

Ex.no:08

Date: 10/09/2024

Roll no: 231901001

## Nmap to discover live hosts

### Aim:

To complete the Nmap discovering of live hosts using Tryhackme platform.

### Result:

The screenshot displays the TryHackMe platform interface for the 'Nmap Live Host Discovery' room. The top navigation bar includes links for Dashboard, Learn, Compete, and Other, along with an 'Access Machines' button and user avatars. The room title 'Nmap Live Host Discovery' is prominently displayed, accompanied by a description: 'Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.' The room is rated 'Medium' and estimated to take '120 min'. Below the title, there are buttons for 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', and 'Options'. A green bar at the bottom of the room header indicates 'Room completed (100%)'. The main content area shows 'Task 1 Introduction' with a green checkmark, indicating completion. The task text explains the purpose of Nmap in network discovery and lists four sub-tasks: 1. Nmap Live Host Discovery, 2. Nmap Basic Port Scans, 3. Nmap Advanced Port Scans, and 4. Nmap Post Port Scans. The text also mentions that this room is the first in a series of four rooms dedicated to Nmap, focusing on port-scanning.

How many devices can see the ARP Request?

4

✓ Correct Answer

🔍 Hint

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

N

✓ Correct Answer

Send a packet with the following:

Send Packet

From:  
computer4

To:  
computer4

Packet Type:  
arp\_request

Data:  
computer6

Send Packet

- From computer4
- To computer4 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4

✓ Correct Answer

🔍 Hint

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

Y

✓ Correct Answer

### Task 3 🟢 Enumerating Targets

We mentioned the different *techniques* we can use for scanning in Task 1. Before we explain each in detail and put it into use against a live target, we need to specify the targets we want to scan. Generally speaking, you can provide a list, a range, or a subnet. Examples of target specification are:

- list: `MACHINE_IP scanme.nmap.org example.com` will scan 3 IP addresses.
- range: `10.11.12.15-20` will scan 6 IP addresses: `10.11.12.15`, `10.11.12.16`, ... and `10.11.12.20`.
- subnet: `MACHINE_IP/30` will scan 4 IP addresses.

You can also provide a file as input for your list of targets, `nmap -iL list_of_hosts.txt`.

If you want to check the list of hosts that Nmap will scan, you can use `nmap -sL TARGETS`. This option will give you a detailed list of the hosts that Nmap will scan without scanning them; however, Nmap will attempt a reverse-DNS resolution on all the targets to obtain their names. Names might reveal various information to the pentester. (If you don't want Nmap to the DNS server, you can add `-n`.)

Launch the AttackBox using the Start AttackBox button, open the terminal when the AttackBox is ready, and use Nmap to answer the following.

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

🔍 Hint

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

6400

✓ Correct Answer

🔍 Hint

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

Room completed (100%)

02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	ARP Announcement for 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.8? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.9? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.10? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.11? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.12? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.13? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.14? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.15? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.16? Tell 10.10.210.6

Address Resolution Protocol: Protocol

Packets: 1207 · Displayed: 512 (42.4%)

Profile: Default

If you have closed the network simulator, click on the "Visit Site" button in Task 2 to display it again.

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

10.11.35.214	10.10.68.2	ICMP	Address mask request	id=0xb793, seq=0/0, ttl=
10.11.35.214	10.10.68.3	ICMP	Address mask request	id=0x2d87, seq=0/0, ttl=
10.11.35.214	10.10.68.4	ICMP	Address mask request	id=0x091c, seq=0/0, ttl=
10.11.35.214	10.10.68.5	ICMP	Address mask request	id=0x692c, seq=0/0, ttl=
10.11.35.214	10.10.68.6	ICMP	Address mask request	id=0x4bec, seq=0/0, ttl=
10.11.35.214	10.10.68.7	ICMP	Address mask request	id=0x4d61, seq=0/0, ttl=
10.11.35.214	10.10.68.8	ICMP	Address mask request	id=0xb84f, seq=0/0, ttl=
10.11.35.214	10.10.68.9	ICMP	Address mask request	id=0x7d19, seq=0/0, ttl=
10.11.35.214	10.10.68.10	ICMP	Address mask request	id=0x92be, seq=0/0, ttl=
10.11.35.214	10.10.68.1	ICMP	Address mask request	id=0xd204, seq=0/0, ttl=
10.11.35.214	10.10.68.2	ICMP	Address mask request	id=0x683d, seq=0/0, ttl=
10.11.35.214	10.10.68.3	ICMP	Address mask request	id=0x2711, seq=0/0, ttl=
10.11.35.214	10.10.68.4	ICMP	Address mask request	id=0xfde3, seq=0/0, ttl=
10.11.35.214	10.10.68.5	ICMP	Address mask request	id=0x2eb1, seq=0/0, ttl=
10.11.35.214	10.10.68.6	ICMP	Address mask request	id=0x8300, seq=0/0, ttl=
10.11.35.214	10.10.68.7	ICMP	Address mask request	id=0x7400, seq=0/0, ttl=

