Nmap Room Tryhackme 💻

1. Task 1

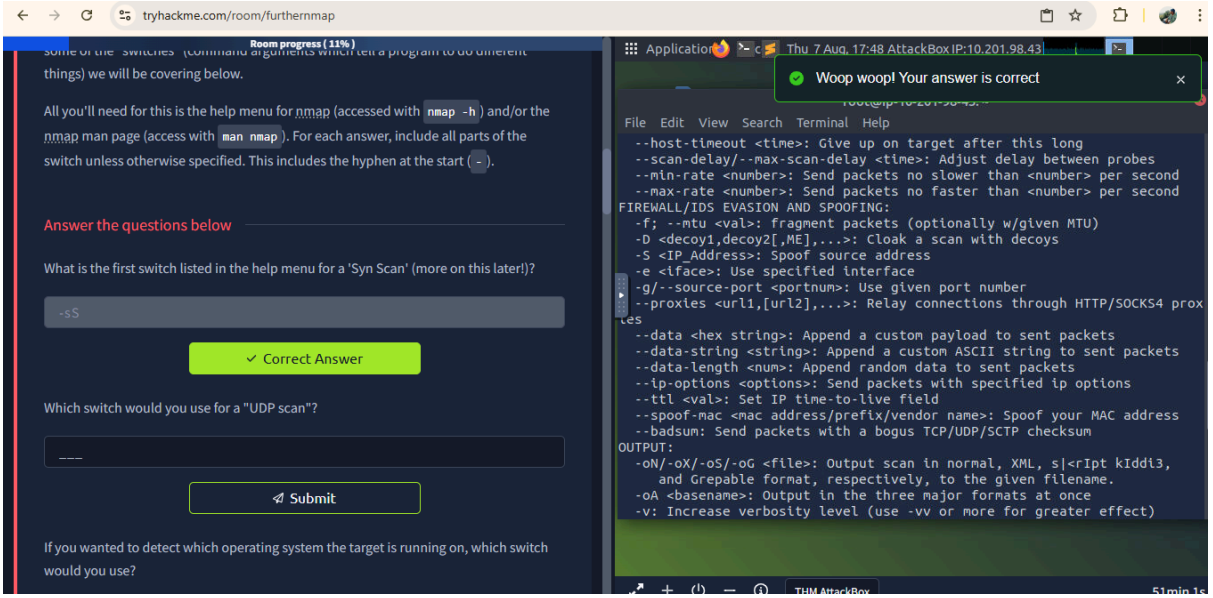
   Firstly, I deployed the machine.

