Lab Report No.3

Scanning using Nmap

Ethical Hacking

Submitted By: Raghad Alharthi 2210003220

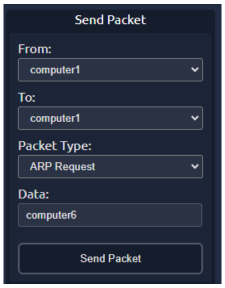
Section: CS Group no. 2

Contents

Room: Nmap Live Host Discovery

Task 2

Q1



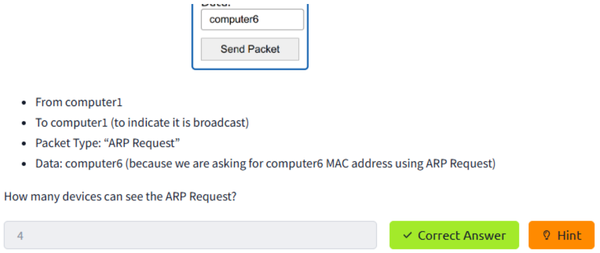
Send Packet

From: computer1

To: computer1

Packet Type: ARP Request

Data: computer6

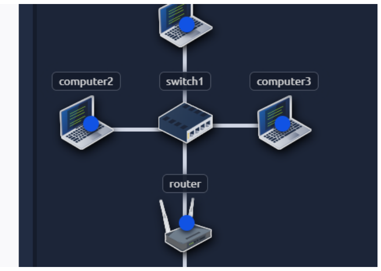


computer6

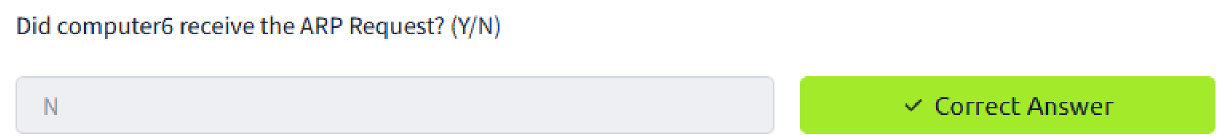
- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4



Q2

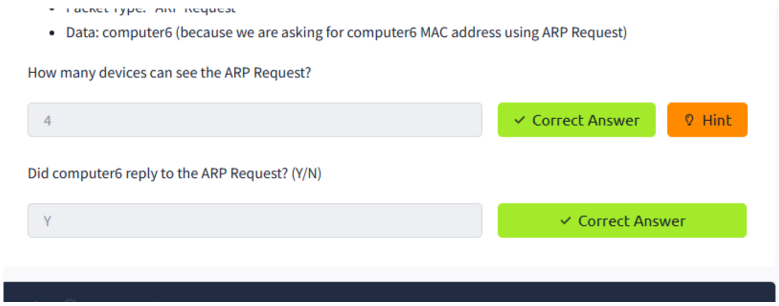


Did computer6 receive the ARP Request? (Y/N)

N

it only goes for computers 1,2,3 and the router.

Q3



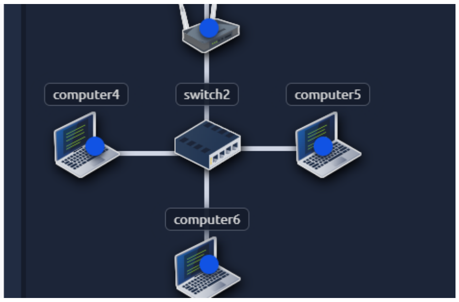
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

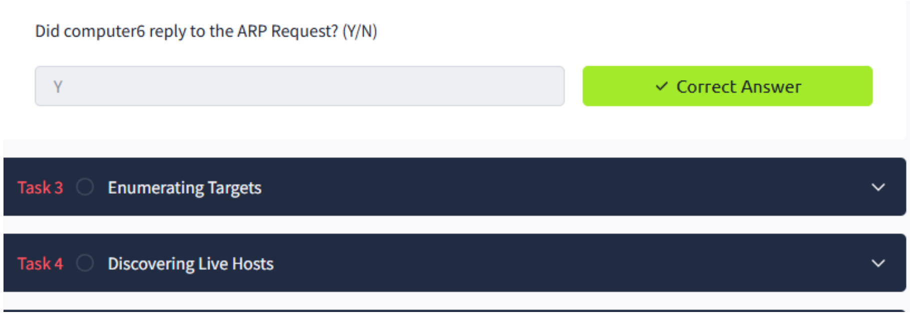
4

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

Y

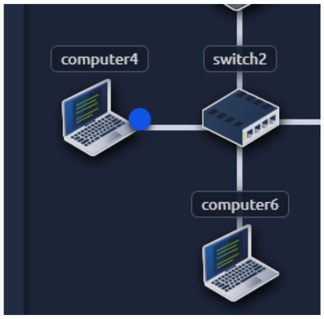


Q4



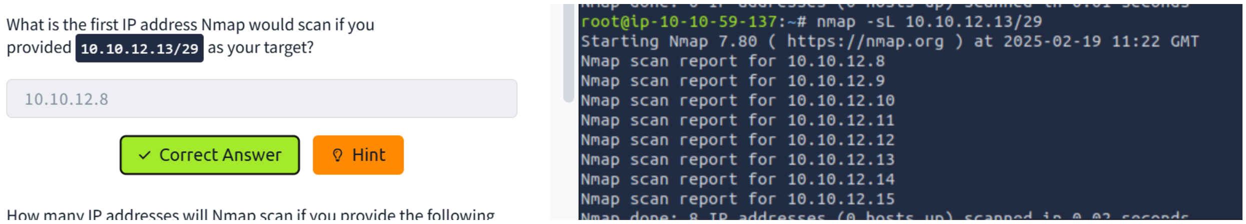
Did computer6 reply to the ARP Request? (Y/N)

Y



Task 3

Q1



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

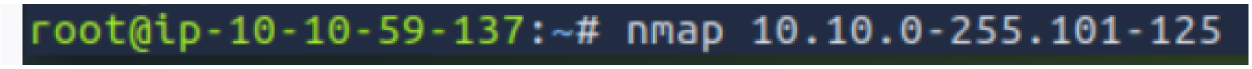
10.10.12.8

✓ Correct Answer   Hint

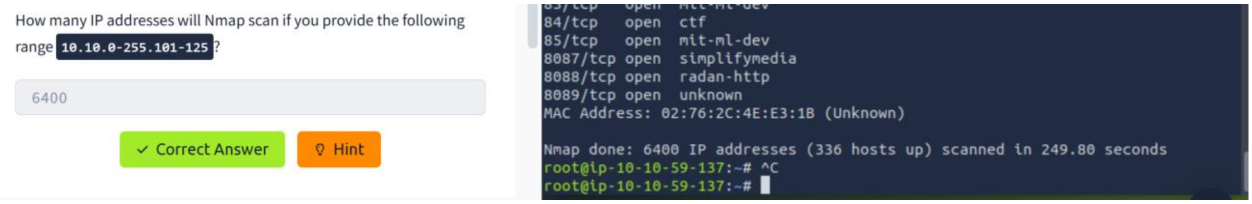
How many IP addresses will Nmap scan if you provide the following

```
root@ip-10-10-59-137:~# nmap -sL 10.10.12.13/29
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 11:22 GMT
Nmap scan report for 10.10.12.8
Nmap scan report for 10.10.12.9
Nmap scan report for 10.10.12.10
Nmap scan report for 10.10.12.11
Nmap scan report for 10.10.12.12
Nmap scan report for 10.10.12.13
Nmap scan report for 10.10.12.14
Nmap scan report for 10.10.12.15
Nmap done: 8 IP addresses (0 hosts up) scanned in 0.02 seconds
```

