V.SWARNAMALA **241901116**

Exp :6 **Nmap Live Host Discovery** **Date:1/9/25**

Aim

To efficiently identify which computers are online in a target network using Nmap's host discovery techniques.

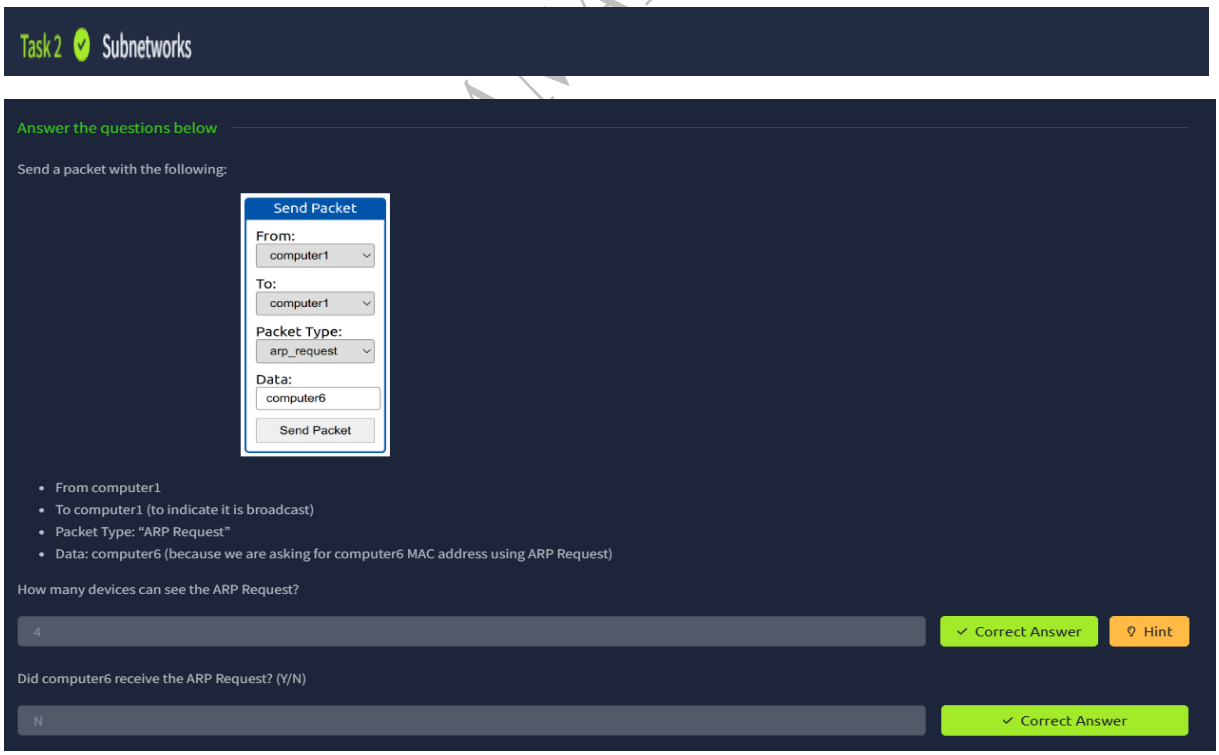
Introduction

Live host discovery is the crucial first step in network scanning. Nmap can find active systems using techniques like ARP scan, ICMP scan, and TCP/UDP ping scan. This process helps avoid wasting time on offline systems and reduces network noise.

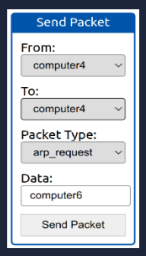
ALGORITHM

- Use Nmap with ARP, ICMP, TCP, or UDP scans to detect live hosts.
- Example commands:
  - ARP: nmap -sn -PR <subnet>
  - ICMP: nmap -sn -PE <subnet>
  - TCP Ping: nmap -sn -PS22,80,443 <range>
- Review scan output to see which systems are up before proceeding with deeper

OUTPUT



Send a packet with the following:



- 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

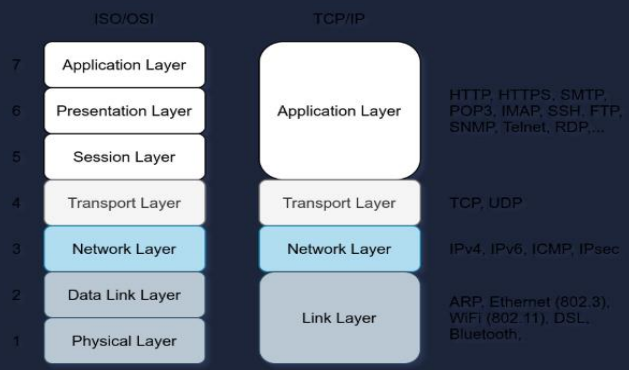
How many IP addresses will Nmap scan if you provide the following range `10.10.0-255.101-125`?

