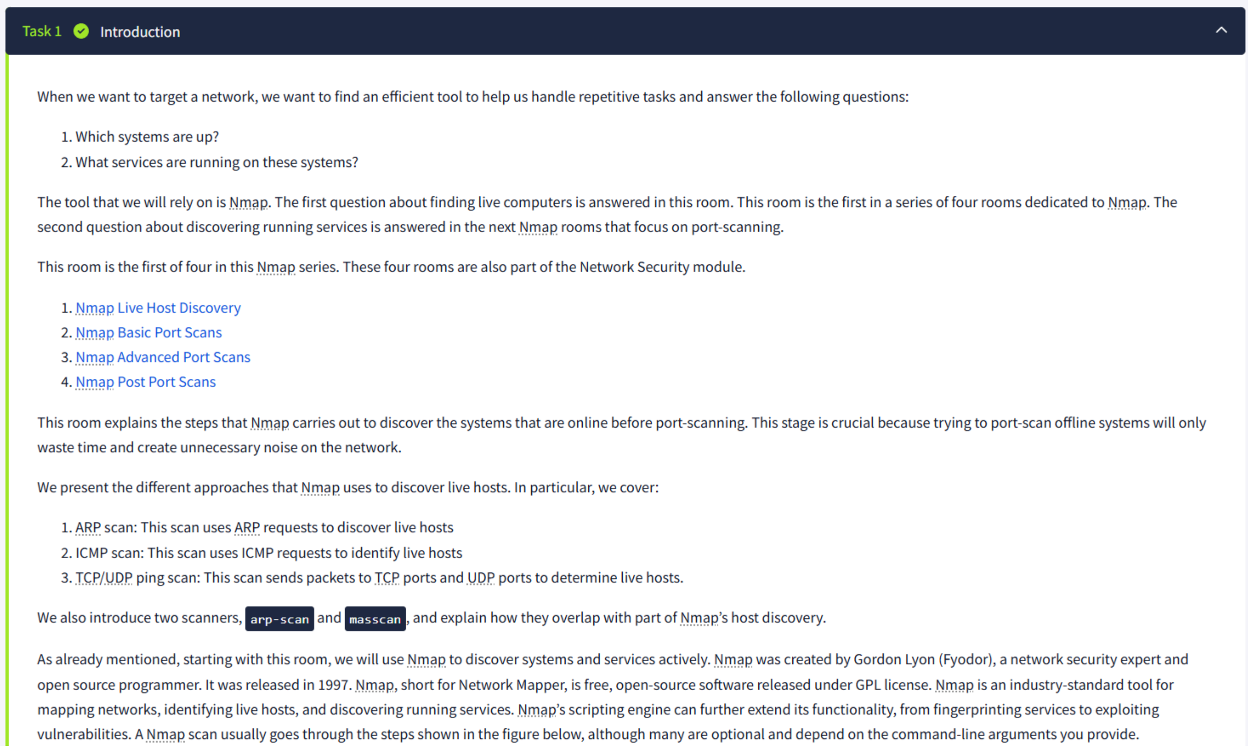
PRACTICAL -8

To Discover Live Hosts Using Nmap Scans (ARP, ICMP, TCP/UDP) on the TryHackMe
Platform Room Link :https://tryhackme.com/room/nmap01

TASK 1



Task 1 Introduction

When we want to target a network, we want to find an efficient tool to help us handle repetitive tasks and answer the following questions:

1. Which systems are up?
2. What services are running on these systems?

The tool that we will rely on is Nmap. The first question about finding live computers is answered in this room. This room is the first in a series of four rooms dedicated to Nmap. The second question about discovering running services is answered in the next Nmap rooms that focus on port-scanning.

This room is the first of four in this Nmap series. These four rooms are also part of the Network Security module.

1. Nmap Live Host Discovery
2. Nmap Basic Port Scans
3. Nmap Advanced Port Scans
4. Nmap Post Port Scans

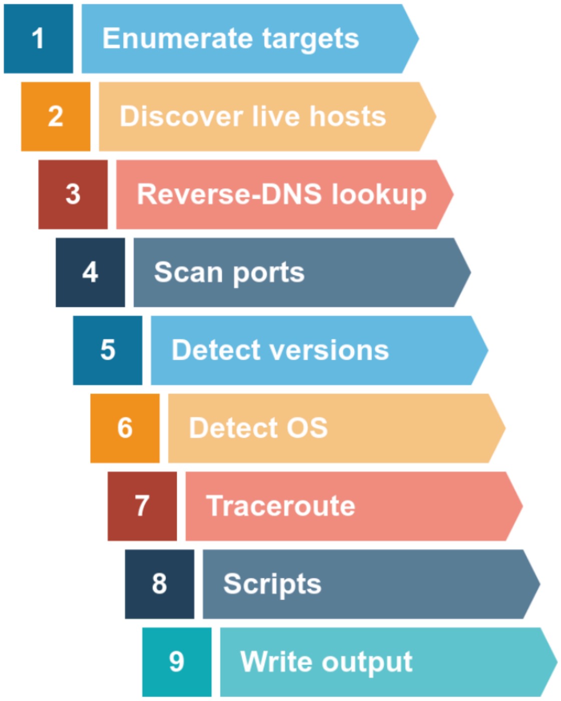
This room explains the steps that Nmap carries out to discover the systems that are online before port-scanning. This stage is crucial because trying to port-scan offline systems will only waste time and create unnecessary noise on the network.

We present the different approaches that Nmap uses to discover live hosts. In particular, we cover:

1. ARP scan: This scan uses ARP requests to discover live hosts
2. ICMP scan: This scan uses ICMP requests to identify live hosts
3. TCP/UDP ping scan: This scan sends packets to TCP ports and UDP ports to determine live hosts.

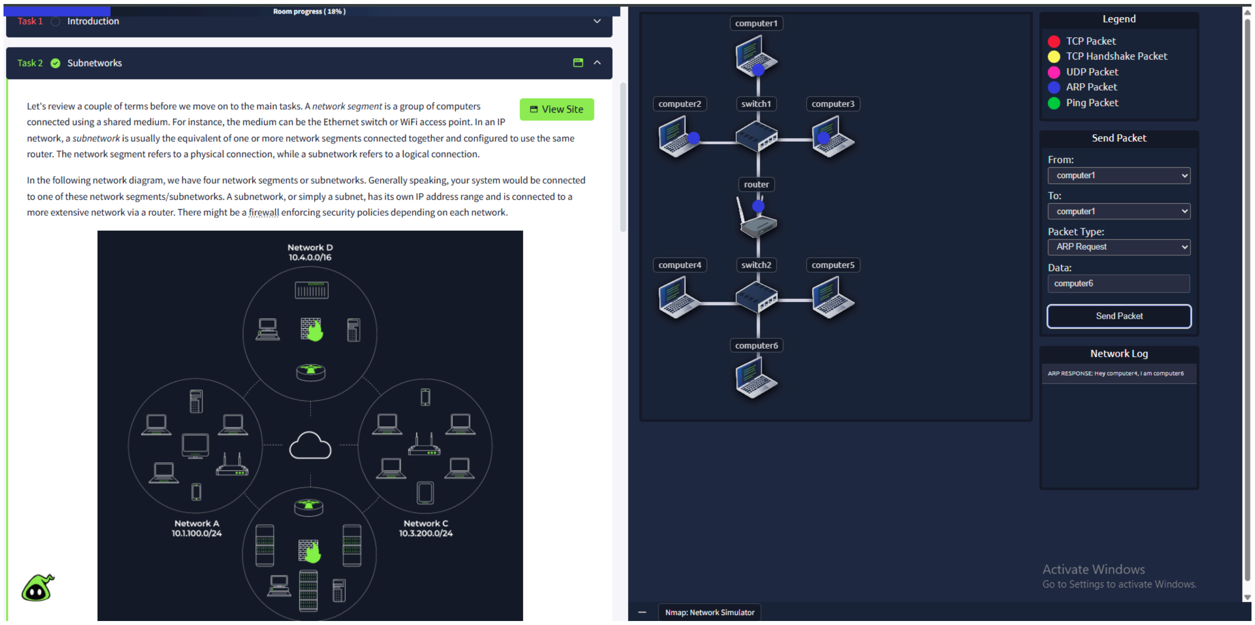
We also introduce two scanners, `arp-scan` and `masscan`, and explain how they overlap with part of Nmap's host discovery.

As already mentioned, starting with this room, we will use Nmap to discover systems and services actively. Nmap was created by Gordon Lyon (Fyodor), a network security expert and open source programmer. It was released in 1997. Nmap, short for Network Mapper, is free, open-source software released under GPL license. Nmap is an industry-standard tool for mapping networks, identifying live hosts, and discovering running services. Nmap's scripting engine can further extend its functionality, from fingerprinting services to exploiting vulnerabilities. A Nmap scan usually goes through the steps shown in the figure below, although many are optional and depend on the command-line arguments you provide.



1 Enumerate targets
2 Discover live hosts
3 Reverse-DNS lookup
4 Scan ports
5 Detect versions
6 Detect OS
7 Traceroute
8 Scripts
9 Write output

TASK 2



Let's review a couple of terms before we move on to the main tasks. A *network segment* is a group of computers connected using a shared medium. For instance, the medium can be the Ethernet switch or WiFi access point. In an IP network, a *subnetwork* is usually the equivalent of one or more network segments connected together and configured to use the same router. The network segment refers to a physical connection, while a subnetwork refers to a logical connection.

In the following network diagram, we have four network segments or subnetworks. Generally speaking, your system would be connected to one of these network segments/subnetworks. A subnetwork, or simply a subnet, has its own IP address range and is connected to a more extensive network via a router. There might be a firewall enforcing security policies depending on each network.

