12/8

Practical-8.

18/9/25 a) To Discover Live hosts using NMap Scan (ARP, ICMP, TCP, UDP) on try Hack Me platform room link: https://tryhackme.com/room/nmap01.

AIM:

To discover Live hosts using NMap Scan (ARP, ICMP, TCP, UDP) on try hack Me platform

Introduction to NMap: Live host discovery

When targeting a network, efficiency is key - we need a tool that can quickly identify active systems and services they running. Nmap, a free, open source, industry-standard tool created by Gordon Lyon in 1997, a tool.

This is first of four part series on Nmap, focusing specifically on live host Discovery. this initial stage is crucial as it prevents wasted time and network traffic attempt to port Scan offline systems

NMap host Discovery Method

1. ARP Scan: Use ARP request to discover live host on local network.

2. ICMP Scan: Uses ICMP (ping) requests to identify live hosts.

3. TCP/UDP ping Scan: send packets to specific TCP & UDP ports determine if host is responsive.

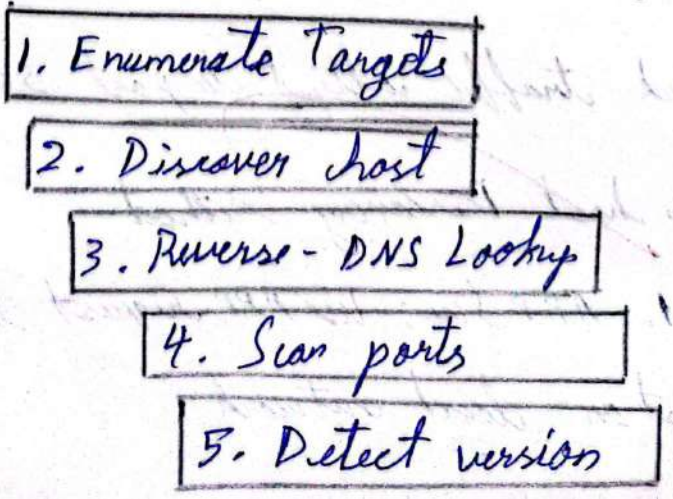
- Nmap Live Host Discovery
- Nmap Base Port Scans
- Nmap Advanced Port Scans
- Nmap Post Port Scan.

There are two Scanners introduced

1. arp-scan
2. masscan.

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

Diagram:



6. Detect OS

7. Traceroute

8. Scripts

9. write output

Task 2 sub net works :

1) How many device can see ARP request?

4

2) Did computer receive ARP request?

N

3) how many device can ARP request?

4

4) Did computer replied to ARP request?

Y

Task 3 Enumerating targets :

1) what is first IP addr Nmap would stan if

10.10.12.13/29 your target

=) 10.10.12.8

2) how many IP addr will Nmap scan if you provid range 10.10-0-255.101-125?

6400

Task 4 Discovering Live hosts

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

ARP request

2) what is type of packet that computer 1 received before being able to send ping?

ARP response

3) how many computer respond to ping request

: 1

4) what is name of first device respond to first ARP resquest?

Router

5) what is name of first device respond to seand ARP request?

Computer

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

N

task 5 Nmap host discovery using ARP

1) how many devices are you able to discover using ARP request?

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 request tell Nmap to use ICMP addr mask to discover live hosts?

-PM

3) what is option requested to tell Nmap to use ICMP Echo to discover live host?

-PE

task 7:

1) which TCP ping scan does not require a privileg account?

tcp syn ping

2) which TCP ping scan requires a privileg account?

tcp ack ping

3) what option do you need to add Nmap to scan 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.