Practical-8

AIM: - To Discover Live Hosts Using Nmap Scans (ARP, ICMP, TCP/UDP) on the TryHackMe Platform Room Link :https://tryhackme.com/room/nmap01

Introduction

When targeting a network, we need an efficient tool to handle repetitive tasks. This tool should help us find out which systems are active and what services are running on those systems. The tool that we will rely on is Nmap. The first question about finding live computers is answered in this room. This room is the first in a series of four rooms dedicated to Nmap. The second question about discovering running services is answered in the next Nmap rooms that focus on port-scanning.

This room is the first of four in this Nmap series. These four rooms are also part of the Network Security module.

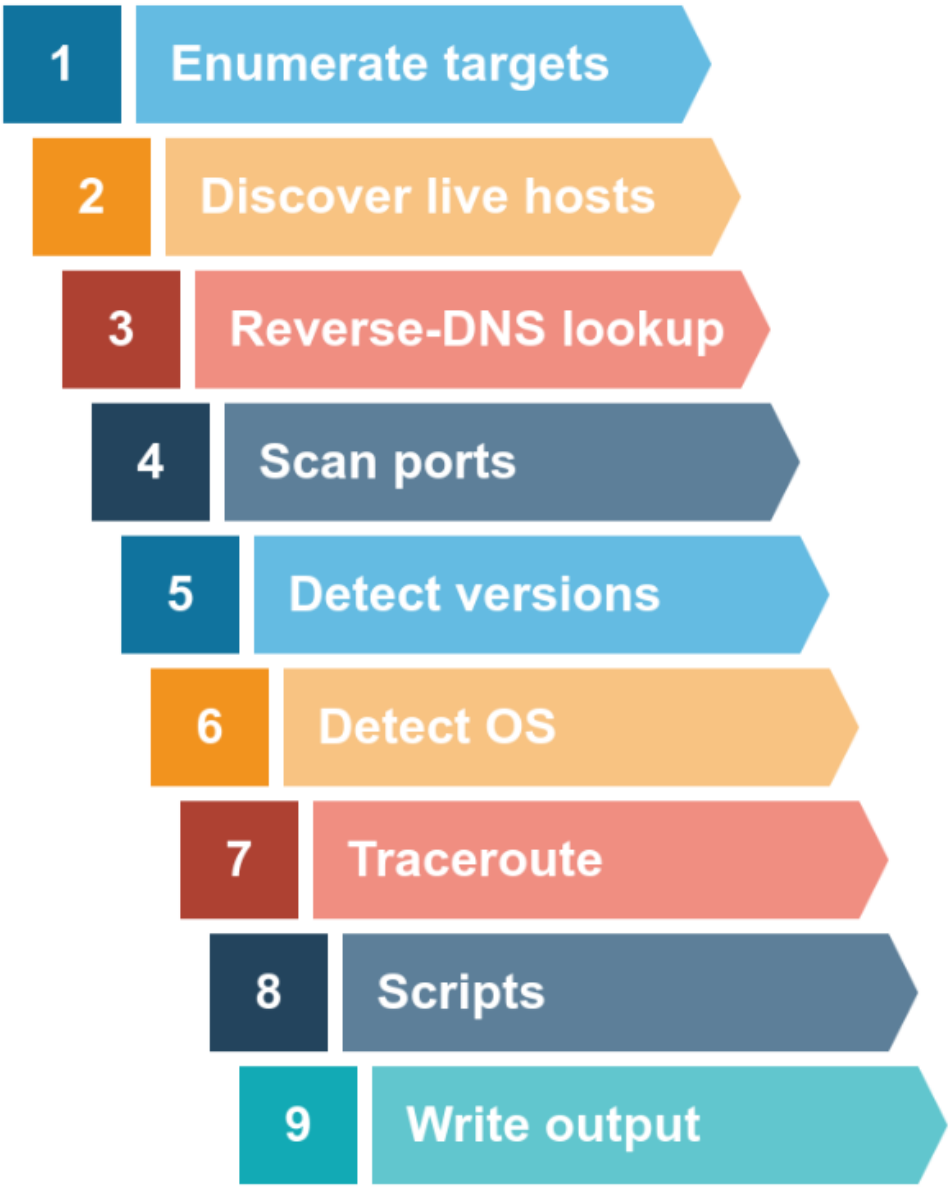
- Nmap Live Host Discovery
- Nmap Basic Port Scans
- Nmap Advanced Port Scans
- Nmap Post Port Scans

This room explains the steps that Nmap carries out to discover the systems that are online before port-scanning. This stage is crucial because trying to port-scan offline systems will only waste time and create unnecessary noise on the network.

We present the different approaches that Nmap uses to discover live hosts. In particular, we cover:
ARP scan: This scan uses ARP requests to discover live hosts
ICMP scan: This scan uses ICMP requests to identify live hosts
TCP/UDP ping scan: This scan sends packets to TCP ports and UDP ports to determine live hosts.

We also introduce two scanners, arp-scan and masscan, and explain how they overlap with part of Nmap's host discovery.