Legend
- 🔴 TCP Packet
- 🟡 TCP Handshake Packet
- 🟣 UDP Packet
- 🔵 ARP Packet
- 🟢 Ping Packet

Send Packet

From: computer1

To: computer1

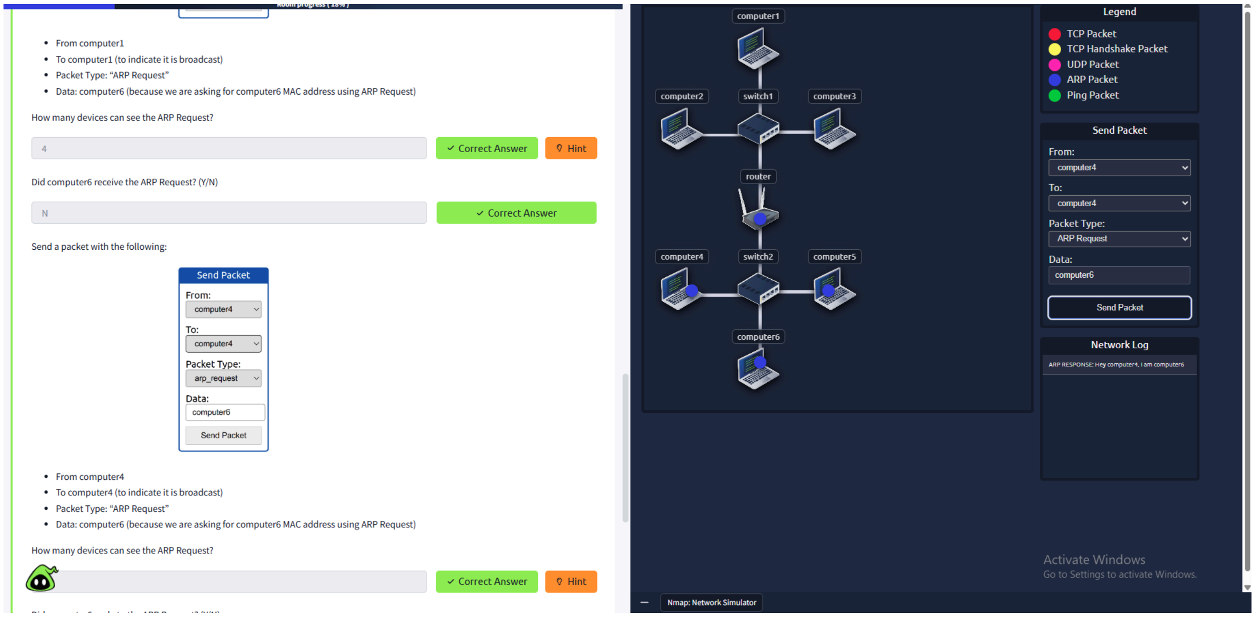
Packet Type: ARP Request

Data: computer6

Send Packet

Network Log

```
ARP RESPONSE: Hey computer4, I am computer6
```



- From computer1
- To computer1 (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 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?

✓ Correct Answer Hint

Legend
- 🔴 TCP Packet
- 🟡 TCP Handshake Packet
- 🟣 UDP Packet
- 🔵 ARP Packet
- 🟢 Ping Packet

Send Packet

From: computer4

To: computer4

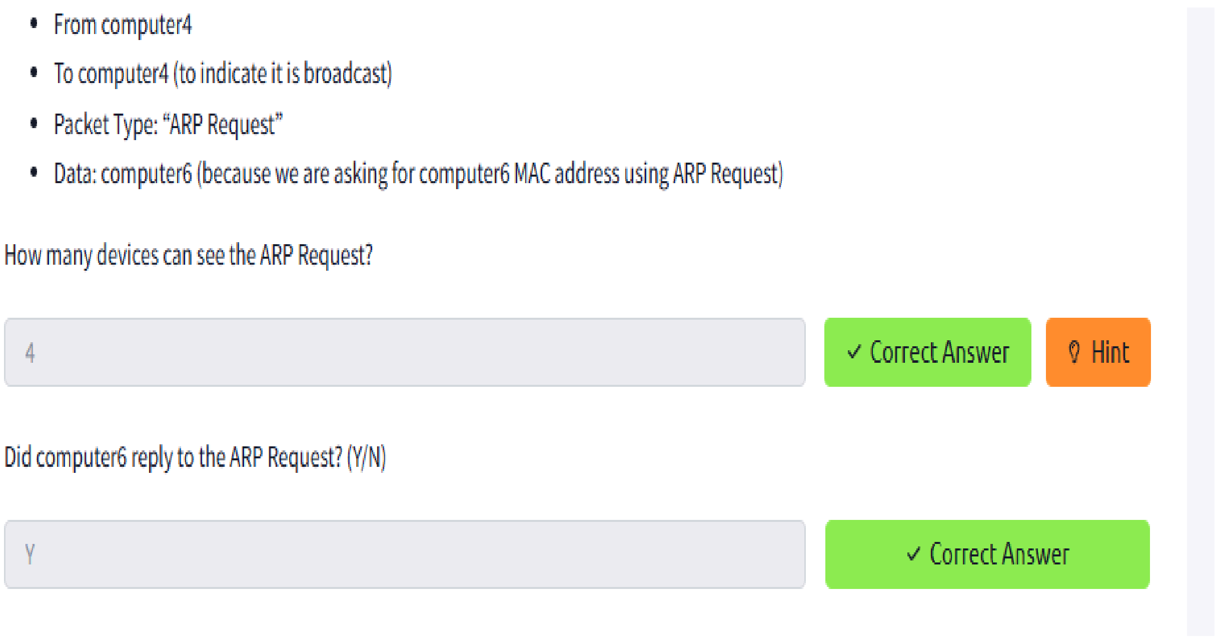
Packet Type: ARP Request

Data: computer6

Send Packet

Network Log

```
ARP RESPONSE: Hey computer4, I am computer6
```



- 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)

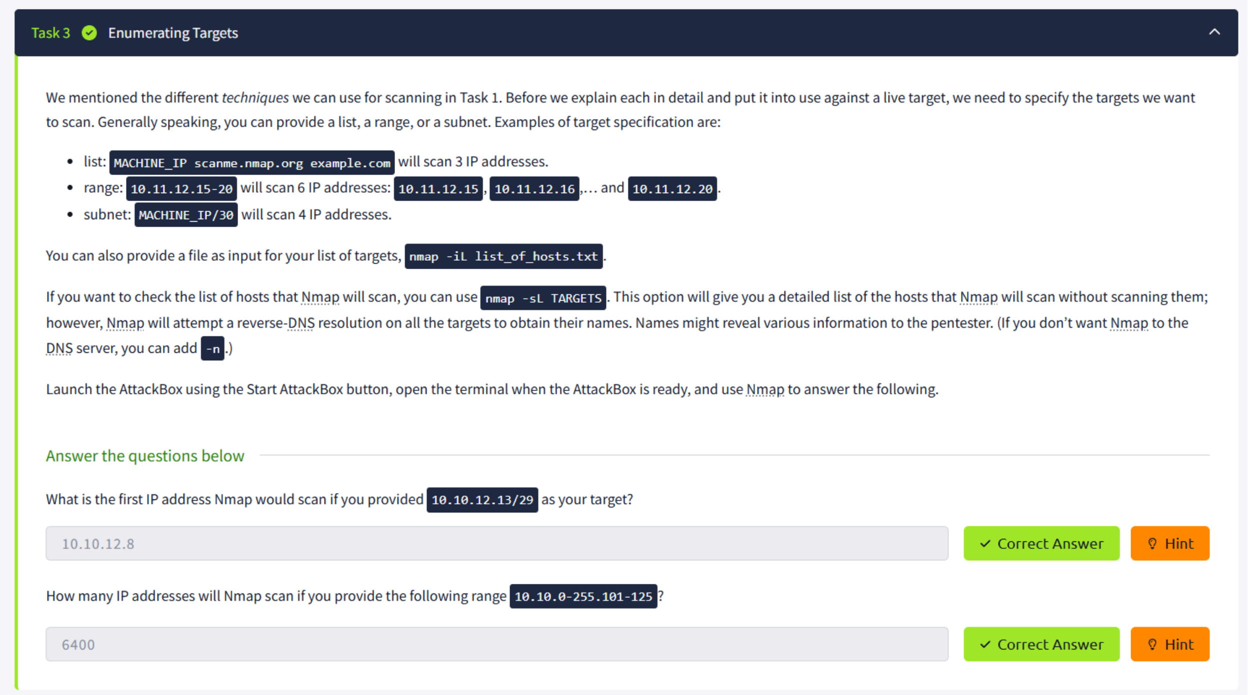
How many devices can see the ARP Request?

4

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

Y

TASK 3



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

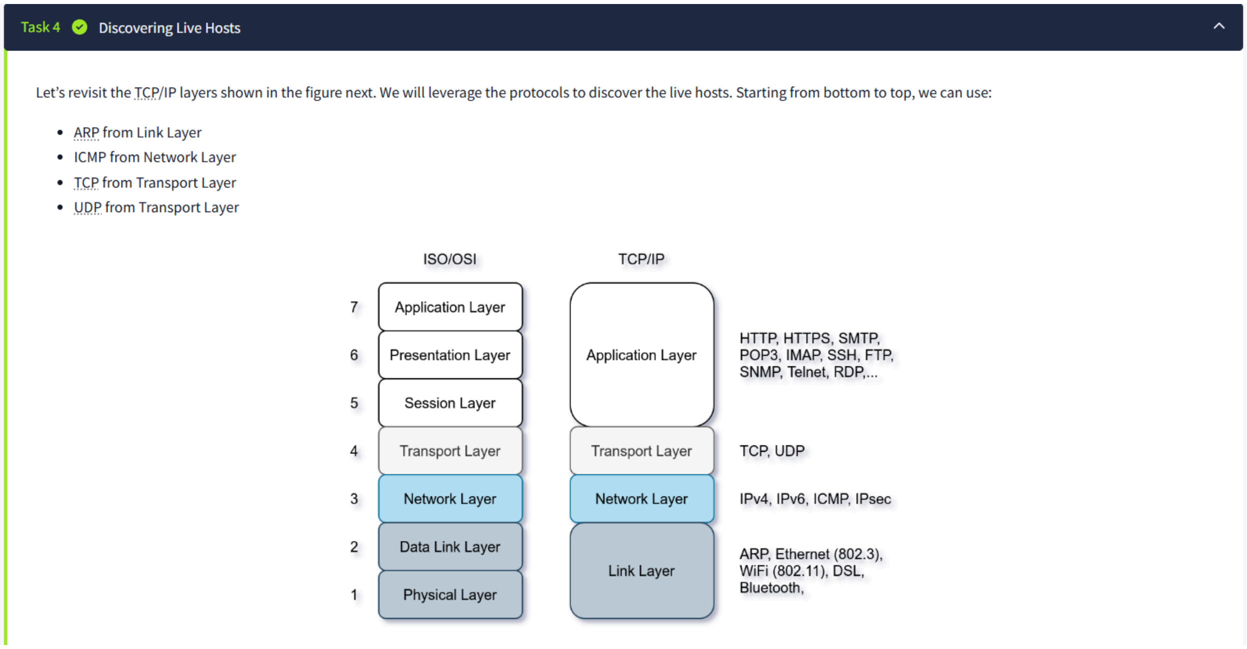
What is the first IP address Nmap would scan if you provided `10.10.12.13/29` as your target?

