Ex.No:12

Practical-12

Aim:

To Discover Live Hosts using Nmap Scans on TryHackMe platform.

Introduction: (Task 1)

* Their experiment outlines processes Nmap takes before port-scanning to find systems are online.
* The following is info that will be covered in an attempt to discover live hosts.

i) ARP scan: Uses ARP requests to discover live hosts.

ii) ICMP scan: Uses ICMP requests to identify live hosts.

iii) TCP / UDP: Sends Packets to TCP ports ie Ping scan UDP ports to determine live hosts.

There will be 2 scenario's introduced:-

i) arp-scan

ii) marscan

* Nmap (Network mapper) → well-known tool for mapping networks, locating live hosts, detecting running devices.

* It extend its capabilities, such are Fingerprinting, exploiting flaws.

* The scan follow the steps represented in the image below.

1 Enumerate Targets

2 Discover Host

3 Reverse - DNS lookup

4 Scan ports

5 Detect versions

6 Detect OS

7 Traceroute

8 Scripts

9 Write output

Task 2 Subnetworks:

1) How many devices can see ARP request?

=> 4

2) Did computer 6 receive ARP request?

=> N

3) How many devices can see ARP request?

=> 4

4) Did computer reply to ARP request?

=> Y

Task 3 Enumerating Targets:

1) What is first IP addr Nmap, would scan if 10.10.12.13/29 your target?

=> 10.10.12.8

2) How many IP addrs will Nmap scan if you provide range 10.10.10-255.101-125?

=> 6400

Task 4: Discovering Live Hosts:

1) What is type of packet computer sent before the ping?

=> ARP request.

2) What is the type of packet that computer received before being able to send ping?

=> ARP response.

3) How many computers responded to the ping request

=> 1

4) What is name of first device respond to first ARP request?

=> Router

5) What is name of first device respond to second ARP request?

=> Computer

6) Send another ping request. Did it require new ARP requests?

=> N.

Task 5 Nmap Host Discovery Using ARP:

i) How many device are you able to discover using ARP requests?

⇒ 3

Task 6 Nmap Host Discovery Using ICMP:

1) What is option required to tell Nmap to use ICMP Timestamp to discover live hosts?

⇒ -PE

2) What is option required to tell Nmap to use ICMP address mask to discover live hosts?

⇒ -PM

3) What is option required to tell Nmap to use ICMP Echo to discover live hosts?

⇒ -PE

Task 7:

1) Which TCP ping scan does not require a Privileged account.

⇒ TCP syn ping

2) which TCP ping scan requires a privileged account?

⇒ tcp ack ping

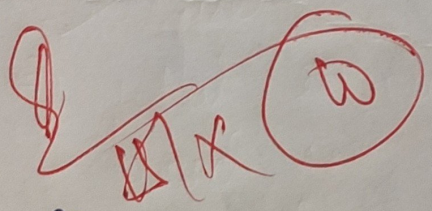
3) What option do you need to added Nmap to run on telnet port?

⇒ -P23

Task 8:

1) We want Nmap to issue reverse DNS. What option should we add?

⇒ -R



Result:

Live Hosts using Nmap scans on TryHackme platform.