Nmap Live Host Discovery – Lab Report

Submitted By:

Name: Arsalan Khan
Position/Role: Internee
Date: August 7, 2025

Platform:

TryHackMe

Objective:

Learn and apply host discovery techniques using Nmap and related protocols to identify live hosts on a network. Understand the limitations of certain protocols such as ARP in cross-subnet discovery, and practice using Nmap's host discovery options for different scenarios.

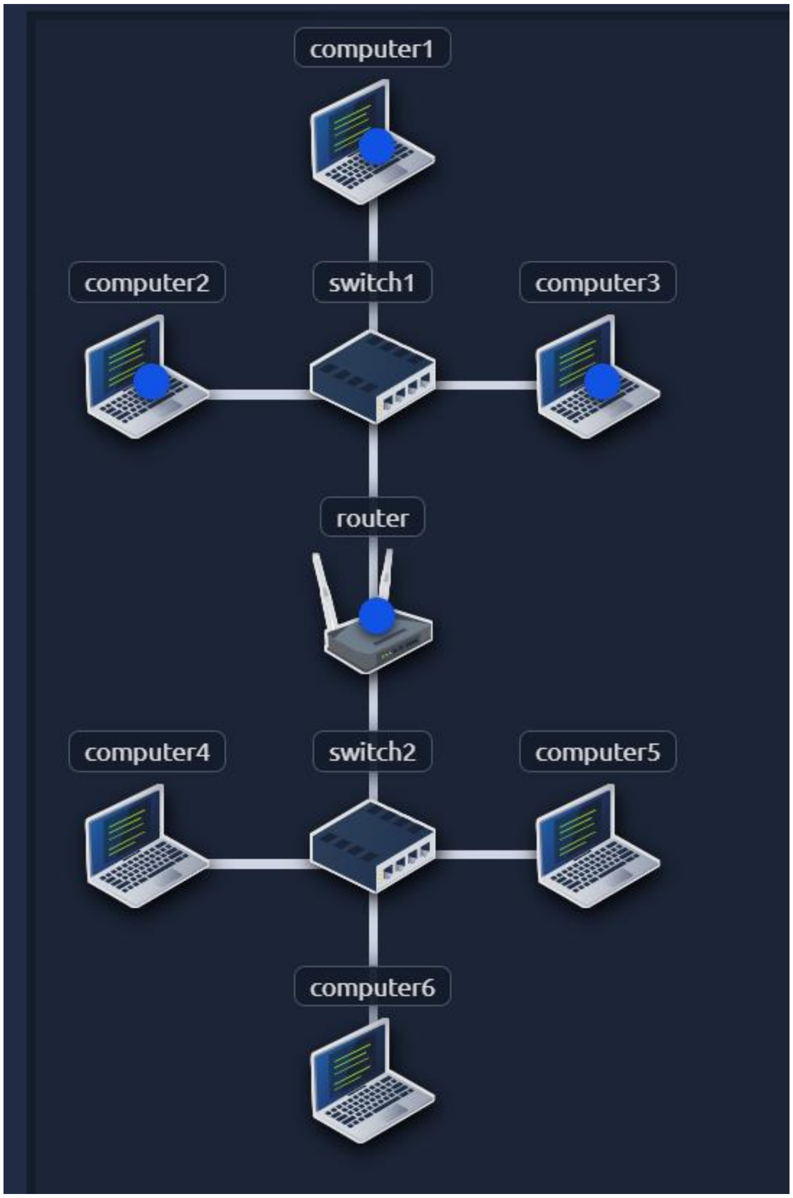
Tools Used:

- Nmap
- ARP (Address Resolution Protocol)
- TryHackMe Network Simulator

Task 1 — Introduction to Nmap Live Host Discovery

Description:
This task introduces Nmap, its purpose, and where it fits in the scanning process. Nmap is used to determine which systems are online before performing port scans. The task outlines the three main live host discovery methods (ARP scan, ICMP scan, TCP/UDP ping scan) and briefly introduces the use of additional tools like `arp-scan` and `masscan`. This room is the first of four in the Nmap series, part of the Network Security module.

