Task 3:

Complete the room: https://tryhackme.com/room/furthernmap. Prepare a report while doing the room, add screenshots and explain what is happening while you are doing the room.

Room: TryHackMe – Further Nmap
Author: ashfin prem
Date: 24-08-2025

1. Introduction

The objective of this room was to explore **advanced Nmap techniques** for enumeration and vulnerability detection. Nmap is a network scanning tool widely used in penetration testing to identify hosts, services, operating systems, and potential vulnerabilities.

This report documents the scans performed against the target machine, explains what each command does, and analyzes the results. Screenshots were taken during the process to validate the findings.

2. Environment Setup

- **Platform:** TryHackMe VPN (OpenVPN)
- **Target IP:** 10.201.10.93
- **Tools Used:**
  - nmap (Network Mapper)
  - Linux terminal (Kali Linux VM)

Task 14 Practical

Use what you've learnt to scan the target machine and answer the following questions!

The IP address of the VM you powered on in Task1 is 10.201.10.93

(**Note:** If you're not a subscriber, make sure that this machine has had around ten minutes to start)

Answer the questions below

Does the target ip respond to ICMP echo (ping) requests (Y/N)?

N — ✓ Correct Answer

Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?

999 — ✓ Correct Answer

There is a reason given for this -- what is it?

Note: The answer will be in your scan results. Think carefully about which switches to use -- and read the hint before asking for help!

No Response — ✓ Correct Answer — Hint

Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

5 — ✓ Correct Answer

Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Y — ✓ Correct Answer

Armoury Cra

Touchpad Disal

kali@kali: ~

```
(kali㉿kali)-[~]
$ nmap 10.201.10.93 --script=ftp-anon -p21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-24 14:12 EDT
Nmap scan report for 10.201.10.93
Host is up (0.00050s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds

(kali㉿kali)-[~]
$
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.201.10.93
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-24 14:28 EDT
Nmap scan report for 10.201.10.93
Host is up (0.00061s latency).
All 1000 scanned ports on 10.201.10.93 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using port 80/tcp)
HOP RTT    ADDRESS
1    ...  30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.02 seconds
```