

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

☐ Advanced

☒ Intermediate

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?

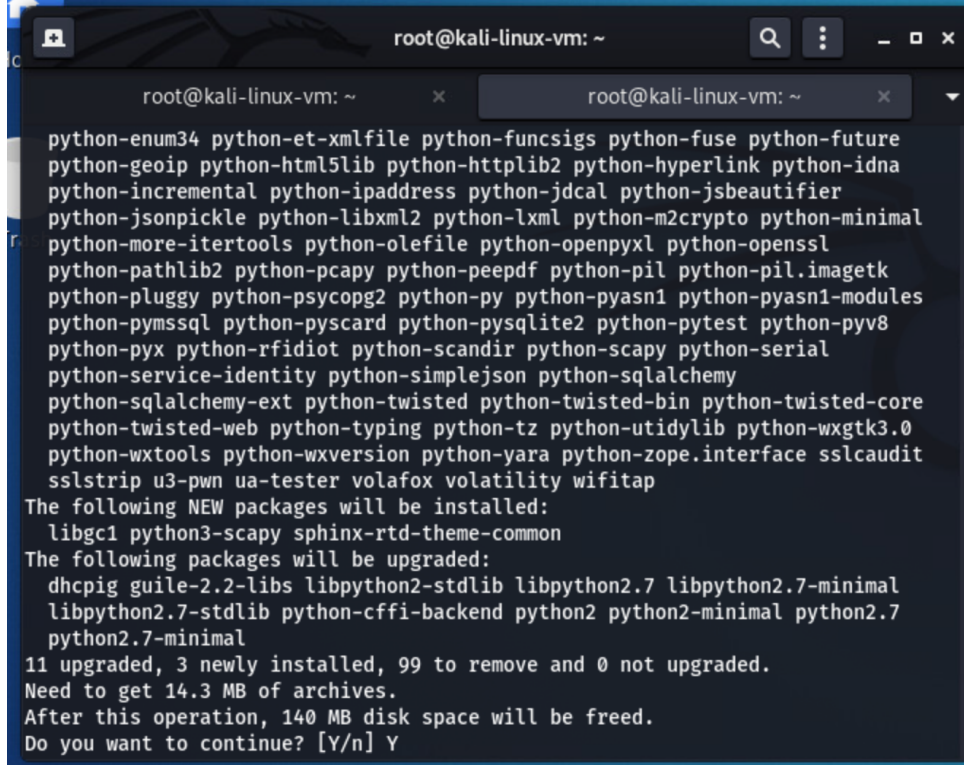
Run nmap -sV

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.)

A terminal window titled 'root@kali-linux-vm: ~' showing the output of a package management command. It lists numerous Python-related packages being installed or upgraded, such as python-enum34, python-et-xmlfile, python-funcsigs, python-fuse, python-future, python-geoip, python-html5lib, python-httplib2, python-hyperlink, python-idna, python-incremental, python-ipaddress, python-jdcal, python-jsbeautifier, python-jsonpickle, python-libxml2, python-lxml, python-m2crypto, python-minimal, python-more-itertools, python-olefile, python-openpyxl, python-openssl, python-pathlib2, python-pcap, python-peepdf, python-pil, python-pil.imagetk, python-pluggy, python-psycopg2, python-py, python-pyasn1, python-pyasn1-modules, python-pymssql, python-pyscard, python-pysqlite2, python-pytest, python-pyv8, python-pyx, python-rfidiot, python-scandir, python-scapy, python-serial, python-service-identity, python-simplejson, python-sqlalchemy, python-sqlalchemy-ext, python-twisted, python-twisted-bin, python-twisted-core, python-twisted-web, python-typing, python-tz, python-utidylib, python-wxgtk3.0, python-wxtools, python-wxversion, python-yara, python-zope.interface, sslcaudit, sslstrip, u3-pwn, ua-tester, volafox, volatility, wifitap. It then lists new packages to be installed (libgc1, python3-scapy, sphinx-rtd-theme-common) and packages to be upgraded (dhcpg, guile-2.2-libs, libpython2-stdlib, libpython2.7, libpython2.7-minimal, libpython2.7-stdlib, python-cffi-backend, python2, python2-minimal, python2.7, python2.7-minimal). The summary shows 11 packages upgraded, 3 newly installed, 99 to be removed, and 0 not upgraded. It also indicates a need for 14.3 MB of archives and that 140 MB of disk space will be freed after the operation. The prompt 'Do you want to continue? [Y/n]' is shown with 'Y' entered.

```
python-enum34 python-et-xmlfile python-funcsigs python-fuse python-future
python-geoip python-html5lib python-httplib2 python-hyperlink python-idna
python-incremental python-ipaddress python-jdcal python-jsbeautifier
python-jsonpickle python-libxml2 python-lxml python-m2crypto python-minimal
python-more-itertools python-olefile python-openpyxl python-openssl
python-pathlib2 python-pcap python-peepdf python-pil python-pil.imagetk
python-pluggy python-psycopg2 python-py python-pyasn1 python-pyasn1-modules
python-pymssql python-pyscard python-pysqlite2 python-pytest python-pyv8
python-pyx python-rfidiot python-scandir python-scapy python-serial
python-service-identity python-simplejson python-sqlalchemy
python-sqlalchemy-ext python-twisted python-twisted-bin python-twisted-core
python-twisted-web python-typing python-tz python-utidylib python-wxgtk3.0
python-wxtools python-wxversion python-yara python-zope.interface sslcaudit
sslstrip u3-pwn ua-tester volafox volatility wifitap
The following NEW packages will be installed:
libgc1 python3-scapy sphinx-rtd-theme-common
The following packages will be upgraded:
dhcpg guile-2.2-libs libpython2-stdlib libpython2.7 libpython2.7-minimal
libpython2.7-stdlib python-cffi-backend python2 python2-minimal python2.7
python2.7-minimal
11 upgraded, 3 newly installed, 99 to remove and 0 not upgraded.
Need to get 14.3 MB of archives.
After this operation, 140 MB disk space will be freed.
Do you want to continue? [Y/n] Y
```