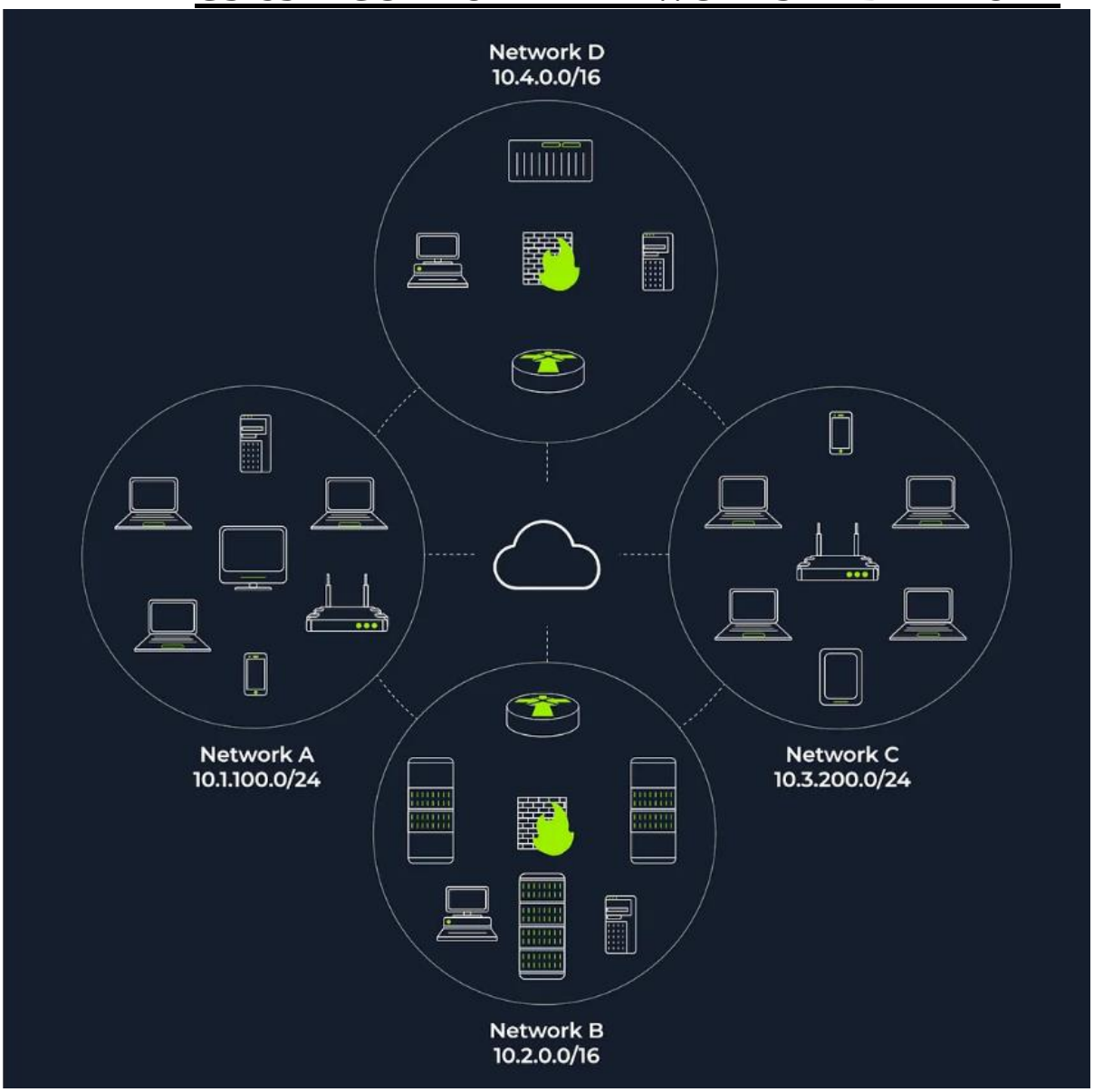
As already mentioned, starting with this room, we will use Nmap to discover systems and services actively. Nmap was created by Gordon Lyon (Fyodor), a network security expert and open source programmer. It was released in 1997. Nmap, short for Network Mapper, is free, open-source software released under GPL license. Nmap is an industry-standard tool for mapping networks, identifying live hosts, and discovering running services. Nmap's scripting engine can further extend its functionality, from fingerprinting services to exploiting vulnerabilities. A Nmap scan usually goes through the steps shown in the figure below, although many are optional and depend on the command-line arguments you provide.



Subnetworks

A network segment is a group of computers linked through a shared medium, like an Ethernet switch or WiFi access point. In IP networks, a subnetwork typically consists of one or more network segments connected together and configured to use the same router. A network segment is a physical connection, while a subnetwork is a logical connection.

In the provided network diagram, there are four network segments or subnetworks. Your system would usually connect to one of these segments/subnetworks. Each subnet has its own IP address range and is connected to a larger network through a router. Depending on the network, there might be a firewall enforcing security policies.