10.10.12.8

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

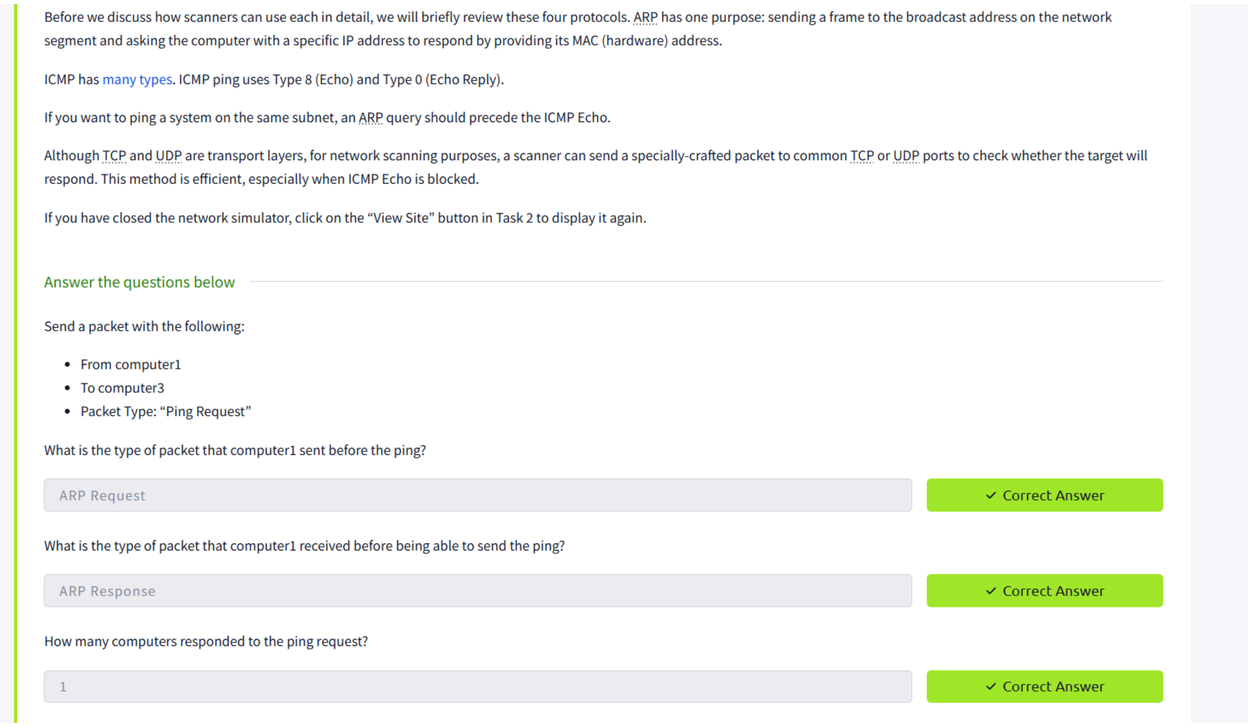
6400

TASK 4



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



Before we discuss how scanners can use each in detail, we will briefly review these four protocols. ARP has one purpose: sending a frame to the broadcast address on the network segment and asking the computer with a specific IP address to respond by providing its MAC (hardware) address.

ICMP has many types. ICMP ping uses Type 8 (Echo) and Type 0 (Echo Reply).

If you want to ping a system on the same subnet, an ARP query should precede the ICMP Echo.

Although TCP and UDP are transport layers, for network scanning purposes, a scanner can send a specially-crafted packet to common TCP or UDP ports to check whether the target will respond. This method is efficient, especially when ICMP Echo is blocked.

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

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?

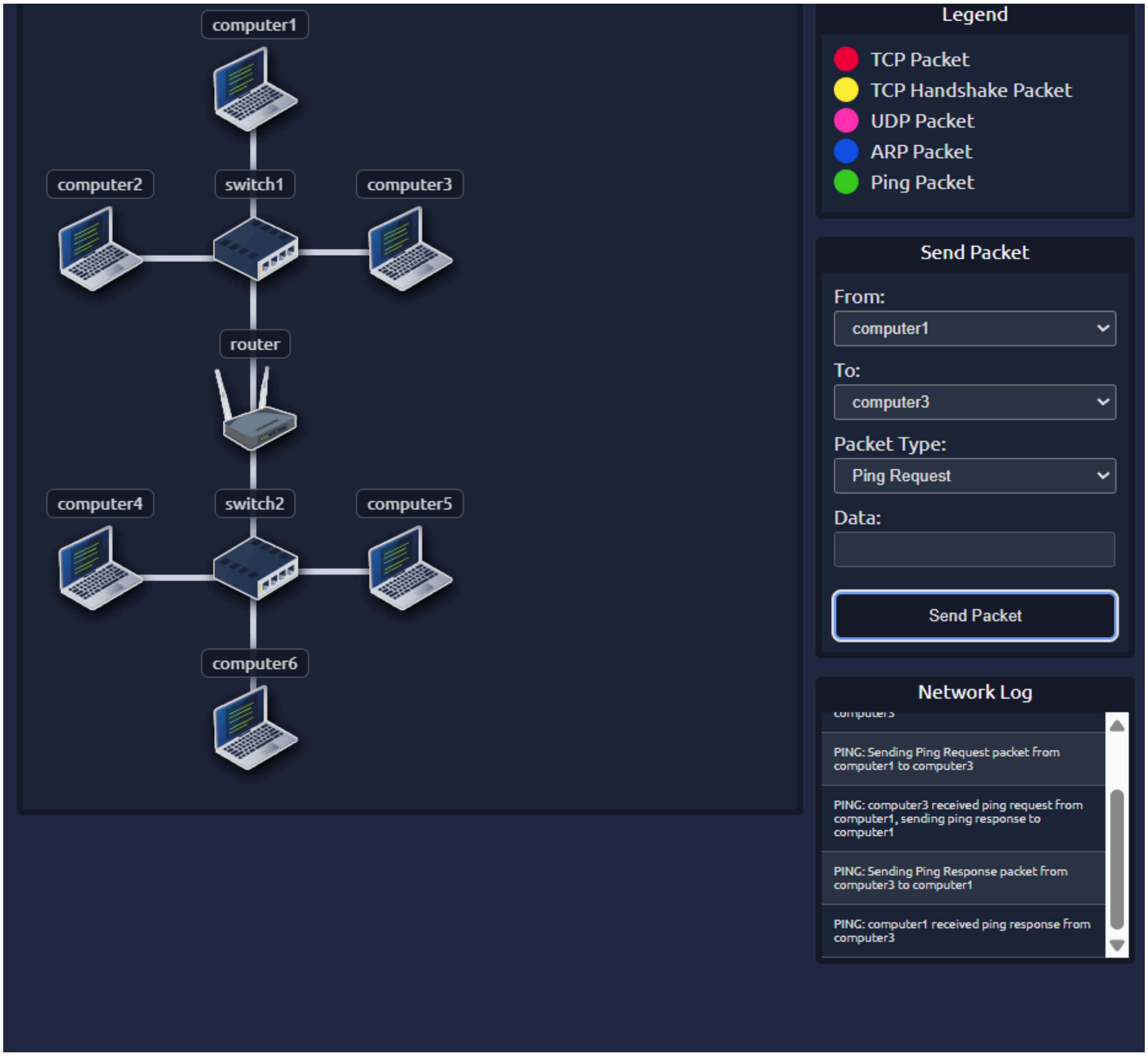
ARP Request

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

ARP Response

How many computers responded to the ping request?

1



Legend

● TCP Packet
● TCP Handshake Packet
● UDP Packet
● ARP Packet
● Ping Packet

Send Packet

From: computer1

To: computer3

Packet Type: Ping Request

Data:

Network Log

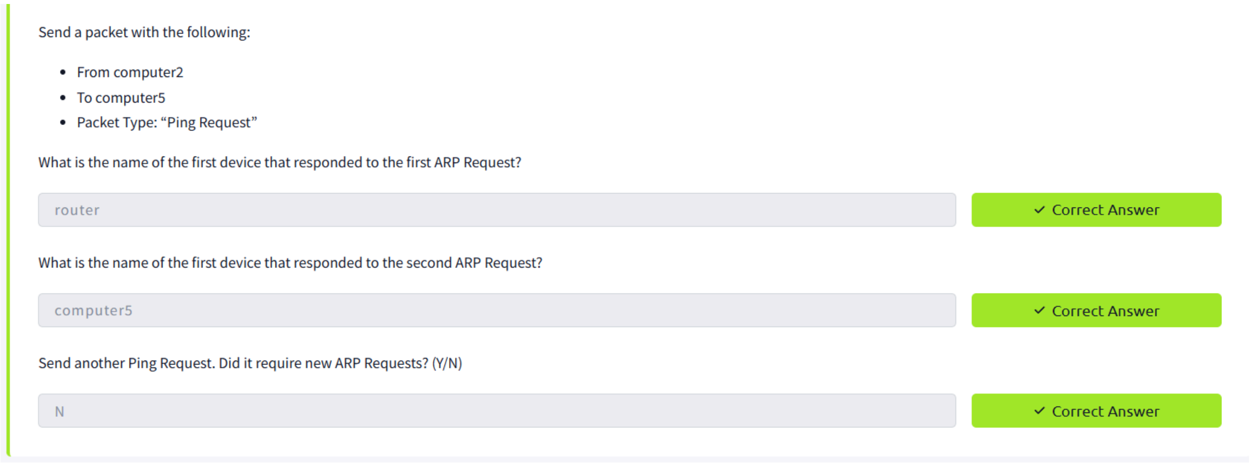
```
computer3

PING: Sending Ping Request packet from computer1 to computer3

PING: computer3 received ping request from computer1, sending ping response to computer1

PING: Sending Ping Response packet from computer3 to computer1

PING: computer1 received ping response from computer3
```



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?

