De La Salle University

College of Computer Studies

Ethical Hacking Laboratory Manual

Module No. 3 – Scanning

Name : Daniel Gavrie Clemente

1 Objectives

- To understand the concept of scanning using ping sweep, port scan, and OS fingerprinting.
- To be able to use tools that can ping sweep, port scan, and detect the OS of a host.
- To be able to understand the effects of firewalls on the system

2 Procedure

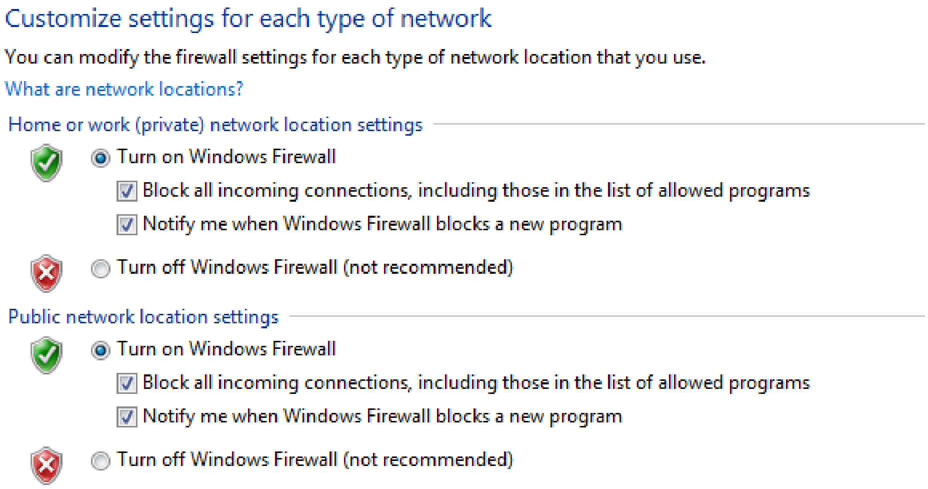
2.1 Initial Setup

1. Set up three machines (whether physical or virtual) with the following specifications :

Machine	Operating System	IP Address/Subnet Mask
Hacker	Kali Linux Username: kali password: kali	172.16.15.5/24 Host only
Victim – Windows	Windows 7 (Firewall Disabled)	172.16.15.10/24 Host only
Victim – Linux	Metasploitable Linux Username : msfadmin password msfadmin	172.16.15.15/24 Host only

**If you are having issues running 3 simultaneous virtual machines, you can run 1 Victim Machine at a time.*

2. Disable the personal firewalls of the machines. When working with physical machines, ensure that the network is isolated. When working with virtual machines, ensure that the network settings of the virtual machines are set to host-only or isolated from the physical network.
3. To turn on the Firewall, go to Control Panel > System and Security > Turn on Windows Firewall On or Off. Make sure to tick the two boxes.



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

☑ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

● Turn on Windows Firewall

☑ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

2.2 ARP Scan / Network Host Discover – netdiscover

4. Open the application “netdiscover” in the Kali Linux system by clicking the following: Application > Kali Linux > Information Gathering > Identify Live Hosts > netdiscover
5. At the command prompt, type in the command

```
netdiscover -i eth0 -p
```

This command executes the “netdiscover” application.

6. If entries do not appear after a long time, try to do a ping between the Windows and Metasploitable Linux machines.

7. List down the discovered IP addresses alive in the table below:

IP Address
192.168.19.1

8. Exit the application by pressing “Ctrl + C” and type in the command

```
netdiscover -i eth0 –r 172.16.15.0/24
```

9. List down the discovered IP addresses alive in the table below:

IP Address
172.16.15.10 172.16.15.15 192.168.19.1

10. Were there any differences between the two commands? What are the differences? Which is faster?

Yes, there was a difference between the two commands. The first command displayed all IP addresses connected to the network, while the second command showed all IP addresses with the IP address configuration of 172.16.15.5. The faster command was the second command.

2.3 Ping Sweep – nmap

11. Open a terminal application in the Kali Linux system.

12. At the command prompt, type in the command

```
nmap -sn 172.16.15.0/24
```

This command executes the “nmap" application.