Q2



```
root@ip-10-10-59-137:~# nmap 10.10.0-255.101-125
```



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

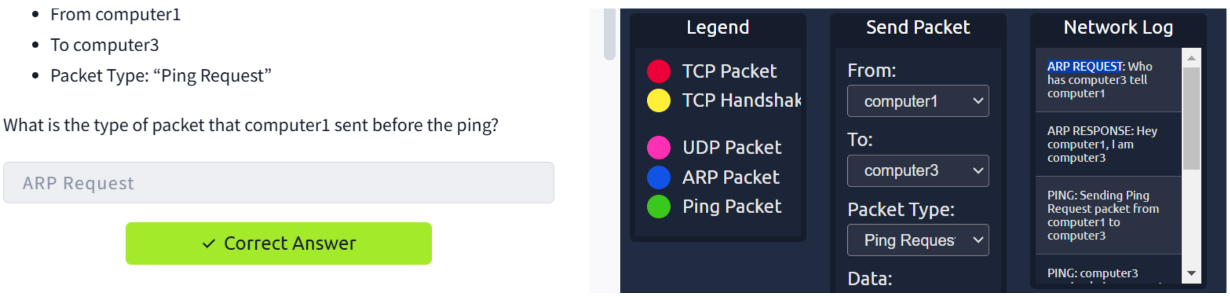
6400

✓ Correct Answer   Hint

```
84/tcp   open  ctf
85/tcp   open  mit-ml-dev
8087/tcp open  simplifymedia
8088/tcp open  radan-http
8089/tcp open  unknown
MAC Address: 02:76:2C:4E:E3:1B (Unknown)

Nmap done: 6400 IP addresses (336 hosts up) scanned in 249.80 seconds
root@ip-10-10-59-137:~# ^C
root@ip-10-10-59-137:~# 
```

Task 4

Q1



- From computer1
- To computer3
- Packet Type: "Ping Request"

What is the type of packet that computer1 sent before the ping?

ARP Request

✓ Correct Answer

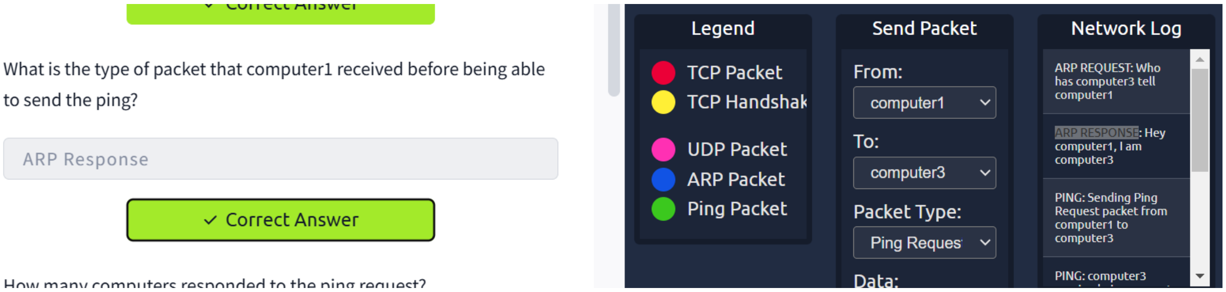
ARP REQUEST: Who has computer3 tell computer1

ARP RESPONSE: Hey computer1, I am computer3

PING: Sending Ping Request packet from computer1 to computer3

PING: computer3

Q2



✓ 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?

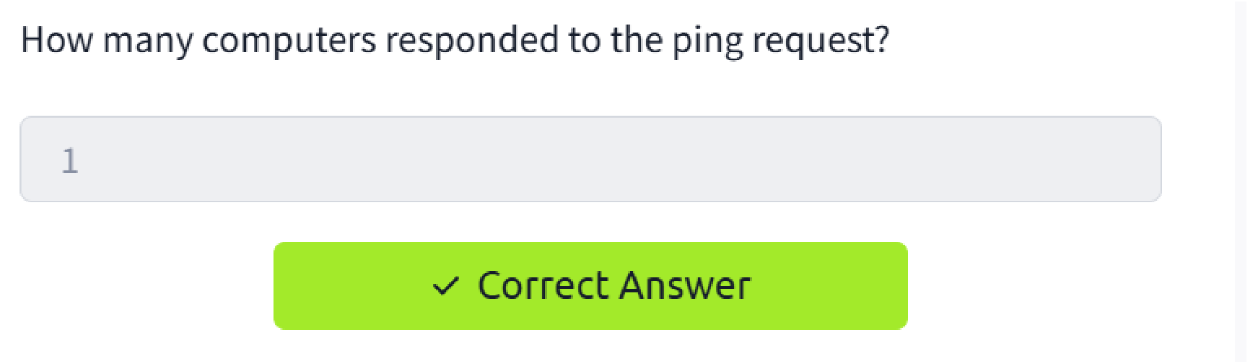
ARP REQUEST: Who has computer3 tell computer1

ARP RESPONSE: Hey computer1, I am computer3

PING: Sending Ping Request packet from computer1 to computer3

PING: computer3

Q3



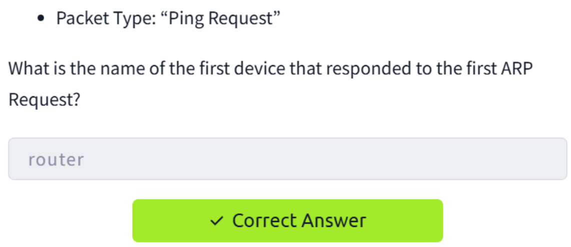
How many computers responded to the ping request?

