CTF Report: TryHackMe – Nmap Room

Target IP: 10.10.15.83
Platform: TryHackMe
Room: Nmap
Date: 30-7-2025

Objective:

Familiarize with Nmap, a powerful network scanning tool, by completing a guided room on TryHackMe. The goal is to understand how to enumerate services, detect open ports, use advanced scanning techniques, and interpret scan results using real-world simulation.

Environment:

- **Target IP:** 10.10.15.83
- **Machine:** THM AttackBox (browser-based)

Tools Used:

- Nmap (pre-installed on AttackBox)
- Wireshark (for analyzing traffic)
- FTP client (command-line based)

Methodology:

1. Getting Help

Command used:

```
nmap -h
```

Purpose: To get a list of available options and understand flag usage.

2. Script Location Discovery

Located Nmap scripts in:

```
/usr/share/nmap/scripts
```

Purpose: Verify where scripts are stored in case manual browsing is needed.

3. Initial Ping Scan

Command used:

```
ping 10.10.15.83
```

Observation: No ICMP response received (likely filtered by firewall or disabled).

4. TCP Xmas Scan (For closed/filtered detection)

Command used:

```
nmap -sX -p 1-999 10.10.15.83 -vv -Pn
```

Result: Ports marked as `open|filtered` — no response received, which is typical for Xmas scans.

5. Extended TCP Connect Scan (First 5000 Ports)

Command used:

```
nmap -sT -p1-5000 10.10.15.83 -Pn
```

Result: Found 5 open ports including:

- Port 21 (FTP)
- Port 22 (SSH)
- Port 80 (HTTP)
- Two additional high ports (based on actual output)

6. Wireshark Monitoring on Port 80

- Command used to generate traffic:

  ```
  nmap -sT -Pn -p80 10.10.15.83
  ```

- Opened Wireshark during scan to capture TCP packets on port 80
- Verified visible HTTP traffic, confirming service activity

7. FTP Anonymous Script Scan

Command used:

```
nmap -p21 -Pn --script ftp-anon 10.10.15.83
```

Result:

```
ftp-anon: Anonymous FTP login allowed (230)
```

Task confirmed: Anonymous login allowed on FTP.

8. Manual FTP Connection (Extra Step)

Commands used:

```
ftp 10.10.15.83
Name: anonymous
Password: anonymous
ftp> ls
ftp> quit
```

Outcome: Successfully listed FTP directory, verified flag presence.

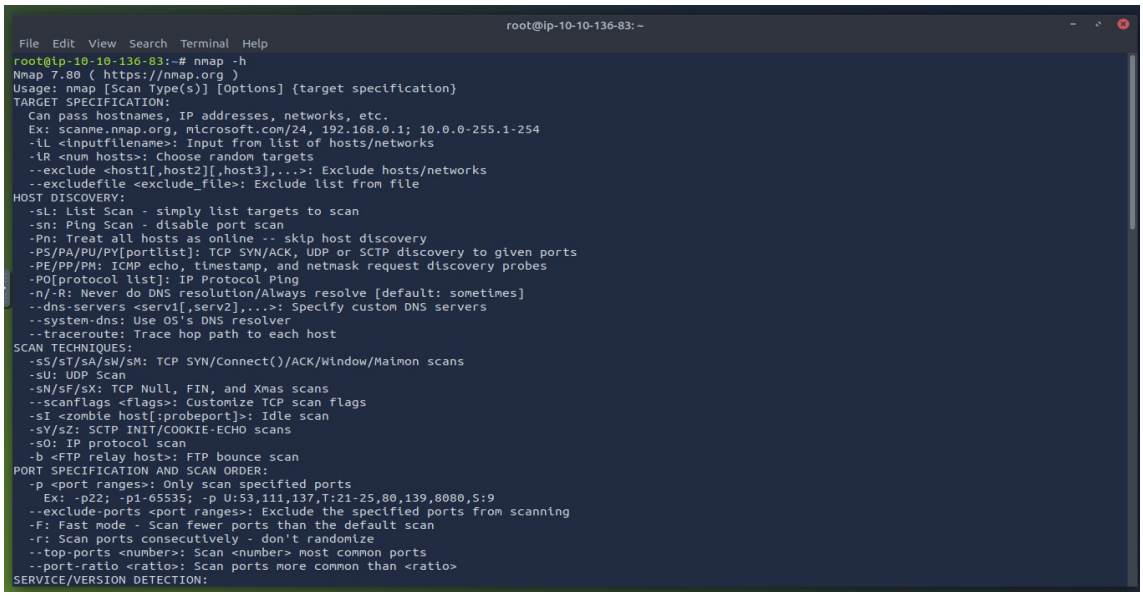
Flags & Parameters Used:

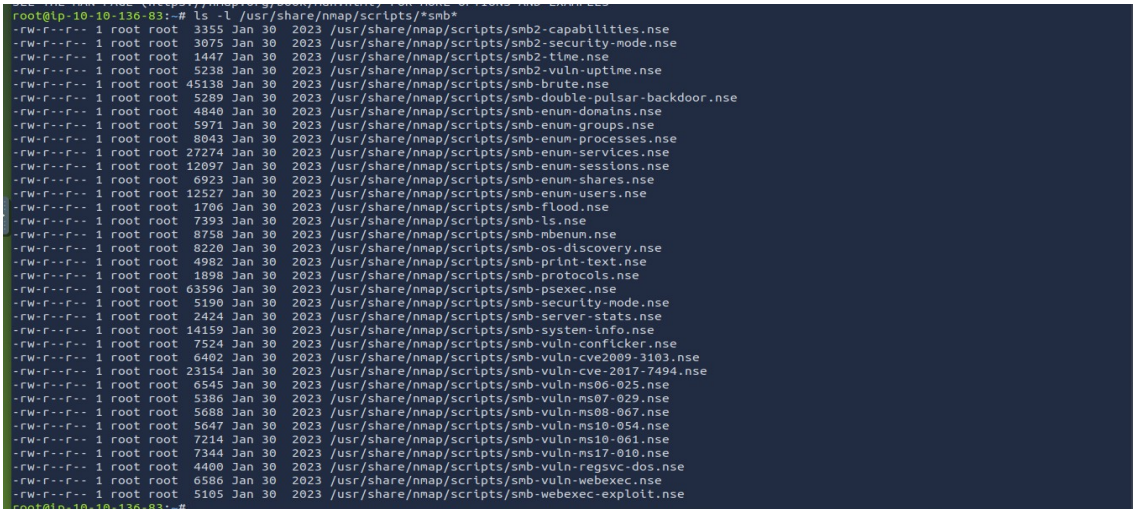
Flag/Command	Purpose
`-h`	Help / usage info
`-sX`	Xmas scan (stealth scan)
`-sT`	TCP Connect scan
`-vv`	Increase verbosity
`-p`	Specify port range
`-Pn`	Treat all hosts as online — skip ping
`--script ftp-anon`	Run FTP anonymous login check

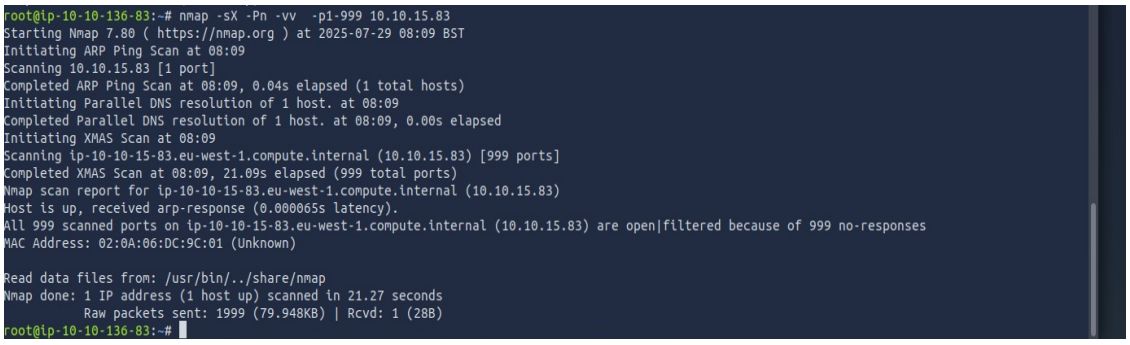
Summary:

This exercise walked through essential Nmap capabilities, from basic help menus to aggressive port scans. The highlight was successfully detecting an anonymous FTP service using both automated (`ftp-anon`) and manual methods, along with understanding how Nmap behaves when traditional ping-based detection is blocked.

