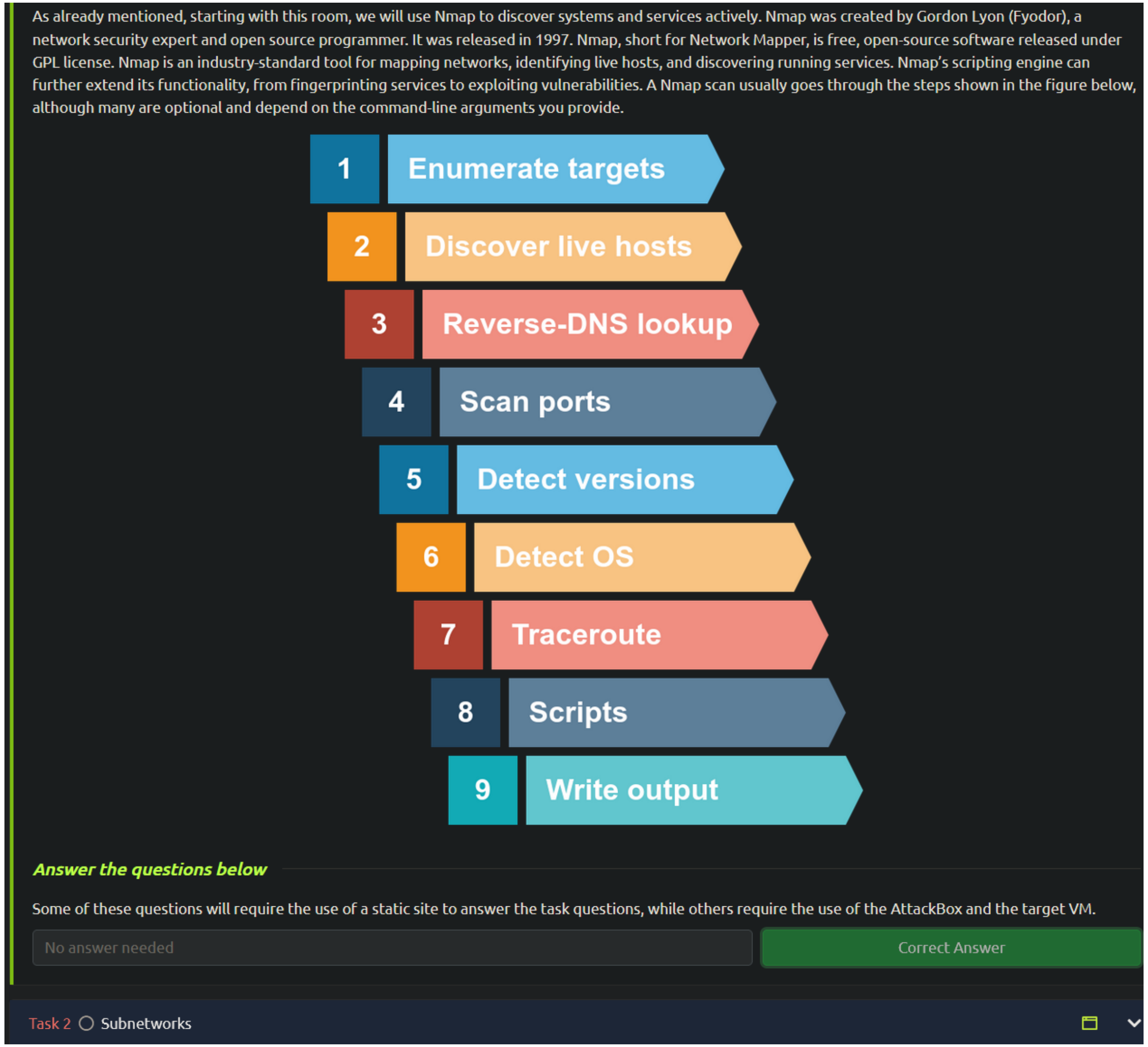
Assignment 6 –John Parr

TryHackme.com nmap

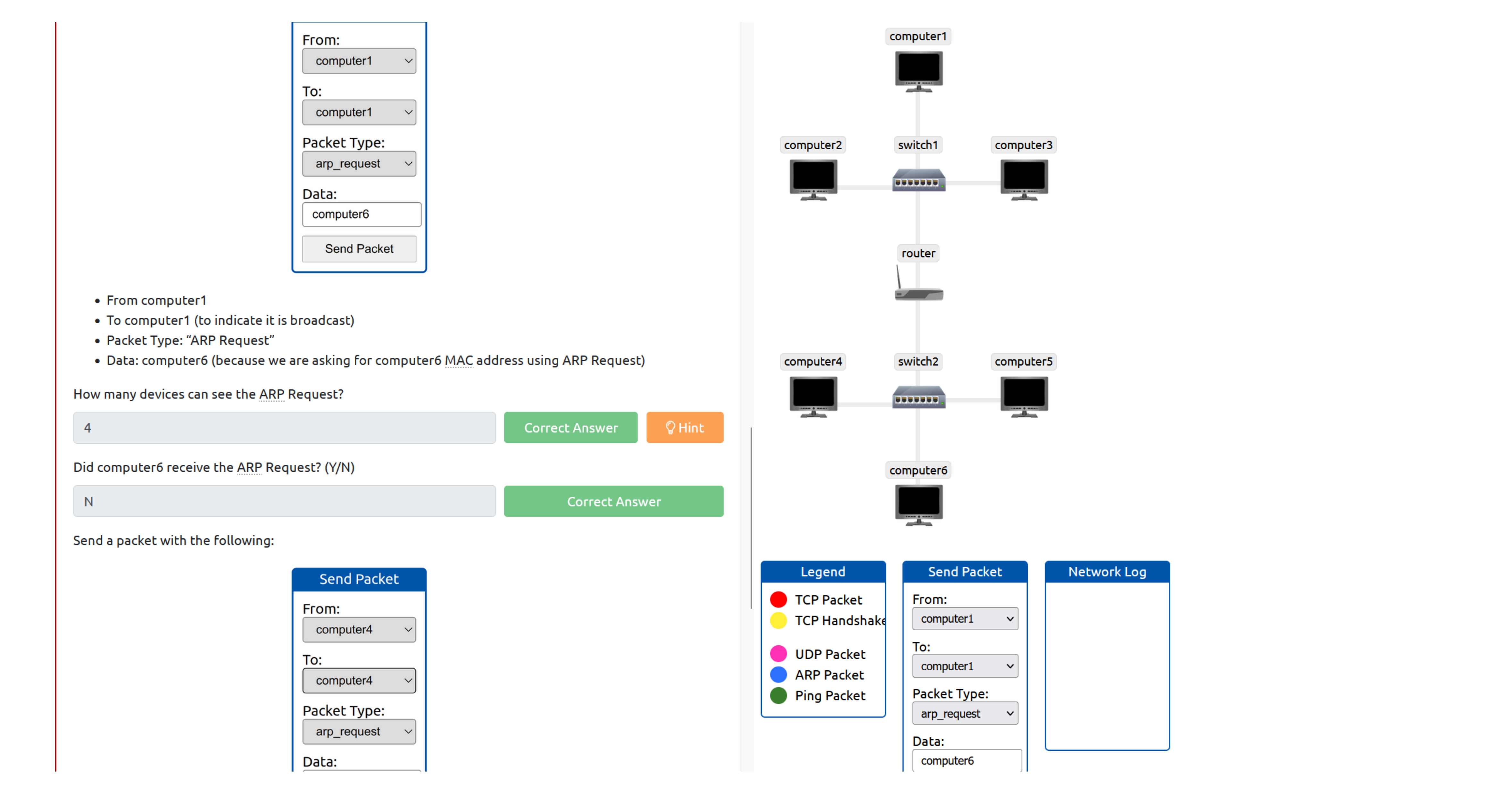


As already mentioned, starting with this room, we will use Nmap to discover systems and services actively. Nmap was created by Gordon Lyon (Fyodor), a network security expert and open source programmer. It was released in 1997. Nmap, short for Network Mapper, is free, open-source software released under 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

Answer the questions below

Some of these questions will require the use of a static site to answer the task questions, while others require the use of the AttackBox and the target VM.



From:

computer1

To:

computer1

Packet Type:

arp_request

Data:

computer6

Send Packet

- 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:

Legend

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

Send Packet

From:

computer1

To:

computer1

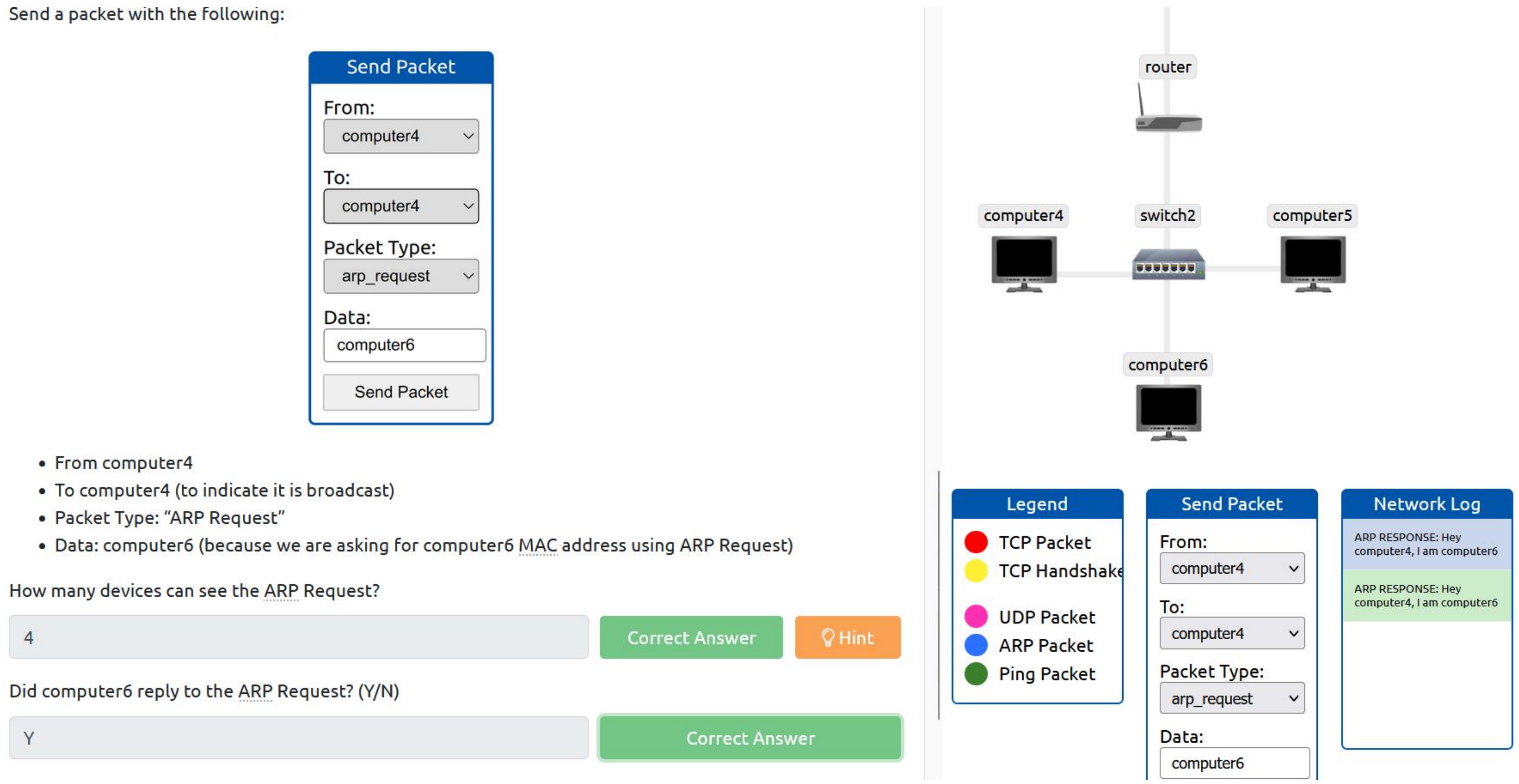
Packet Type:

arp_request

Data:

computer6

Network Log



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

Legend

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

Send Packet

From:
computer4

To:
computer4

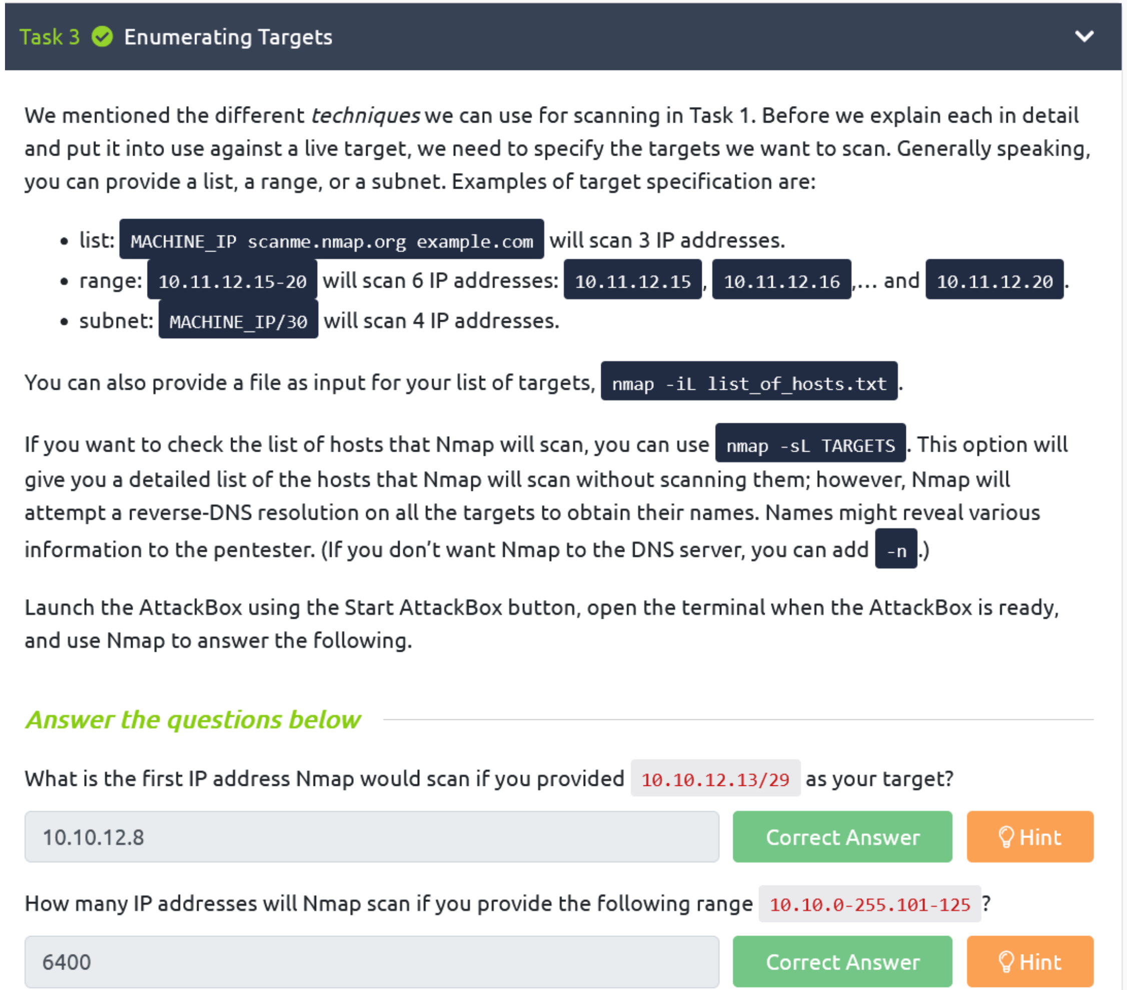
Packet Type:
arp_request

Data:
computer6

Network Log

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

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



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?