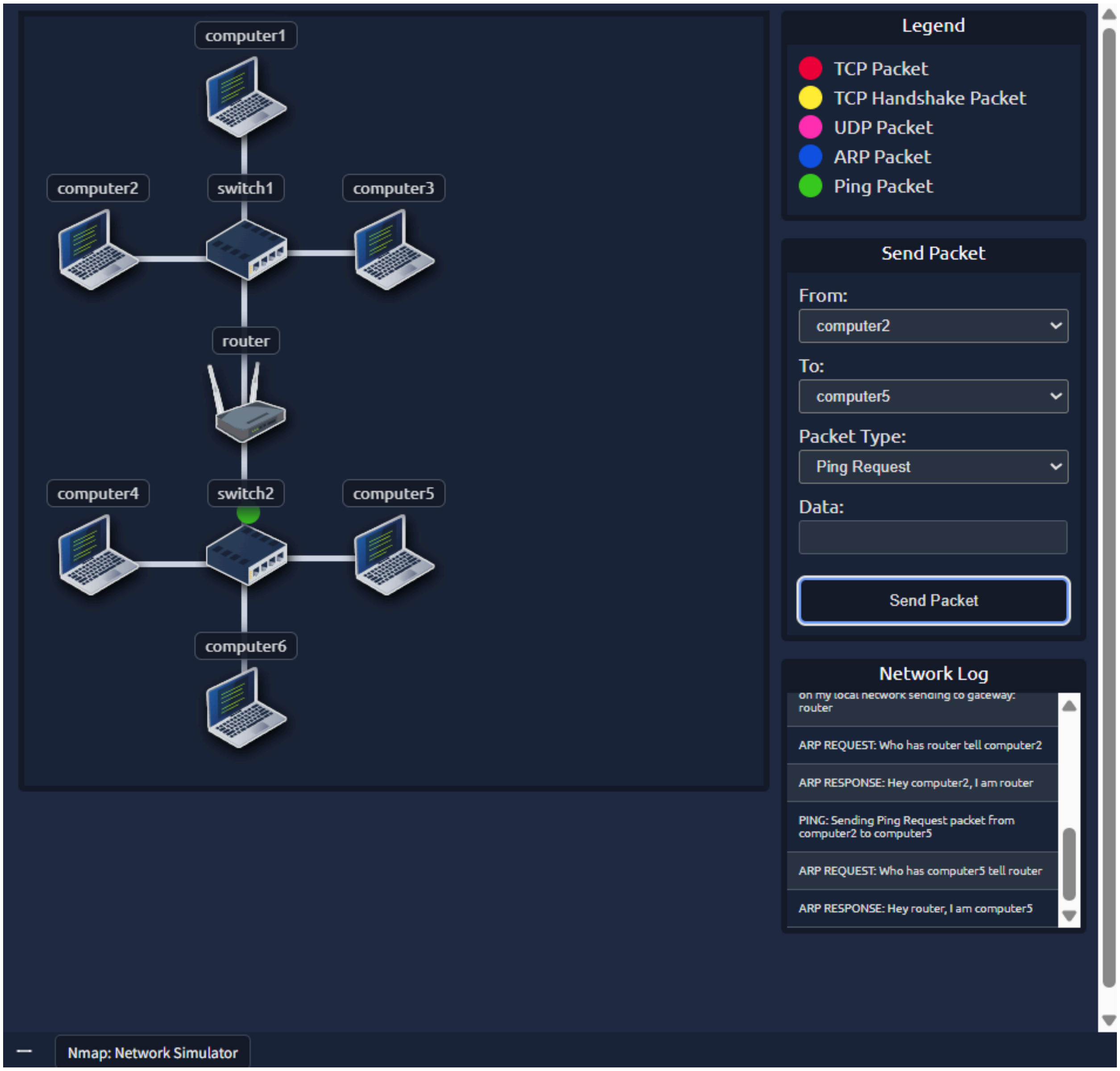
router

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

computer5

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

N



Legend

- 🔴 TCP Packet
- 🟡 TCP Handshake Packet
- 🟣 UDP Packet
- 🔵 ARP Packet
- 🟢 Ping Packet

Send Packet

From: computer2

To: computer5

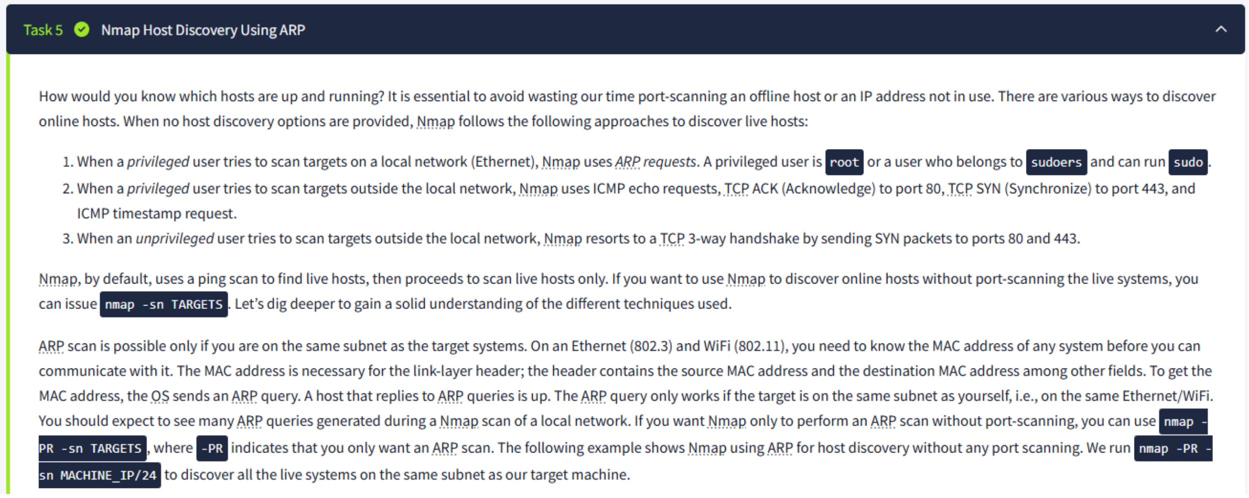
Packet Type: Ping Request

Data:

Network Log

```
on my local network sending to gateway:
router
ARP REQUEST: Who has router tell computer2
ARP RESPONSE: Hey computer2, I am router
PING: Sending Ping Request packet from
computer2 to computer5
ARP REQUEST: Who has computer5 tell router
ARP RESPONSE: Hey router, I am computer5
```

TASK 5



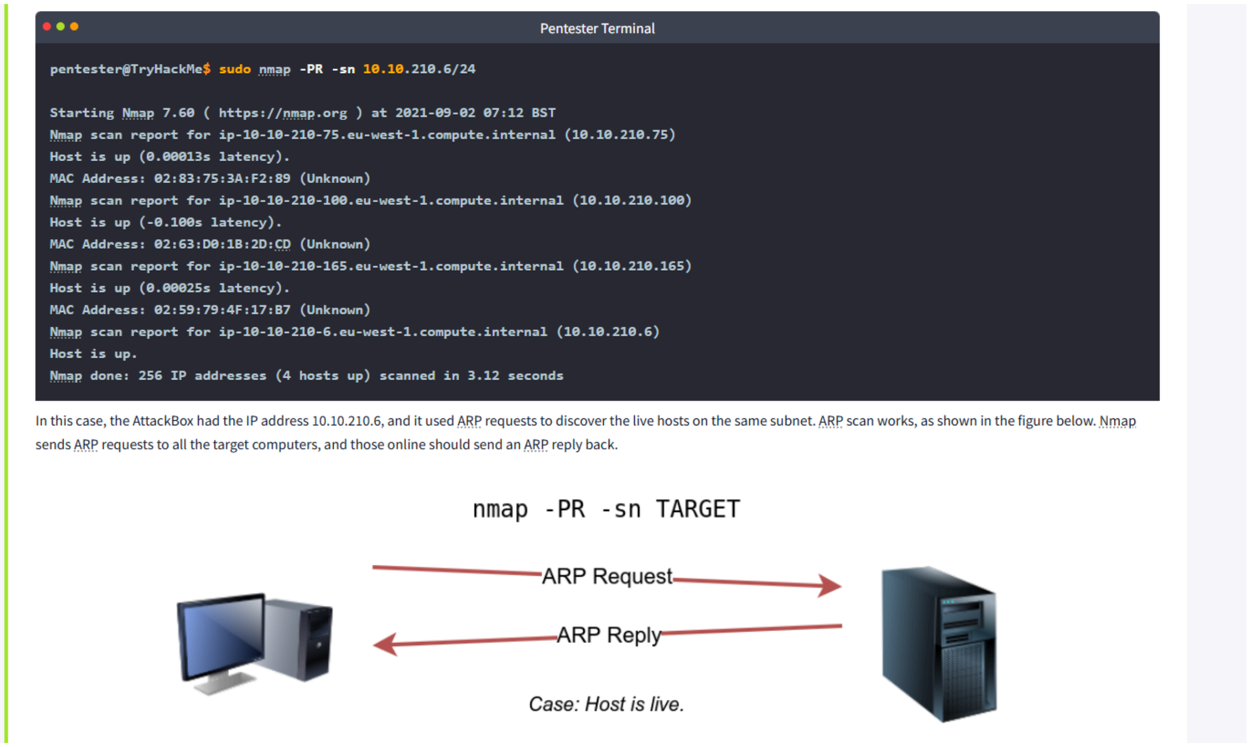
Task 5 Nmap Host Discovery Using ARP

How would you know which hosts are up and running? It is essential to avoid wasting our time port-scanning an offline host or an IP address not in use. There are various ways to discover online hosts. When no host discovery options are provided, Nmap follows the following approaches to discover live hosts:

1. When a *privileged* user tries to scan targets on a local network (Ethernet), Nmap uses *ARP requests*. A privileged user is `root` or a user who belongs to `sudoers` and can run `sudo`.
2. When a *privileged* user tries to scan targets outside the local network, Nmap uses ICMP echo requests, TCP ACK (Acknowledge) to port 80, TCP SYN (Synchronize) to port 443, and ICMP timestamp request.
3. When an *unprivileged* user tries to scan targets outside the local network, Nmap resorts to a TCP 3-way handshake by sending SYN packets to ports 80 and 443.