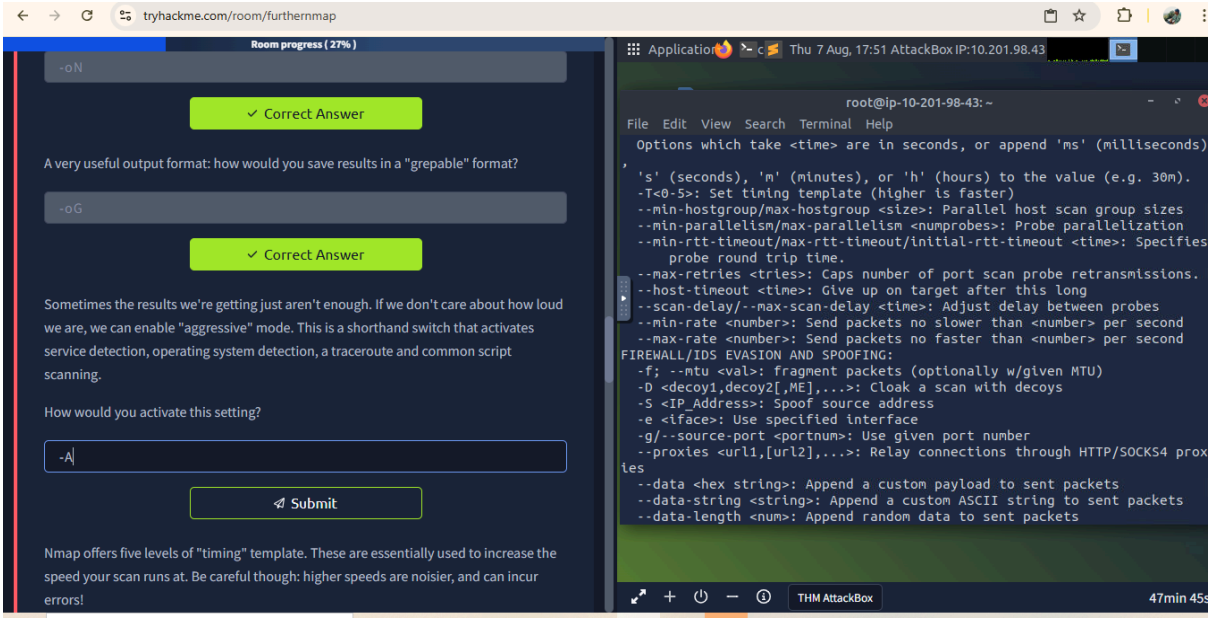
2. Task 2: **Introduction**

   Introduction on networking constructs and three questions on it.

3. Task 3: **Nmap Switches**

Nmap can be accessed by typing `nmap` into the terminal command line, followed by some of the "switches" (command arguments which tell a program to do different things)
help menu for nmap (accessed with `nmap -h`) and/or the nmap man page (access with `man nmap`).





4. Task 4: **Scan Types Overview**

There are three basic scan types:

- TCP Connect Scans (`-sT`)
- SYN “Half-open” Scans (`-sS`)

- UDP Scans (`-sU`)

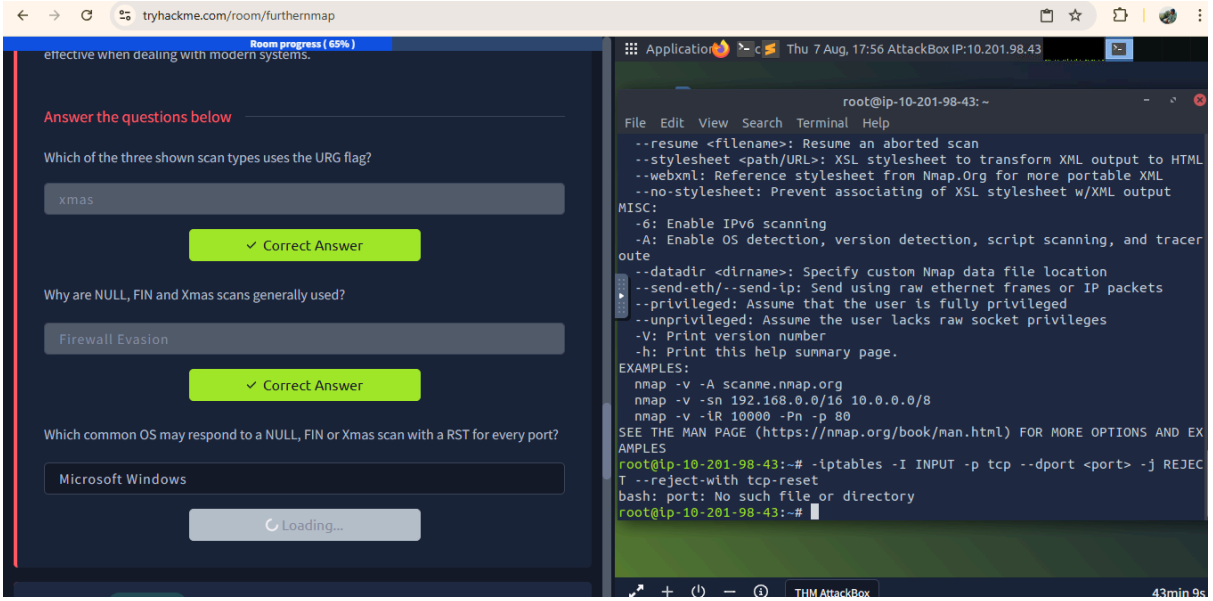
5. Task 5 : **Scan Types TCP Connect Scans**