13. List down the discovered IP addresses alive in the table below:

IP Address
172.16.15.10 172.16.15.15 172.16.15.5

2.4 Effects of Firewall on Ping Sweep

14. Turn on the firewall on the Windows machine and use nmap again to discover any live hosts.

15. List down the discovered IP addresses alive in the table below:

IP Address
172.16.15.10 172.16.15.15 172.16.15.5

16. Were the discovered IP addresses the same before? Why?

The discovered IP addresses were the same as before because Nmap uses ARP requests on local networks to detect live hosts, and ARP responses are not blocked by standard firewalls, allowing Nmap to identify devices even when their firewalls are enabled.

17. Turn off the firewall for the Windows Machine.

2.5 Scanning – nmap (Normal TCP Scan)

18. Start from a command prompt on the Kali Linux system.
19. At the command prompt, type in the command "nmap". Read the switches or what "nmap" can do.
20. At the command prompt, type in the command

```
nmap -sT [IP address]
```

where "IP address" is the IP address of the Windows machine and the Metasploitable Linux machine discovered in the network.

21. List down the ports open, state of the port, and service (Up to 5 ports):

Windows			Linux		
Port	**State**	**Service**	**Port**	**State**	**Service**
135/tcp	open	msrpc	21/tcp	open	ftp
139/tcp	open	netbios-ssn	22/tcp	open	ssh
445/tcp	open	microsoft-ds	23/tcp	open	telnet
5357/tcp	open	wsdapi	25/tcp	open	smtp
			53/tcp	open	domain
49152/tcp	open	unknown			

2.6 Scanning – nmap (SYN Scan)

22. Start from a command prompt on the Kali Linux system

23. At the command prompt, type in the command

```
nmap –sS [IP address]
```

where “IP address” is the IP address of the Windows machine and the Metasploitable Linux machine discovered in the network.

24. List down the ports open, state of the por,t and service (Up to 5 ports):

Windows			Linux		
Port	**State**	**Service**	**Port**	**State**	**Service**
135/tcp	open	msrpc	21/tcp	open	ftp
139/tcp	open	netbios-ssn	22/tcp	open	ssh
445/tcp	open	microsoft-ds	23/tcp	open	telnet
5357/tcp	open	wsdapi	25/tcp	open	smtp
			53/tcp	open	domain
49152/tcp	open	unknown			

25. How many ports are open or closed?

In the Windows machine, there are 990 closed ports and 10 open ports.
In the Linux machine, there are 977 closed ports and 23 open ports.

26. Is there a difference from a TCP scan? What are the differences, if there are any?

There are no differences from the TCP scan.

2.7 Scanning – nmap (FIN Scan)

27. Start from a command prompt on the Kali Linux system.

28. At the command prompt, type in the command

```
nmap –sF [IP address]
```

where “IP address” is the IP address of the Windows machine and the Metasploitable Linux machine discovered in the network.

29. List down the ports open, state of the port, and service (Up to 5 ports):

Windows			Linux		
Port	**State**	**Service**	**Port**	**State**	**Service**
135/tcp	closed	msrpc	21/tcp	open/filtered	ftp
139/tcp	closed	netbios-ssn	22/tcp	open/filtered	ssh
445/tcp	closed	microsoft-ds	23/tcp	open/filtered	telnet
5357/tcp	closed	wsdapi	25/tcp	open/filtered	smtp
49152/tcp	closed	unknown	53/tcp	open/filtered	domain

30. How many ports are open or closed?

There are 1000 ports closed for the Windows machine.
In the Linux machine, there are 977 closed ports and 23 open ports.

2.8 Scanning – nmap (null Scan)

31. Open a terminal application on Kali Linux.

32. Issue a null scan using the “nmap” application and complete the table below (if there is any output):

Windows			Linux		
Port	**State**	**Service**	**Port**	**State**	**Service**
N/A	N/A	N/A	21/tcp 22/tcp 23/tcp 25/tcp 53/tcp	open/filtered open/filtered open/filtered open/filtered open/filtered	ftp ssh telnet smtp domain

33. How many ports are open or closed?

The Windows machine has 1000 closed ports.
The Linux machine has 977 closed ports and 22 open and filtered ports.

34. How did you issue the null scan in “nmap”?

```
    nmap –sN [IP address]
```

2.9 Scanning – nmap (UDP Scan)

35. Start from a command prompt on the Kali Linux system.
36. At the command prompt, type in the command

```
nmap –sU [IP address]
```

where “IP address” is the IP address of the Windows machine and the Metasploitable Linux machine discovered in the network.