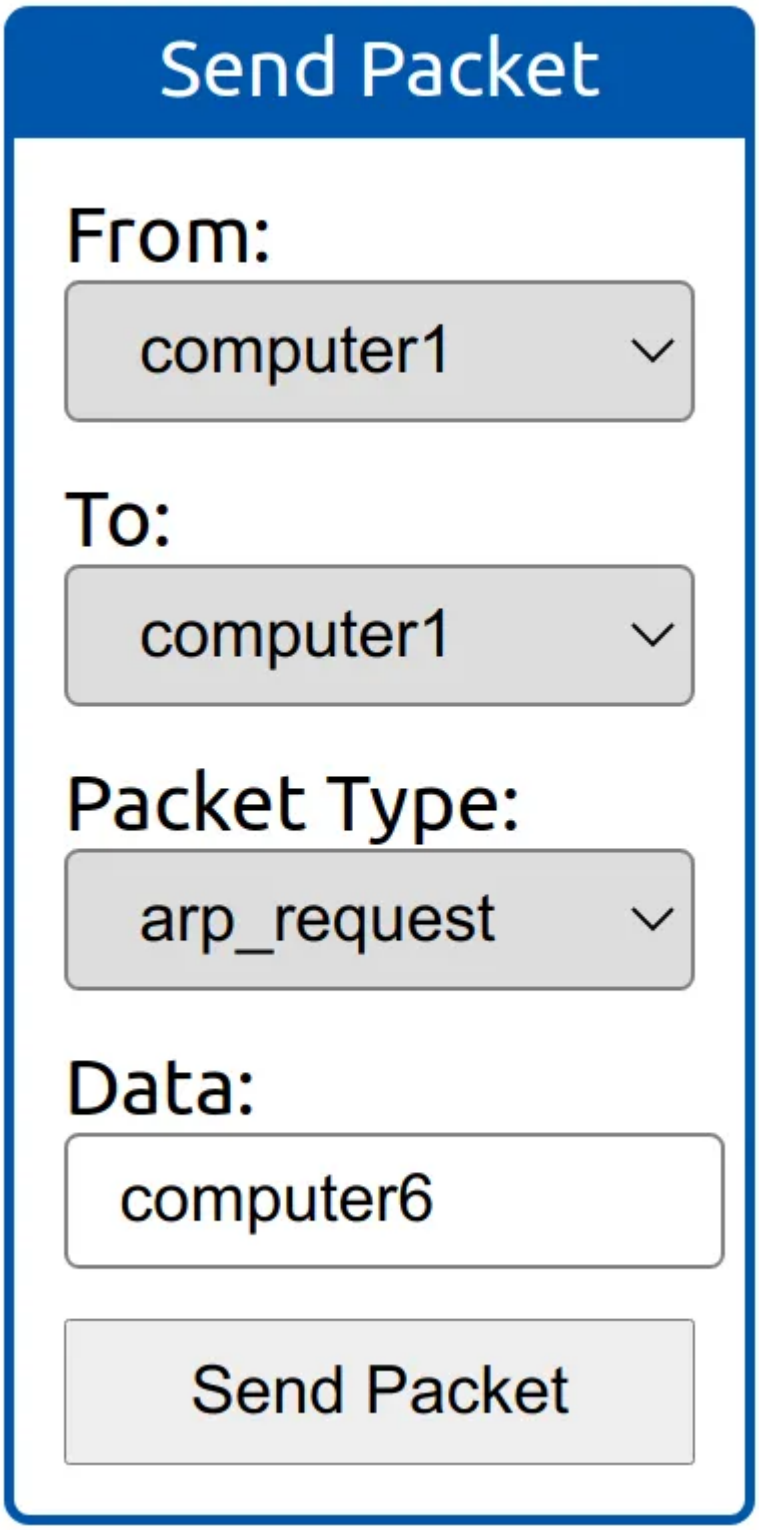


The figure displays two types of subnets:

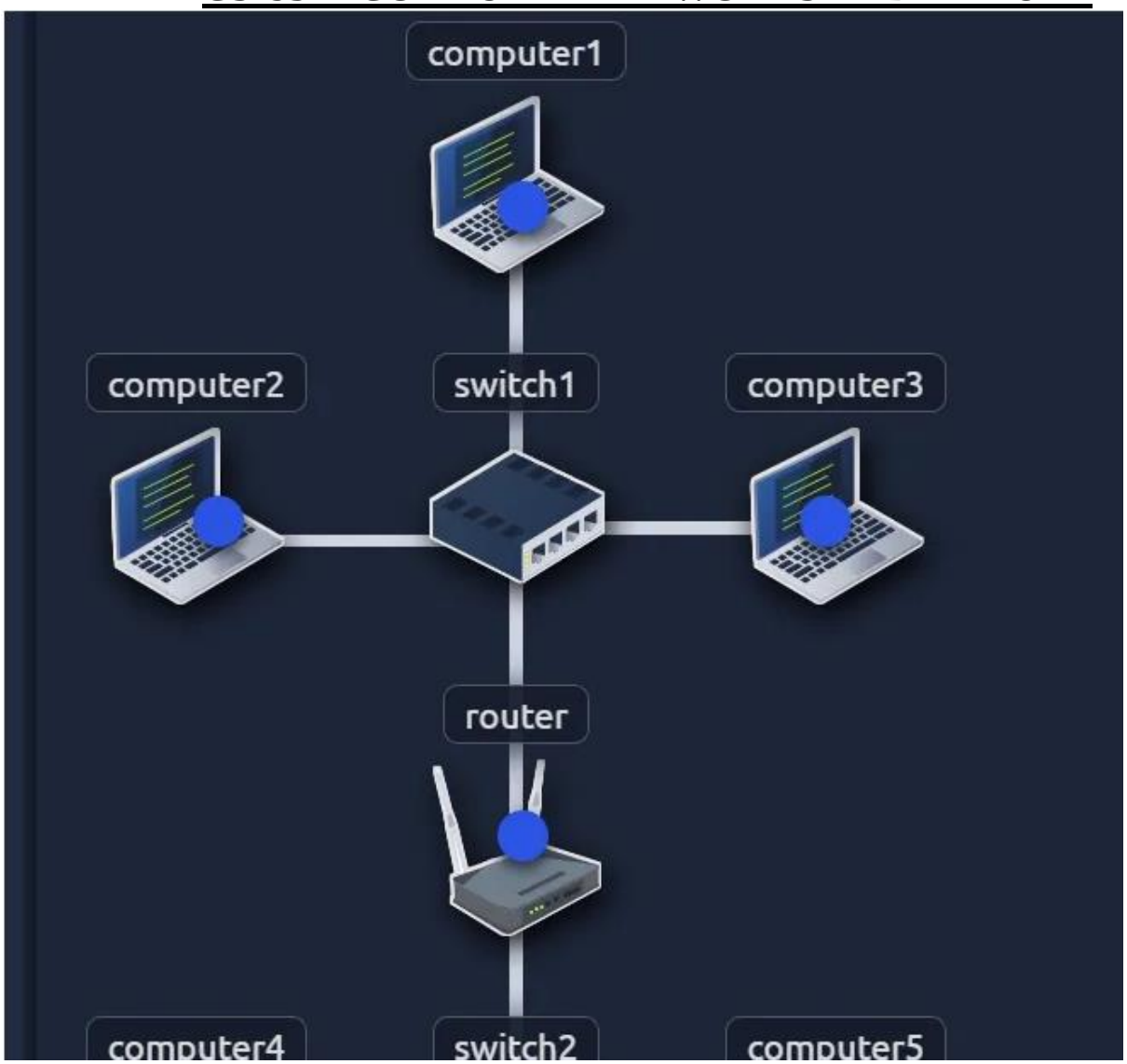
/16 Subnets: These have a subnet mask of 255.255.0.0 and can accommodate approximately 65 thousand hosts.

/24 Subnets: These feature a subnet mask of 255.255.255.0 and can support around 250 hosts.