Simulation:



Task 2 — Subnetworks

Description:
This task explains the difference between network segments and subnetworks, describes subnet mask notations (/16 and /24), and clarifies that ARP works only within a local subnet. It emphasizes that ARP broadcasts are not routed, so they cannot discover devices in different subnets.

Questions & Answers:

1. **Question:**
   Send a packet with the following:

- From: computer1
- To: computer1 (broadcast)
- Packet Type: ARP Request
- Data: computer6

How many devices can see the ARP Request?
Answer: 4

2. **Question:**
   Did computer6 receive the ARP Request? (Y/N)
   Answer: N
3. **Question:**
   Send a packet with the following:

- From: computer4
- To: computer4 (broadcast)
- Packet Type: ARP Request
- Data: computer6

How many devices can see the ARP Request?
Answer: 4

4. **Question:**
   Did computer6 reply to the ARP Request? (Y/N)
   Answer: N

Task 3 — Target Specification in Nmap

Description:
This task explains how to specify scan targets in Nmap using lists, ranges, and subnets. It also covers how to list the hosts Nmap will scan without actually scanning them using -sL, and how to avoid DNS resolution using -n.

Questions & Answers:

1. **Question:**
   What is the first IP address Nmap would scan if you provided 10.10.12.13/29 as your target?
   Answer: 10.10.12.9
2. **Question:**
   How many IP addresses will Nmap scan if you provide the range 10.10.0-255.101-125?
   Answer: 6400

Task 4 — Discovering Live Hosts
Description:
This task revisits the TCP/IP layers and shows how different protocols can be leveraged to discover live hosts:

- **Link Layer:** ARP (Address Resolution Protocol) — sends broadcast requests asking for MAC addresses of specific IPs.
- **Network Layer:** ICMP — uses Echo Request (Type 8) and Echo Reply (Type 0) for pinging.
- **Transport Layer:** TCP/UDP — scanners send packets to common ports to check for responses, which is useful when ICMP is blocked.

In this task, the simulator demonstrates how ARP queries precede ICMP pings within the same subnet, and how previously learned MAC addresses are reused without sending new ARP requests.

Questions & Answers:

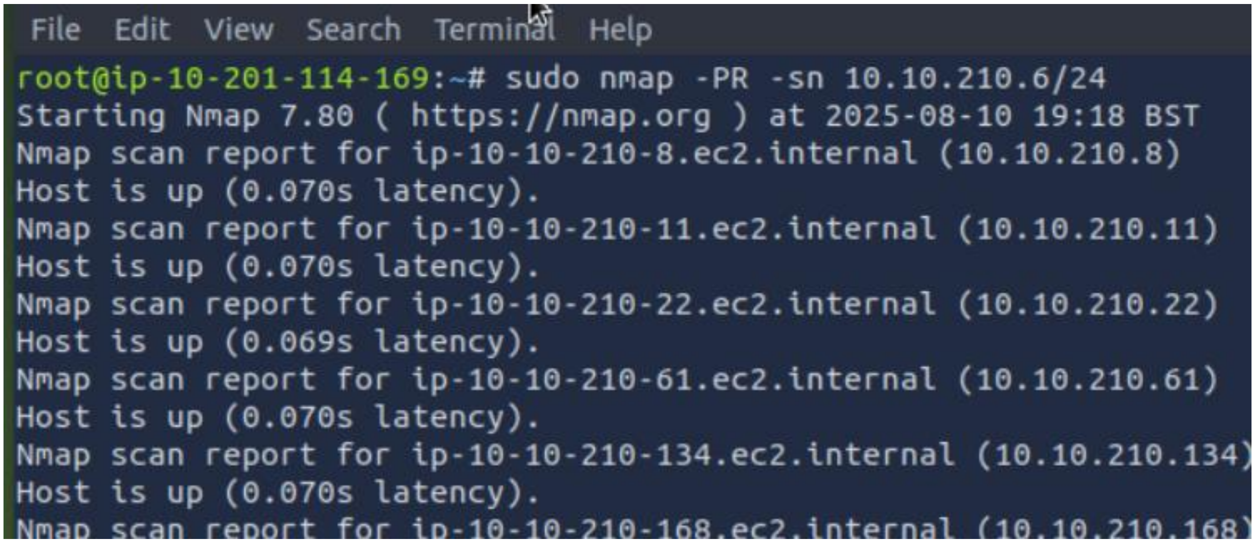
1. **Q:** From computer1 → computer3, Ping Request — What is the type of packet that computer1 sent before the ping?
   A: ARP Request
2. **Q:** What is the type of packet that computer1 received before being able to send the ping?
   A: ARP Response
3. **Q:** How many computers responded to the ping request?
   A: 1

