Exp: No: 8
10/10/25

NMAP to discover live hosts using Nmap scans On Tryhackme.

Aim:

To discover live hosts using Nmap scans on Tryhack.

Intro:

This experiment outlines the processes that Nmap takes before pot-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 line 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. argp-scan
2. mass can.

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

1 Enumerate targets

2 Discover live hosts.

3 Reverse DNS look up

4 Scan ports

5 Detect Versions.

6 Detail-OS

7 Terace route

8 Scripts

9 Onto Output.

fingerprinting services & exploriting flaws.

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

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?

-RP

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

-PM

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

PE

What is the type of packet that computer 1 received before being able to send the ping?

ARP Response.

How many computers respond to the ping request

1

Send a packet with the following.

* From Computer 2
* To Computer 5
* Packet Type: "Ping Request"

14/x/25 9/10