Ex. No. 07 **NMAP Live Host Discovery**

Date: 02-09-2025

Aim:

To NAMP discover live hosts using ARP Scan, ICMP Scan ANd TCP/UDP ping Scan in TryHackMe platform

Task 1 Introduction

When we want to target a network, we want to find an efficient tool to help us handle repetitive tasks and answer the following questions:

Which systems are up?

What services are running on these systems?

The tool that we will rely on is Nmap.

The first question about finding live computers is answered in this room.

This room is the first in a series of four rooms dedicated to Nmap.

The second question about discovering running services is answered in the next Nmap rooms that focus on port-scanning.

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

This room explains the steps that Nmap carries out to discover the systems that are online before port-scanning.

This stage is crucial because trying to port-scan offline systems will only waste time and create unnecessary noise on the network.

We present the different approaches that Nmap uses to discover live hosts. In particular, we cover:

ARP scan: This scan uses ARP requests to discover live hosts

ICMP scan: This scan uses ICMP requests to identify live hosts

TCP/UDP ping scan: This scan sends packets to TCP ports and UDP ports to determine live hosts.

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.

Nmap was created by Gordon Lyon (Fyodor), a network security expert and open source programmer.

It was released in 1997. Nmap, short for Network Mapper, is free, open-source software released under GPL license.

Nmap is an industry-standard tool for mapping networks, identifying live hosts, and discovering running services.

Nmap's scripting engine can further extend its functionality, from fingerprinting services to exploiting vulnerabilities.

A Nmap scan usually goes through the steps shown in the figure below, although many are optional and depend on the command-line arguments you provide.

****

Task 2 Subnetworks

How many devices can see the ARP Request?

4

Did computer6 receive the ARP Request? (Y/N)

N

How many devices can see the ARP Request?

4

Did computer6 reply to the ARP Request? (Y/N)

Y

****

Task 3 Enumerating Targets

What is the first IP address Nmap would scan if you provided 10.10.12.13/29 as your target?

10.10.12.8

How many IP addresses will Nmap scan if you provide the following range 10.10.0-255.101-125?

6400

****

Task 4 Discovering Live Hosts

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

ARP Request

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

ARP Response

How many computers responded to the ping request?

1

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 the second ARP Request?

computer5

Send another Ping Request. Did it require new ARP Requests? (Y/N)

N

****

Task 5 Nmap Host Discovery Using ARP

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

3

****

Task 6 Nmap Host Discovery Using ICMP

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

-PE

****

Task 7 Nmap Host Discovery Using TCP and UDP

Which TCP ping scan does not require a privileged account?

TCP SYN Ping

Which TCP ping scan requires a privileged account?

TCP ACK Ping

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

-PS23

****

Task 8 Using Reverse-DNS Lookup

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

-R

****

Task 9 Summary

Ensure you have taken note of all the Nmap options explained in this room. To continue learning about Nmap, please join the room Nmap Basic Port Scans, which introduces the basic types of port scans.

No answer needed

Result:

Thus, NAMP discover live hosts using ARP Scan, ICMP Scan ANd TCP/UDP ping Scan in TryHackMe platform Complete