4. **Q:** From computer2 → computer5, Ping Request — What is the name of the first device that responded to the first ARP Request?
   A: router
5. **Q:** What is the name of the first device that responded to the second ARP Request?
   A: computer5
6. **Q:** Send another Ping Request. Did it require new ARP Requests? (Y/N)
   A: N

Task 5 — Nmap Host Discovery Using ARP

Description:
Nmap uses ARP requests for local subnet scans by privileged users. The -PR option forces ARP-only scans without port scanning, e.g.:

sudo nmap -PR -sn TARGETS



```
root@ip-10-201-114-169:~# sudo nmap -PR -sn 10.10.210.6/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 19:18 BST
Nmap scan report for ip-10-10-210-8.ec2.internal (10.10.210.8)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-210-11.ec2.internal (10.10.210.11)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-210-22.ec2.internal (10.10.210.22)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-210-61.ec2.internal (10.10.210.61)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-210-134.ec2.internal (10.10.210.134)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-210-168.ec2.internal (10.10.210.168)
```

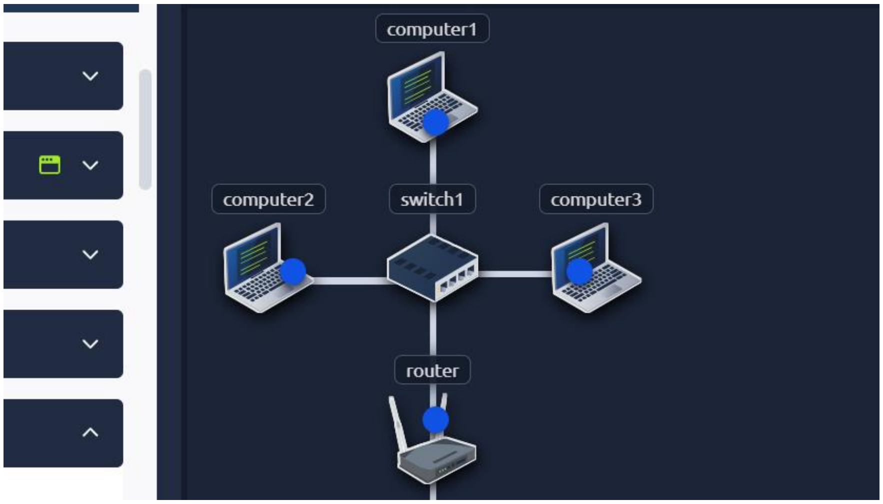
arp-scan is a dedicated ARP discovery tool with commands such as:

sudo arp-scan -l
sudo arp-scan -I eth0 -l

Both methods generate similar broadcast traffic visible in Wireshark or tcpdump.

Questions & Answers:

1. **Q:** From Computer1 (broadcast ARP request to all 8 possible devices) — how many devices discovered?
   A: 3

