

# 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:~#
File Edit View Search Terminal Help
root@ip-10-10-136-83:~# nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] [target specification]
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilenames>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PI[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <Flags>: Customize TCP scan flags
  -sT <enable host[probeoptions]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sQ: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,I:113,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Enable service/version detection
  --script <script[,script]...>: Only run the specified script(s)
  --script-timeout <seconds>: Timeout for each script
  --script-trace: Print debug output from scripts
  --script-args <script> <args>: Set script arguments
  --script-args <script> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args> <args>: Set script arguments
  --script-args <script> <args> <args> <args>
```

```

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:~#

```

| No.   | Time          | Source       | Destination  | Protocol | Length | Info  |
|-------|---------------|--------------|--------------|----------|--------|---|
| 46407 | 195.418957028 | 10.10.136.83 | 10.10.15.83  | TCP      | 70     | 36614 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=1737623739  |
| 46408 | 195.419520600 | 10.10.15.83  | 10.10.136.83 | TCP      | 68     | 80 → 36614 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 46409 | 195.419566470 | 10.10.136.83 | 10.10.15.83  | TCP      | 56     | 36614 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0                                |
| 46410 | 195.419603021 | 10.10.136.83 | 10.10.15.83  | TCP      | 56     | 36614 → 80 [RST, ACK] Seq=1 Ack=1 Win=62848 Len=0                           |

|  |      |                         |                         |                    |
|--|------|-------------------------|-------------------------|--------------------|
| Frame 46407: 76 bytes on wire (608 bits) captured on interface eth0          | 0000 | 00 04 00 01 00 06 02 5c | 58 44 59 13 be 3d 08 00 | .....\XDY-=-       |
| Ethernet II, Src: Linux cooked capture (00:00:00:00:00:00), Dst: 10.10.15.83 | 0010 | 45 00 00 3c 5e 70 40 00 | 40 06 30 92 0a 0a 88 53 | E-...<^p@_@_0-...S |
| Internet Protocol Version 4, Src: 10.10.136.83, Dst: 10.10.15.83             | 0020 | 0a 0a 0f 53 0f 06 00 50 | 83 fe a0 68 00 00 00 00 | ...S...P...h....   |
| Transmission Control Protocol, Src Port: 36614, Dst Port: 80                 | 0030 | a0 02 f5 07 ab e8 00 00 | 02 04 23 01 04 02 08 0a | .....#.....        |
| TCP, Seq=0, Win=62727, Len=0   | 0040 | 67 92 08 bb 00 00 00 00 | 01 03 03 07             | g...-...-....      |

```

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)

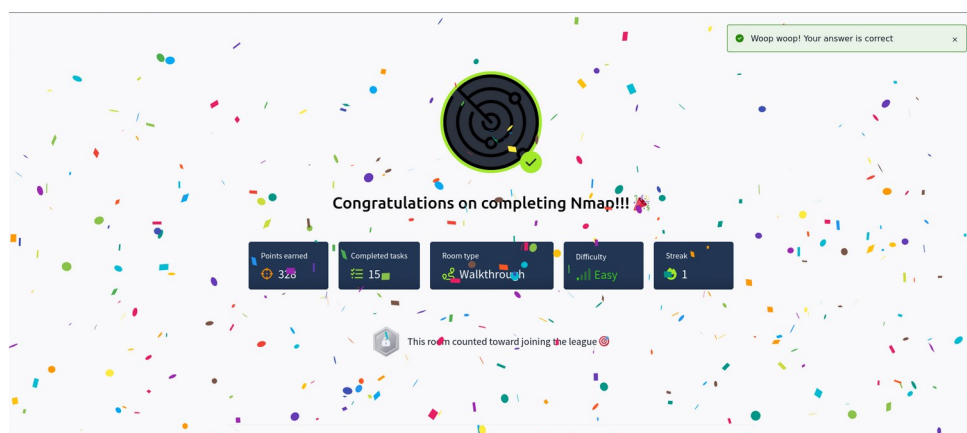
Nmap done: 1 IP address (1 host up) scanned in 30.81 seconds
root@ip-10-10-136-83:~#

```

```

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.