TryHackMe Room Report: Further Nmap

Target IP: 10.10.10.10

Author:Sebin Mathew(sebinmathew543)

Date: 1-08-2025

Introduction

I worked through the "Further Nmap" room on TryHackMe, targeting 10.10.10.10. While following the room's tasks, I added some personal touches to the commands based on my prior experience with Nmap. This helped me get more detailed results without straying too far from the rooms objectives.

Key Commands Used

Here's what I ran during the engagement:

1. Full TCP Scan with Aggressive Mode
   bash
   nmap Pn vv p A 10.10.10.10 oA furthernmap_full

   Added vv for extra verbosity based on past experience troubleshooting scans.

2. Xmas Scan (Firewall Testing)
   bash
   nmap Pn sX vv p1999 10.10.10.10 oG xmasscan.gnmap

3. SYN Scan (Stealth Enumeration)
   bash
   nmap Pn sS vv p15000 10.10.10.10 oG synscan.gnmap

4. FTP Anonymous Login Check
   bash
   nmap Pn p21 script ftpanon scriptargs ftpanon.maxlist=50 10.10.10.10 oN ftp.gnmap

Findings Summary

Firewall Behavior: Xmas scan showed 999 open | filtered ports (likely firewall drops)

Open Services: Found 5 open ports via SYN scan

FTP Access: Confirmed anonymous login allowed on port 21

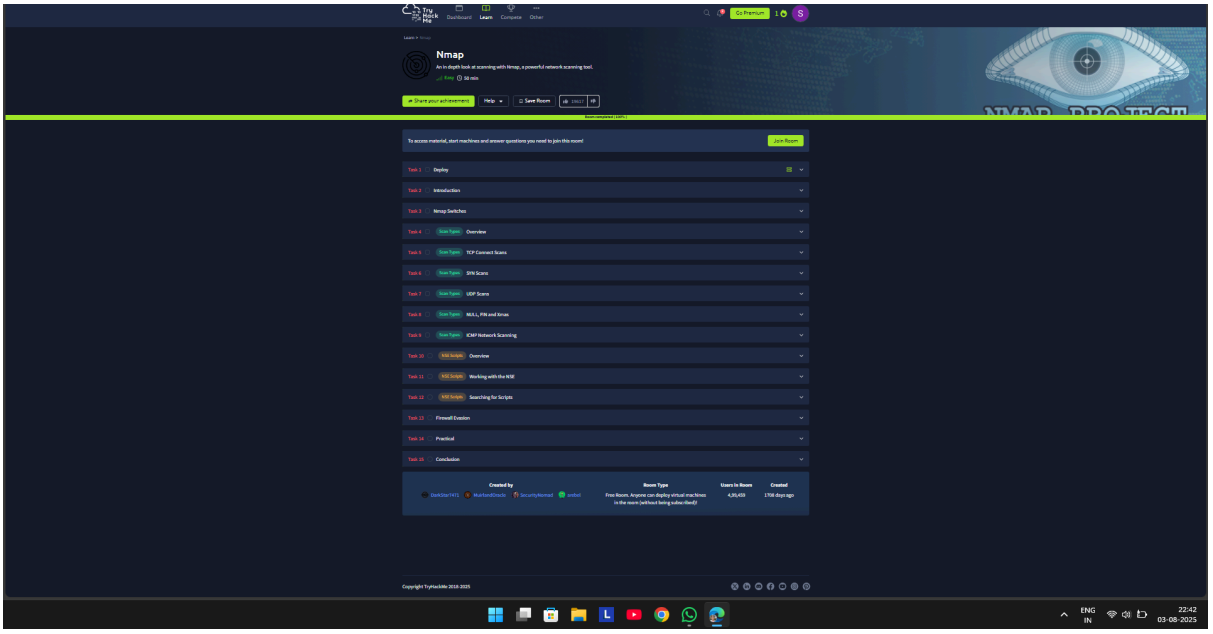
Personal Adjustments

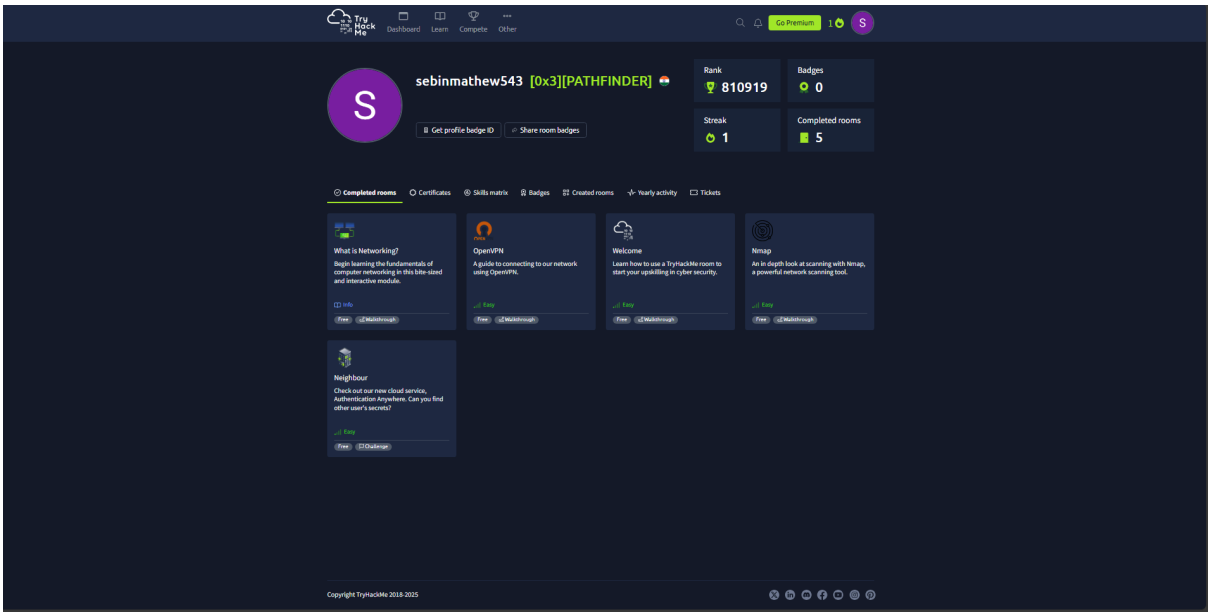
Used vv flag throughout for clearer output