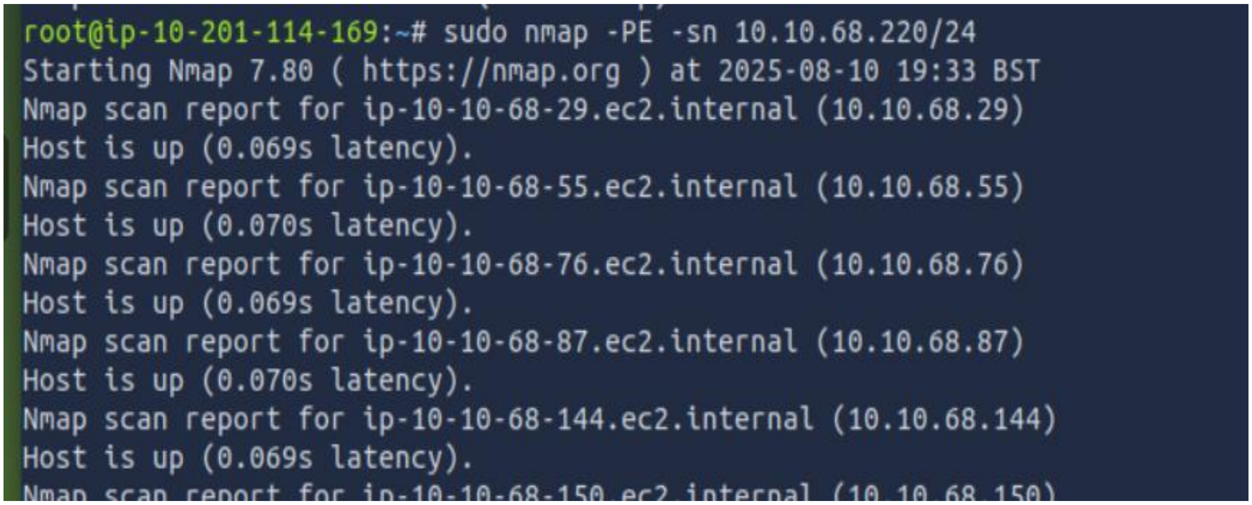


Task 6 — Nmap Host Discovery Using ICMP

Description:
This task explores the use of ICMP-based scans in Nmap to discover live hosts. ICMP Echo Requests (`Type 8`) are the most straightforward but can be blocked by firewalls or OS configurations (e.g., Windows host firewalls). When the target is on the same subnet, an ARP query precedes the ICMP request.

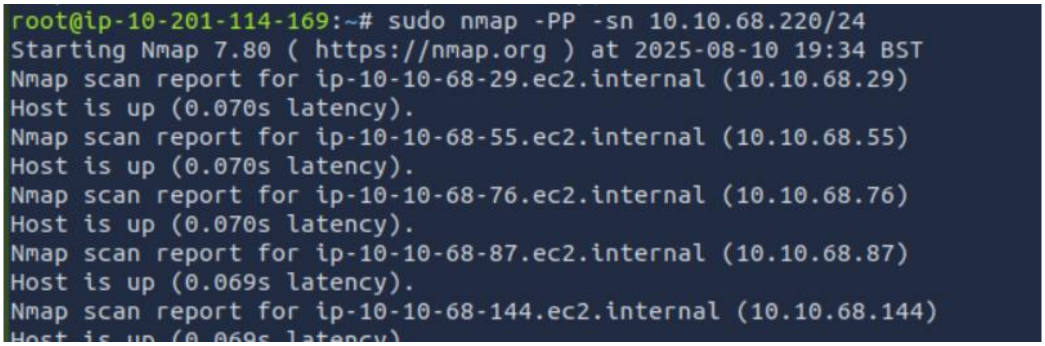
Scan Types Covered:

1. **ICMP Echo Scan** (`-PE`) — Sends ICMP Echo Request, expects ICMP Echo Reply (`Type 0`).



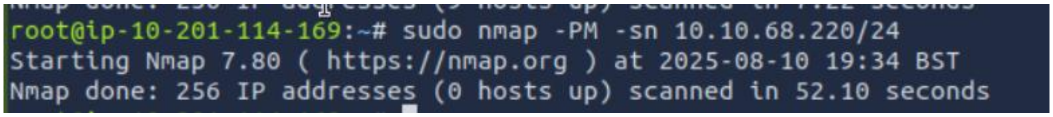
```
root@ip-10-201-114-169:~# sudo nmap -PE -sn 10.10.68.220/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 19:33 BST
Nmap scan report for ip-10-10-68-29.ec2.internal (10.10.68.29)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-55.ec2.internal (10.10.68.55)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-76.ec2.internal (10.10.68.76)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-87.ec2.internal (10.10.68.87)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-144.ec2.internal (10.10.68.144)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-150.ec2.internal (10.10.68.150)
```

2. **ICMP Timestamp Scan** (`-PP`) — Sends ICMP Timestamp Request (`Type 13`), expects Timestamp Reply (`Type 14`).



```
root@ip-10-201-114-169:~# sudo nmap -PP -sn 10.10.68.220/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 19:34 BST
Nmap scan report for ip-10-10-68-29.ec2.internal (10.10.68.29)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-55.ec2.internal (10.10.68.55)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-76.ec2.internal (10.10.68.76)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-87.ec2.internal (10.10.68.87)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-144.ec2.internal (10.10.68.144)
Host is up (0.069s latency).
```

