Try Hack Me Room – Network Scanning Report

Objective: To analyze open ports and service behavior on a target system using various Nmap scanning techniques and Wireshark packet captures. This is essential for penetration testing and vulnerability assessments.

Name: Linto Baby

Link to the room:https://tryhackme.com/room/furthernmap

Summary of Activities

This report summarizes the completion of the "Nmap" room on TryHackMe, a walkthrough that covered the fundamental and advanced features of the Nmap network scanning tool. The tasks involved deploying a virtual machine and using Nmap to perform various scans.

Key Learning Outcomes

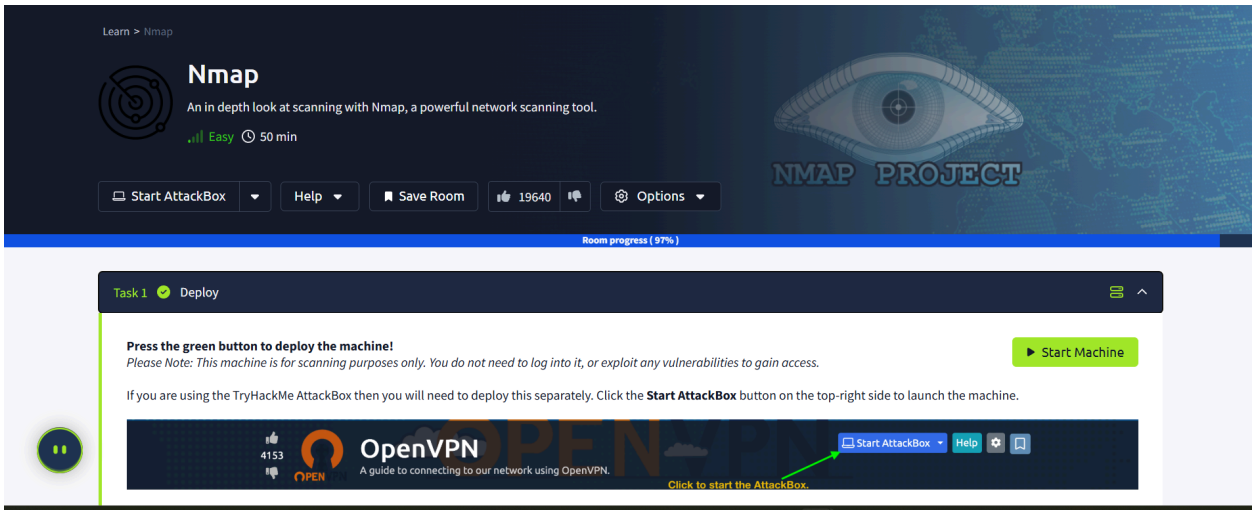
- **Nmap Fundamentals:** Nmap is the industry-standard tool for port scanning and is a powerful tool for initial network enumeration. It's run from the terminal and uses "switches" (command arguments) to perform different functions.
- **Nmap Switches:** I learned and applied various Nmap switches, including:
    - `-sS` for a "Syn Scan".
    - `-sU` for a "UDP scan".
    - `-sV` for version detection.
    - `-p` to specify which ports to scan.
- **Scan Types:** I explored different types of port scans.
    - **TCP Connect Scans (`-sT`)**.
    - **SYN "Half-open" Scans (`-sS`)**.
    - **UDP Scans (`-sU`)**.
    - **Stealthier Scans:** Covered NULL, FIN, and Xmas scans, which are primarily used for firewall evasion. These scans can bypass firewalls configured to drop incoming TCP packets with the SYN flag set by sending requests without that flag.
- **Network Scripting Engine (NSE):** The NSE makes Nmap a more powerful tool for vulnerability scanning and direct exploitation. Nmap stores its scripts on Linux in the `/usr/share/nmap/scripts` directory.

