EX. NO: 8A. DISCOVER LIVE HOSTS USING NMAP SCANS.

DATE: 15.09.25

AIM:

To Discover live hosts using Nmap scans (ARP, ICMP, TCP/UDP) on the Try HackMe platform

link: https://tryhackme.com/room/nmap01.

Introduction:

When targeting a network, we need an efficient tool to handle repetitive tasks. The tool we rely on is Nmap. The first question about finding live computers is answered in this room. This room is the first series of four rooms dedicated to Nmap. The second question about running services is answered in the next Nmap rooms.

This room is the first of four in this Nmap series. These four rooms are also part of the Network Security module.

* Nmap Live Host Discovery
* Nmap Basic port Scans
* Nmap Advanced port Scans.
* Nmap post port scans.

We also introduce two scanners, arp-scan and masscan, and explain how they overlap with part of Nmap's host discovery.

As already mentioned, starting with this room, we will use Nmap to discover systems and services actively.

Subnetworks: A network segment is a group of computers linked through a shared medium like an Ethernet switch or wifi Access point. In IP networks a subnetwork typically consists of one or more network segments connected together and configured

to use the same router. A Network segment is (21) a physical connection, while a Subnetwork is a logical connection. 25

Requests within a Subnet

(4 - computer Subnet)

Send packet.

From:

Computer 1

To:

Computer 2

Packet type:

arp - request

Data:

computer 6

Send packet.

* from computer 1
* TO computer 1 (to indicate it is broadcast)
* packet Type: "ARP Request".
* Data: computer 6 (because we are asking for computer 6 MAC address using ARP request)
* How Many devices can see ARP request ? 4
* Did computer 6 receive the ARP Request ? N.

Sending packets b/w Subnets.

Send packet.

From:

Computer 4

To:

Computer 4

Packet Type:

arp - request

Data:

Computer 6

Send packet -

* From computer 4
* TO computer 6 (to indicate it is Broadcast) 25?
* packet type: "ARP Request".
* Data: Computer 6 (because we are asking for computer 6 MAC address using ARP Request)

How many device can see the ARP Request?

4

Did computer 6 reply to the ARP. Request?

(Y, N) Y.

Enumerating Targets:

Targets can be specified in 3 ways.

1) List 2) Range 3) subnet.

Discovering live Hosts:

TCP/IP layers.

* ARP from Link Layer.
* ICMP from Network layer.
* TCP from Transport layer
* UDP from Transport Layer.

NMAP Host Discovery using ARP:

NMAP typically uses a ping scan to find live hosts and there proceed to scan those live hosts.

NMAP Host Discovery using ICMP:

A simple method to identify live hosts on a target network is by pinging each IP address and checking for response (ICMP Type 8(echo request and Type 0(Echo reply).

Tcp Ack ping:

To utilize Ack ping in Nmap, which sends a packet with the Ack flag set, you need to run Nmap on a privileged user. If you attempt this is an unprivileged user, Nmap will perform a 3-way handshake by default.

UDP ping:

You can also employ UDP to check if the host is online. Unlike tcp SYN ping, sending a UDP packet to an open port typically does not elicit a response.

Student observation:

1) which tcp ping scan does not require a privileged account?

Ans: Tcp SYN ping.

2) Which Tcp ping scan require privileged account?

Ans: Tcp Ack ping

3) What option do you need to add to Nmap to run a Tcp SYN ping scan on the telnet port.

Ans: -ps 23.

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

Ans: -pp.

5) What is the option required to tell nmap to use ICMP Address Mask to discover live hosts?

Ans: -PM.

25/1

RESULT :

Thus we have learned how ARP, ICMP, TCP & UDP can detect live hosts by completing this room.

22/X/22