1

✓ Correct Answer

Only computer 1 answered

Q4

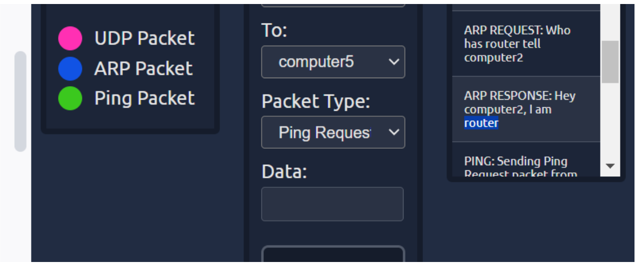


- Packet Type: “Ping Request”

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

router

✓ Correct Answer



To: computer5

Packet Type: Ping Reques

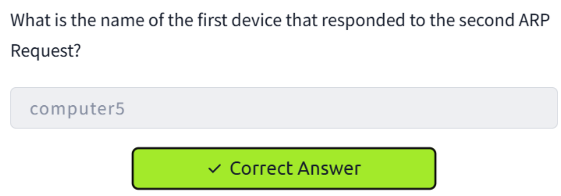
Data:

ARP REQUEST: Who has router tell computer2

ARP RESPONSE: Hey computer2, I am router

PING: Sending Ping Request packet from

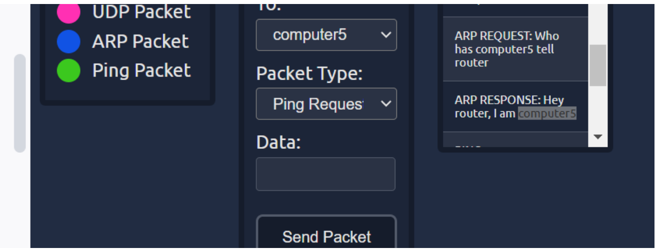
Q5



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

computer5

✓ Correct Answer



To: computer5

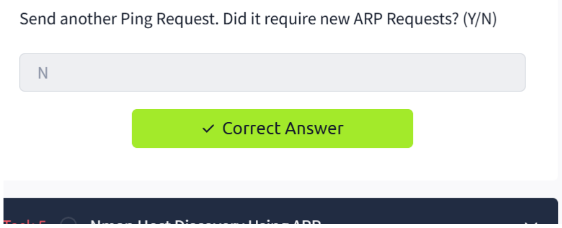
Packet Type: Ping Reques

Data:

ARP REQUEST: Who has computer5 tell router

ARP RESPONSE: Hey router, I am computer5

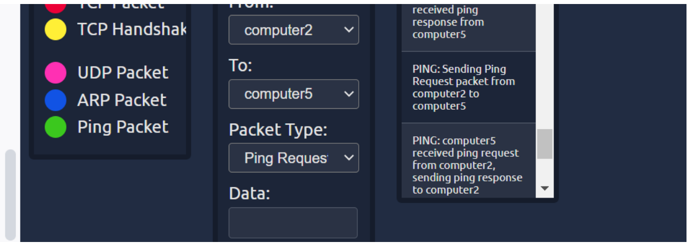
Q6



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

N

✓ Correct Answer



From: computer2

To: computer5

Packet Type: Ping Reques

Data:

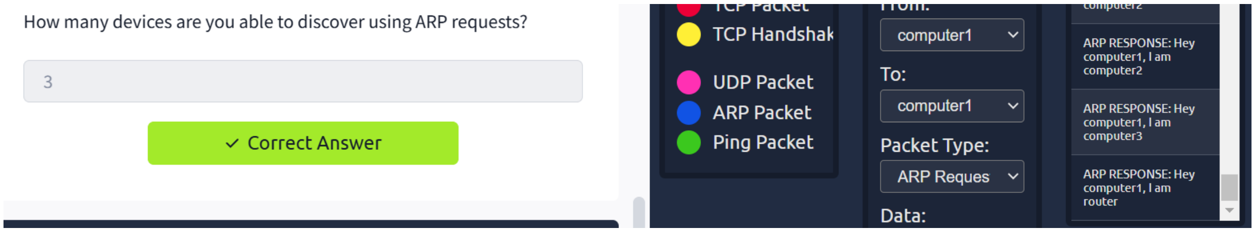
received ping response from computer5

PING: Sending Ping Request packet from computer2 to computer5

PING: computer5 received ping request from computer2, sending ping response to computer2

Task 5

Q1



How many devices are you able to discover using ARP requests?

3

✓ Correct Answer

From:
computer1

To:
computer1

Packet Type:
ARP Reques

Data:

computer2

ARP RESPONSE: Hey computer1, I am computer2

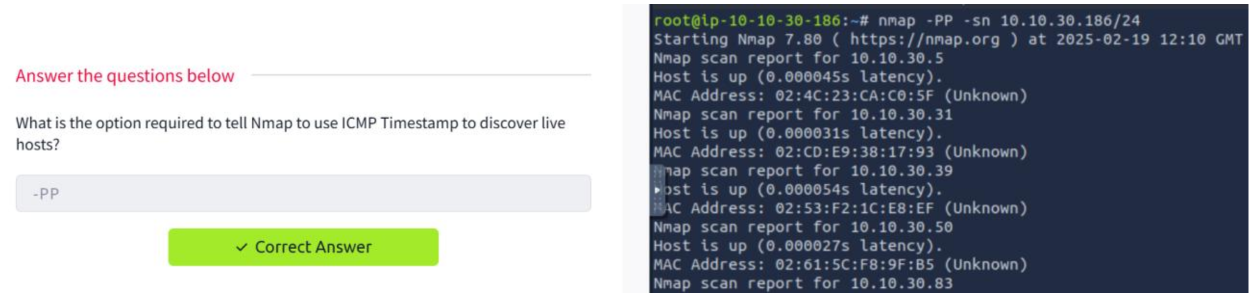
ARP RESPONSE: Hey computer1, I am computer3

ARP RESPONSE: Hey computer1, I am router

Devices are : computer2, computer3, and router.

Task 6

Q1



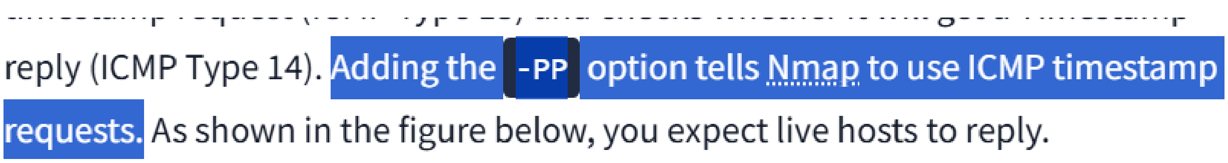
Answer the questions below

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

-PP

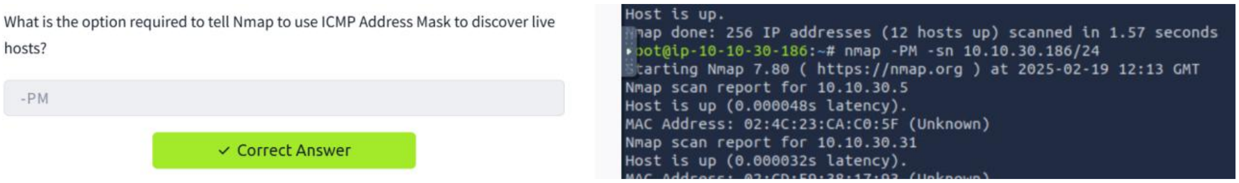
✓ Correct Answer

```
root@ip-10-10-30-186:~# nmap -PP -sn 10.10.30.186/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 12:10 GMT
Nmap scan report for 10.10.30.5
Host is up (0.000045s latency).
MAC Address: 02:4C:23:CA:C0:5F (Unknown)
Nmap scan report for 10.10.30.31
Host is up (0.000031s latency).
MAC Address: 02:CD:E9:38:17:93 (Unknown)
Nmap scan report for 10.10.30.39
Host is up (0.000054s latency).
MAC Address: 02:53:F2:1C:E8:EF (Unknown)
Nmap scan report for 10.10.30.50
Host is up (0.000027s latency).
MAC Address: 02:61:5C:F8:9F:B5 (Unknown)
Nmap scan report for 10.10.30.83
```



reply (ICMP Type 14). Adding the `-PP` option tells Nmap to use ICMP timestamp requests. As shown in the figure below, you expect live hosts to reply.