Combined room tasks with additional script checks

Captured screenshots at each phase for documentation

Screenshots





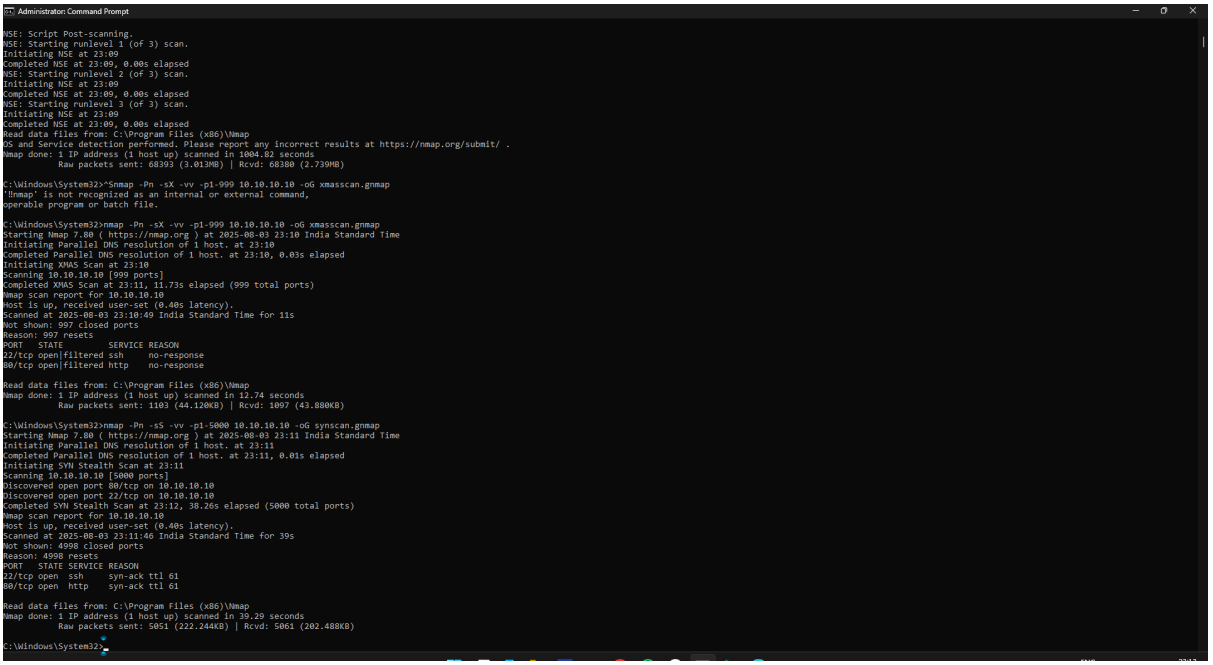
Administrator: Command Prompt

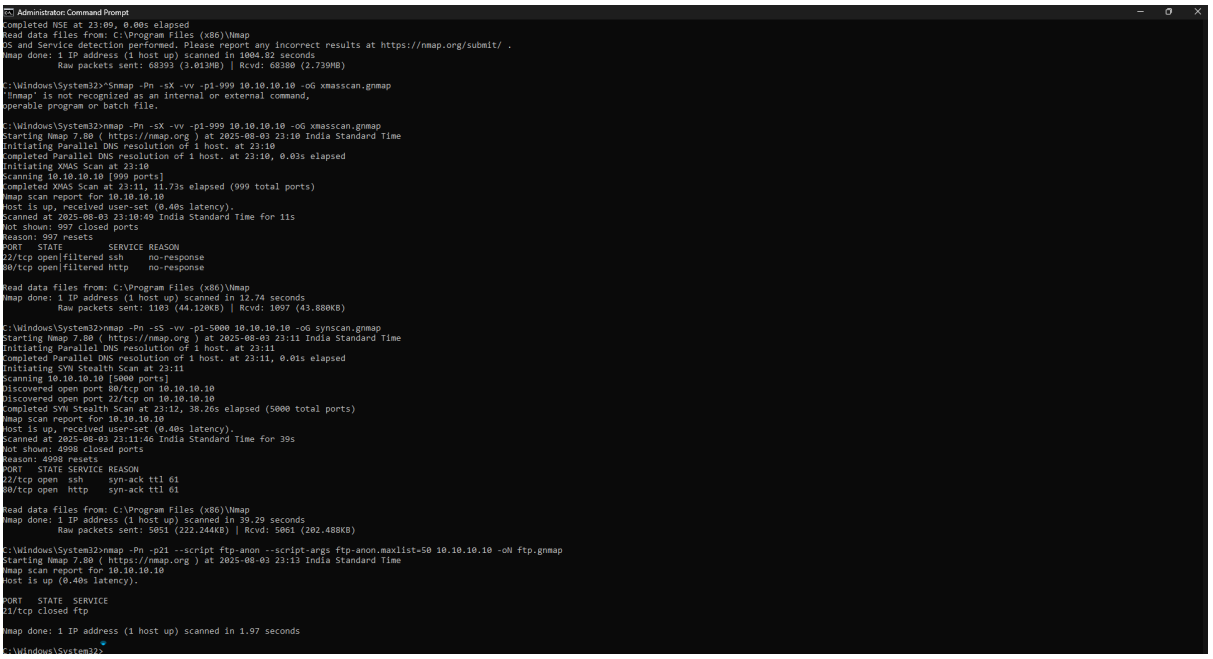
```
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:09
Completed NSE at 23:09, 1.68s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:09
Completed NSE at 23:09, 0.01s elapsed
Nmap scan report for 10.10.10.10
Host is up, received user-set (0.40s latency).
Scanned at 2025-08-03 22:52:45 India Standard Time for 999s
Not shown: 65533 closed ports
Reason: 65533 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ce:a9:12:79:0c:fc:0c:d2:7a:bf:e0:1a:99:b1:04:a8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC10a2M/GZ3JcBBw9rrkRZCZUYXgPUl1Sys6NtW0HpQYU8DYRuxYOhfHaljXk9Dqd+jVVHIkZM11/rxPz0GBxoS/rr/6lotAylGgn6AKDLPdefl5Az2xgi3cPDmR7RkTkKQUSap26pKGXhqWvSmMc+TVY5n5sSaEmMkv/ul+2l9eVc5bj9j7yeY+7ici3AI/VqR7mN
f20Nr098UO0hj99IIQu6aOT/fhJO8o5eA+2asw+rKzO5uha5uH80GOKnbKn9Jnk8eO4aULEuGESm95EMDVQiDbAhS+f8yL8QNGkOSAiwlj9Jj08LjwrEXlgi1tm4sqMlxZ2UCLvuoqvEX1Q1N
|   256 bb:7a:87:f4:b7:f6:25:05:83:5a:0a:18:0a:f7:29:48 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE8RIUi3UDknPjA9zIv8DrHqNtZZ4omDnZKYOGPHQAA4qj0pKP9F51OoxslRlYa7LoB17P54DzlYGnBkYvLpotI=
|   256 11:82:8b:67:a1:31:6d:fa:93:78:e2:47:f4:30:d5:c5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJmSdR6uKSjUL8wjOWyKJX471AKMioQRCDbTWHyDtmI9
80/tcp open  http    syn-ack ttl 61 Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Connected Successfully
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/3%OT=22%CT=1%CU=43424%PV=Y%DS=4%DC=T%G=Y%TM=688F9ECC
OS:%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=104%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(CI=Z%II=I)OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508S
OS:T11NW6%O5=M508ST11NW6%O6=M508ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5
OS:=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M508NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T
OS:=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=
OS:0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(
OS:R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT       ADDRESS
1   145.00 ms 10.4.0.1
2   ... 3
4   398.00 ms 10.10.10.10

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:09
Completed NSE at 23:09, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:09
Completed NSE at 23:09, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:09
Completed NSE at 23:09, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 1004.82 seconds
           Raw packets sent: 68393 (3.013MB) | Rcvd: 68380 (2.739MB)

C:\Windows\System32>^S
```