3. **ICMP Address Mask Scan** (`-PM`) — Sends ICMP Address Mask Request (`Type 17`), expects Address Mask Reply (`Type 18`).



```
Nmap done: 256 IP addresses (9 hosts up) scanned in 7.22 seconds
root@ip-10-201-114-169:~# sudo nmap -PM -sn 10.10.68.220/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 19:34 BST
Nmap done: 256 IP addresses (0 hosts up) scanned in 52.10 seconds
```

Observations:

- When scanning from the same subnet, MAC addresses are also detected because ARP is used before ICMP.
- When scanning from a different subnet, only IP addresses and latency are displayed.
- Some ICMP types may be blocked entirely by the target host or intermediate firewalls, resulting in zero detections.
- Using multiple ICMP methods increases the chances of discovering hosts when one packet type is blocked.

Example Commands:

```
sudo nmap -PE -sn MACHINE_IP/24    # ICMP Echo Scan
sudo nmap -PP -sn MACHINE_IP/24    # ICMP Timestamp Scan
sudo nmap -PM -sn MACHINE_IP/24    # ICMP Address Mask Scan
```

Questions & Answers:

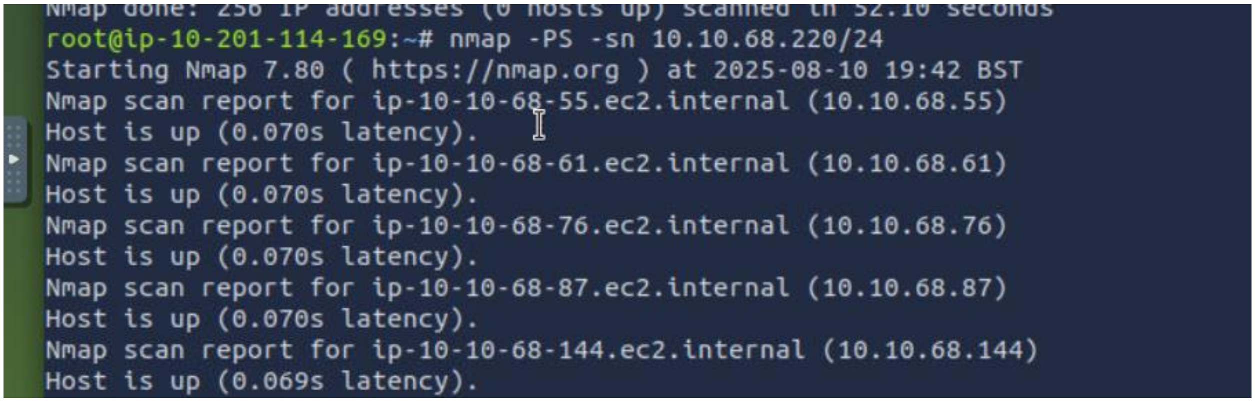
1. **Q:** Option to tell Nmap to use ICMP Timestamp?
   A: -PP
2. **Q:** Option to tell Nmap to use ICMP Address Mask?
   A: -PM
3. **Q:** Option to tell Nmap to use ICMP Echo?
   A: -PE

Task 7 — Nmap Host Discovery Using TCP and UDP

Description:
In this task, we explore host discovery using TCP SYN ping**,** TCP ACK ping**,** and UDP ping. Unlike ICMP-based scans, these methods leverage transport layer protocols to detect live systems, which can be more effective when ICMP is blocked.