Q2

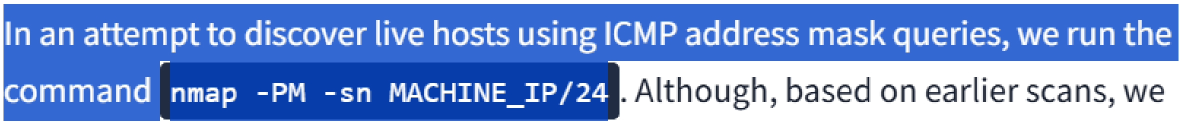


What is the option required to tell Nmap to use ICMP Address Mask to discover live hosts?

-PM

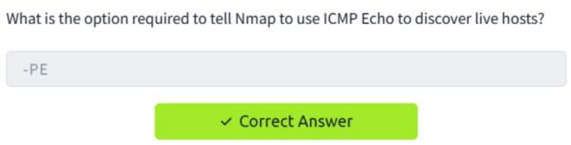
✓ Correct Answer

```
Host is up.
Nmap done: 256 IP addresses (12 hosts up) scanned in 1.57 seconds
root@ip-10-10-30-186:~# nmap -PM -sn 10.10.30.186/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 12:13 GMT
Nmap scan report for 10.10.30.5
Host is up (0.000048s latency).
MAC Address: 02:4C:23:CA:C0:5F (Unknown)
Nmap scan report for 10.10.30.31
Host is up (0.000032s latency).
```



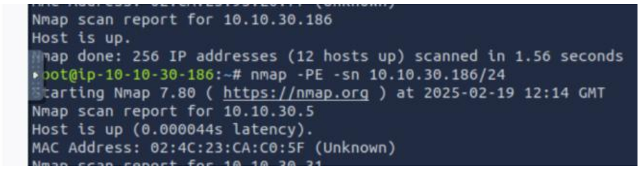
In an attempt to discover live hosts using ICMP address mask queries, we run the command `nmap -PM -sn MACHINE_IP/24`. Although, based on earlier scans, we

Q3

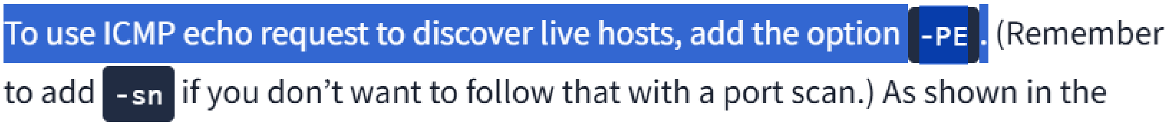


What is the option required to tell Nmap to use ICMP Echo to discover live hosts?

-PE



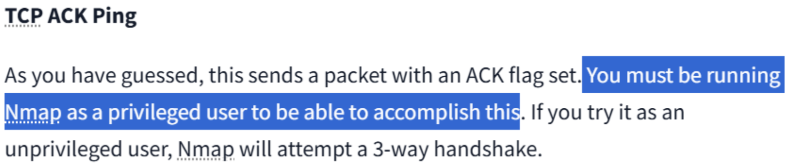
```
Nmap scan report for 10.10.30.186
Host is up.
map done: 256 IP addresses (12 hosts up) scanned in 1.56 seconds
oot@ip-10-10-30-186:~# nmap -PE -sn 10.10.30.186/24
tarting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 12:14 GMT
Nmap scan report for 10.10.30.5
Host is up (0.000044s latency).
MAC Address: 02:4C:23:CA:C0:5F (Unknown)
```



To use ICMP echo request to discover live hosts, add the option `-PE`. (Remember to add `-sn` if you don't want to follow that with a port scan.) As shown in the

Task 7

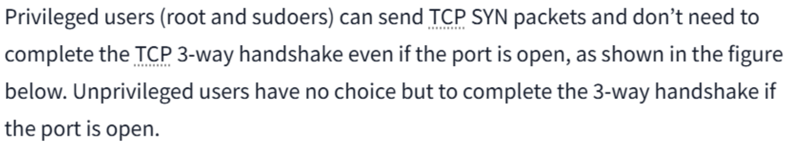
Q1 and Q2



TCP ACK Ping

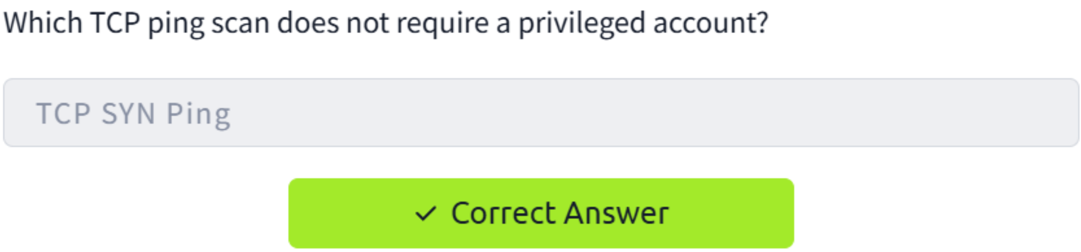
As you have guessed, this sends a packet with an ACK flag set. You must be running Nmap as a privileged user to be able to accomplish this. If you try it as an unprivileged user, Nmap will attempt a 3-way handshake.

Figure 1: TCP ACK



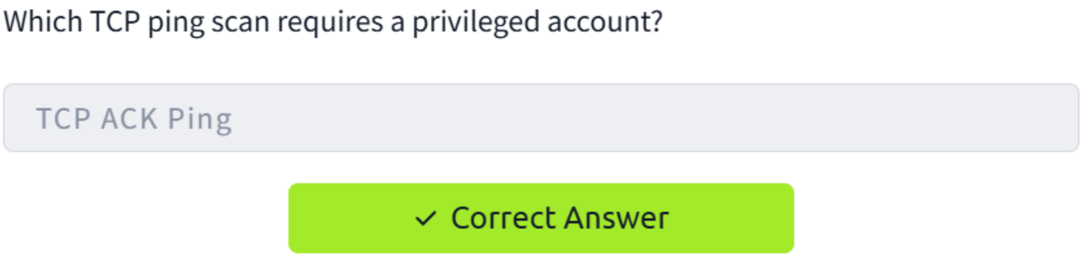
Privileged users (root and sudoers) can send TCP SYN packets and don't need to complete the TCP 3-way handshake even if the port is open, as shown in the figure below. Unprivileged users have no choice but to complete the 3-way handshake if the port is open.