Nmap, by default, uses a ping scan to find live hosts, then proceeds to scan live hosts only. If you want to use Nmap to discover online hosts without port-scanning the live systems, you can issue `nmap -sn TARGETS`. Let's dig deeper to gain a solid understanding of the different techniques used.

ARP scan is possible only if you are on the same subnet as the target systems. On an Ethernet (802.3) and WiFi (802.11), you need to know the MAC address of any system before you can communicate with it. The MAC address is necessary for the link-layer header; the header contains the source MAC address and the destination MAC address among other fields. To get the MAC address, the OS sends an ARP query. A host that replies to ARP queries is up. The ARP query only works if the target is on the same subnet as yourself, i.e., on the same Ethernet/WiFi. You should expect to see many ARP queries generated during a Nmap scan of a local network. If you want Nmap only to perform an ARP scan without port-scanning, you can use `nmap -PR -sn TARGETS`, where `-PR` indicates that you only want an ARP scan. The following example shows Nmap using ARP for host discovery without any port scanning. We run `nmap -PR -sn MACHINE_IP/24` to discover all the live systems on the same subnet as our target machine.



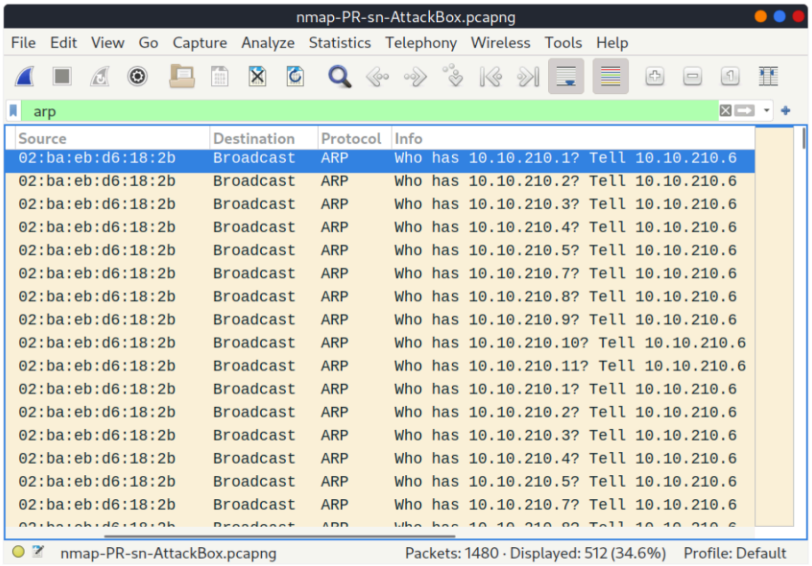
Pentester Terminal

```
pentester@TryHackMe$ sudo nmap -PR -sn 10.10.210.6/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-02 07:12 BST
Nmap scan report for ip-10-10-210-75.eu-west-1.compute.internal (10.10.210.75)
Host is up (0.00013s latency).
MAC Address: 02:83:75:3A:F2:89 (Unknown)
Nmap scan report for ip-10-10-210-100.eu-west-1.compute.internal (10.10.210.100)
Host is up (-0.100s latency).
MAC Address: 02:63:D0:1B:2D:CD (Unknown)
Nmap scan report for ip-10-10-210-165.eu-west-1.compute.internal (10.10.210.165)
Host is up (0.00025s latency).
MAC Address: 02:59:79:4F:17:B7 (Unknown)
Nmap scan report for ip-10-10-210-6.eu-west-1.compute.internal (10.10.210.6)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.12 seconds
```

In this case, the AttackBox had the IP address 10.10.210.6, and it used ARP requests to discover the live hosts on the same subnet. ARP scan works, as shown in the figure below. Nmap sends ARP requests to all the target computers, and those online should send an ARP reply back.

If we look at the packets generated using a tool such as tcpdump or Wireshark, we will see network traffic similar to the figure below. In the figure below, Wireshark displays the source MAC address, destination MAC address, protocol, and query related to each ARP request. The source address is the MAC address of our AttackBox, while the destination is the broadcast address as we don't know the MAC address of the target. However, we see the target's IP address, which appears in the Info column. In the figure, we can see that we are requesting the MAC addresses of all the IP addresses on the subnet, starting with `10.10.210.1`. The host with the IP address we are asking about will send an ARP reply with its MAC address, and that's how we will know that it is online.