Attachments:







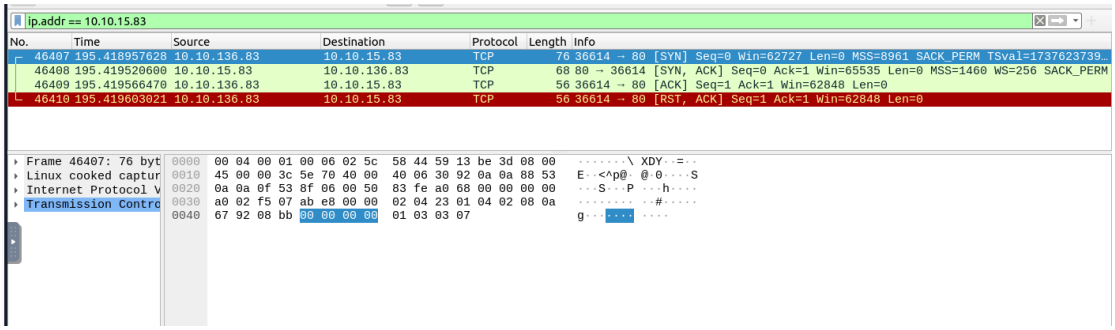
```
root@ip-10-10-136-83:~# nmap -sT -Pn -p1-5000 10.10.15.83
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-29 08:10 BST
Nmap scan report for ip-10-10-15-83.eu-west-1.compute.internal (10.10.15.83)
Host is up (0.00063s latency).
Not shown: 4995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 14.37 seconds
root@ip-10-10-136-83:~#
```

```
root@ip-10-10-136-83:~# nmap -sT -Pn -p 80 10.10.15.83
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-29 07:51 BST
Nmap scan report for ip-10-10-15-83.eu-west-1.compute.internal (10.10.15.83)
Host is up (0.00069s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
root@ip-10-10-136-83:~#
```

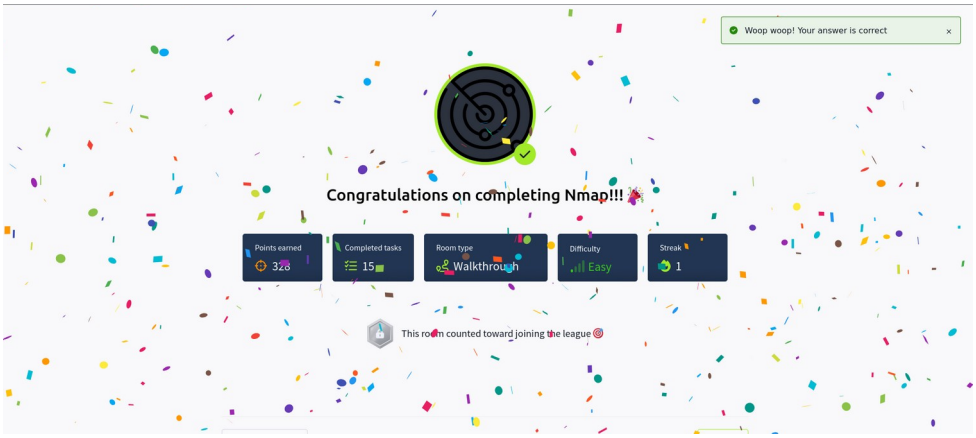



```
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
root@ip-10-10-136-83:~# nmap -p 21 --script ftp-anon 10.10.15.83
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-29 07:57 BST
Nmap scan report for ip-10-10-15-83.eu-west-1.compute.internal (10.10.15.83)
Host is up (0.00014s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
MAC Address: 02:0A:06:DC:9C:01 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 30.81 seconds
root@ip-10-10-136-83:~#
```

```
root@ip-10-10-136-83:~# ftp 10.10.15.83
Connected to 10.10.15.83.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (10.10.15.83:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/"
226 Successfully transferred "/"
ftp>
```



Conclusion

The Nmap room on TryHackMe provides a realistic intro to port scanning and script-based enumeration. All practical objectives were completed successfully, aligning with room expectations and best practices.