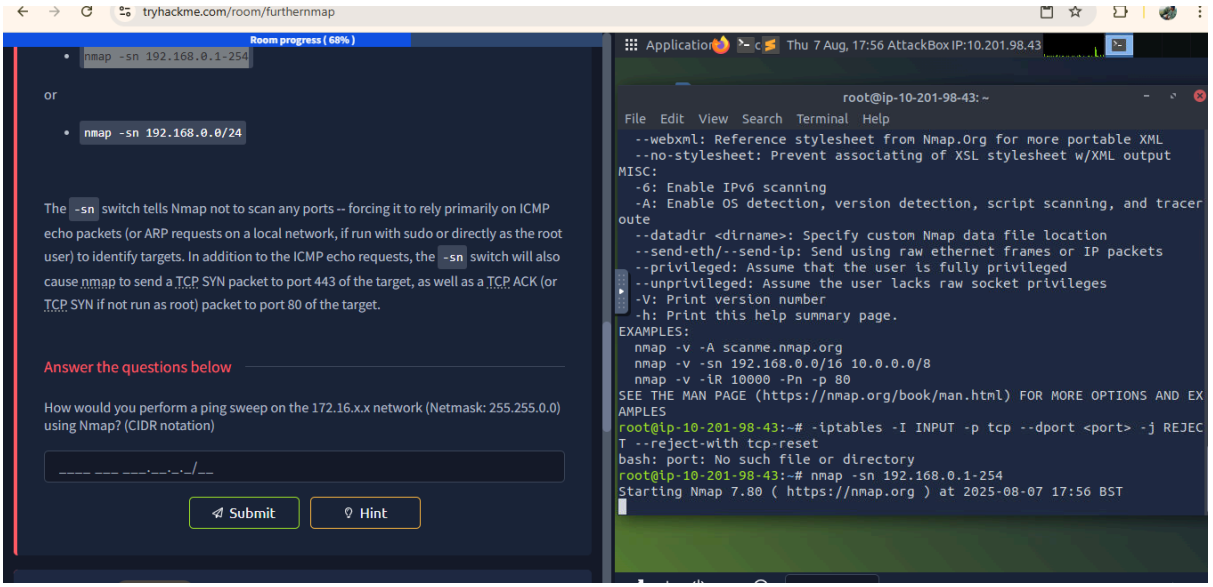
The three-way handshake consists of three stages. First the connecting terminal (our attacking machine, in this instance) sends a TCP request to the target server with the SYN flag set. The server then acknowledges this packet with a TCP response containing the SYN flag, as well as the ACK flag. Finally, our terminal completes the handshake by sending a TCP request with the ACK flag set.

6. Task 6: **Scan Types SYN Scans**

SYN scans are sometimes referred to as "*Half-open*" scans, or *"Stealth"* scans. Where TCP scans perform a full three-way handshake with the target, SYN scans sends back a RST TCP packet after receiving a SYN/ACK from the server.

7. Task 7: **Scan Types UDP Scans**





Task 8: **Scan Types NULL, FIN and Xmas**

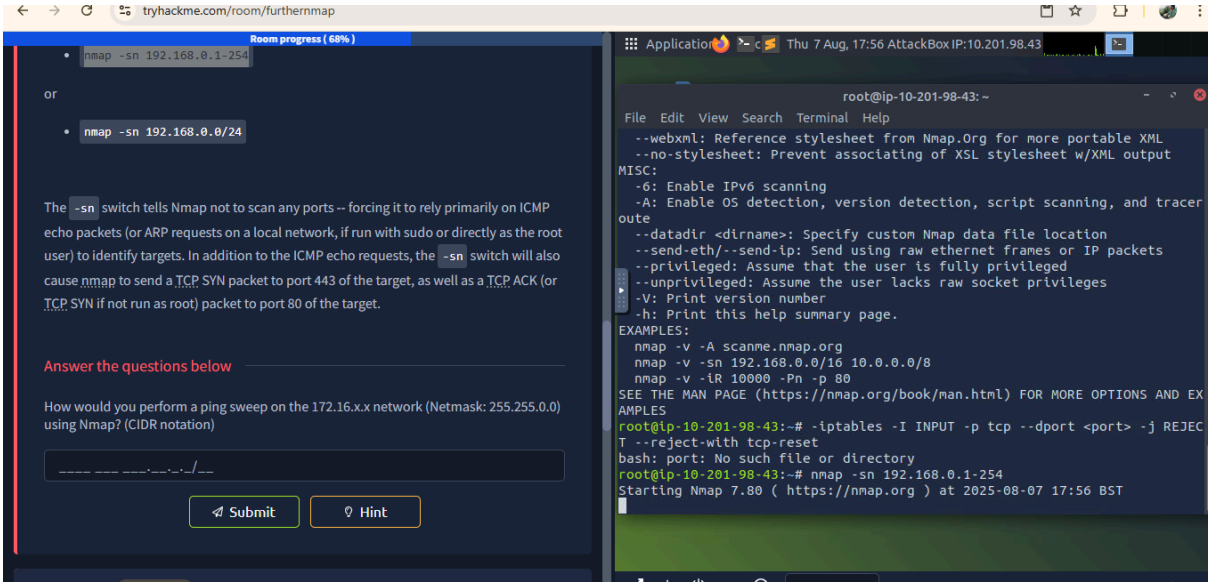
- FIN scans (`-sF`)