nmap-PR-sn-AttackBox.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
Source             Destination  Protocol  Info
02:ba:eb:d6:18:2b  Broadcast    ARP       Who has 10.10.210.1? Tell 10.10.210.6
02:ba:eb:d6:18:2b  Broadcast    ARP       Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b  Broadcast    ARP       Who has 10.10.210.3? Tell 10.10.210.6
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       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 10.10.210.1? Tell 10.10.210.6
02:ba:eb:d6:18:2b  Broadcast    ARP       Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b  Broadcast    ARP       Who has 10.10.210.3? Tell 10.10.210.6
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       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
```

nmap-PR-sn-AttackBox.pcapng Packets: 1480 · Displayed: 512 (34.6%) Profile: Default

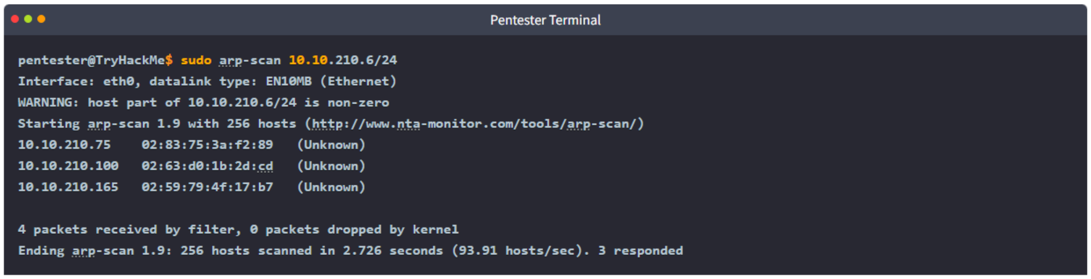
Talking about ARP scans, we should mention a scanner built around ARP queries: `arp-scan`; it provides many options to customize your scan. Visit the arp-scan wiki for detailed information. One popular choice is `arp-scan --localnet` or simply `arp-scan -l`. This command will send ARP queries to all valid IP addresses on your local networks. Moreover, if

Talking about ARP scans, we should mention a scanner built around ARP queries: `arp-scan`; it provides many options to customize your scan. Visit the arp-scan wiki for detailed information. One popular choice is `arp-scan --localnet` or simply `arp-scan -l`. This command will send ARP queries to all valid IP addresses on your local networks. Moreover, if

your system has more than one interface and you are interested in discovering the live hosts on one of them, you can specify the interface using `-I`. For instance, `sudo arp-scan -I eth0 -l` will send ARP queries for all valid IP addresses on the `eth0` interface.

Note that `arp-scan` is not installed on the AttackBox; however, it can be installed using `apt install arp-scan`.

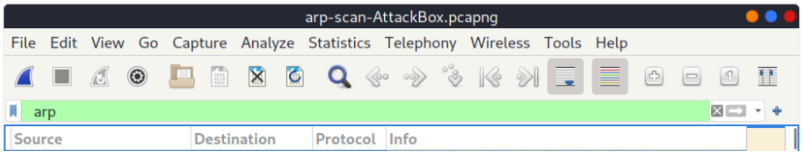
In the example below, we scanned the subnet of the AttackBox using `arp-scan ATTACKBOX_IP/24`. Since we ran this scan at a time frame close to the previous one `nmap -PR -sn ATTACKBOX_IP/24`, we obtained the same three live targets.



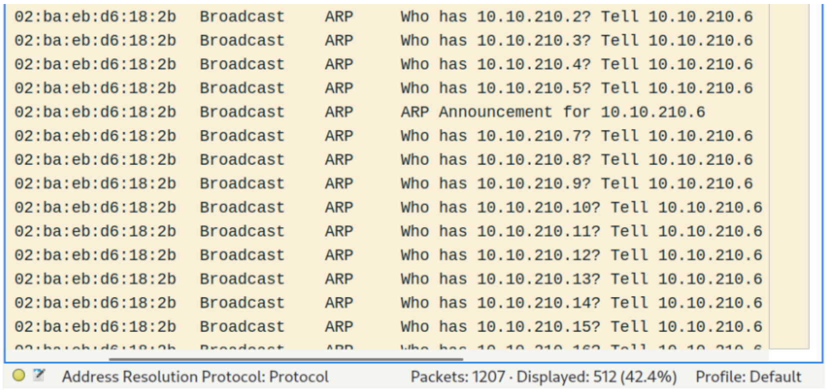
```
pentester@TryHackMe$ sudo arp-scan 10.10.210.6/24
Interface: eth0, datalink type: EN10MB (Ethernet)
WARNING: host part of 10.10.210.6/24 is non-zero
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
10.10.210.75    02:83:75:3a:f2:89    (Unknown)
10.10.210.100   02:63:d0:1b:2d:cd    (Unknown)
10.10.210.165   02:59:79:4f:17:b7    (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.726 seconds (93.91 hosts/sec). 3 responded
```

Similarly, the command `arp-scan` will generate many ARP queries that we can see using tcpdump, Wireshark, or a similar tool. We can notice that the packet capture for `arp-scan` and `nmap -PR -sn` yield similar traffic patterns. Below is the Wireshark output.


arp-scan-AttackBox.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
Source             Destination  Protocol  Info
```



```
02:ba:eb:d6:18:2b   Broadcast    ARP     Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b   Broadcast    ARP     Who has 10.10.210.3? Tell 10.10.210.6
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

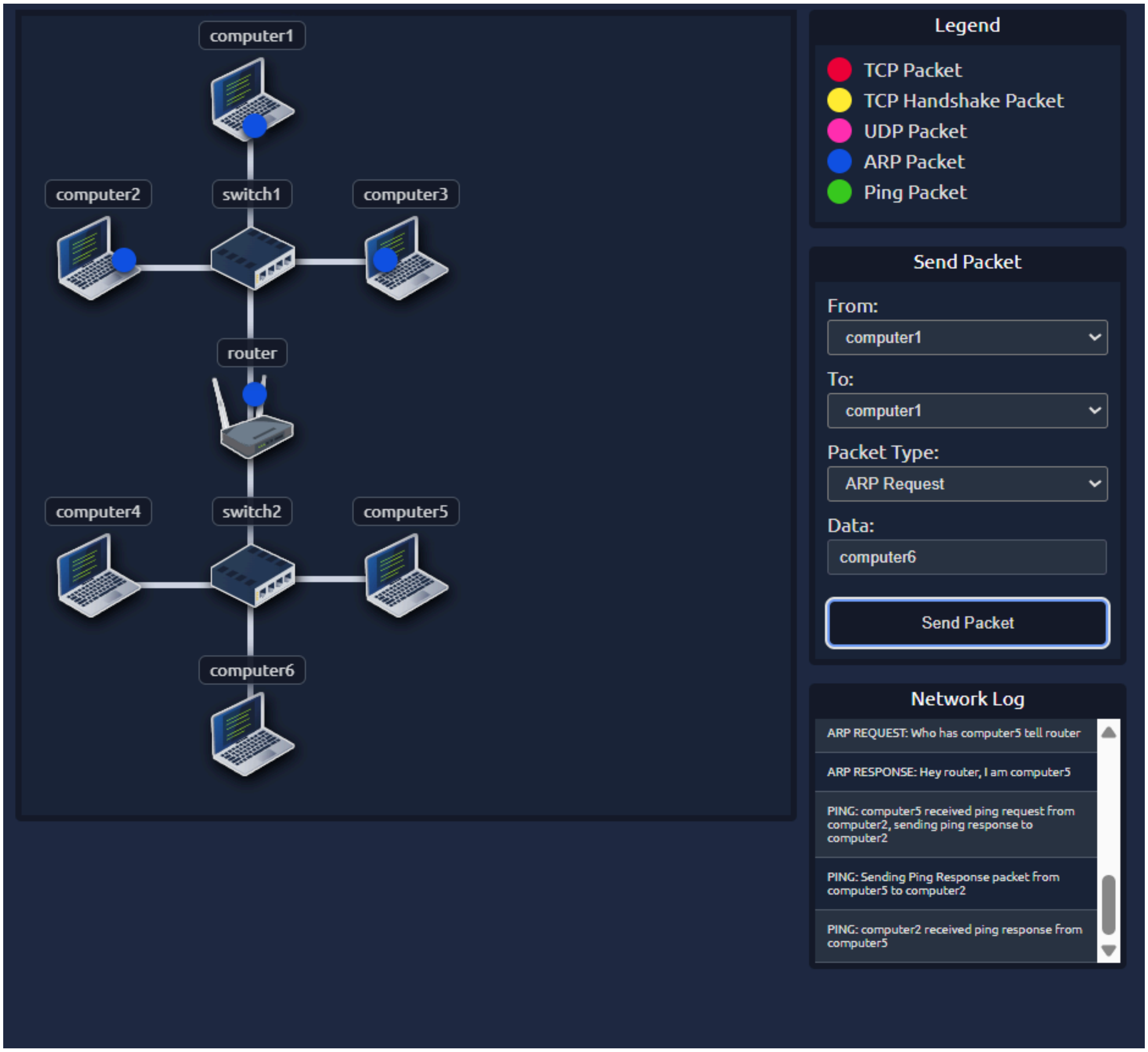
We will be sending broadcast ARP Requests packets with the following options:

- 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



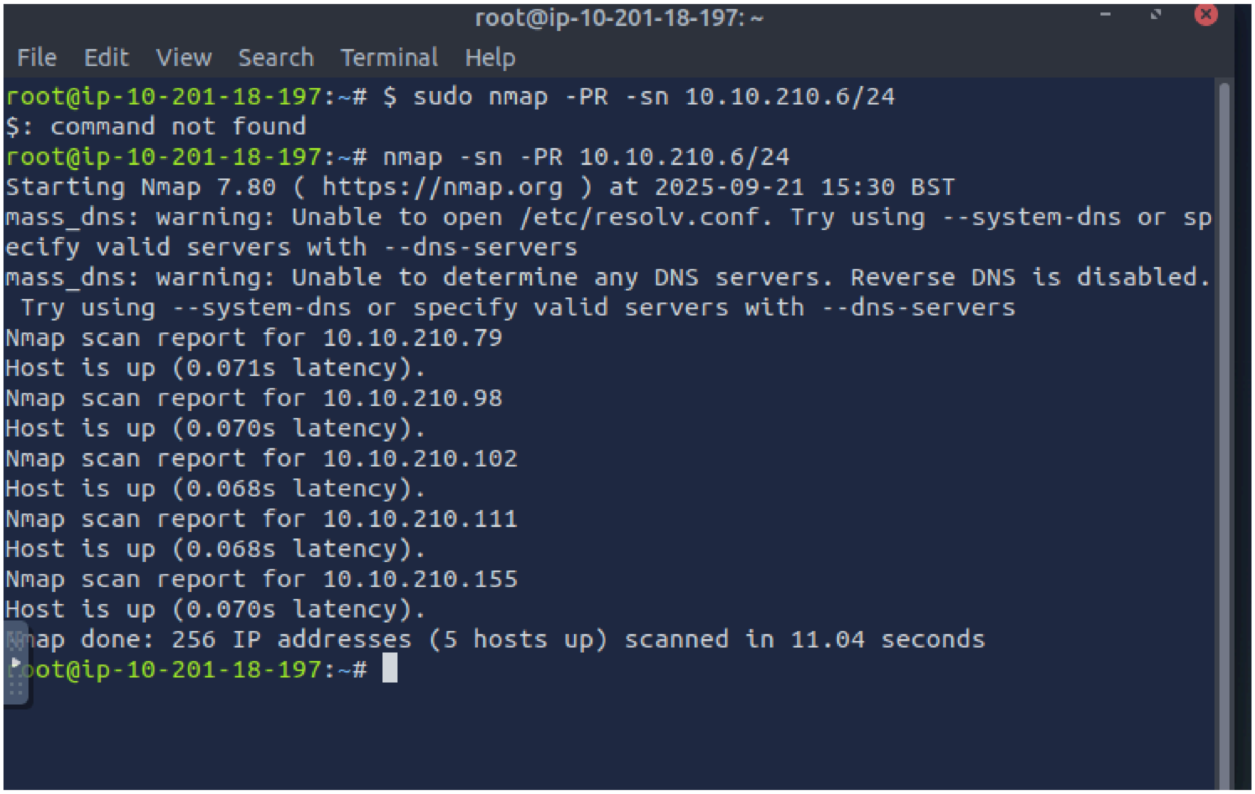
From: computer1

To: computer1

Packet Type: ARP Request

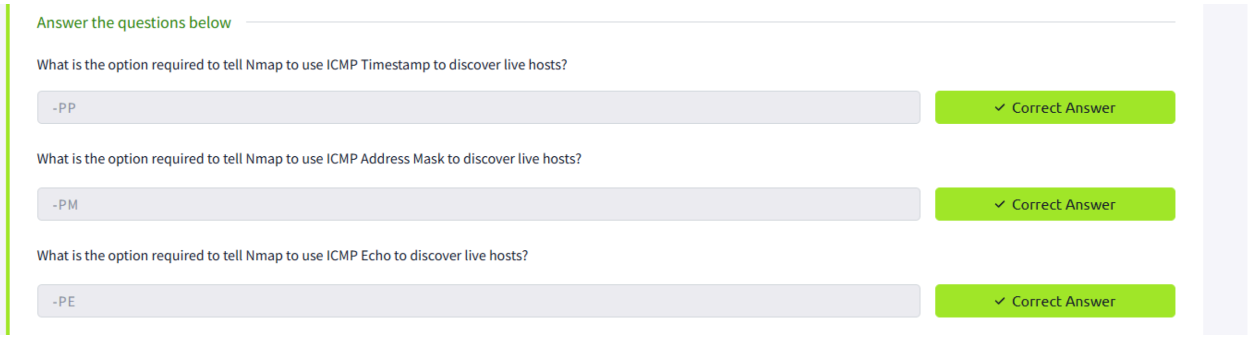
Data: computer6

```
ARP REQUEST: Who has computer5 tell router
ARP RESPONSE: Hey router, I am computer5
PING: computer5 received ping request from computer2, sending ping response to computer2
PING: Sending Ping Response packet from computer5 to computer2
PING: computer2 received ping response from computer5
```