nmap-PM-sn-openvpn.pcapng

Packets: 1178 · Displayed: 512 (43.5%)

Profile: Default

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

10.11.35.214	10.10.68.1	UDP	57192 → 40125	Len=40
10.11.35.214	10.10.68.2	UDP	57192 → 40125	Len=40
10.11.35.214	10.10.68.3	UDP	57192 → 40125	Len=40
10.11.35.214	10.10.68.4	UDP	57192 → 40125	Len=40
10.11.35.214	10.10.68.5	UDP	57192 → 40125	Len=40
10.11.35.214	10.10.68.6	UDP	57192 → 40125	Len=40
10.11.35.214	10.10.68.7	UDP	57192 → 40125	Len=40

nmap-PU-sn-openvpn.pcapng

Packets: 1118 · Displayed: 602 (53.8%)

Profile: Default

## Masscan

On a side note, Masscan uses a similar approach to discover the available systems. However, to finish its network scan quickly, Masscan is quite aggressive with the rate of packets it generates. The syntax is quite similar: `-p` can be followed by a port number, list, or range. Consider the following examples:

- `masscan MACHINE_IP/24 -p443`
- `masscan MACHINE_IP/24 -p80,443`
- `masscan MACHINE_IP/24 -p22-25`
- `masscan MACHINE_IP/24 --top-ports 100`

Masscan is not installed on the AttackBox; however, it can be installed using `apt install masscan`.

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

Nmap's default behaviour is to use reverse-DNS online hosts. Because the hostnames can reveal a lot, this can be a helpful step. However, if you don't want to send such DNS queries, you use `-n` to skip this step.

By default, Nmap will look up online hosts; however, you can use the option `-R` to query the DNS server even for offline hosts. If you want to use a specific DNS server, you can add the `-dns-servers DNS_SERVER` option.

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?

✓ Correct Answer

#### Room Summary

You have learned how ARP, ICMP, TCP, and UDP can detect live hosts by completing this room. Any response from a host is an indication that it is online. Below is a quick summary of the command-line options for Nmap that we have covered.

Scan Type	Example Command
ARP Scan	<code>sudo nmap -PR -sn MACHINE_IP/24</code>
ICMP Echo Scan	<code>sudo nmap -PE -sn MACHINE_IP/24</code>
ICMP Timestamp Scan	<code>sudo nmap -PP -sn MACHINE_IP/24</code>
ICMP Address Mask Scan	<code>sudo nmap -PM -sn MACHINE_IP/24</code>
TCP SYN Ping Scan	<code>sudo nmap -PS22,80,443 -sn MACHINE_IP/30</code>
TCP ACK Ping Scan	<code>sudo nmap -PA22,80,443 -sn MACHINE_IP/30</code>
UDP Ping Scan	<code>sudo nmap -PU53,161,162 -sn MACHINE_IP/30</code>

Remember to add `-sn` if you are only interested in host discovery without port-scanning. Omitting `-sn` will let Nmap default to port-scanning the live hosts.

Option	Purpose
<code>-n</code>	no DNS lookup
<code>-R</code>	reverse-DNS lookup for all hosts
<code>-sn</code>	host discovery only

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.

✓ Correct Answer

Thus, the experiment of Nmap was done in tryhackme platform.