TCP SYN Ping (-PS)

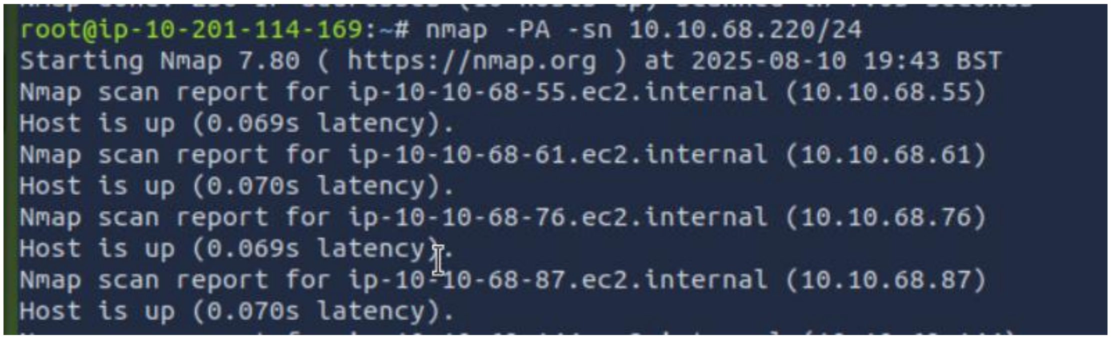
- Sends a TCP packet with the SYN flag to the specified port(s).
- If the port is open → Target replies with SYN/ACK.
- If the port is closed → Target replies with RST**.**
- This scan does not require completing the TCP handshake (if run as a privileged user).



```
Nmap done: 256 IP addresses (0 hosts up) scanned in 52.10 seconds
root@ip-10-201-114-169:~# nmap -PS -sn 10.10.68.220/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 19:42 BST
Nmap scan report for ip-10-10-68-55.ec2.internal (10.10.68.55)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-61.ec2.internal (10.10.68.61)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-76.ec2.internal (10.10.68.76)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-87.ec2.internal (10.10.68.87)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-144.ec2.internal (10.10.68.144)
Host is up (0.069s latency).
```

TCP ACK Ping (-PA)

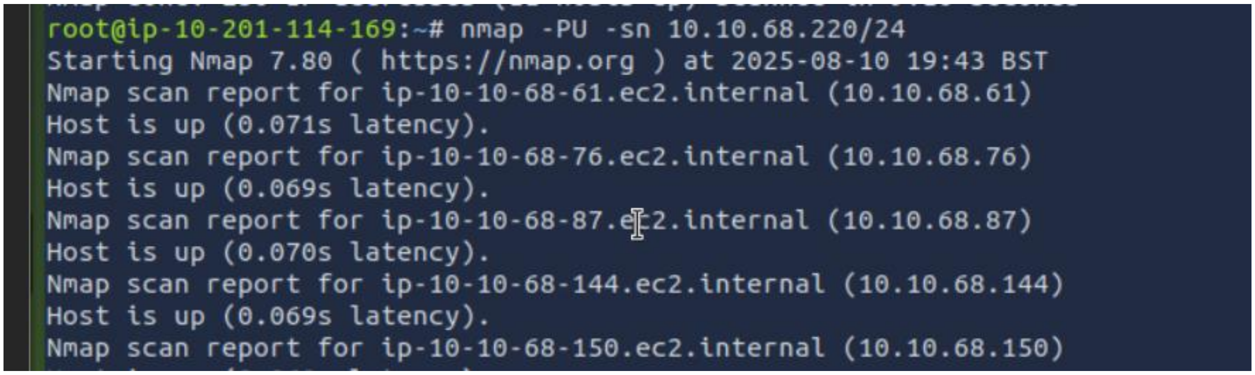
- Sends a TCP packet with the ACK flag to the specified port(s).
- If no active connection exists, the target responds with RST, indicating the host is online.
- Requires privileged **access** to send crafted TCP ACK packets without completing a handshake.



```
root@ip-10-201-114-169:~# nmap -PA -sn 10.10.68.220/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 19:43 BST
Nmap scan report for ip-10-10-68-55.ec2.internal (10.10.68.55)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-61.ec2.internal (10.10.68.61)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-76.ec2.internal (10.10.68.76)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-87.ec2.internal (10.10.68.87)
Host is up (0.070s latency).
```

UDP Ping (-PU)

- Sends a UDP packet to the specified port(s).
- Open UDP ports → Usually no response.
- Closed UDP ports → Often respond with ICMP "Port Unreachable" (Type 3, Code 3), indicating host is online.



```
root@ip-10-201-114-169:~# nmap -PU -sn 10.10.68.220/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 19:43 BST
Nmap scan report for ip-10-10-68-61.ec2.internal (10.10.68.61)
Host is up (0.071s latency).
Nmap scan report for ip-10-10-68-76.ec2.internal (10.10.68.76)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-87.ec2.internal (10.10.68.87)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-144.ec2.internal (10.10.68.144)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-150.ec2.internal (10.10.68.150)
```