Figure 2: TCP SYN



Which TCP ping scan does not require a privileged account?

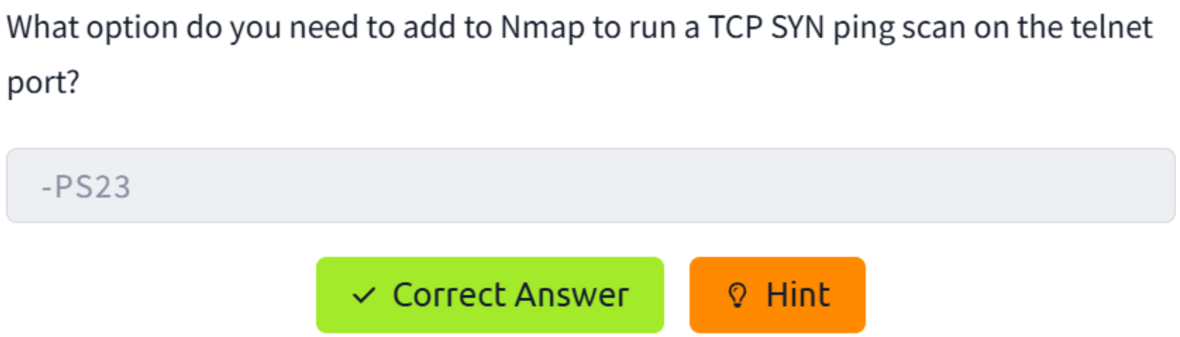
TCP SYN Ping



Which TCP ping scan requires a privileged account?

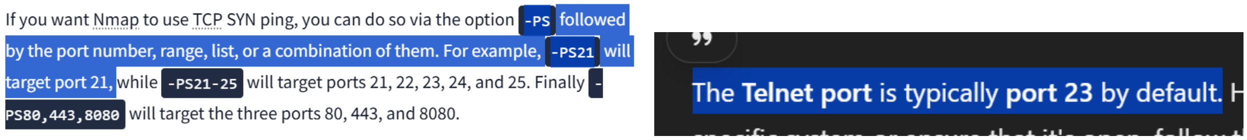
TCP ACK Ping

Q3



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

-PS23



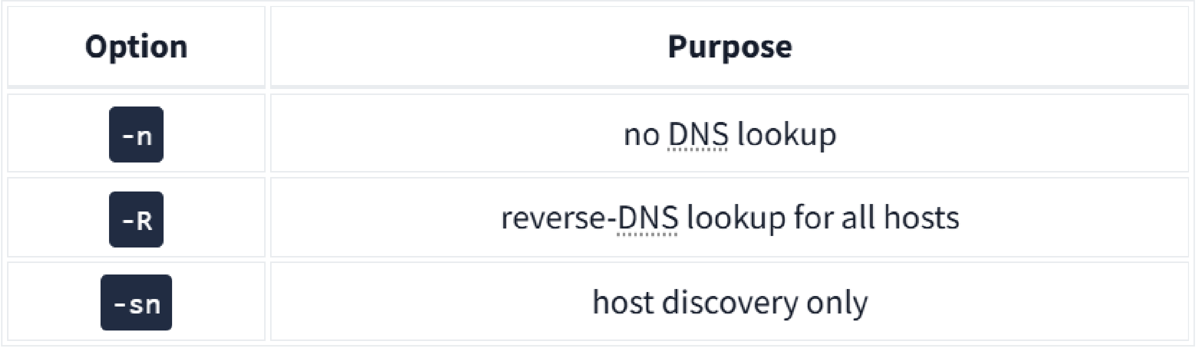
If you want Nmap to use TCP SYN ping, you can do so via the option `-PS` followed by the port number, range, list, or a combination of them. For example, `-PS21` will target port 21, while `-PS21-25` will target ports 21, 22, 23, 24, and 25. Finally `-PS80,443,8080` will target the three ports 80, 443, and 8080.

The **Telnet port** is typically **port 23** by default. H

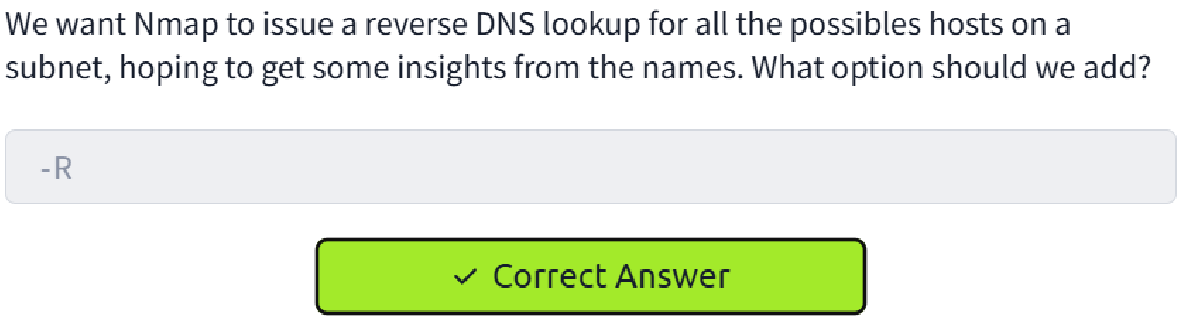
Figure 3: ChatGPT and lab content

Task 8

Q1



Option	Purpose
`-n`	no DNS lookup
`-R`	reverse-DNS lookup for all hosts
`-sn`	host discovery only



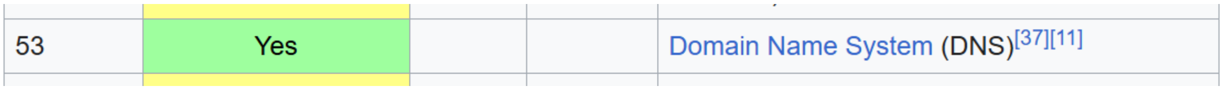
We want Nmap to issue a reverse DNS lookup for all the possibles hosts on a subnet, hoping to get some insights from the names. What option should we add?

-R

Room: Nmap Basic Port Scans

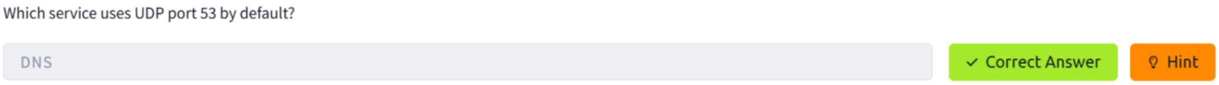
Task 2

Q1



53	Yes			Domain Name System (DNS)[37][11]

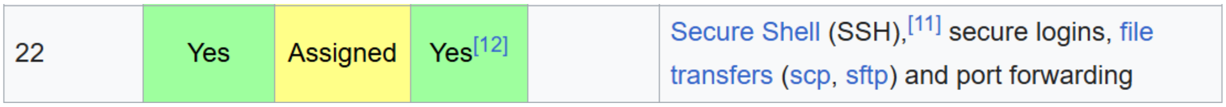
Figure 4: Wikipedia "List of TCP and UDP port numbers"



Which service uses UDP port 53 by default?

