NAME:THULASI.S EXPERIMENT:7

ROLL:NO:241901118 DATE:15/9/25

NMAP TO DISCOVER LIVE HOSTS USING ARP/ICMP/TCP/UDP/PING SCAN

AIM:

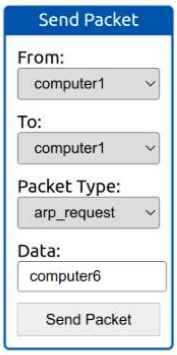
To perform nmap to discover live hosts using ARP/ICMP/TCP/UDP/PING SCAN.

TASK 1: INTRODUCTION

In this module we focus on discovering live hosts on a network using Nmap.Finding which systems are in online is crucial before scanning ports or services to save time and avoid unnecessary network traffic.This forms the foundation for effective network mapping and security auditing.

TASK 2: SUBNETWORKS

Send a packet with the following:



- 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)

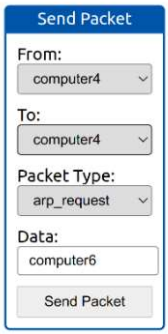
How many devices can see the ARP Request?

4 ✓ Correct Answer Hint

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

N ✓ Correct Answer

Send a packet with the following:



- 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

TASK 3: ENUMERATING TARGETS

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

TASK 4: DISCOVERING LIVE HOSTS

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

TASK 5: NMAP HOST DISCOVERY USING ARP

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

TASK 6: NMAP HOST DISCOVERY USING ICMP

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

-PP ✓ Correct Answer

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

-PM ✓ Correct Answer

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

-PE ✓ Correct Answer

TASK 7: NMAP HOST DISCOVERY USING TCP/UDP

Answer the questions below

Which TCP ping scan does not require a privileged account?

TCP SYN Ping ✓ Correct Answer

Which TCP ping scan requires a privileged account?

TCP ACK Ping ✓ Correct Answer

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

RESULT:

Thus,the Nmap using to discoverf live hosts using ARP,ICMP,TCP,UDP have been done successfully.