In active reconnaissance, when attempting to gather information about a group of hosts or a subnet, if you're on the same subnet, your scanner relies on ARP (Address Resolution Protocol) queries to find live hosts. ARP queries seek to obtain the MAC address, enabling link-layer communication, which implies the host is online. However, ARP can only discover devices within the same subnet. If you're on a different subnet from the target, your scanner's packets will be routed through the default gateway, but ARP queries cannot cross subnet routers since ARP packets are tied to their specific subnet due to being a link-layer protocol.



- 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)

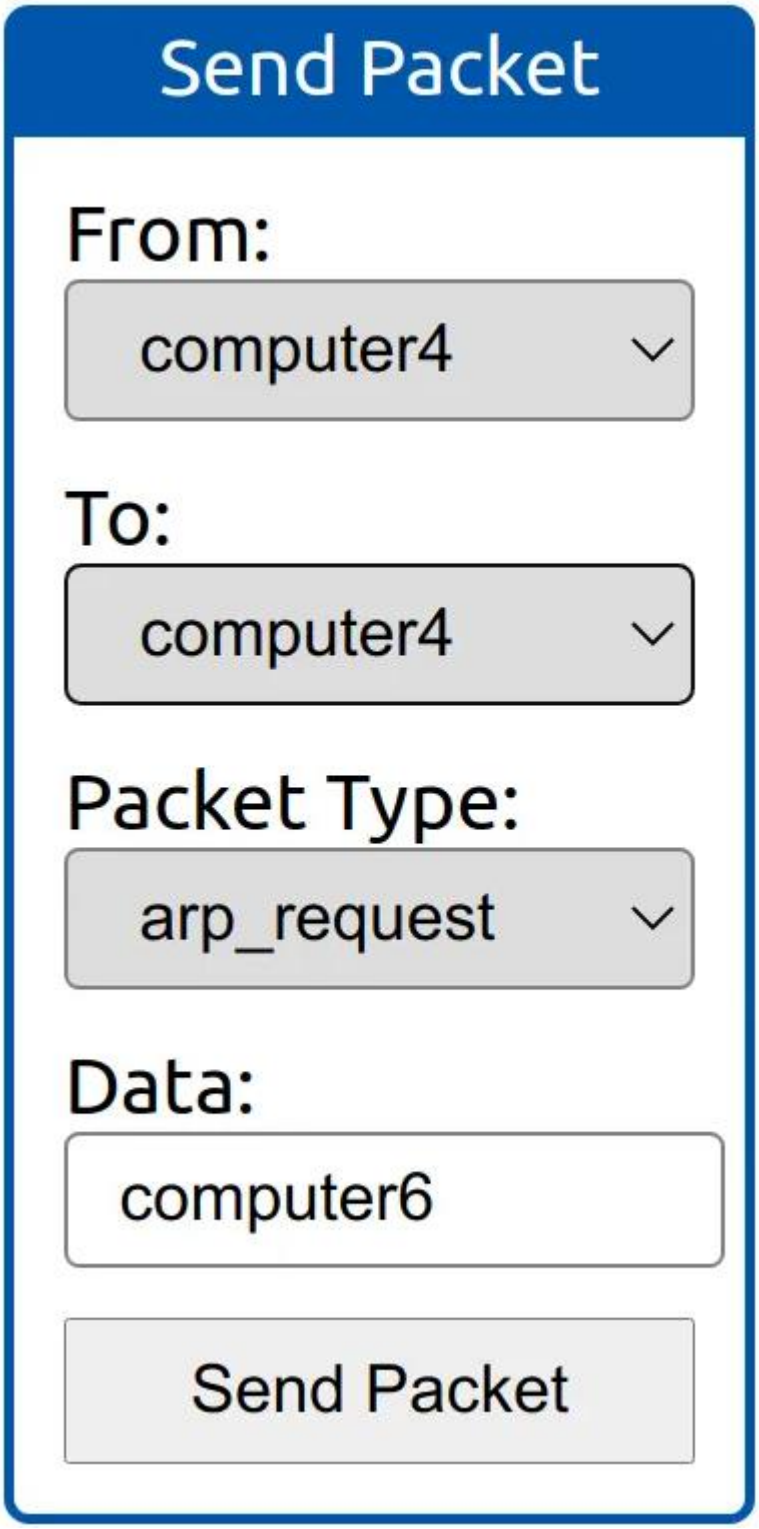


How many devices can see the ARP Request?

