

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:

Answer the questions below

Send a packet with the following:

Send Packet

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: 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

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

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?

✓ Correct Answer

Answer the questions below

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

✓ Correct Answer

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

✓ Correct Answer

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

✓ Correct Answer

Answer the questions below

Which TCP ping scan does not require a privileged account?

✓ Correct Answer

Which TCP ping scan requires a privileged account?

✓ Correct Answer

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

✓ Correct Answer

💡 Hint

Answer the questions below

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

✓ 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.