6400 ✓ Correct Answer Hint

Task 4 Discovering Live Hosts

Let's revisit the TCP/IP layers shown in the figure next. We will leverage the protocols to discover the live hosts. Starting from bottom to top, we can use

- ARP from Link Layer
- ICMP from Network Layer
- TCP from Transport Layer
- UDP from Transport Layer



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

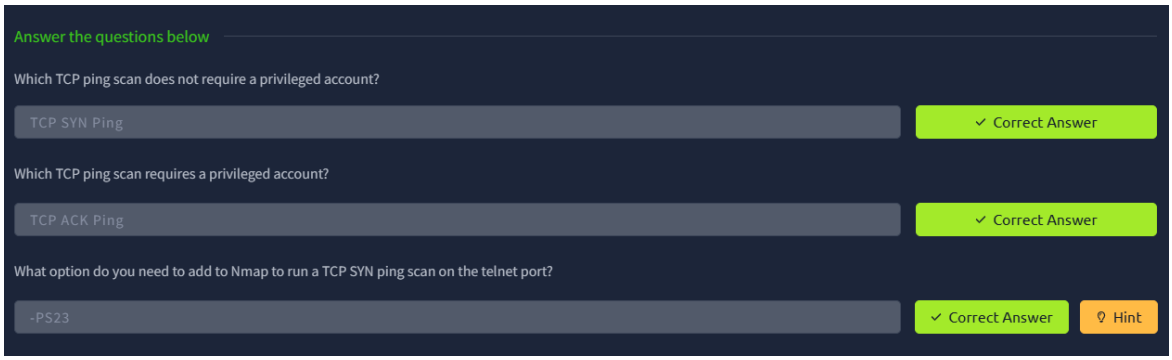
What is the option required to tell Nmap to use ICMP Address Mask to discover live hosts?

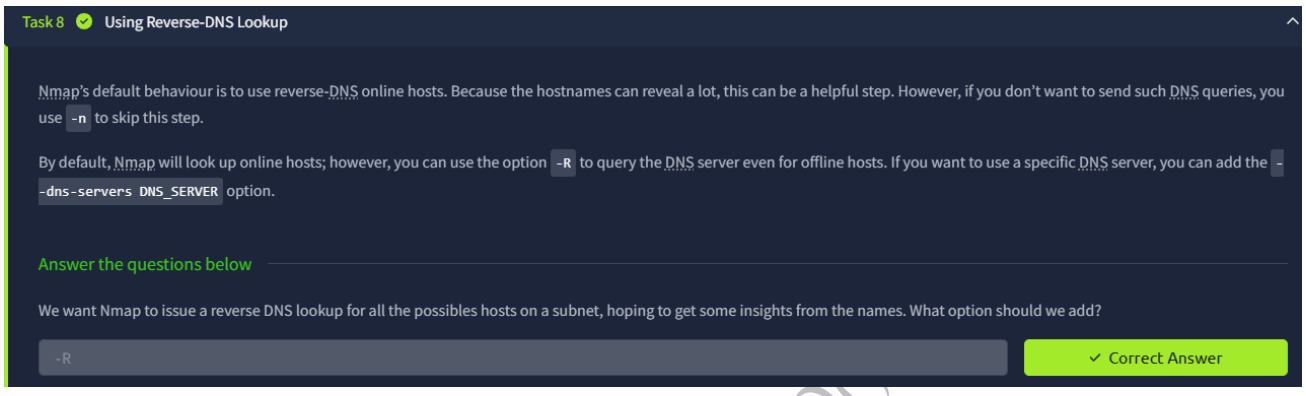
-PM — ✓ Correct Answer

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





Result:

Thus we completed and understand how Nmap Live Host Discovery used and how it helps us .