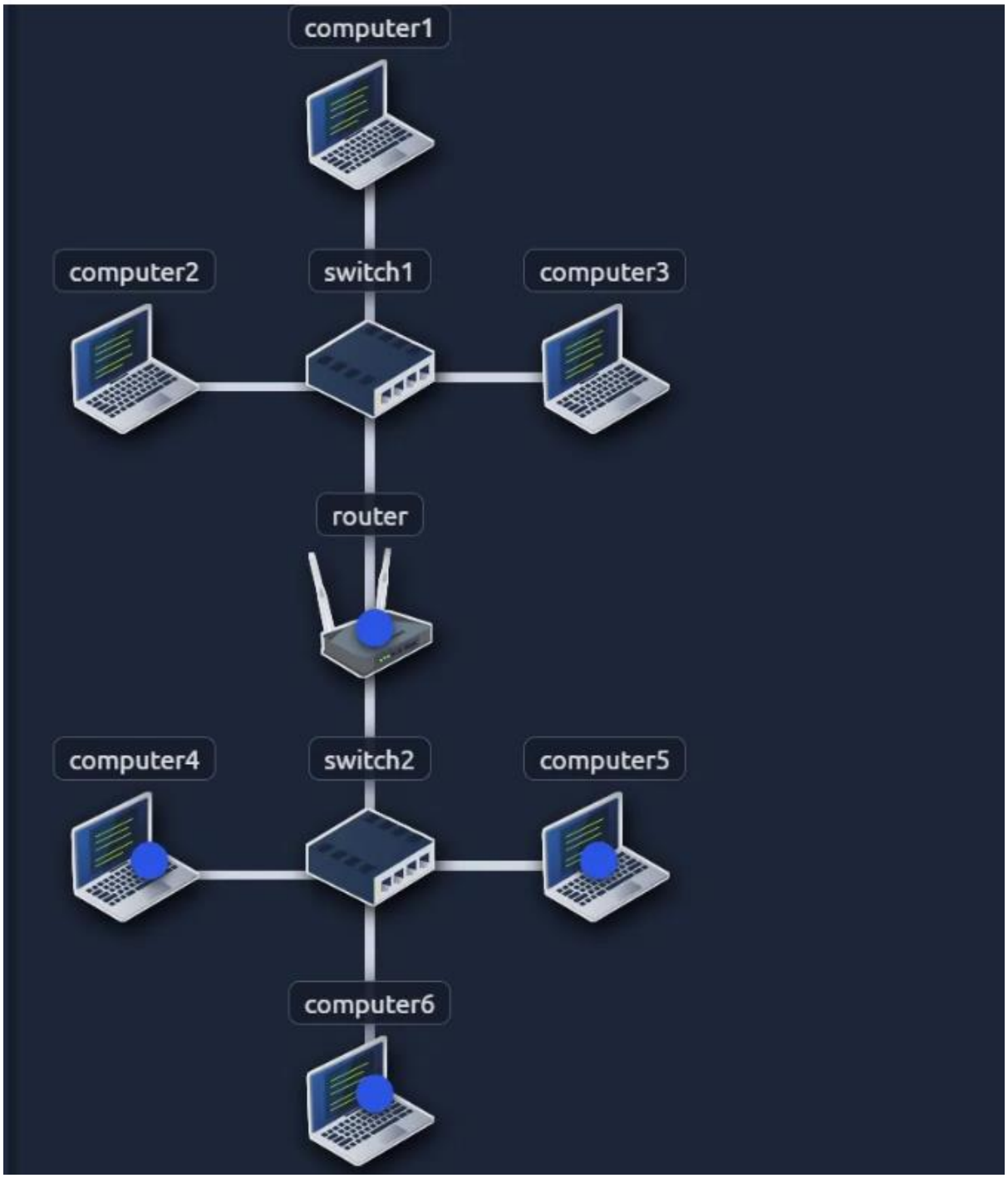
4

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

N



- 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

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

Y

Enumerating Targets

Before delving into the details of scanning techniques, it's essential to define the targets we want to scan. Targets can be specified in three ways:

1. List: You can provide a list of specific IP addresses or hostnames, like "MACHINE_IP," "scanme.nmap.org," and "example.com," which would result in scanning 3 IP addresses.
2. Range: You can specify a range, such as "10.11.12.15–20," which will scan 6 IP addresses: 10.11.12.15, 10.11.12.16, and so on, up to 10.11.12.20.

3. Subnet: You can define a subnet like "MACHINE_IP/30," which will scan 4 IP addresses within that subnet.

Nmap allows you to input a list of targets from a file using "nmap -iL list_of_hosts.txt." You can also preview the list of hosts that Nmap intends to scan by using "nmap -sL TARGETS," which provides a detailed list without actually scanning them. However, Nmap will attempt reverse-DNS resolution to obtain host names, potentially revealing valuable information to the pentester. To prevent DNS resolution, you can add the "-n" flag.

What is the first IP address Nmap would scan if you provided 10.10.12.13/29 as your target?

=>/29= 8 address,

=> 10.10.12.[0–7][8–15]

=>10.10.12.8

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

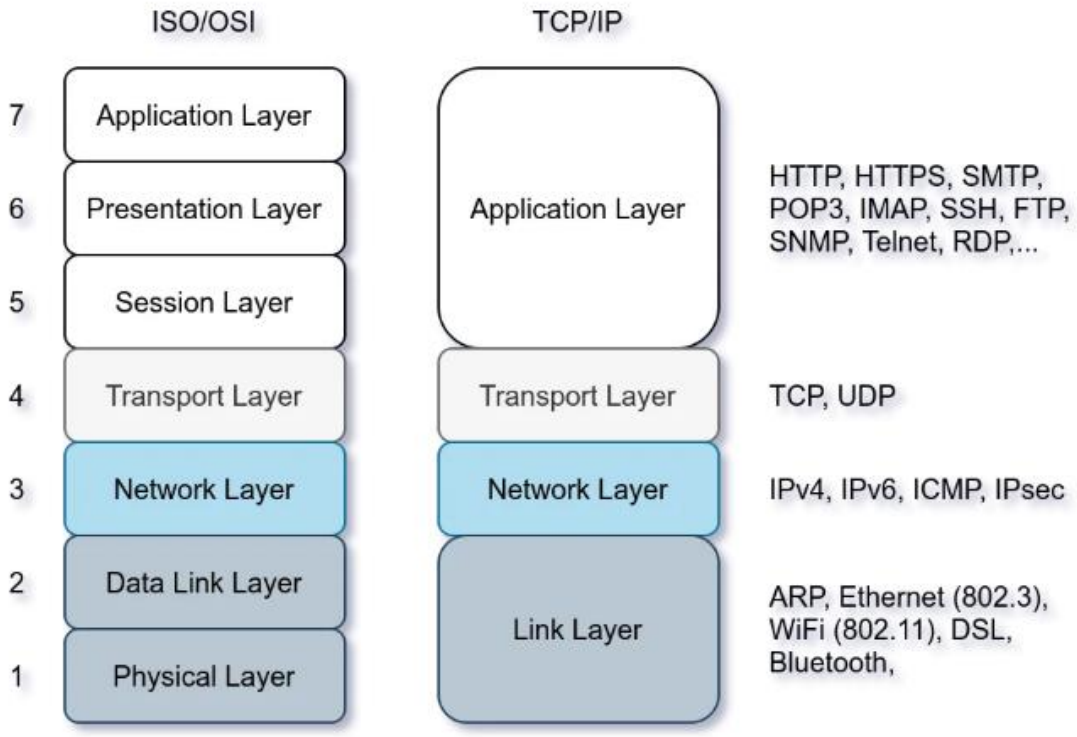
*=> 255*25*

=>6400

Discvoering Live hosts

TCP/IP layers:

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



This passage discusses four network protocols: ARP, ICMP, TCP, and UDP, and their roles in network scanning. ARP is used to request a computer's MAC address with a specific IP address. ICMP has various types, including ping (Type 8 and Type 0). When pinging a system on the same subnet, an ARP query should be sent before ICMP Echo. Additionally, network scanners can use specially-crafted packets to common TCP or UDP ports for efficient target response checking, especially when ICMP Echo is blocked.