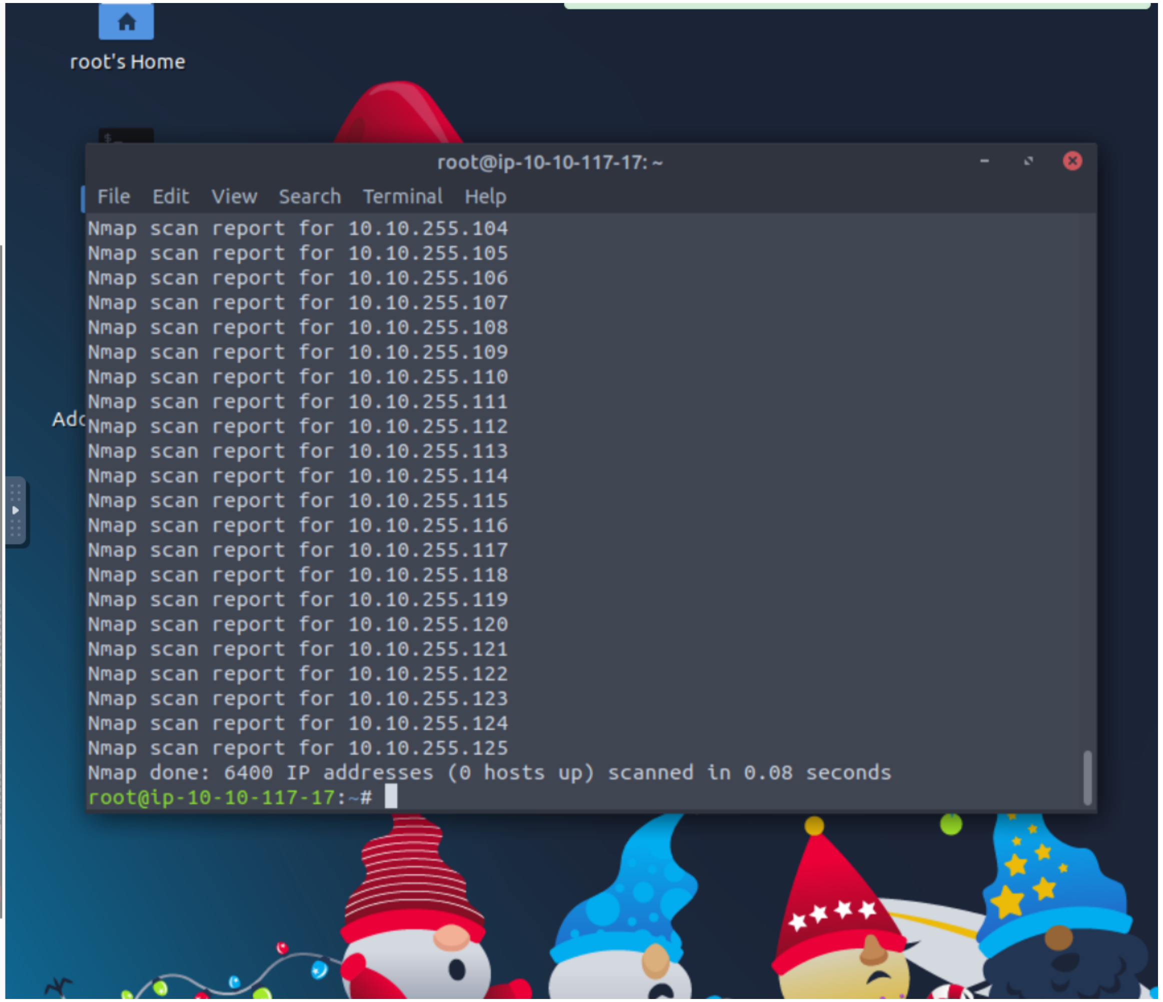
10.10.12.8

Correct Answer | Hint

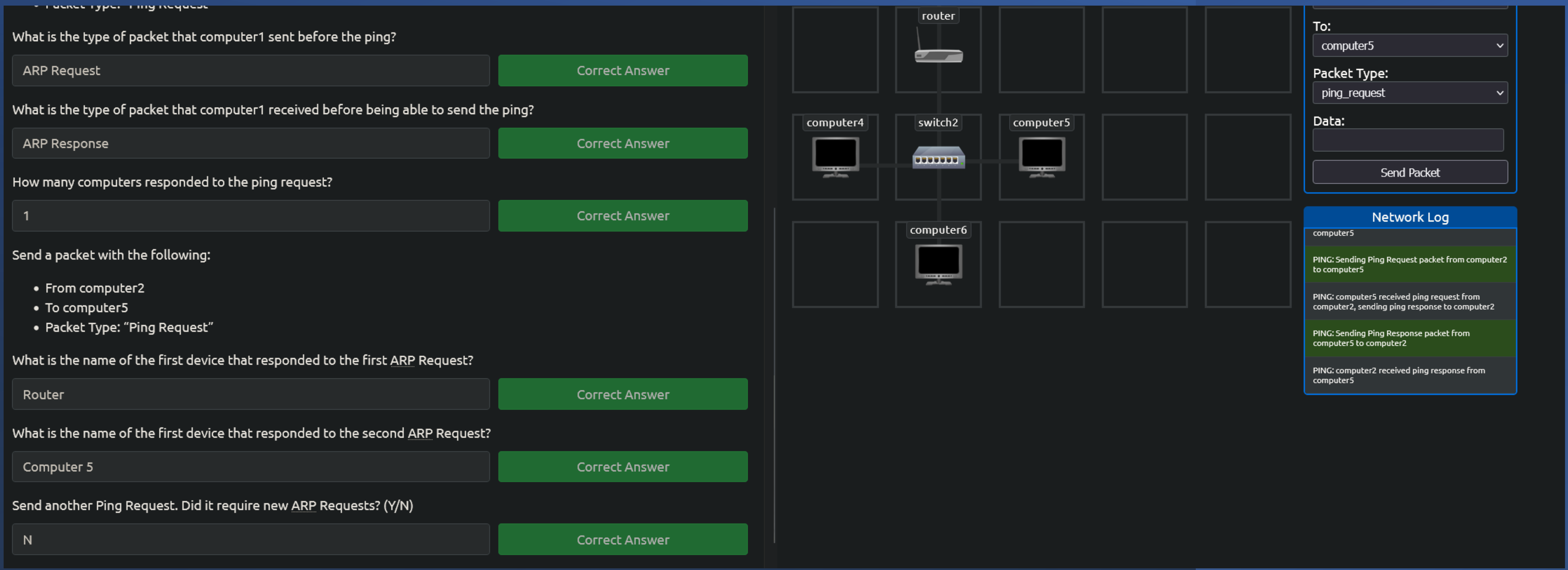
How many IP addresses will Nmap scan if you provide the following range `10.10.0-255.101-125`?

6400

Correct Answer | Hint



```
Nmap scan report for 10.10.255.104
Nmap scan report for 10.10.255.105
Nmap scan report for 10.10.255.106
Nmap scan report for 10.10.255.107
Nmap scan report for 10.10.255.108
Nmap scan report for 10.10.255.109
Nmap scan report for 10.10.255.110
Nmap scan report for 10.10.255.111
Nmap scan report for 10.10.255.112
Nmap scan report for 10.10.255.113
Nmap scan report for 10.10.255.114
Nmap scan report for 10.10.255.115
Nmap scan report for 10.10.255.116
Nmap scan report for 10.10.255.117
Nmap scan report for 10.10.255.118
Nmap scan report for 10.10.255.119
Nmap scan report for 10.10.255.120
Nmap scan report for 10.10.255.121
Nmap scan report for 10.10.255.122
Nmap scan report for 10.10.255.123
Nmap scan report for 10.10.255.124
Nmap scan report for 10.10.255.125
Nmap done: 6400 IP addresses (0 hosts up) scanned in 0.08 seconds
root@ip-10-10-117-17:~#
```



- 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?

