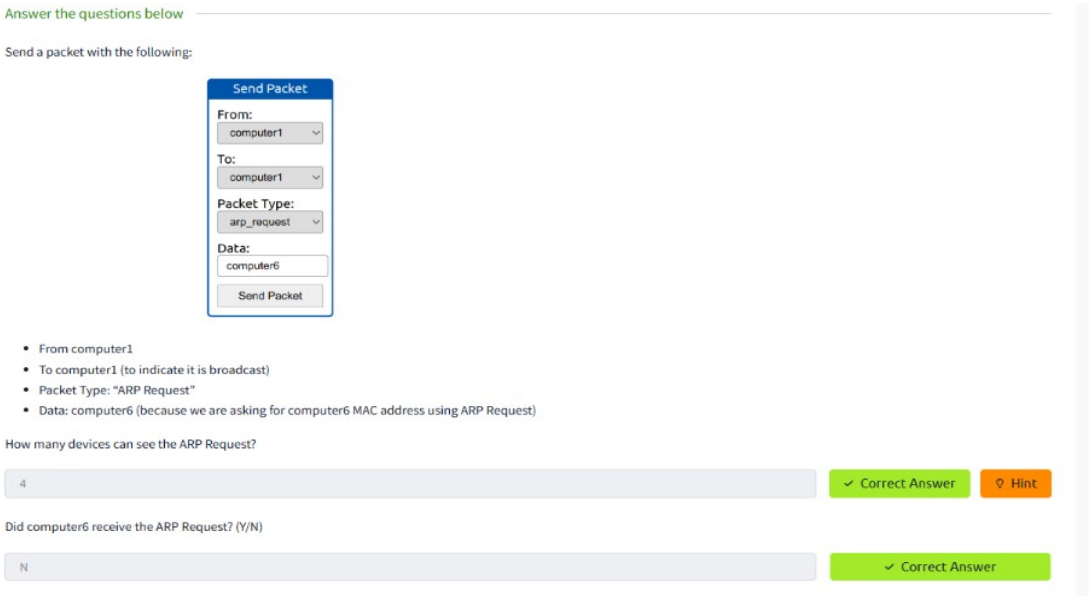
S.Balamurugan
241901014

EXPT: 7 NMAP TO DISCOVER LIVE HOSTS USING ARP SCAN AND TCP/UDP PING SCAN

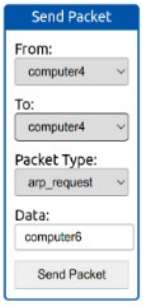
Aim:

• Perform an ARP scan to find active devices on the local network.
• Use ICMP (ping) scanning to identify machines that respond to echo requests.
• Capture both ARP and ICMP packets using tcpdump to verify the scan traffic.
• Compare the results and understand why certain hosts may respond to one scan type but not the other.

Tasks:



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

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

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?

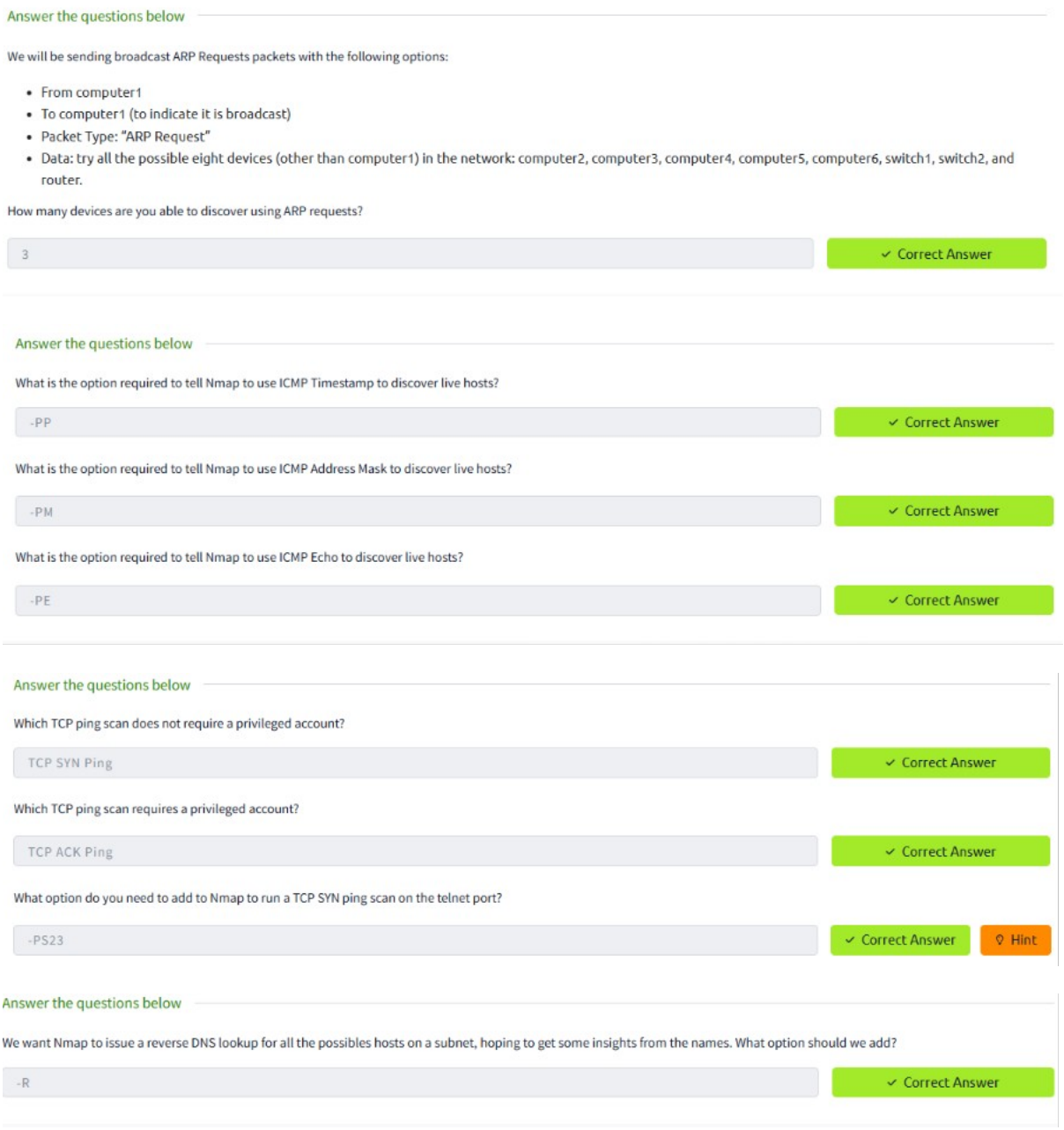
router ✓ Correct Answer

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



Result:

ARP and ICMP scans were run on the local network. ARP identified all active hosts, while ICMP only showed devices that replied to pings. `tcpdump` captured the corresponding ARP and ICMP packets, helping verify the scans. Some hosts appeared in ARP but not ICMP due to ping being blocked or disabled.