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
What is the type of packet that computer1 received before being able to send the ping?
ARP Response
How many computers responded to the ping request?
1
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
What is the name of the first device that responded to the second ARP Request?
computer5
Send another Ping Request. Did it require new ARP Requests? (Y/N)
N
NMAP Host Discovery Using ARP

How can we determine which hosts are operational? It’s crucial to prevent unnecessary port scanning on hosts that are offline or not in use. There are several methods to identify active hosts. When no specific host discovery options are specified, Nmap employs the following strategies to find live hosts:

When a privileged user tries to scan targets on a local network (Ethernet), Nmap uses ARP requests. A privileged user is root or a user who belongs to sudoers and can run sudo.

When a privileged user tries to scan targets outside the local network, Nmap uses ICMP echo requests, TCP ACK (Acknowledge) to port 80, TCP SYN (Synchronize) to port 443, and ICMP timestamp request.

When an unprivileged user tries to scan targets outside the local network, Nmap resorts to a TCP 3-way handshake by sending SYN packets to ports 80 and 443.

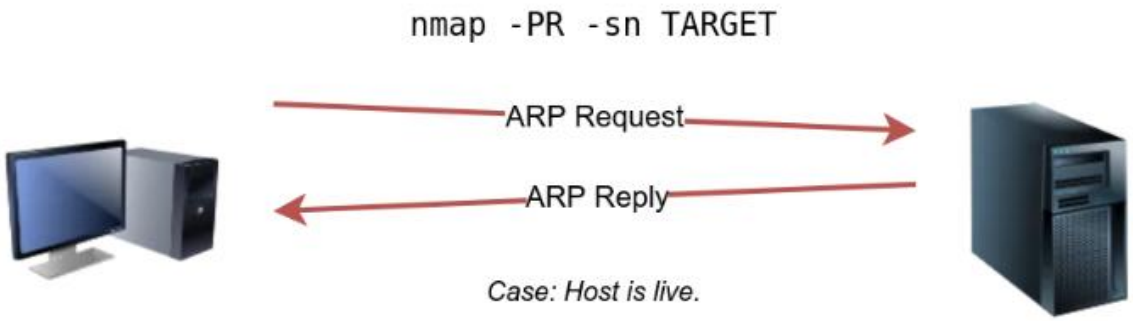
Nmap typically uses a ping scan to find live hosts and then proceeds to scan those live hosts. However, you can use the “nmap -sn TARGETS” command to discover online hosts without conducting port scans. ARP scan is one such method, but it only works when you are on the same subnet as the target systems because it relies on MAC addresses for communication. ARP queries are sent to obtain MAC addresses, and hosts that respond to these queries are considered up. You may see many ARP queries during a local network scan with Nmap. To perform only an ARP scan without port scanning, you can use “nmap -PR -sn TARGETS,” where “-PR” specifies an ARP scan. This allows you to discover live systems on the same subnet as your target machine without conducting any port scans.

```
Pentester Terminal

pentester@TryHackMe$ sudo nmap -PR -sn 10.10.210.6/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-02 07:12 BST
Nmap scan report for ip-10-10-210-75.eu-west-1.compute.internal (10.10.210.75)
Host is up (0.00013s latency).
MAC Address: 02:83:75:3A:F2:89 (Unknown)
Nmap scan report for ip-10-10-210-100.eu-west-1.compute.internal (10.10.210.100)
Host is up (-0.100s latency).
MAC Address: 02:63:D0:1B:2D:CD (Unknown)
Nmap scan report for ip-10-10-210-165.eu-west-1.compute.internal (10.10.210.165)
Host is up (0.00025s latency).
MAC Address: 02:59:79:4F:17:B7 (Unknown)
Nmap scan report for ip-10-10-210-6.eu-west-1.compute.internal (10.10.210.6)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.12 seconds
```

In this scenario, the AttackBox had the IP address 10.10.210.6 and employed ARP requests to identify active hosts within the same subnet. Nmap sends ARP requests to all the target machines, and those that are online will respond with an ARP reply. The ARP scan operates as depicted in the accompanying figure.



- 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?

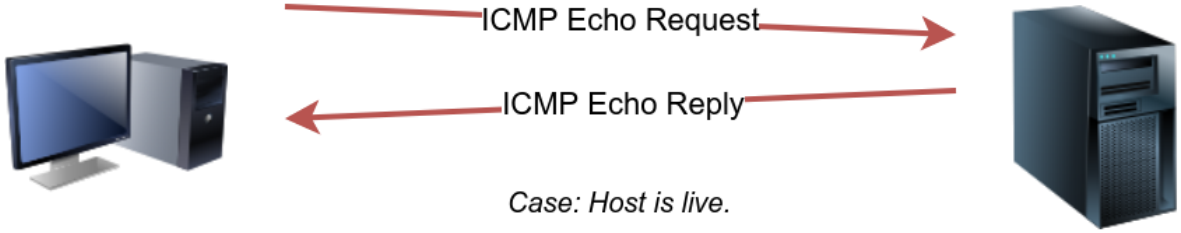
3

NMAP Host Discovery Using ICMP

A simple method to identify live hosts on a target network is by pinging each IP address and checking for responses (ICMP Type 8/Echo requests and Type 0/Echo replies). However, this approach is not always reliable because some firewalls block ICMP echo requests, and newer versions of Windows have default settings that do so as well. If the target is on the same subnet, an ARP query will precede the ICMP request. To perform host discovery using ICMP echo requests, you can use the option “-PE” and include “-sn” if you don’t want to conduct a subsequent port scan.