Computer 5 | Correct Answer

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

N | Correct Answer

To: computer5

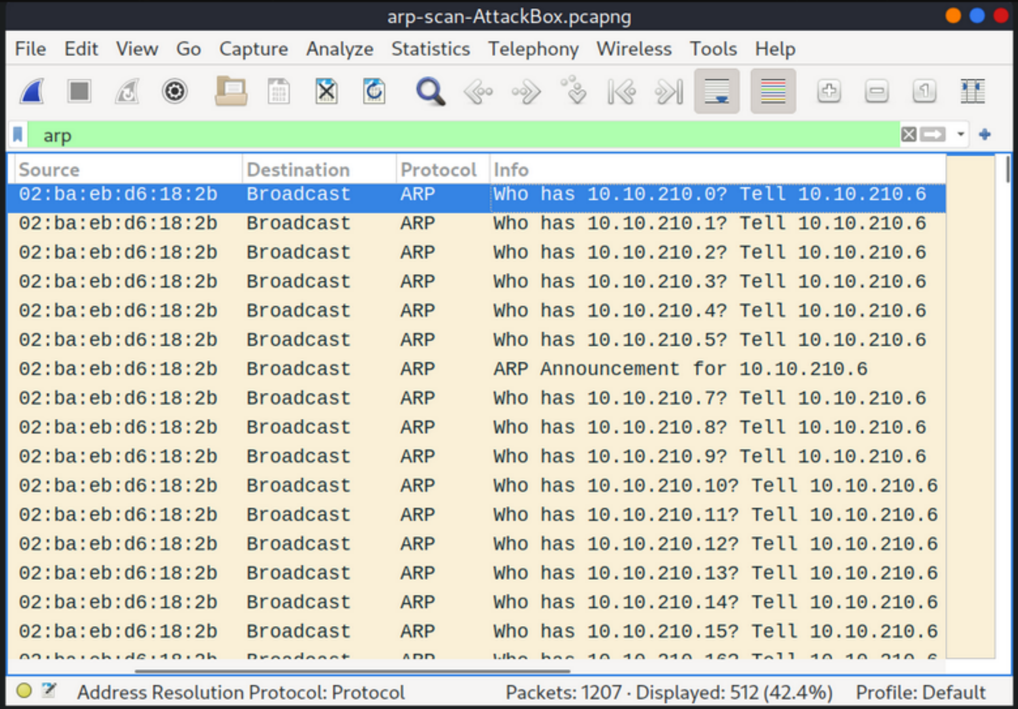
Packet Type: ping_request

Data:

Send Packet

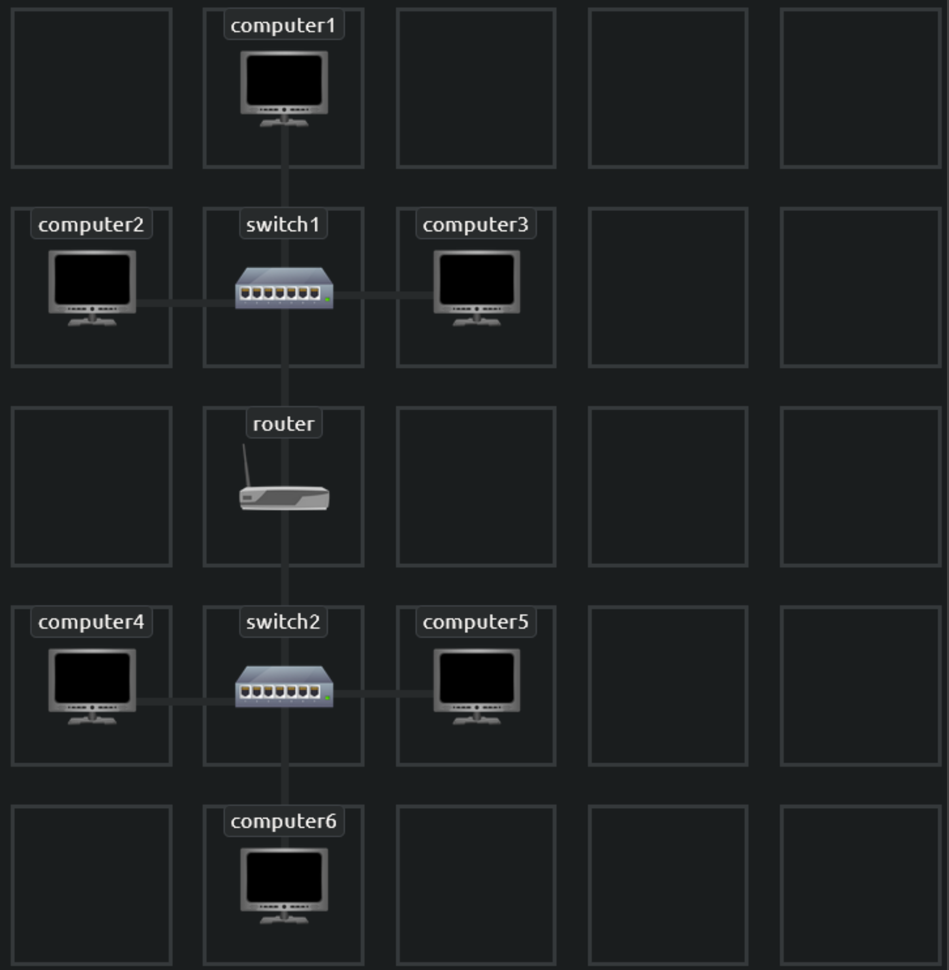
Network Log

```
computer5
PING: Sending Ping Request packet from computer2 to 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
```