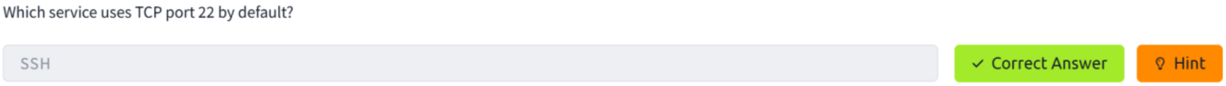
DNS

Q2



22	Yes	Assigned	Yes[12]		Secure Shell (SSH),[11] secure logins, file transfers (scp, sftp) and port forwarding

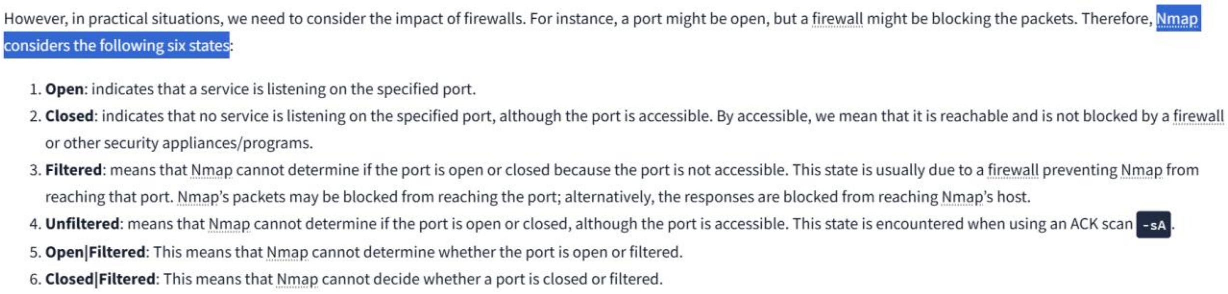
Figure 5: Wikipedia "List of TCP and UDP port numbers"



Which service uses TCP port 22 by default?

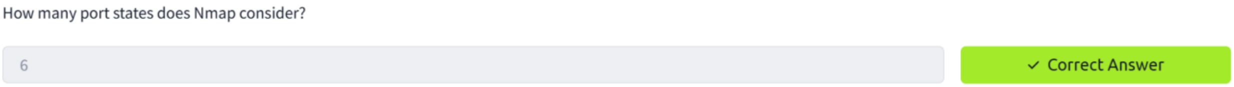
SSH

Q3



However, in practical situations, we need to consider the impact of firewalls. For instance, a port might be open, but a firewall might be blocking the packets. Therefore, Nmap considers the following six states:

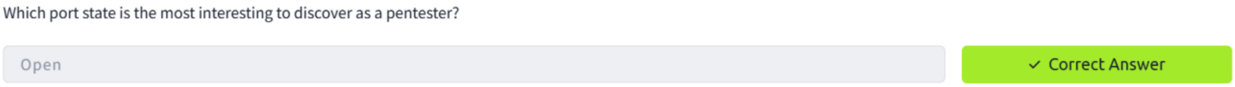
1. **Open**: indicates that a service is listening on the specified port.
2. **Closed**: indicates that no service is listening on the specified port, although the port is accessible. By accessible, we mean that it is reachable and is not blocked by a firewall or other security appliances/programs.
3. **Filtered**: means that Nmap cannot determine if the port is open or closed because the port is not accessible. This state is usually due to a firewall preventing Nmap from reaching that port. Nmap's packets may be blocked from reaching the port; alternatively, the responses are blocked from reaching Nmap's host.
4. **Unfiltered**: means that Nmap cannot determine if the port is open or closed, although the port is accessible. This state is encountered when using an ACK scan `-sA`.
5. **Open|Filtered**: This means that Nmap cannot determine whether the port is open or filtered.
6. **Closed|Filtered**: This means that Nmap cannot decide whether a port is closed or filtered.



How many port states does Nmap consider?

6

Q4

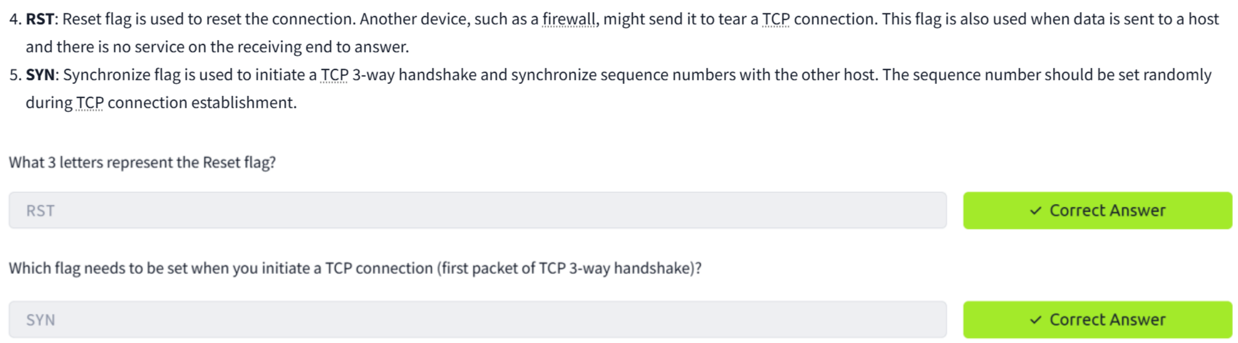


Which port state is the most interesting to discover as a pentester?

Open

Task 3

Q1 and Q2



4. **RST**: Reset flag is used to reset the connection. Another device, such as a firewall, might send it to tear a TCP connection. This flag is also used when data is sent to a host and there is no service on the receiving end to answer.
5. **SYN**: Synchronize flag is used to initiate a TCP 3-way handshake and synchronize sequence numbers with the other host. The sequence number should be set randomly during TCP connection establishment.

What 3 letters represent the Reset flag?

RST

✓ Correct Answer

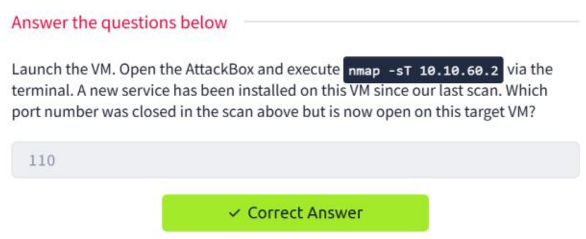
Which flag needs to be set when you initiate a TCP connection (first packet of TCP 3-way handshake)?