As shown in the following figure, an ICMP echo scan works by sending an ICMP echo request and expects the target to reply with an ICMP echo reply if it is online.

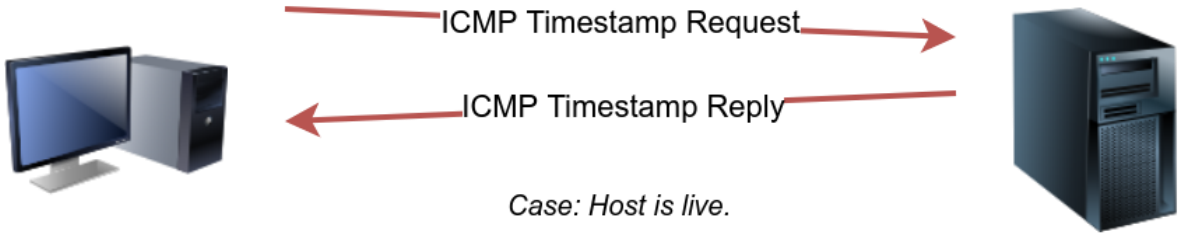
```
nmap -PE -sn TARGET
```



Case: Host is live.

Nmap uses timestamp request (ICMP Type 13) and checks whether it will get a Timestamp reply (ICMP Type 14). Adding the -PP option tells Nmap to use ICMP timestamp requests. As shown in the figure below, you expect live hosts to reply.

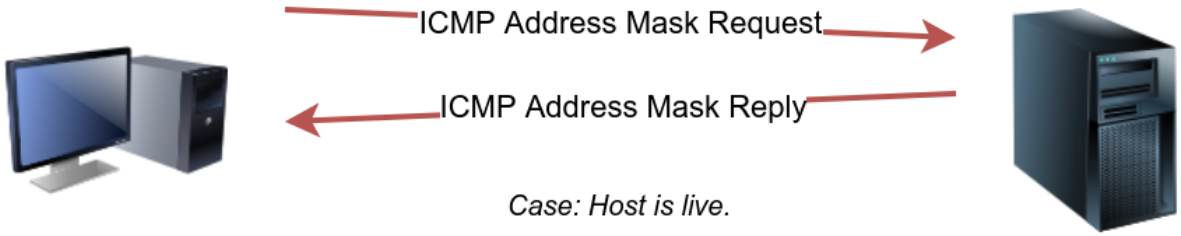
```
nmap -PP -sn TARGET
```



Case: Host is live.

Similarly, Nmap uses address mask queries (ICMP Type 17) and checks whether it gets an address mask reply (ICMP Type 18). This scan can be enabled with the option -PM. As shown in the figure below, live hosts are expected to reply to ICMP address mask requests.

```
nmap -PM -sn TARGET
```



Case: Host is live.

Answer the questions below

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

-PP

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

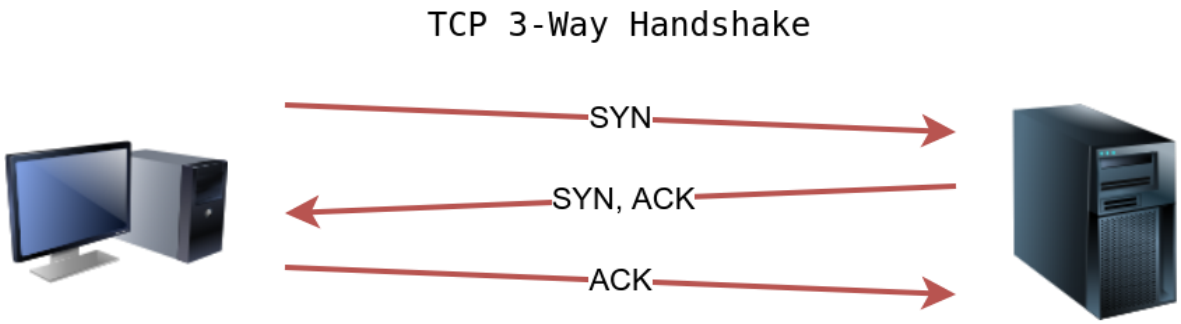
-PM

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

-PE

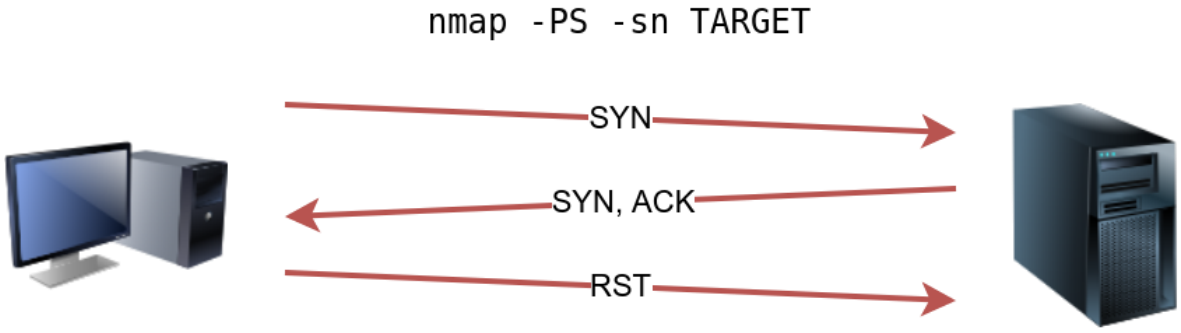
NMAP Host Discovery Using TCP AND UDP

TCP SYN Ping



Case: TCP port is open.