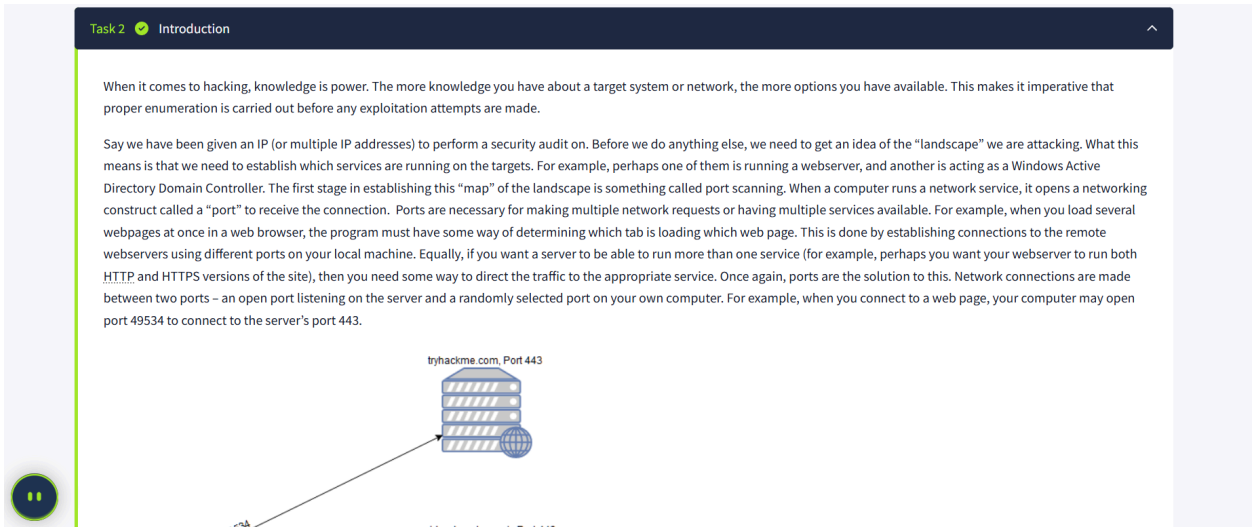
- **Firewall Evasion:** I explored techniques to bypass common firewall configurations, such as the default Windows firewall blocking all ICMP packets. Nmap provides options to skip the host discovery phase, treating the target as alive to bypass ICMP blocks.

Completion Status

- **Points Earned:** 328.
- **Completed Tasks:** 15.
- **Room Type:** Walkthrough.
- **Difficulty:** Easy.
- **Streak:** 1.

Screenshots





Task 3 Nmap Switches

Like most pentesting tools, 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 Linux; however, the switches should be identical. Nmap is installed by default in both Kali Linux and the TryHackMe Attack Box.

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) we will be covering below.

All you'll need for this 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 the switch unless otherwise specified. This includes the hyphen at the start (`-`).

Answer the questions below

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

`-sS` ✓ Correct Answer

Which switch would you use for a "UDP scan"?

`-sU` ✓ Correct Answer

If you wanted to detect which operating system the target is running on, which switch would you use?

Task 4 Scan Types Overview

When port scanning with Nmap, there are three basic scan types. These are:

- TCP Connect Scans (`-sT`)
- SYN "Half-open" Scans (`-sS`)
- UDP Scans (`-sU`)

Additionally there are several less common port scan types, some of which we will also cover (albeit in less detail). These are:

- TCP Null Scans (`-sN`)
- TCP FIN Scans (`-sF`)
- TCP Xmas Scans (`-sX`)

Most of these (with the exception of UDP scans) are used for very similar purposes, however, the way that they work differs between each scan. This means that, whilst one of the first three scans are likely to be your go-to in most situations, it's worth bearing in mind that other scan types exist.

In terms of network scanning, we will also look briefly at ICMP (or "ping") scanning.

Answer the questions below

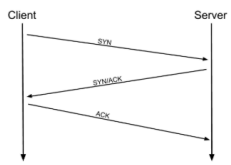
Read the Scan Types Introduction.

No answer needed ✓ Correct Answer

Task 5 Scan Types TCP Connect Scans

To understand TCP Connect scans (`-sT`), it's important that you're comfortable with the *TCP three-way handshake*. If this term is new to you then completing Introductory Networking before continuing would be advisable.

As a brief recap, 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.



No.	Time	Source	Destination	Protocol	Length	Info
21	2.009477639	192.168.1.142	192.168.1.141	TCP	74	60516 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2310196 TSecr=0 WS=128
22	2.009847598	192.168.1.141	192.168.1.142	TCP	66	80 → 60516 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
23	2.009886244	192.168.1.142	192.168.1.141	TCP	54	60516 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0

This is one of the fundamental principles of TCP/IP networking, but how does it relate to Nmap?