Questions & Answers:

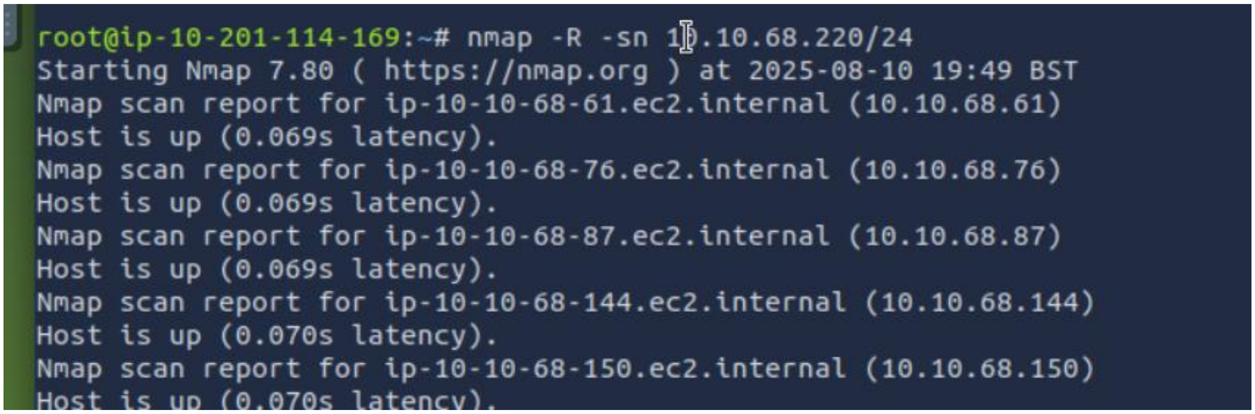
1. **Q:** Which TCP ping scan does not require a privileged account?
   A: TCP Connect Scan
2. **Q:** Which TCP ping scan requires a privileged account?
   A: TCP ACK Ping
3. **Q:** What option do you need to add to Nmap to run a TCP SYN ping scan on the telnet port?
   A: -PS23

Task 8 — Using Reverse-DNS Lookup

Description:
By default, Nmap performs reverse-DNS lookups for online hosts only. Reverse-DNS can reveal valuable information through hostnames, such as function, location, or internal naming conventions.

- **Default behaviour:** Reverse-DNS lookup only for hosts that respond.
- **To skip DNS lookups entirely:** Use -n.
- **To force DNS lookups for all possible hosts, including offline ones:** Use `-R`.
- **To specify a custom DNS server:** Use --dns-servers <DNS_SERVER>.

Example Commands:



```
root@ip-10-201-114-169:~# nmap -R -sn 10.10.68.220/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 19:49 BST
Nmap scan report for ip-10-10-68-61.ec2.internal (10.10.68.61)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-76.ec2.internal (10.10.68.76)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-87.ec2.internal (10.10.68.87)
Host is up (0.069s latency).
Nmap scan report for ip-10-10-68-144.ec2.internal (10.10.68.144)
Host is up (0.070s latency).
Nmap scan report for ip-10-10-68-150.ec2.internal (10.10.68.150)
Host is up (0.070s latency).
```

Question & Answer:

Q: 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?
A: `-R`

Task 9 – Summary

Description:
This task provided a recap of all the Nmap host discovery techniques covered in the lab. It emphasized that any kind of valid network response — whether via ARP, ICMP, TCP, or UDP can indicate a live host. It also summarized the exact commands used for each scan type and explained important Nmap options such as -n, -R, and -sn.

