TryHackMe – Further Nmap Room Report

Name: Aswana Ashok
Room: Further Nmap
Date Completed: 🗓 Date

1. Introduction

The Further Nmap room is designed to explore advanced scanning techniques using Nmap, the Nmap Scripting Engine (NSE), and firewall evasion methods. The objective of this activity was to:

- Gain hands-on experience with multiple scan types
- Understand NSE scripts and their applications
- Learn firewall evasion strategies
- Apply all skills in a final practical task

2. Personal Learning Journey

The lab provided a largely positive learning experience despite some challenges. The introduction to novel scan types like NULL, FIN, and Xmas scans expanded knowledge of network security. However, challenges included unintuitive command syntax, difficulty anticipating output, and technical hurdles like AttackBox timeouts and slow scans. Moments of clarity and straightforward tasks boosted confidence, while leveraging external resources like ChatGPT helped clarify complex concepts. The task-based structure of the lab fostered motivation through consistent progress.

3. Task-by-Task Documentation

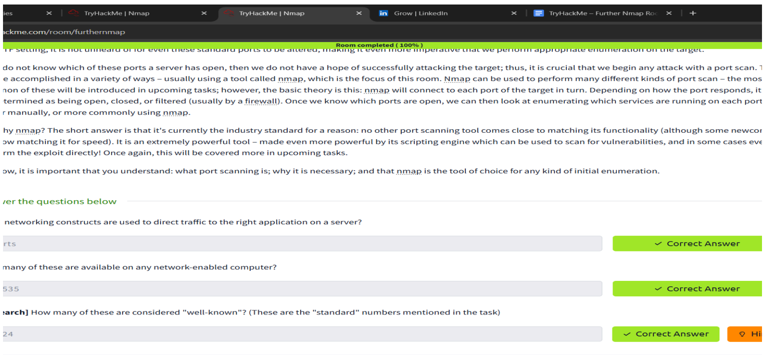
For each task, I’ve listed the goal, command(s) used, observations, and screenshots.

Task 1 – Deploy

Goal: Start the AttackBox and deploy the target machine.
Steps: Click "Start Machine" and note down the target IP.
Observation: Target is now reachable.

Task 2 – Introduction

Goal: Read room overview and understand objectives.
Observation: The room focuses on advanced Nmap functionalities and bypass techniques.



TF setting, it is not unheard of for even these standard ports to be altered, making it even more imperative that we perform appropriate enumeration on the target.

do not know which of these ports a server has open, then we do not have a hope of successfully attacking the target; thus, it is crucial that we begin any attack with a port scan. T e accomplished in a variety of ways – usually using a tool called nmap, which is the focus of this room. Nmap can be used to perform many different kinds of port scan – the mos non of these will be introduced in upcoming tasks; however, the basic theory is this: nmap will connect to each port of the target in turn. Depending on how the port responds, it termined as being open, closed, or filtered (usually by a firewall). Once we know which ports are open, we can then look at enumerating which services are running on each port r manually, or more commonly using nmap.

hy nmap? The short answer is that it's currently the industry standard for a reason: no other port scanning tool comes close to matching its functionality (although some newcor ow matching it for speed). It is an extremely powerful tool – made even more powerful by its scripting engine which can be used to scan for vulnerabilities, and in some cases eve rm the exploit directly! Once again, this will be covered more in upcoming tasks.

ow, it is important that you understand: what port scanning is; why it is necessary; and that nmap is the tool of choice for any kind of initial enumeration.

ver the questions below

networking constructs are used to direct traffic to the right application on a server?

rts

many of these are available on any network-enabled computer?

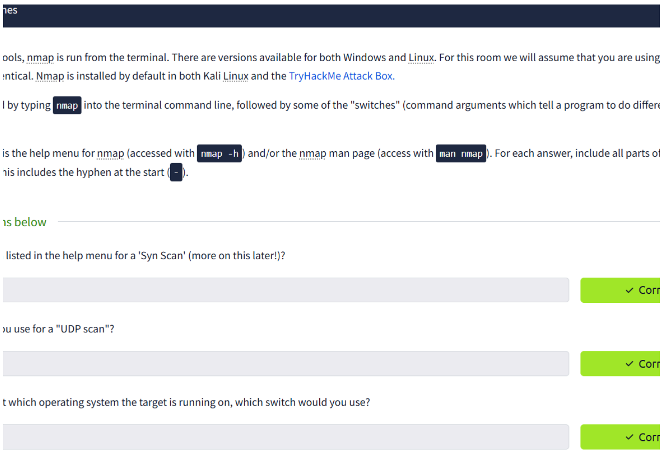
535

earch] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

24

Task 3 – Nmap Switches

Goal: Learn about key Nmap switches.
Command: `nmap --help`
Observation: Identified useful switches like `-p`, `-A`, `-O`, `-Pn`.



