

## Aim

To efficiently identify which computers are online in a target network using Nmap's host discovery techniques.

## Introduction

Live host discovery is the crucial first step in network scanning. Nmap can find active systems using techniques like ARP scan, ICMP scan, and TCP/UDP ping scan. This process helps avoid wasting time on offline systems and reduces network noise.

## ALGORITHM

- Use Nmap with ARP, ICMP, TCP, or UDP scans to detect live hosts.
- Example commands:
  - ARP: nmap -sn -PR <subnet>
  - ICMP: nmap -sn -PE <subnet>
  - TCP Ping: nmap -sn -PS22,80,443 <range>
- Review scan output to see which systems are up before proceeding with deeper

## OUTPUT

Task 2 ✓ Subnetworks

Answer the questions below

Send a packet with the following:

Send Packet

From: computer1

To: computer1

Packet Type: arp\_request

Data: 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)

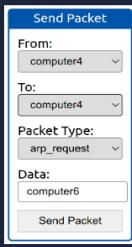
How many devices can see the ARP Request?

4 ✓ 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?

✓ Correct Answer

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

✓ Correct Answer

### Task 3 Enumerating Targets

We mentioned the different *techniques* we can use for scanning in Task 1. Before we explain each in detail and put it into use against a live target, we need to specify the targets we want to scan. Generally speaking, you can provide a list, a range, or a subnet. Examples of target specification are:

- list: `MACHINE_IP scanme.nmap.org example.com` will scan 3 IP addresses.
- range: `10.11.12.15-20` will scan 6 IP addresses: `10.11.12.15`, `10.11.12.16` ... and `10.11.12.20`.
- subnet: `MACHINE_IP/30` will scan 4 IP addresses.

You can also provide a file as input for your list of targets, `nmap -l list_of_hosts.txt`.

If you want to check the list of hosts that Nmap will scan, you can use `nmap -SL TARGETS`. This option will give you a detailed list of the hosts that Nmap will scan without scanning them; however, Nmap will attempt a reverse-DNS resolution on all the targets to obtain their names. Names might reveal various information to the pentester. (If you don't want Nmap to do the DNS server, you can add `-n`.)

Launch the AttackBox using the Start AttackBox button, open the terminal when the AttackBox is ready, and use Nmap to answer the following.

**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

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

✓ Correct Answer

### Task 4 Discovering Live Hosts

Let's revisit the TCP/IP layers shown in the figure next. We will leverage the protocols to discover the live hosts. Starting from bottom to top, we can use:

- ARP from Link Layer
- ICMP from Network Layer
- TCP from Transport Layer
- UDP from Transport Layer

ISO/OSI	TCP/IP		
7 Application Layer	Application Layer		HTTP, HTTPS, SMTP, POP3, IMAP, SSH, FTP, SNMP, Telnet, RDP,...
6 Presentation Layer			
5 Session Layer	Transport Layer		TCP, UDP
4 Transport Layer			
3 Network Layer	Network Layer		IPv4, IPv6, ICMP, IPsec
2 Data Link Layer			
1 Physical Layer	Link Layer		ARP, Ethernet (802.3), WiFi (802.11), DSL, Bluetooth,

#### Answer the questions below

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

### Task 5 Nmap Host Discovery Using ARP

#### 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?

3

✓ Correct Answer

### Task 6 Nmap Host Discovery Using ICMP

#### Answer the questions below

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 and 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

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

-PS23 ✓ Correct Answer 💡 Hint

**Task 8** ✓ Using Reverse-DNS Lookup

Nmap's default behaviour is to use reverse-DNS online hosts. Because the hostnames can reveal a lot, this can be a helpful step. However, if you don't want to send such DNS queries, you use `-n` to skip this step.

By default, Nmap will look up online hosts; however, you can use the option `-R` to query the DNS server even for offline hosts. If you want to use a specific DNS server, you can add the `-dns-servers DNS_SERVER` option.

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?

`-R` ✓ Correct Answer

**Result:**

Thus we completed and understand how Nmap Live Host Discovery used and how it helps us .