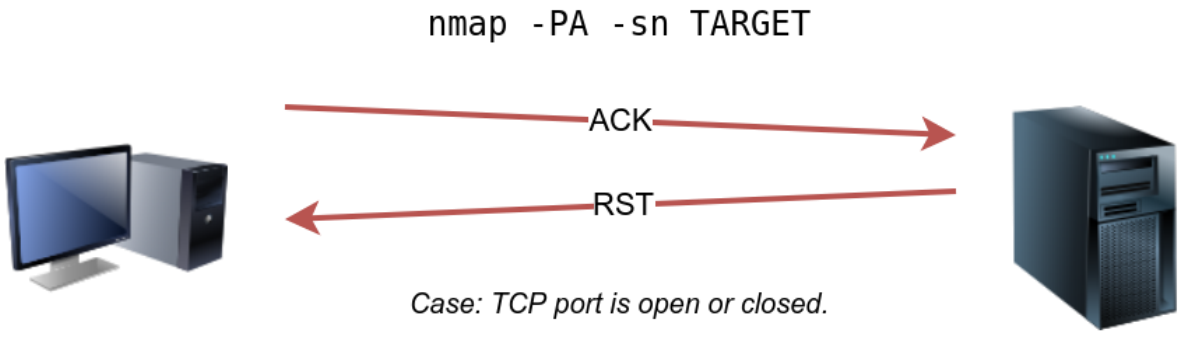
To determine if a host is up, you can send a packet with the SYN (Synchronize) flag set to a default TCP port, usually 80, and wait for a response. An open port will reply with SYN/ACK, while a closed port will result in an RST. In this method, the specific state of the port is not crucial; it's about checking for any response to confirm the host's status. You can enable Nmap to use TCP SYN ping with the option "-PS" followed by the port number, range, or list. For example, "-PS21" targets port 21, while "-PS21–25" targets ports 21 to 25. Privileged users can send TCP SYN packets without completing the 3-way handshake, unlike unprivileged users who must complete it if the port is open.



Case: TCP port is open.

TCP ACK Ping

To utilize ACK ping in Nmap, which sends a packet with the ACK flag set, you need to run Nmap as a privileged user. If you attempt this as an unprivileged user, Nmap will perform a 3-way handshake by default.



Case: TCP port is open or closed.

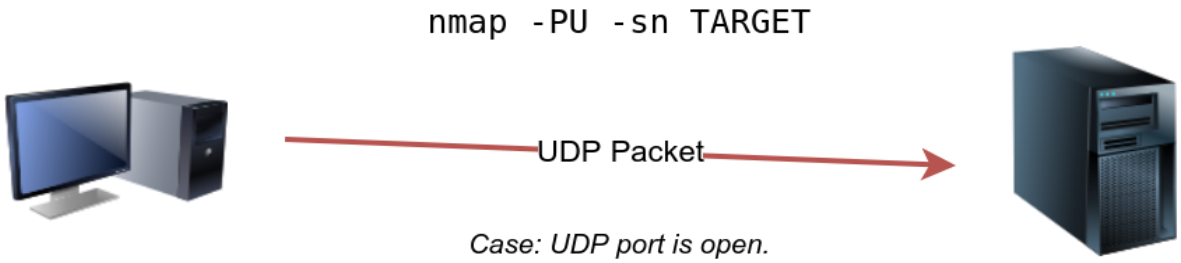
By default, Nmap uses port 80, and you can specify the port(s) using the "-PA" option, followed by a port number, range, list, or a combination thereof. For instance, you can use "-PA21," "-PA21–25," or "-PA80,443,8080." If no port is specified, Nmap will use port 80.

The expected response for an ACK ping is a TCP packet with the RST flag set because the ACK packet is not part of an established connection. This response helps determine if the target host is up.

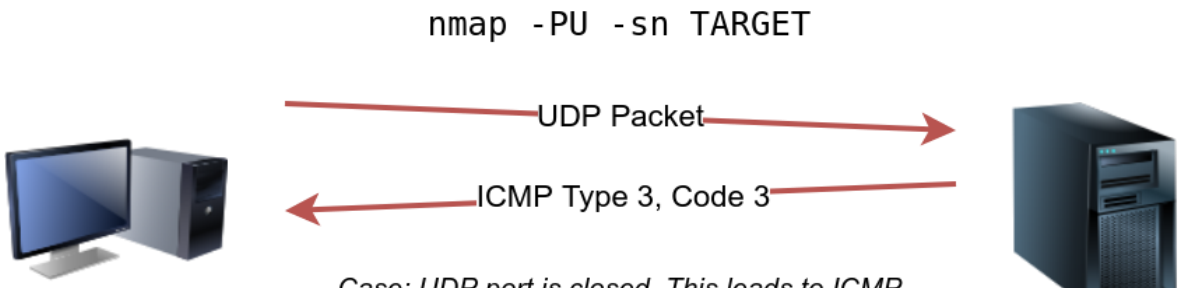
UDP Ping

You can also employ UDP to check if the host is online. Unlike TCP SYN ping, sending a UDP packet to an open port typically doesn't elicit a response. However, when sending a UDP packet to a closed UDP port, you anticipate receiving an ICMP "port unreachable" packet, which indicates the target system is active and reachable.

In summary, while sending UDP packets to open UDP ports may not trigger a response, sending them to closed UDP ports can indirectly indicate that the target is online, as it may generate a "port unreachable" ICMP message.



Case: UDP port is open.



Case: UDP port is closed. This leads to ICMP Destination Unreachable (Port Unreachable)

Answer the questions below

Which TCP ping scan does not require a privileged account?

TCP SYN Ping

Which TCP ping scan requires a privileged account?

TCP ACK Ping

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

-PS23

Using Reverse-DNS Lookup

Nmap's standard operation is to perform reverse-DNS lookups for online hosts, which can provide valuable information through hostnames. If you prefer not to conduct these DNS queries, you can use the "-n" option to bypass this process.

By default, Nmap performs DNS queries for online hosts, but you can use the "-R" option to query the DNS server even for hosts that are offline. Additionally, if you wish to specify a particular DNS server, you can include the " — dns-servers DNS_SERVER" option.

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

Summary

We have learned how ARP, ICMP, TCP, and UDP can detect live hosts by completing this room.