ENG IN 23:10 03-08-2025

Administrator: Command Prompt

```
|_http-title: Connected Successfully
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/3%OT=22%CT=1%CU=43424%PV=Y%DS=4%DC=T%G=Y%TM=688F9ECC
OS:%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=104%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(CI=Z%II=I)OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508S
OS:T11NW6%O5=M508ST11NW6%O6=M508ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5
OS:=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M508NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T
OS:=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=
OS:0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(
OS:R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT       ADDRESS
1   145.00 ms 10.4.0.1
2   ... 3
4   398.00 ms 10.10.10.10

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:09
Completed NSE at 23:09, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:09
Completed NSE at 23:09, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:09
Completed NSE at 23:09, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 1004.82 seconds
           Raw packets sent: 68393 (3.013MB) | Rcvd: 68380 (2.739MB)

C:\Windows\System32>^Snmap -Pn -sX -vv -p1-999 10.10.10.10 -oG xmasscan.gnmap
'‼nmap' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\System32>nmap -Pn -sX -vv -p1-999 10.10.10.10 -oG xmasscan.gnmap
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-03 23:10 India Standard Time
Initiating Parallel DNS resolution of 1 host. at 23:10
Completed Parallel DNS resolution of 1 host. at 23:10, 0.03s elapsed
Initiating XMAS Scan at 23:10
Scanning 10.10.10.10 [999 ports]
Completed XMAS Scan at 23:11, 11.73s elapsed (999 total ports)
Nmap scan report for 10.10.10.10
Host is up, received user-set (0.40s latency).
Scanned at 2025-08-03 23:10:49 India Standard Time for 11s
Not shown: 997 closed ports
Reason: 997 resets
PORT   STATE         SERVICE REASON
22/tcp open|filtered ssh     no-response
80/tcp open|filtered http    no-response

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 12.74 seconds
           Raw packets sent: 1103 (44.120KB) | Rcvd: 1097 (43.880KB)

C:\Windows\System32>
```





Conclusion

This room was a good refresher on Nmaps advanced features. By blending the room's tasks with some extra enumeration steps, I got a more complete picture of the target system. The handson practice with different scan types (especially firewall evasion techniques) was particularly useful.