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

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

Module Activity Description:

Part Two: Starting Metasploit Framework

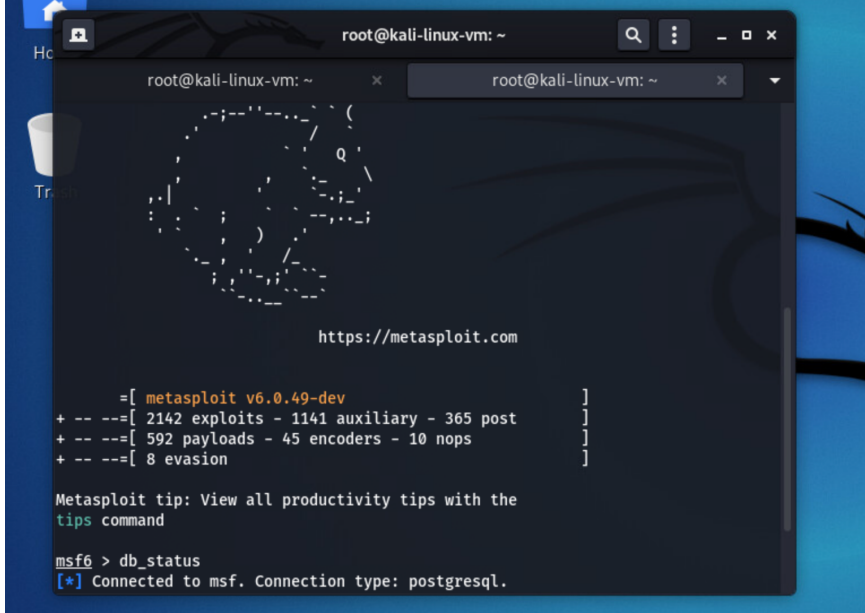
Use the [Metasploit Unleashed](#) site for help completing this portion of the lab.

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

Metasploit is a software 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

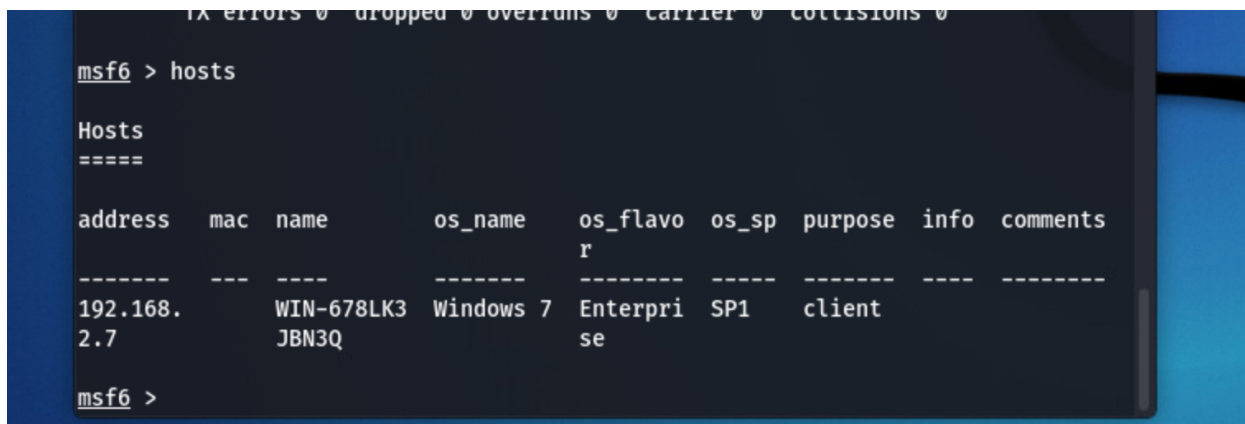
11. What is the IP and subnet mask of your Kali Linux System?