ools, nmap is run from the terminal. There are versions available for both Windows and Linux. For this room we will assume that you are using entical. Nmap is installed by default in both Kali Linux and the TryHackMe Attack Box.

l by typing `nmap` into the terminal command line, followed by some of the "switches" (command arguments which tell a program to do differe

is the help menu for nmap (accessed with `nmap -h`) and/or the nmap man page (access with `man nmap`). For each answer, include all parts of his includes the hyphen at the start (`-`).

ns below

listed in the help menu for a 'Syn Scan' (more on this later!)?

ou use for a "UDP scan"?

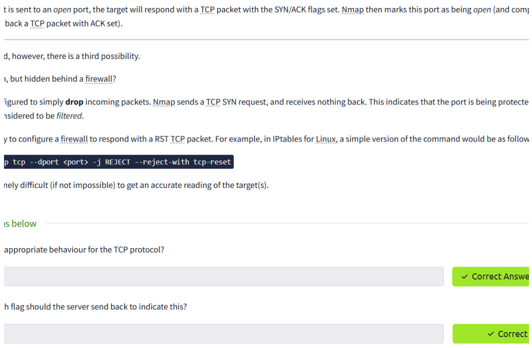
t which operating system the target is running on, which switch would you use?

Task 4 – Scan Types Overview

Goal: Understand the difference between various scan types.
Observation: TCP Connect, SYN, UDP, NULL, FIN, Xmas, and ICMP scans all have unique use cases.

Task 5 – TCP Connect Scan

Command: `nmap -sT <TARGET_IP>`
Observation: Detected open ports with a full TCP handshake.



t is sent to an *open* port, the target will respond with a TCP packet with the SYN/ACK flags set. Nmap then marks this port as being *open* (and comp
back a TCP packet with ACK set).

d, however, there is a third possibility.

ı, but hidden behind a firewall?

ïgured to simply **drop** incoming packets. Nmap sends a TCP SYN request, and receives nothing back. This indicates that the port is being protecte
ısidered to be *filtered*.

y to configure a firewall to respond with a RST TCP packet. For example, in IPtables for Linux, a simple version of the command would be as follow

```
p tcp --dport <port> -j REJECT --reject-with tcp-reset
```

nely difficult (if not impossible) to get an accurate reading of the target(s).

ıs below

appropriate behaviour for the TCP protocol?

h flag should the server send back to indicate this?

Task 6 – SYN Scan

Command: `nmap -sS <TARGET_IP>`
Observation: Faster and stealthier than TCP Connect, identified similar open ports.

Task 7 – UDP Scan

Command: `nmap -sU <TARGET_IP>`
Observation: Found UDP services; scan was slower than TCP scans.

Task 8 – NULL, FIN, Xmas Scans

Commands:

```
 nmap -sN <TARGET_IP>
 nmap -sF <TARGET_IP>
nmap -sX <TARGET_IP>
```

Observation: Used for firewall evasion; some ports showed as filtered.

Task 9 – ICMP Network Scanning

Command: `nmap -sn <TARGET_SUBNET>`
Observation: Identified live hosts in the network.

Task 10 – NSE Scripts Overview

Command: `ls /usr/share/nmap/scripts`
Observation: NSE scripts can detect vulnerabilities, brute force logins, and gather more info.

Task 11 – Working with NSE

Command: `nmap --script <script-name> <TARGET_IP>`
Observation: Ran a script to gather specific service information.

Task 12 – Searching for Scripts

Command: `locate *.nse | grep ftp`
Observation: Found NSE scripts related to FTP services.