Key Command Reference Table:

Scan Type	Example Command
ARP Scan	sudo nmap -PR -sn MACHINE_IP/24
ICMP Echo Scan	sudo nmap -PE -sn MACHINE_IP/24
ICMP Timestamp Scan	sudo nmap -PP -sn MACHINE_IP/24
ICMP Address Mask Scan	sudo nmap -PM -sn MACHINE_IP/24
TCP SYN Ping Scan	sudo nmap -PS22,80,443 -sn MACHINE_IP/30
TCP ACK Ping Scan	sudo nmap -PA22,80,443 -sn MACHINE_IP/30
UDP Ping Scan	sudo nmap -PU53,161,162 -sn MACHINE_IP/30

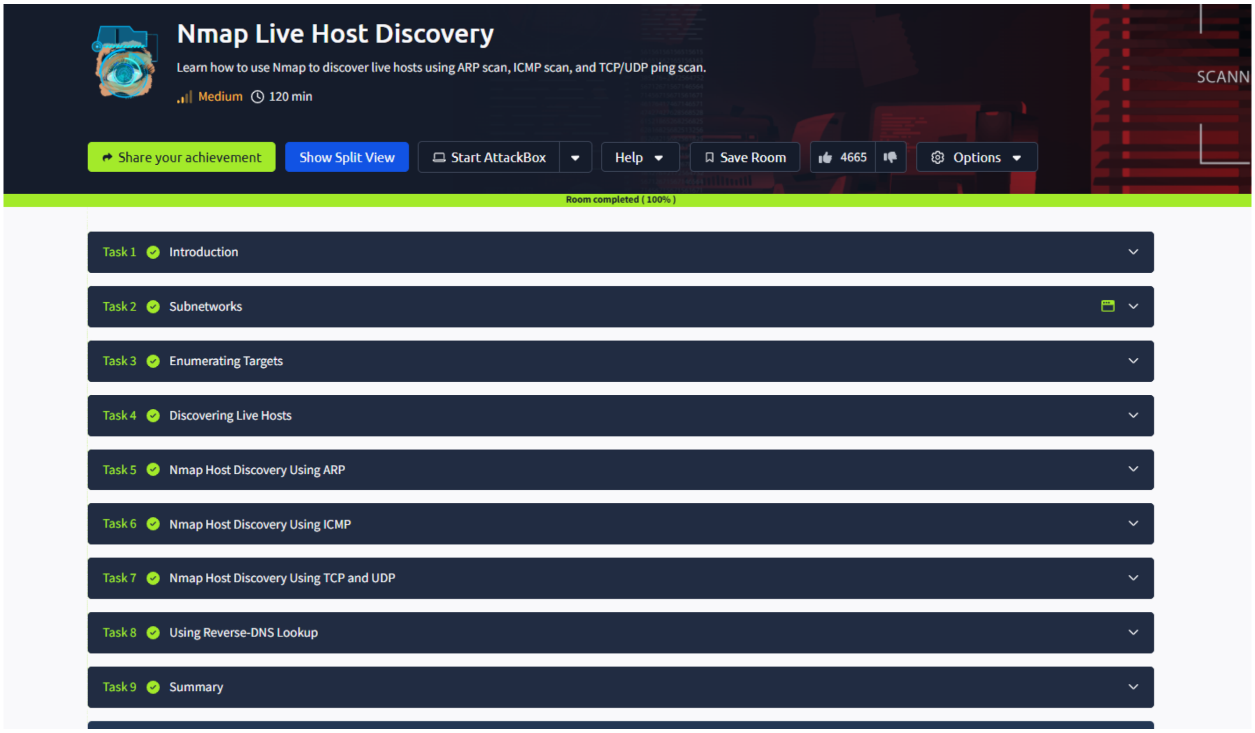
Important Options:

Option	Purpose
-n	No DNS lookup
-R	Reverse-DNS lookup for all hosts
-sn	Host discovery only (no port scan)

Remarks:

- Adding -sn ensures that Nmap only performs host discovery without scanning ports.
- Omitting -sn makes Nmap proceed to port scanning for all detected live hosts.
- Understanding these flags is essential before progressing to Nmap Basic Port Scans in the next module.

Room Completed



Nmap Live Host Discovery

Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.

Medium 120 min

Room completed (100%)

Task 1 Introduction

Task 2 Subnetworks

Task 3 Enumerating Targets

Task 4 Discovering Live Hosts

Task 5 Nmap Host Discovery Using ARP

Task 6 Nmap Host Discovery Using ICMP

Task 7 Nmap Host Discovery Using TCP and UDP

Task 8 Using Reverse-DNS Lookup

Task 9 Summary

End…