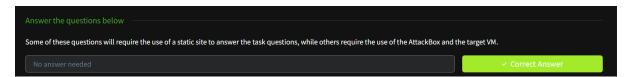**Ex.no:8**

Date:10.9.2024

<div align="center">

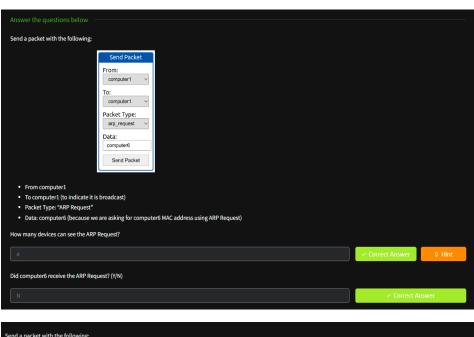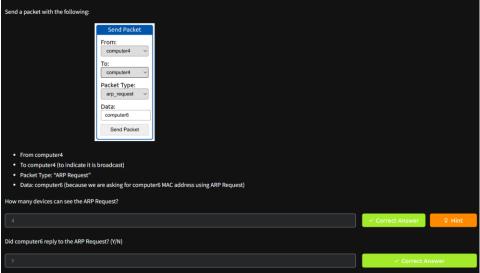**NMAP TO DISCOVER LIVE HOSTS**

</div>

AIM:

To study Nmap tool using TryHackMe platform**.**

TASK 1 – INTRODUCTION:

TASK 2 – SUBNETWORKS:

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 |

TASK4 - 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:

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 possibles hosts on a subnet, hoping to get some insights from the names. What option should we add?

| -R | ✓ Correct Answer |

TASK 9 – 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	`sudo nmap -PR -sn MACHINE_IP/24`
ICMP Echo Scan	`sudo nmap -PE -sn MACHINE_IP/24`
ICMP Timestamp Scan	`sudo nmap -PP -sn MACHINE_IP/24`
ICMP Address Mask Scan	`sudo nmap -PM -sn MACHINE_IP/24`
TCP SYN Ping Scan	`sudo nmap -PS22,80,443 -sn MACHINE_IP/30`
TCP ACK Ping Scan	`sudo nmap -PA22,80,443 -sn MACHINE_IP/30`
UDP Ping Scan	`sudo nmap -PU53,161,162 -sn MACHINE_IP/30`

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
`-n`	no DNS lookup
`-R`	reverse-DNS lookup for all hosts
`-sn`	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.

No answer needed	✓ Correct Answer

RESULT:

Hence, Nmap to discover live hosts is studied.