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 10.10.210.0? 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       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
```

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

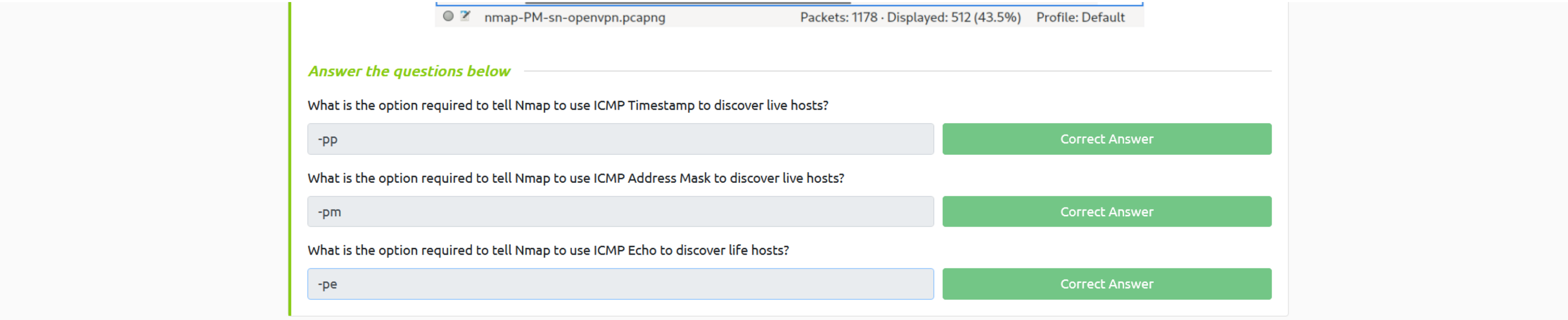
We will be sending broadcast ARP Requests packets with the following options:

- 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



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?

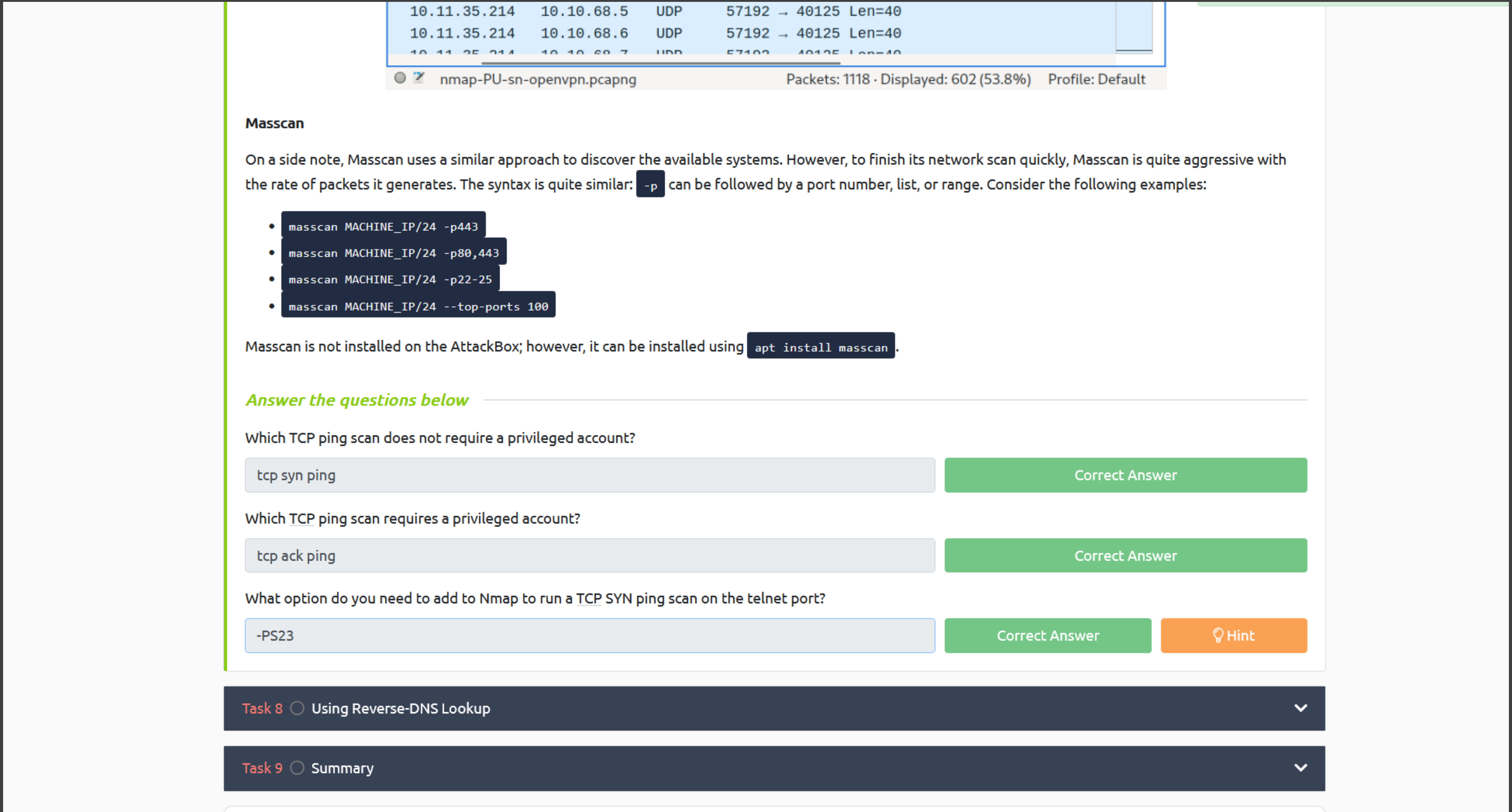
-pp

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 life hosts?

-pe