- NULL scans (`-sN`)

9. Task 9: **Scan Types ICMP Network Scanning**

Learned to perform ping sweep

nmap -sn

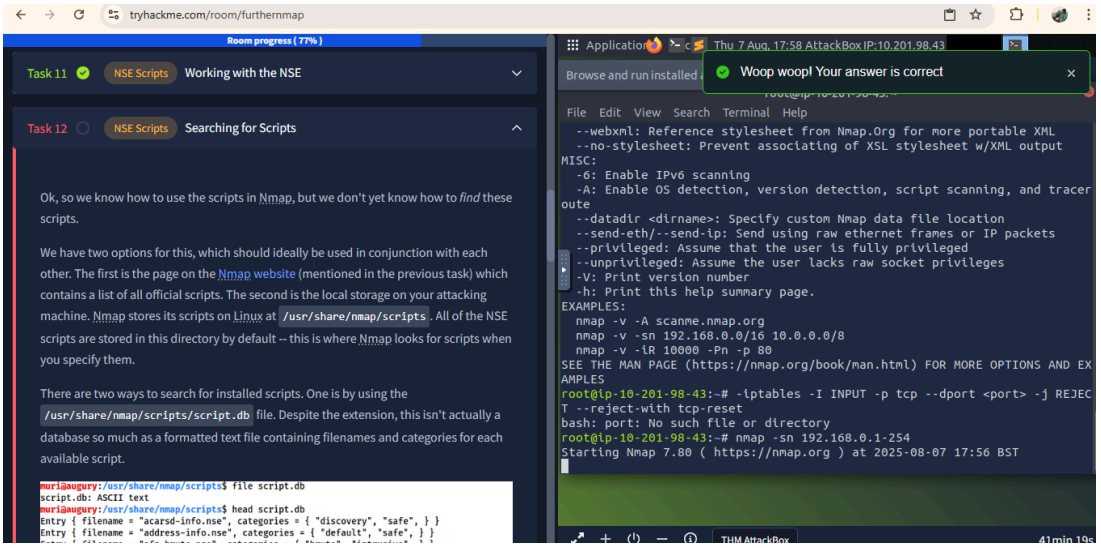


10. Task 10: **NSE Scripts Overview**

- `safe`:- Won't affect the target
- `intrusive`:- Not safe: likely to affect the target
- `vuln`:- Scan for vulnerabilities
- `exploit`:- Attempt to exploit a vulnerability

- `auth`:- Attempt to bypass authentication for running services (e.g. Log into an FTP server anonymously)
- `brute`:- Attempt to bruteforce credentials for running services
- `discovery`:- Attempt to query running services for further information about the network (e.g. query an SNMP server).

11. Task 11: **NSE Scripts**



- *smb-brute*

12. Task 3: **Firewall Evasion**

- `-f`:- Used to fragment the packets
- `--scan-delay <time>ms`:- used to add a delay between packets sent
- `--badsum`:- this is used to generate in invalid checksum for packets.

And lastly, there was a practical one too.

I completed the room successfully.

– Abhinav V R

https://tryhackme.com/p/lushfog