

EXP NO:8 NMAP TO DISCOVER LIVE HOSTS DATE:4.9.24

AIM:

To learn how to use Nmap to discover live hosts using ARP scan, ICMP scan and TCP/UDP ping scan.

PROCEDURE:

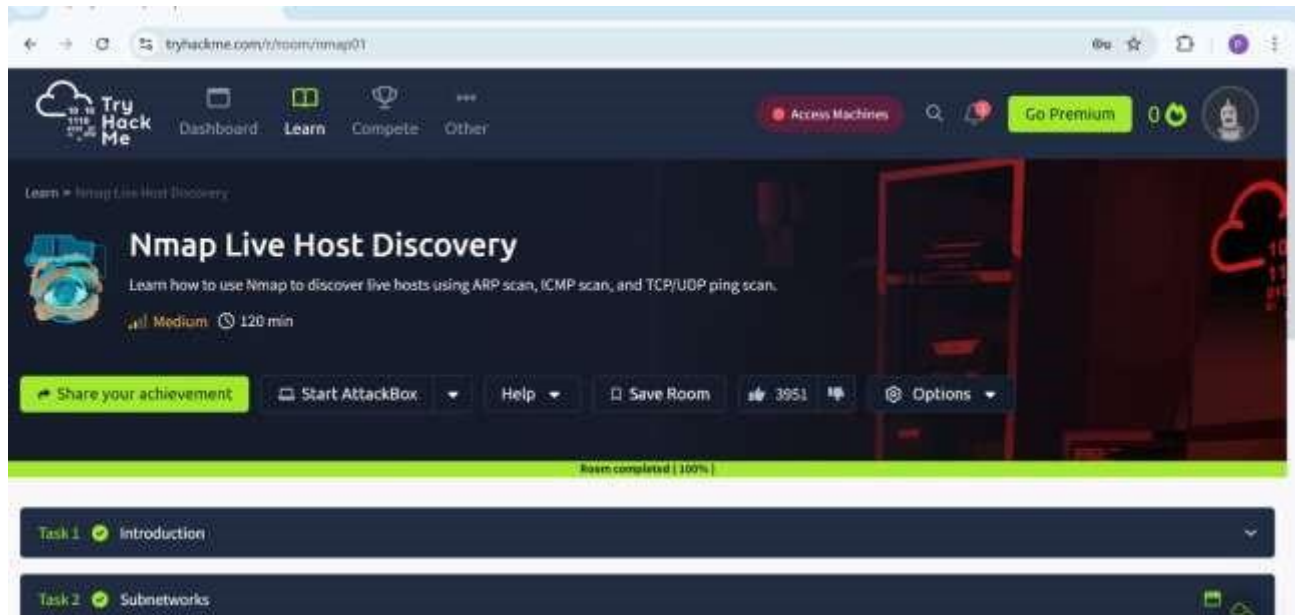
To perform the Nmap to discover the live hosts the following tasks need to be performed.

- ☐ TASK 1:Introduction
- ☐ TASK2: Subnetworks
- ☐ TASK 3:Enumerating Targets
- ☐ TASK 4:Discovering Live hosts
- ☐ TASK 5:Nmap host discovery using ARP
- ☐ TASK 6:Nmap host discovery using ICMP
- ☐ TASK 7:Nmap host discovery using TCP and UDP

TASK 8: Using reverse-dns lookup

TASK 9:Summary

OUTPUT:



TASK 1:INTRODUCTION

Answer the questions below

Some of these questions will require the use of a static site to answer the task questions, while others require the use of the AttackBox and the target VM.

TASK2: SUBNETWORKS

Answer the questions below

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

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

TASK 3:ENUMERATING TARGETS

Answer the questions below

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

10.10.12.8

✓ Correct Answer

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

6400

✓ Correct Answer

TASK 4:DISCOVERING LIVE HOSTS

Answer the questions below

Send a packet with the following:

- From computer1
- To computer3
- Packet Type: "Ping Request"

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

ARP Request

✓ Correct Answer

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

ARP Response

✓ Correct Answer

How many computers responded to the ping request?

1

✓ Correct Answer

Send a packet with the following:

- From computer2
- To computer5
- Packet Type: "Ping Request"

What is the name of the first device that responded to the first ARP Request?

router

✓ Correct Answer

What is the name of the first device that responded to the second ARP Request?

computer5

✓ Correct Answer

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

N

✓ Correct Answer

TASK 5:NMAP HOST DISCOVERY USING ARP

Answer the questions below

We will be sending broadcast ARP Requests packets with the following options:

- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: try all the possible eight devices (other than computer1) in the network: computer2, computer3, computer4, computer5, computer6, switch1, switch2, and router.

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

3

✓ Correct Answer

TASK 6:NMAP HOST DISCOVERY USING ICMP

Answer the questions below

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

-PP

✓ Correct Answer

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

-PM

✓ Correct Answer

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

-PE

✓ Correct Answer

TASK 7:NMAP HOST DISCOVERY USING TCP AND UDP

Answer the questions below

Which TCP ping scan does not require a privileged account?

TCP SYN Ping

✓ Correct Answer

Which TCP ping scan requires a privileged account?

TCP ACK Ping

✓ Correct Answer

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

-PS23

✓ Correct Answer

💡 Hint

TASK 8: USING REVERSE-DNS LOOKUP

Answer the questions below

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

-R

✓ Correct Answer

TASK 9: SUMMARY

Answer the questions below

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

✓ Correct Answer

RESULT:

Nmap to discover live hosts using ARP scan,ICMP scan and TCP and UDP ping scan in the tryhackme platform.