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)



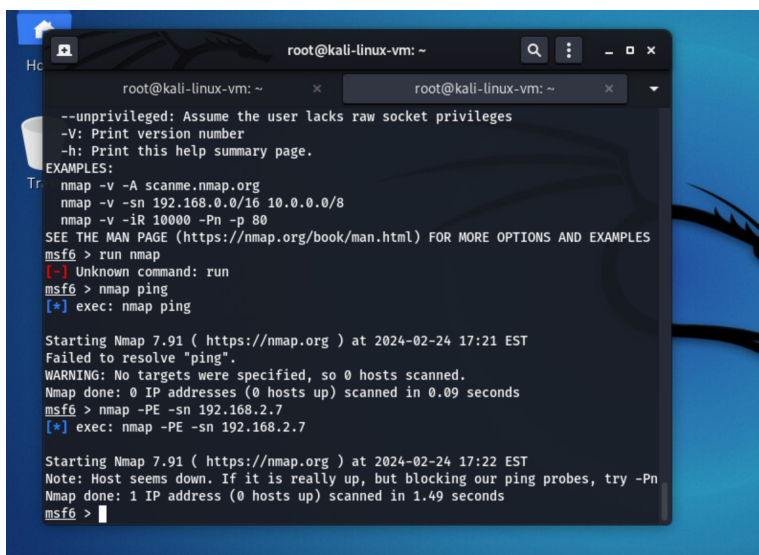
14. What services are listed in your database now? (Show a screen shot)

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

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

Run an nmap ping sweep in your “network.”

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



```
root@kali-linux-vm: ~
root@kali-linux-vm: ~
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
msf6 > run nmap
[-] Unknown command: run
msf6 > nmap ping
[*] exec: nmap ping

Starting Nmap 7.91 ( https://nmap.org ) at 2024-02-24 17:21 EST
Failed to resolve "ping".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.09 seconds
msf6 > nmap -PE -sn 192.168.2.7
[*] exec: nmap -PE -sn 192.168.2.7

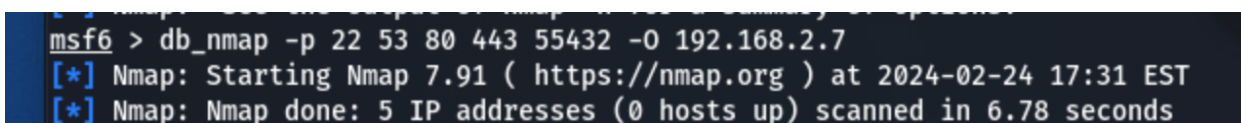
Starting Nmap 7.91 ( https://nmap.org ) at 2024-02-24 17:22 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.49 seconds
msf6 >
```

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)

```
msf6 > services
Services
=====
host      port  proto  name  state  info
-----
192.168.2.7 445   tcp
```

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

```
msf6 > db_nmap -F 192.168.2.7
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2024-02-24 17:34 EST
[*] Nmap: Note: Host seems down. If it is really up, but blocking our ping probe
s, try -Pn
[*] Nmap: Nmap done: 1 IP address (0 hosts up) scanned in 1.53 seconds
msf6 > db_nmap -Pn 192.168.2.7
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and
scan times will be slower.'
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2024-02-24 17:34 EST
[*] Nmap: Nmap done: 1 IP address (0 hosts up) scanned in 1.52 seconds
msf6 >
```

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

```
msf6 > services -u
Services
=====
host      port  proto  name  state  info
-----
192.168.2.7 445   tcp
```

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

```
root@kali-linux-vm: ~
-----
0  auxiliary/scanner/portscan/ftpbounce
No  FTP Bounce Port Scanner
1  auxiliary/scanner/natpmp/natpmp_portscan
No  NAT-PMP External Port Scanner
2  auxiliary/scanner/sap/sap_router_portscanner
No  SAPRouter Port Scanner
3  auxiliary/scanner/portscan/xmas
No  TCP "XMas" Port Scanner
4  auxiliary/scanner/portscan/ack
No  TCP ACK Firewall Scanner
5  auxiliary/scanner/portscan/tcp
No  TCP Port Scanner
6  auxiliary/scanner/portscan/syn
No  TCP SYN Port Scanner
7  auxiliary/scanner/http/wordpress_pingback_access
No  Wordpress Pingback Locator
```

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.