```
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
```

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?

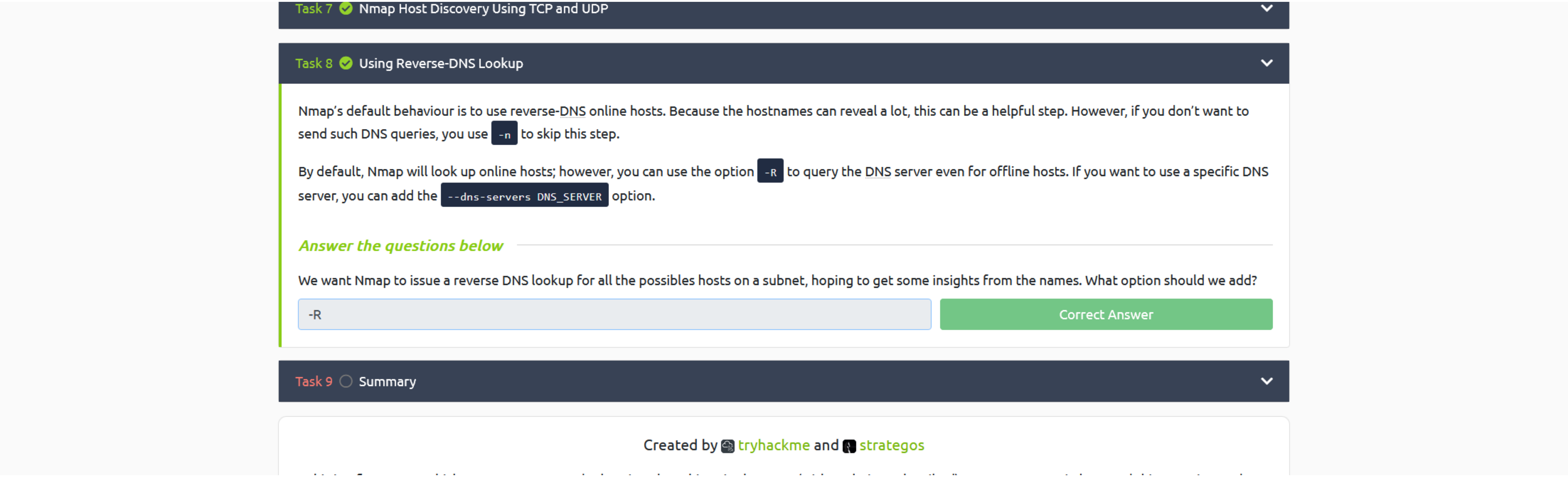
tcp syn ping

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 7 ✓ Nmap Host Discovery Using TCP and UDP

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

Created by tryhackme and strategos