```
root@ip-10-201-18-197:~# $ sudo nmap -PR -sn 10.10.210.6/24
$: command not found
root@ip-10-201-18-197:~# nmap -sn -PR 10.10.210.6/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-21 15:30 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.210.79
Host is up (0.071s latency).
Nmap scan report for 10.10.210.98
Host is up (0.070s latency).
Nmap scan report for 10.10.210.102
Host is up (0.068s latency).
Nmap scan report for 10.10.210.111
Host is up (0.068s latency).
Nmap scan report for 10.10.210.155
Host is up (0.070s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 11.04 seconds
root@ip-10-201-18-197:~#
```

TASK 6



Answer the questions below

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

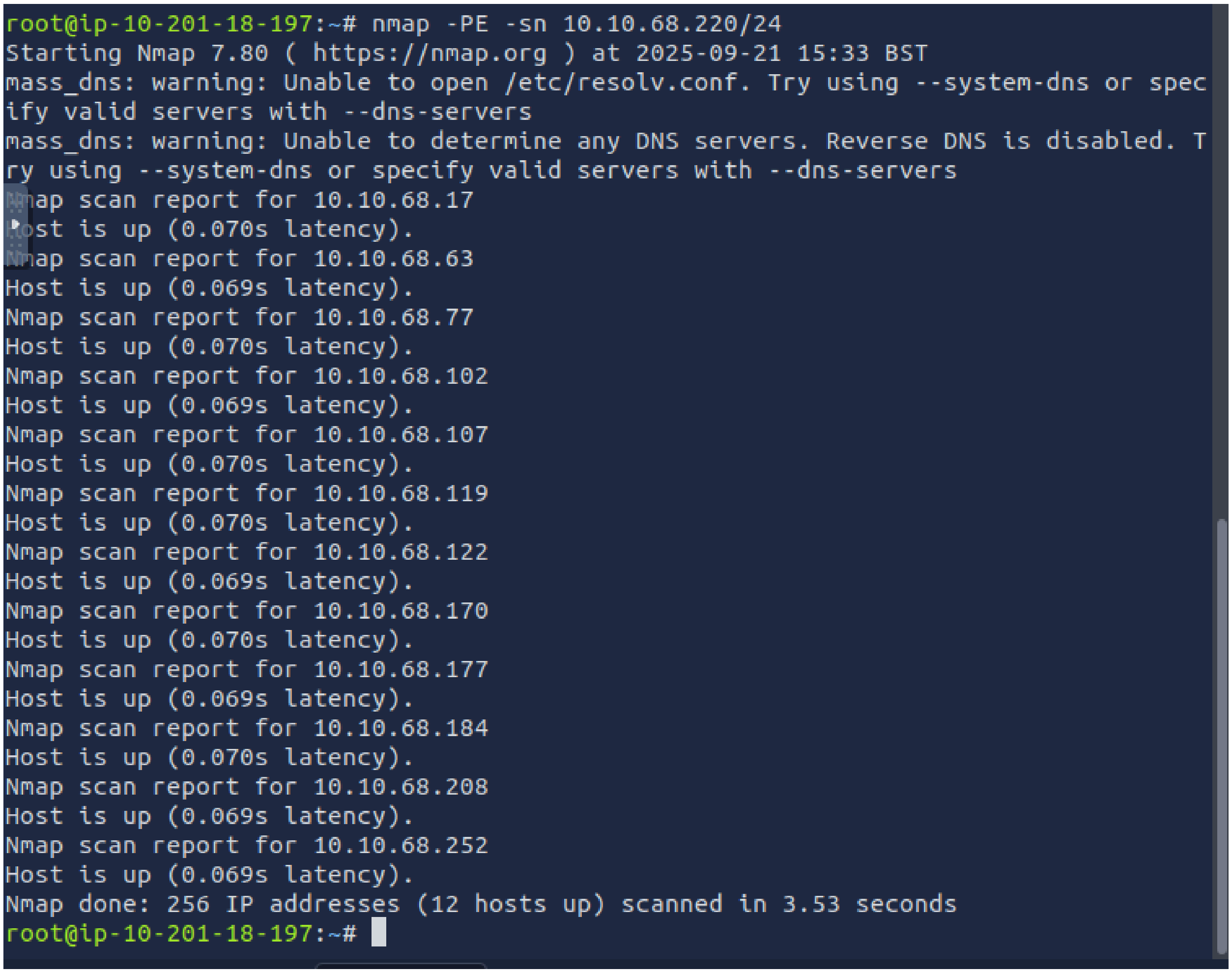
-PP

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

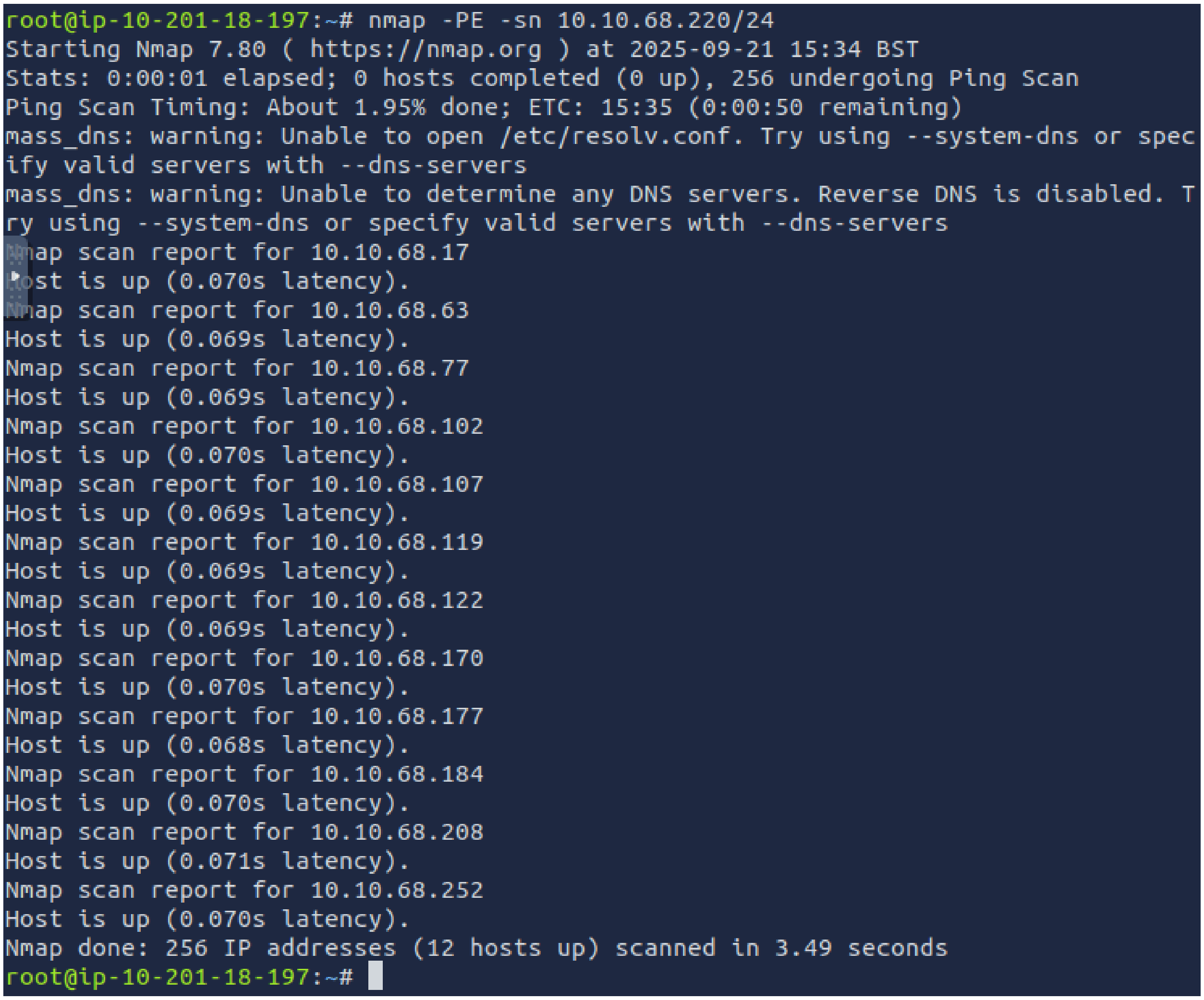
-PM

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

-PE

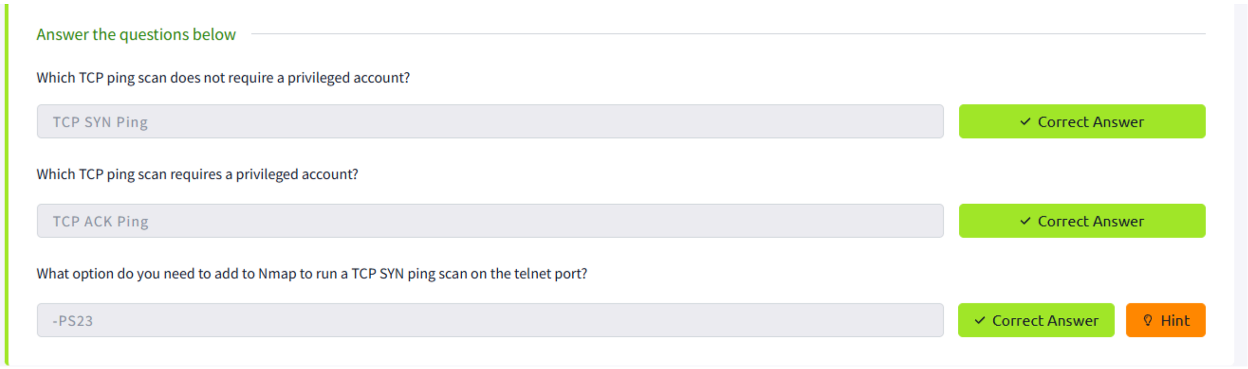


```
root@ip-10-201-18-197:~# nmap -PE -sn 10.10.68.220/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-21 15:33 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or spec
ify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. T
ry using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.68.17
Host is up (0.070s latency).
Nmap scan report for 10.10.68.63
Host is up (0.069s latency).
Nmap scan report for 10.10.68.77
Host is up (0.070s latency).
Nmap scan report for 10.10.68.102
Host is up (0.069s latency).
Nmap scan report for 10.10.68.107
Host is up (0.070s latency).
Nmap scan report for 10.10.68.119
Host is up (0.070s latency).
Nmap scan report for 10.10.68.122
Host is up (0.069s latency).
Nmap scan report for 10.10.68.170
Host is up (0.070s latency).
Nmap scan report for 10.10.68.177
Host is up (0.069s latency).
Nmap scan report for 10.10.68.184
Host is up (0.070s latency).
Nmap scan report for 10.10.68.208
Host is up (0.069s latency).
Nmap scan report for 10.10.68.252
Host is up (0.069s latency).
Nmap done: 256 IP addresses (12 hosts up) scanned in 3.53 seconds
root@ip-10-201-18-197:~# 
```