37. List down the ports open, state of the por,t and service (Up to 5 ports):

Windows			Linux		
Port	**State**	**Service**	**Port**	**State**	**Service**
137/udp	open	netbios-ns	53/udp 68/udp 69/udp 111/udp 137/udp	open open/filtered open/filtered open open	domain dhcpc tftp rpcbind netbios-ns

38. How many ports are open or filtered

The Windows machine has 1 open UDP port, 170 open and filtered UDP ports, and 829 closed UDP ports.
The Linux machine has 4 open ports, 3 open and filtered ports, and 993 closed ports.

2.10 Rescan Windows Machine with Firewall

39. Turn on the firewall of the Windows machine.

40. Issue a TCP, SYN and UDP scan on the Windows machine using nmap.

41. List down the ports open, state of the port and service (combine ports from all scans):

Port	State	Service
N/A	N/A	N/A

42. Are the discovered open ports different from the previous TCP, SYN and UDP scan? Why?

The discovered open ports are different from the previous TCP, SYN, and UDP scan because each scanning technique interacts with the target system and its firewall in different ways, leading to varying results.

2.11 OS Fingerprinting – nmap (OS Detection)

43. Turn off the firewall of the windows machine.

44. At the command prompt of Kali Linux type in the command

```
nmap –v –O [IP address]
```

where “IP address” is the IP address of the Window machine discovered in the network.

45. What are the guessed operating system of nmap? List it down in the table below:

OS Guesses
Microsoft Windows 2008|7|Vista|8.1

46. Was the guess accurate? Why?

The guess was accurate because it had a close guess to the actual OS and the firewall was turned off.

47. Use “nmap” again to detect the OS of the other IP address, list down the guessed operating system below:

OS Guesses
Linux 2.6.X

48. Was the guess accurate?

Metasploitable 2 is a deliberately insecure Linux target that fully responds to Nmap OS detection, making it easy for Nmap to accurately identify it as a Linux-based system

3 Guide Questions:

1. What is ping sweep? How can it be used to detect live hosts on the network?

A ping sweep is a network scanning technique used to determine which hosts are active by sending ICMP Echo Request packets to multiple IP addresses.It detects live hosts by identifying which IP addresses respond with an ICMP Echo Reply.

2. What does the application “netdiscover” do? Is it the same as “netenum”?
   Netdiscover is a passive and active network reconnaissance tool used to discover live hosts and their associated IP and MAC addresses on a subnet. No, netdiscover and netenum are different tools with distinct functions, and "netenum" is less common and typically refers to a different or custom enumeration tool.
3. What does the application “netenum” do? What are the input parameters?
   Netenum is generally used for automated enumeration of network resources like shared files and services across multiple hosts. Input parameters for netenum usually include target IP ranges, username/password credentials (if needed), and output file options, though specifics depend on the version or script used.
4. Using a ping sweep, can you automatically assume that a host is down if there is not reply from it? Why or why not?
   No, because a host may block ICMP traffic, be behind a firewall, or be configured not to respond to pings.
5. What is the purpose of port scan? How can it be used to detect live hosts and services on the network?
   A port scan identifies open ports and services running on a host to assess potential vulnerabilities and available services. If a host responds to probes on specific ports, it confirms the host is live and reveals which services are accessible.
6. Are there any scan types that do not work against all OS? Which are these?
   Yes, scans like FIN, NULL, and XMAS may not work reliably against Windows systems because they do not conform to RFC 793.
7. Why use different types of port scan aside from the normal TCP connect scan (even FIN and SYN scan) to detect services on a hosts?
   Different scan types can bypass certain firewalls or logging mechanisms and provide stealthier or more accurate results.
8. How can you use the “nmap” application to detect services on a live hosts? What are some of the important switches to use to able to do port scanning and OS detection?
   You can use `nmap -sV` to detect services and `-O` for OS detection on live hosts. Important switches include `-sS` (SYN scan), `-sV` (version detection), `-O` (OS detection), and `-T4` (faster execution).
9. What is the significance of discovering open ports on system?
   Discovering open ports reveals possible entry points for attackers and indicates which services are exposed to the network.

Kali Linux - Hacker Machine
https://www.kali.org/get-kali/#kali-virtual-machines

Metasploitable 2 - Victim Machine
https://sourceforge.net/projects/metasploitable/

Windows 7 Victim Machine
https://drive.google.com/file/d/1JevakPpWjH8qqHD6lTqPkdFjzHYWYcaL/view?pli=1