Well, as the name suggests, a TCP Connect scan works by performing the three-way handshake with each target port in turn. In other words, Nmap tries to connect to each specified TCP

Task 12 NSE Scripts Searching for Scripts

Ok, so we know how to use the scripts in Nmap, but we don't yet know how to *find* these scripts.

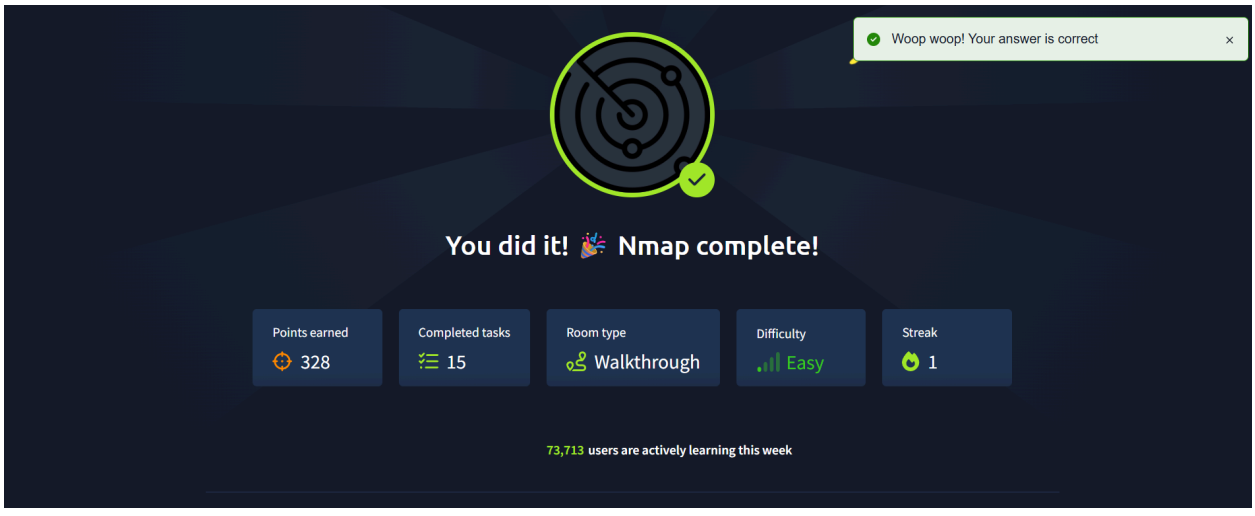
We have two options for this, which should ideally be used in conjunction with each other. The first is the page on the Nmap website (mentioned in the previous task) which contains a list of all official scripts. The second is the local storage on your attacking machine. Nmap stores its scripts on Linux at `/usr/share/nmap/scripts`. All of the NSE scripts are stored in this directory by default -- this is where Nmap looks for scripts when you specify them.

There are two ways to search for installed scripts. One is by using the `/usr/share/nmap/scripts/script.db` file. Despite the extension, this isn't actually a database so much as a formatted text file containing filenames and categories for each available script.

```
muri@augury:/usr/share/nmap/scripts$ file script.db
script.db: ASCII text
muri@augury:/usr/share/nmap/scripts$ head script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
```

Nmap uses this file to keep track of (and utilise) scripts for the scripting engine; however, we can also *grep* through it to look for scripts. For example: `grep "ftp"`

- Task 5 Scan Types TCP Connect Scans
- Task 6 Scan Types SYN Scans
- Task 7 Scan Types UDP Scans
- Task 8 Scan Types NULL, FIN and Xmas
- Task 9 Scan Types ICMP Network Scanning
- Task 10 NSE Scripts Overview
- Task 11 NSE Scripts Working with the NSE
- Task 12 NSE Scripts Searching for Scripts
- Task 13 Firewall Evasion
- Task 14 Practical



Conclusion

This lab successfully demonstrated the use of Nmap for detailed network enumeration. The exercise provided hands-on experience with various scanning techniques, command-line switches, and an introduction to Nmap's scripting engine and firewall evasion capabilities. This knowledge is fundamental for further penetration testing and vulnerability assessment tasks.