

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

Aim :

- Use ARP scanning to detect live hosts on the local subnet.
- Use ICMP (ping) scanning to discover hosts that reply to echo requests.
- Use tcpdump to capture and inspect the probe and reply packets for verification.
- Compare results and explain why a host may appear in one scan but not another.

Tasks in TryHackMe :

Answer the questions below

Send a packet with the following:

The dialog box has the following fields:

- From: computer1
- To: computer1 (indicated by a dropdown arrow)
- Packet Type: arp_request
- Data: computer6
- Send Packet button

- 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?

✓ Correct Answer
✗ Hint

Did computer6 receive the ARP Request? (Y/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

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

✓ 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?

✓ Correct Answer

✗ Hint

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

✓ 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?

✓ Correct Answer

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

✓ Correct Answer

How many computers responded to the ping request?

✓ 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?

✓ Correct Answer

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

✓ Correct Answer

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

Ran an ARP scan on the local network (e.g. arp-scan or nmap -PR) and noted responsive IPs/MACs.