SYN

✓ Correct Answer

Task 4

Q1

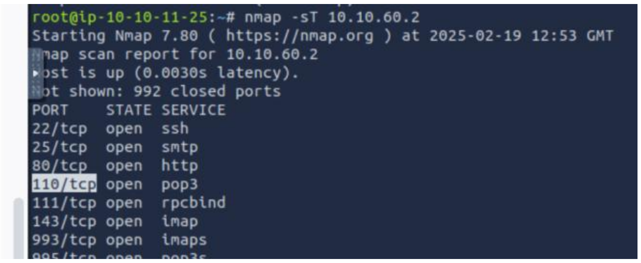


Answer the questions below

Launch the VM. Open the AttackBox and execute `nmap -sT 10.10.60.2` via the terminal. A new service has been installed on this VM since our last scan. Which port number was closed in the scan above but is now open on this target VM?

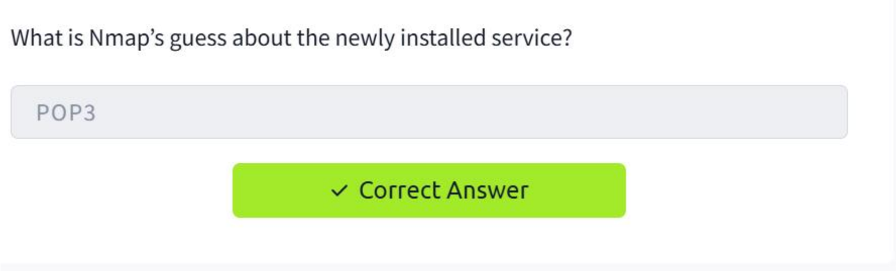
110

✓ Correct Answer



```
root@ip-10-10-11-25:~# nmap -sT 10.10.60.2
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 12:53 GMT
map scan report for 10.10.60.2
ost is up (0.0030s latency).
ot shown: 992 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
993/tcp open  imaps
995/tcp open  pop3s
```

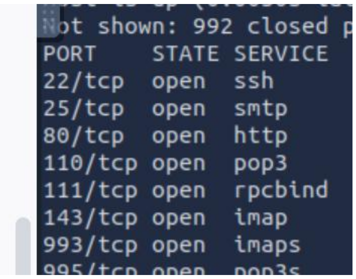
Q2



What is Nmap's guess about the newly installed service?

POP3

✓ Correct Answer

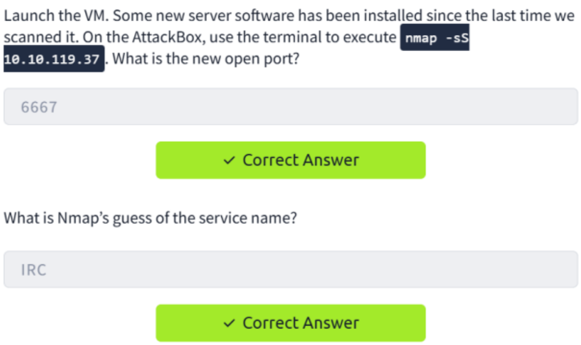


```
ot shown: 992 closed p
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
993/tcp open  imaps
995/tcp open  pop3s
```

Note: actually there was 3 new ports.

Task 5

Q1 and Q2



Launch the VM. Some new server software has been installed since the last time we scanned it. On the AttackBox, use the terminal to execute `nmap -sS 10.10.119.37`. What is the new open port?

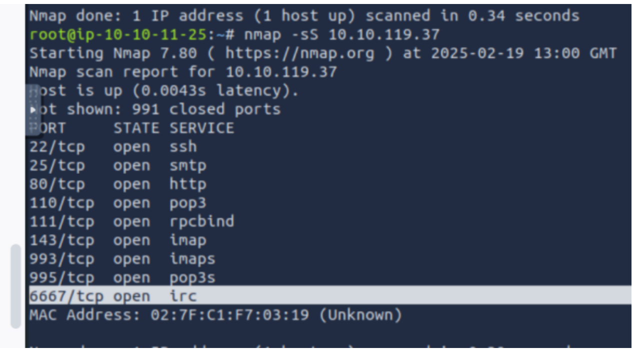
6667

✓ Correct Answer

What is Nmap's guess of the service name?

IRC

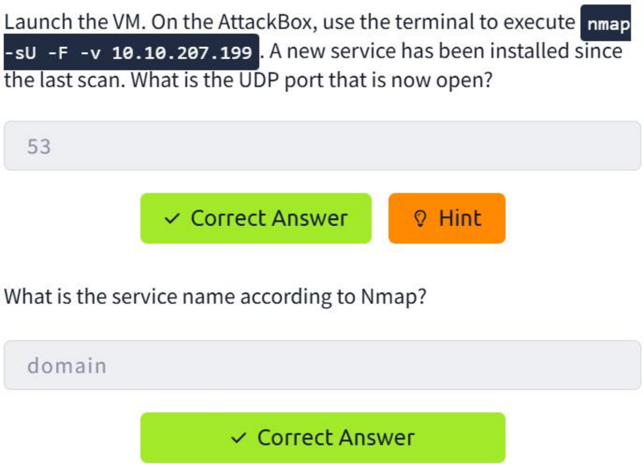
✓ Correct Answer



```
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
root@ip-10-10-11-25:~# nmap -sS 10.10.119.37
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 13:00 GMT
Nmap scan report for 10.10.119.37
Host is up (0.0043s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
993/tcp  open  imaps
995/tcp  open  pop3s
6667/tcp open  irc
MAC Address: 02:7F:C1:F7:03:19 (Unknown)
```

Task 6

Q1 and Q2



Launch the VM. On the AttackBox, use the terminal to execute `nmap -sU -F -v 10.10.207.199`. A new service has been installed since the last scan. What is the UDP port that is now open?

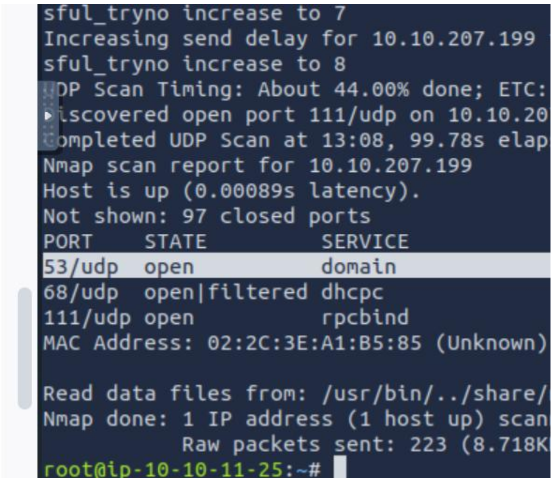
53

✓ Correct Answer 💡 Hint

What is the service name according to Nmap?

