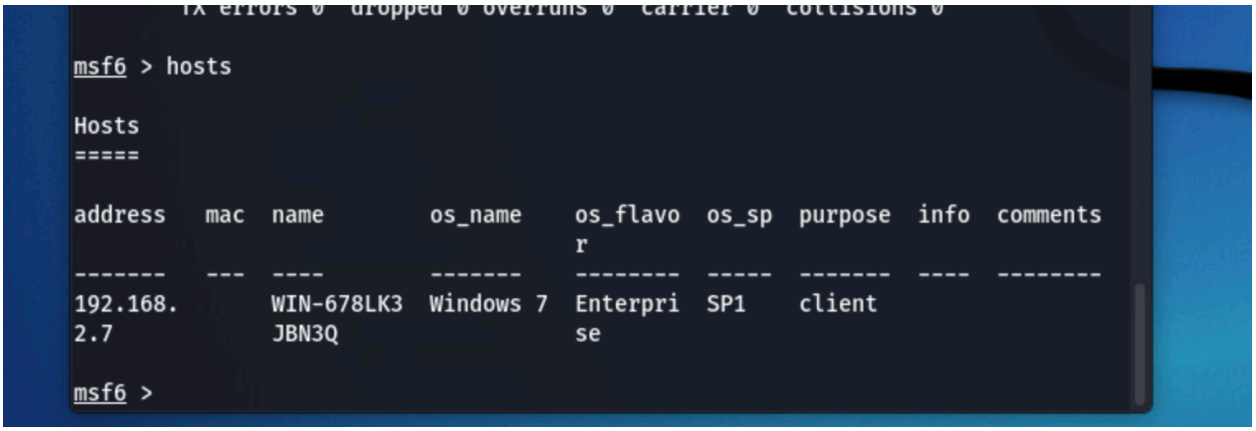
11. What is the IP and subnet mask of your Kali Linux System?

192.168.2.6 and 255.0.0.0

12. What is the Network Address of your network?

192.168.2.6/24

13. What hosts are listed in your database now? (Show a screen shot)



14. What services are listed in your database now? (Show a screen shot)

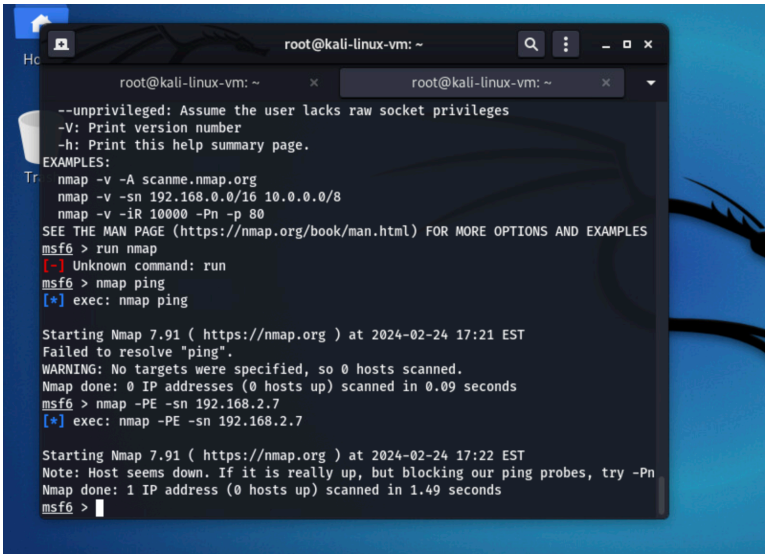
```
msf6 > services
Services
========

host         port  proto  name  state  info
----         ----  -----  ----  -----  ----
192.168.2.7  445   tcp

msf6 >
```

Run an nmap ping sweep in your "network."

15. Paste a screen shot of the command and results.



16. What is the IP address of your metasploit2 target? (Take note of this for future assignments). 192.168.2.7

Run a nmap scan against your target. This time us db_nmap to store the results in your database. Specify options to meet the following criteria:

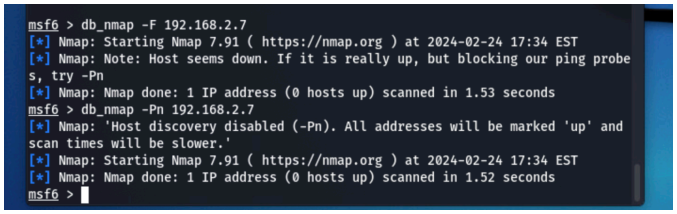
- *Scan ports 22,53,80,443 and 55432*
- *Run OS detection*

17. Show a screen shot of the command and the results.

```
msf6 > db_nmap -p 22 53 80 443 55432 -O 192.168.2.7
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2024-02-24 17:31 EST
[*] Nmap: Nmap done: 5 IP addresses (0 hosts up) scanned in 6.78 seconds
```

18. What services are now listed in your database? (Show a screen shot)

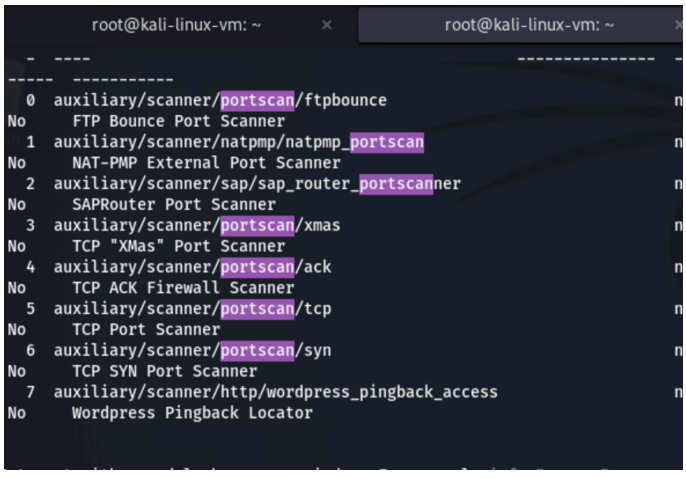
19. Run another nmap scan against your target, this time choose the top 100 ports. (Show a screen shot)



20. What services are <u>running</u> on your target? (Show a screen shot)

Run a scan with one of Metasploit's built in port scanning tools against your target. You choose the tool and the options.

21. Paste a screen shot of the options you choose and the results of running the scanner



22. Did you find any additional services that are running? List the service and ports below. No I didn't see any other services running

Exit the msfconsole.