Ex.no:08 Date: 10/09/2024

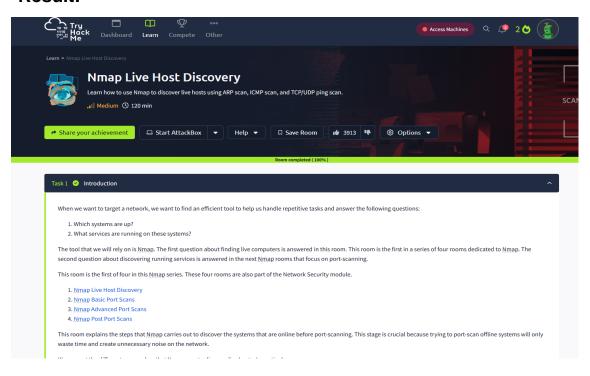
Roll no: 231901001

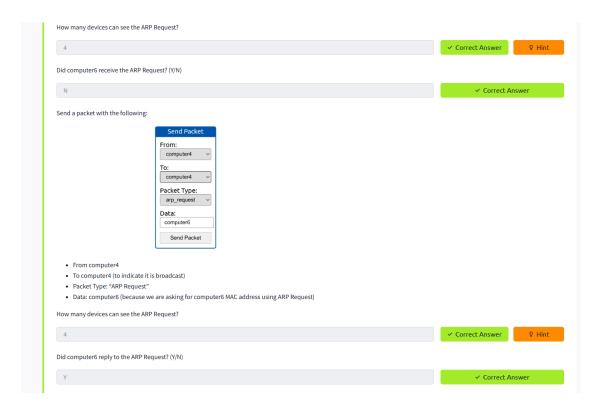
## Nmap to discover live hosts

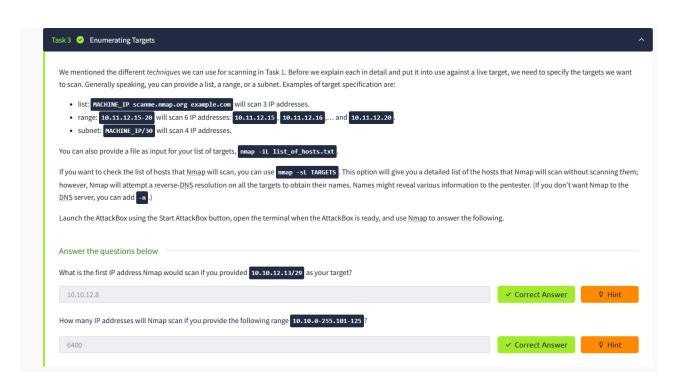
## Aim:

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

## Result:







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? ✓ Correct Answer ARP Request 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? ✓ Correct Answer Send a packet with the following: To computer5 • Packet Type: "Ping Request" What is the name of the first device that responded to the first ARP Request? ✓ Correct Answer router What is the name of the first device that responded to the second ARP Request? ✓ Correct Answer computer5 Send another Ping Request. Did it require new ARP Requests? (Y/N) ✓ Correct Answer

			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
02.60.06.40.40.06	Broadonat	ADD	Who has 10 10 210 162 Tall 10 10 210 6

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?

✓ Correct Answer

```
10.11.35.214 10.10.68.4 ICMP Address mask request id=0x091c, seq=0/0, ttl=
         10.11.35.214 10.10.68.8 ICMP Address mask request id=0xb84f, seq=0/0, ttl=
         10 11 25 214
                 10 10 60 7
                        TOMP
                            Address mask request id-0v74e0
        map-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?

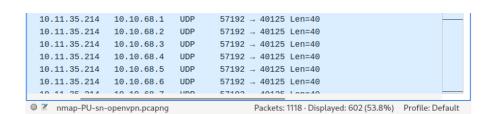
✓ Correct Answer

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

✓ Correct Answer

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

✓ Correct Answer
```



## 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 

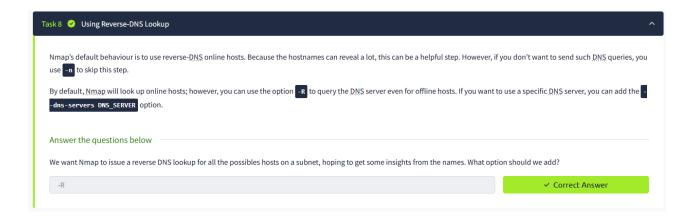
✓ Correct Answer

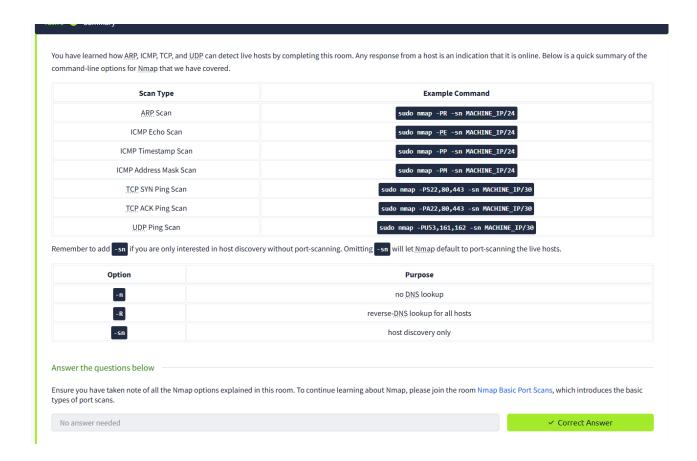
 $Which \ TCP \ ping \ scan \ requires \ a \ privileged \ account?$ 

TCP ACK Ping

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

-PS23 ✓ Correct Answer ♥ Hint





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