```
root@ip-10-201-18-197:~# nmap -PE -sn 10.10.68.220/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-21 15:34 BST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 1.95% done; ETC: 15:35 (0:00:50 remaining)
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or spec
ify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. T
ry using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.68.17
Host is up (0.070s latency).
Nmap scan report for 10.10.68.63
Host is up (0.069s latency).
Nmap scan report for 10.10.68.77
Host is up (0.069s latency).
Nmap scan report for 10.10.68.102
Host is up (0.070s latency).
Nmap scan report for 10.10.68.107
Host is up (0.069s latency).
Nmap scan report for 10.10.68.119
Host is up (0.069s latency).
Nmap scan report for 10.10.68.122
Host is up (0.069s latency).
Nmap scan report for 10.10.68.170
Host is up (0.070s latency).
Nmap scan report for 10.10.68.177
Host is up (0.068s latency).
Nmap scan report for 10.10.68.184
Host is up (0.070s latency).
Nmap scan report for 10.10.68.208
Host is up (0.071s latency).
Nmap scan report for 10.10.68.252
Host is up (0.070s latency).
Nmap done: 256 IP addresses (12 hosts up) scanned in 3.49 seconds
root@ip-10-201-18-197:~#
```

TASK 7



Answer the questions below

Which TCP ping scan does not require a privileged account?

TCP SYN Ping

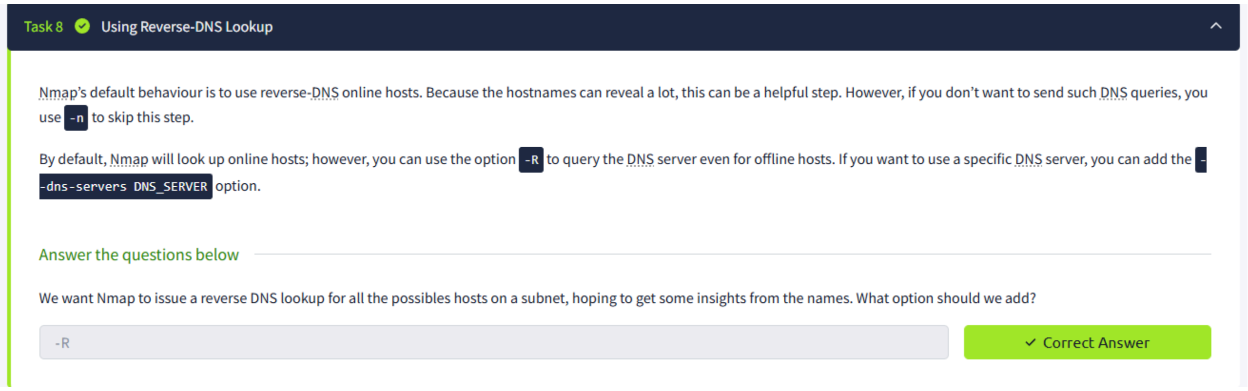
Which TCP ping scan requires a privileged account?

TCP ACK Ping

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

-PS23

TASK 8



Task 8 ✓ Using Reverse-DNS Lookup

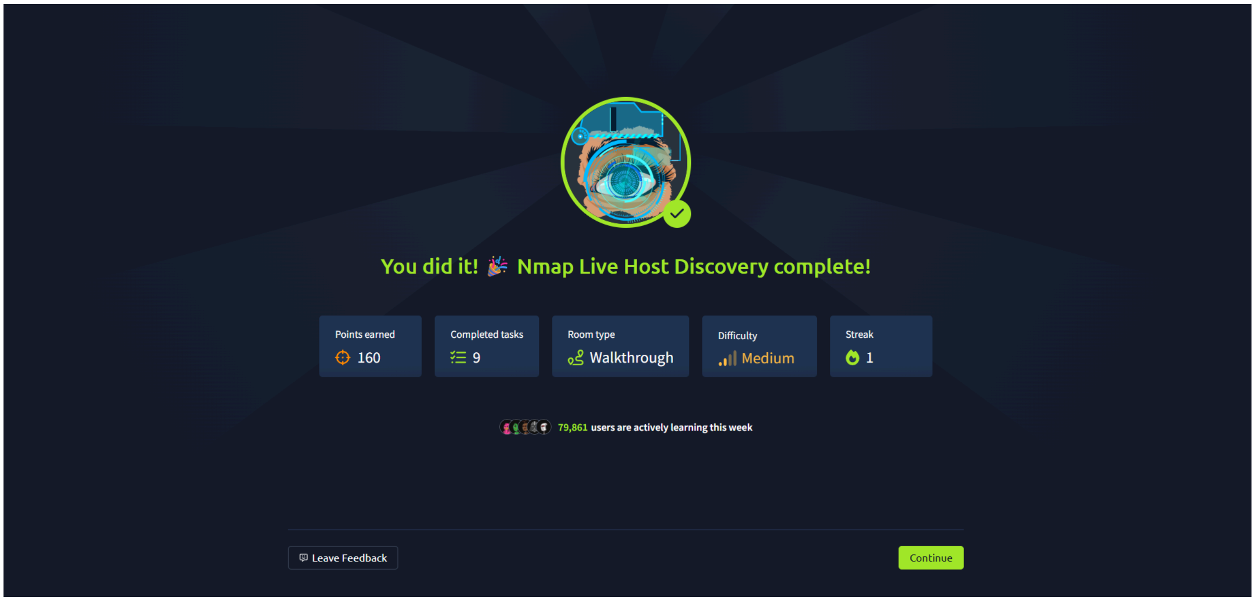
Nmap's default behaviour is to use reverse-DNS online hosts. Because the hostnames can reveal a lot, this can be a helpful step. However, if you don't want to send such DNS queries, you use `-n` to skip this step.

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?

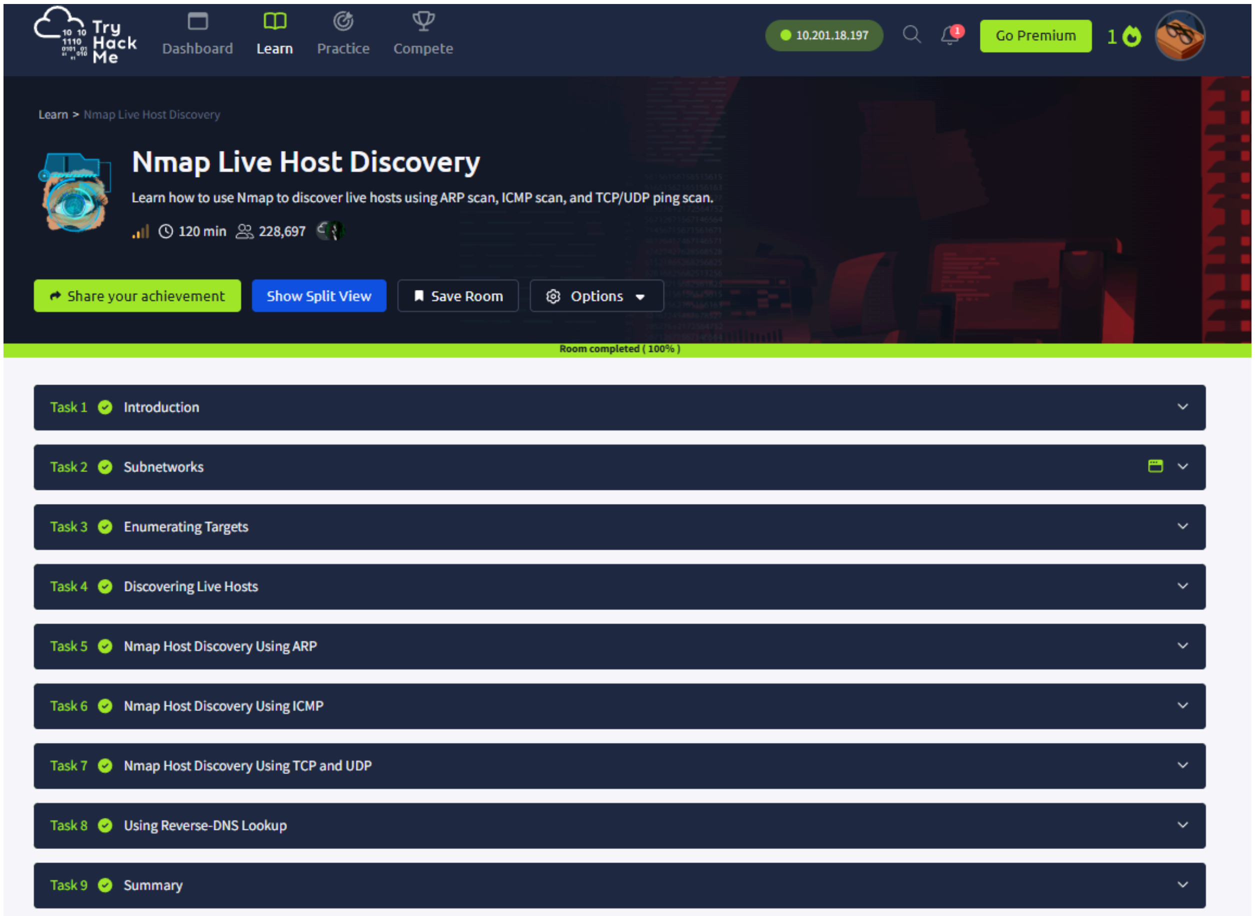
-R



You did it! 🎉 Nmap Live Host Discovery complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
160	9	Walkthrough	Medium	1

79,861 users are actively learning this week



Learn > Nmap Live Host Discovery

Nmap Live Host Discovery

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

120 min 228,697

Room completed (100%)

- Task 1 ✓ Introduction
- Task 2 ✓ 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