Task 13 – Firewall Evasion

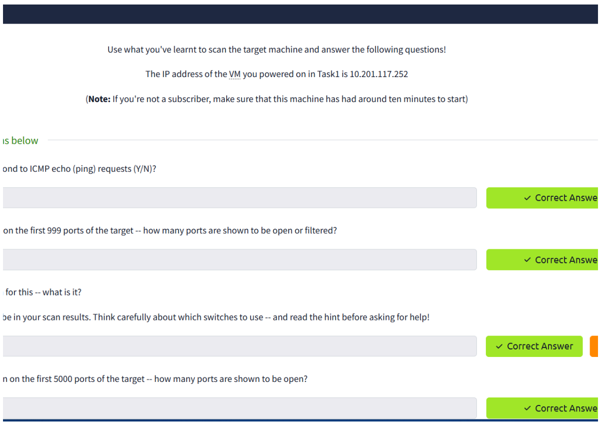
Commands:

```
nmap -f <TARGET_IP>
nmap --data-length 50 <TARGET_IP>
nmap -D RND:10 <TARGET_IP>
```

Observation: These methods fragmented packets, added random data, and used decoys to avoid detection.

Task 14 – Practical

Command: `nmap -sS -A -p- --script vuln <TARGET_IP>`
Observation: Combined multiple techniques to get a complete enumeration.



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 10.201.117.252

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

ıs below

ond to ICMP echo (ping) requests (Y/N)?

✓ Correct Answe

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

✓ Correct Answe

ı for this -- what is it?

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

✓ Correct Answer

n on the first 5000 ports of the target -- how many ports are shown to be open?

✓ Correct Answe

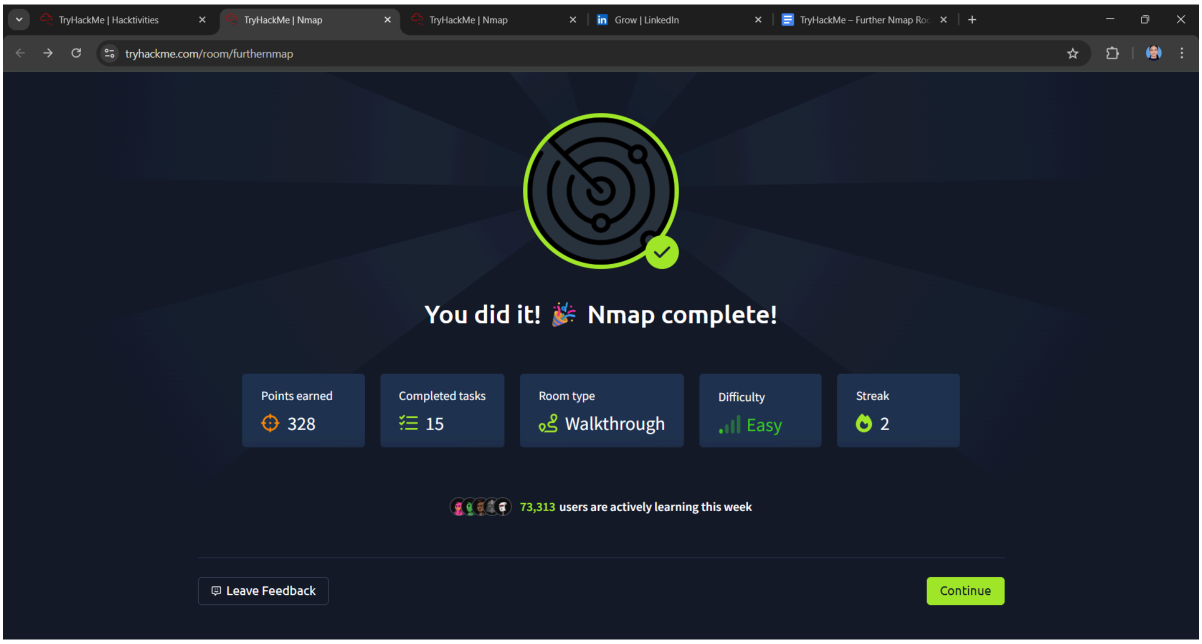
15. Conclusion

The Further Nmap room helped me:

- Understand advanced scan types and when to use them
- Gain experience with NSE scripts for targeted enumeration
- Learn firewall evasion tactics
- Develop problem-solving skills when scans failed or timed out

4. Final Reflection

This exercise was a mix of technical challenge and personal growth. Even when scans failed or the AttackBox timed out, I learned the importance of patience, troubleshooting, and using multiple resources for clarification. By the end, I felt more confident using Nmap beyond just basic scans.



You did it! 🎉 Nmap complete!

Points earned 328

Completed tasks 15

Room type Walkthrough

Difficulty Easy

Streak 2

73,313 users are actively learning this week