domain

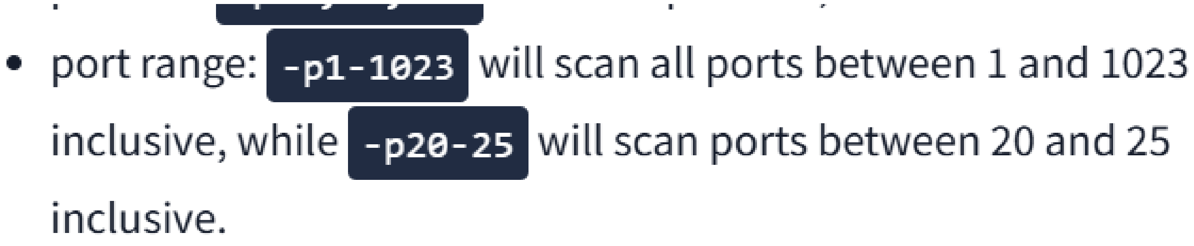
✓ Correct Answer



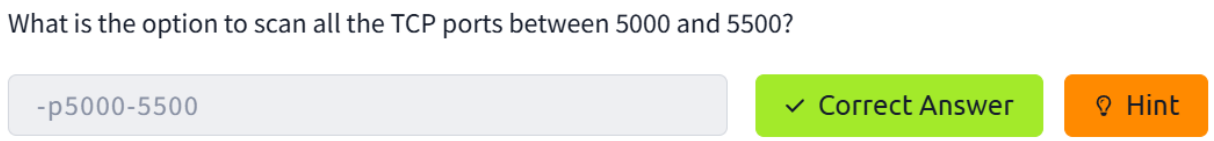
```
sful_tryno increase to 7
Increasing send delay for 10.10.207.199
sful_tryno increase to 8
UDP Scan Timing: About 44.00% done; ETC:
Discovered open port 111/udp on 10.10.20
Completed UDP Scan at 13:08, 99.78s elap
Nmap scan report for 10.10.207.199
Host is up (0.00089s latency).
Not shown: 97 closed ports
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
111/udp  open          rpcbind
MAC Address: 02:2C:3E:A1:B5:85 (Unknown)

Read data files from: /usr/bin/../share/
Nmap done: 1 IP address (1 host up) scan
           Raw packets sent: 223 (8.718K
root@ip-10-10-11-25:~#
```

Task 7

Q1



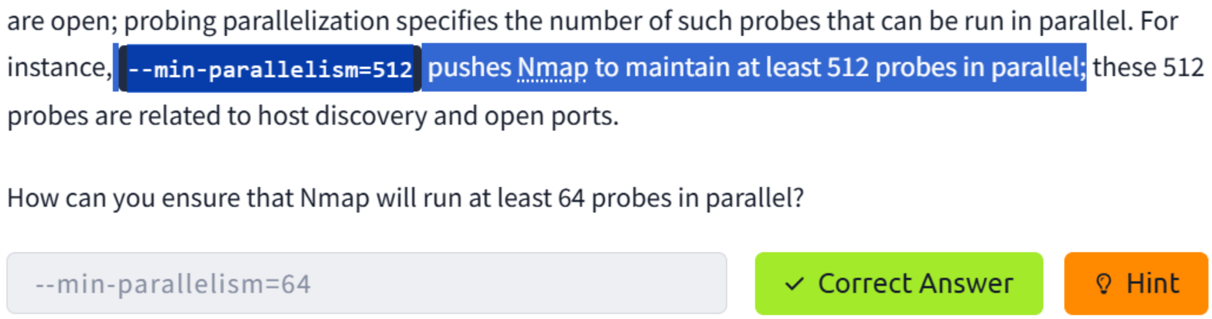
- port range: `-p1-1023` will scan all ports between 1 and 1023 inclusive, while `-p20-25` will scan ports between 20 and 25 inclusive.



What is the option to scan all the TCP ports between 5000 and 5500?

-p5000-5500

Q2

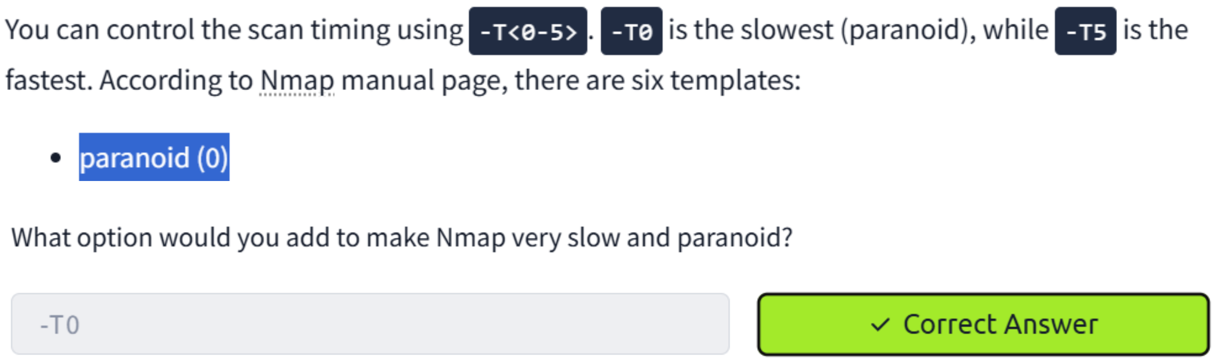


are open; probing parallelization specifies the number of such probes that can be run in parallel. For instance, `--min-parallelism=512` pushes Nmap to maintain at least 512 probes in parallel; these 512 probes are related to host discovery and open ports.

How can you ensure that Nmap will run at least 64 probes in parallel?

--min-parallelism=64

Q3



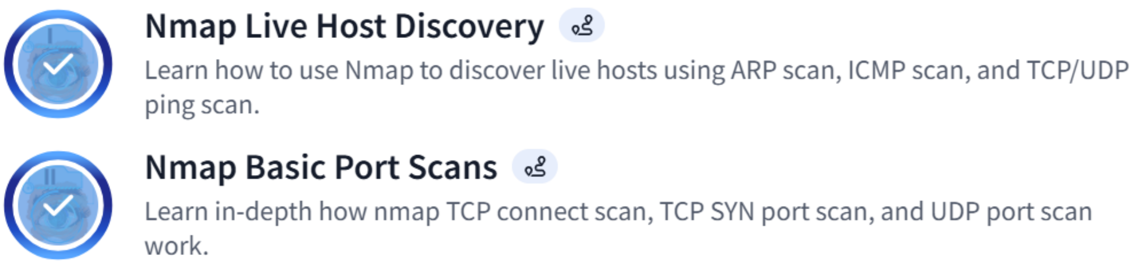
You can control the scan timing using `-T<0-5>`. `-T0` is the slowest (paranoid), while `-T5` is the fastest. According to Nmap manual page, there are six templates:

- paranoid (0)

What option would you add to make Nmap very slow and paranoid?

-T0

Rooms Completed!



Nmap Live Host Discovery

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

Nmap Basic Port Scans

Learn in-depth how nmap TCP connect scan, TCP SYN port scan, and UDP port scan work.

Resources:

1- https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers