Experiment-8

Aim: NMAP to discover Live hosts using Nmap Scans on TryHackMe Platform
To discover live hosts using Nmap scans on TryHackme.

Intro
This experiment outlines the processes that Nmap takes before port-scanning to find which systems are online. This stage is critical since attempting to port-scan offline systems will merely waste time & create unneeded network noise.

The following is the information that will be covered in an attempt to discover live hosts:

1) ARP scan: This scan uses ARP requests to discover live hosts.

2) ICMP scan: This scan uses ICMP requests to identify live hosts.

3) TCP/UDP Ping scan: This scan sends Packets to TCP ports and UDP ports to determine live hosts.

There will be two scanners introduced
1. arp-scan
2. masscan

Nmap (Network Mapper) - It is well known tool for mapping networks, locating live hosts and detecting running services. Nmap's scripting engine can be used to extend its capabilities such as fingerprinting services & exploiting flaws.

The scans typically follow the steps represented in the image below, but several are optional and are conditional on the "command-line" options Prior to the scan.

1	Enumerate targets
2	Discover live hosts
3	Reverse DNS lookup
4	Scan ports
5	Detect versions
6	Detect O.S
7	Trace route
8.	Scripts
9	write output

5/5
13/X/23

How many devices are you able to discover using ARP requests?

3

What is the option required to tell Nmap to use ICMP Timestamp to discuss live hosts?

-PP

What is the option required to tell Nmap to use ICMP address Mask to discover live hosts?

- PM.

What is the option requried to tell Nmap to use ICMP Echo to discover live hosts?

-PE

Which TCP ping scan does not require a Privileged account?

TCP SYN Ping.

What option do you need to add a Nmap to run a TCP SYN ping scan on telnet Port?

-PS23.

We want Nmap to issue a reverse DNS lookup for all possible hosts on subnet hoping to get some insights from names. What option should we add?

- R.

What is the type of packet that computer1 sent before the ping?

ARP Request

What is the type of packet that computer1 recevied before being able to send the ping?

ARP Response.

How many computers responded to the ping request?

1

Send a packet with the following

- From Computer2
- To Computer5
- Packet Type : "Ping Request"

What is the name of the first device that responded to the first ARP Request?

router.

What is the name of the first device that responded to second ARP Request?

Computer 5