Further Nmap — TryHackMe

Abhimanyu S

Room link: https://tryhackme.com/room/furthernmap

Summary

The *Further Nmap* TryHackMe room was completed to practice and understand advanced scanning techniques in Nmap. The exercise involved performing various types of scans, including quick top-port scans, full TCP scans, UDP scans, service and version detection, OS fingerprinting, and running Nmap Scripting Engine (NSE) scripts for vulnerability detection. Each scan was conducted against the provided target machine, and results were saved using Nmap's output options. Screenshots and explanations were documented at every step to demonstrate the commands used, the reasoning behind them, and the findings obtained. This process improved practical skills in using Nmap for reconnaissance, enumeration, and reporting in a cybersecurity workflow.

TryHackMe — Further Nmap Room Tasks

The *Further Nmap* room was completed to develop advanced scanning and enumeration skills using Nmap. The process began by deploying the room's machine and noting the assigned target IP address, which served as the focus for all subsequent scans. Using nmap -h and the Nmap manual (man nmap), the essential switches required for different scan types and output formats were identified. This allowed the execution of SYN scans (-sS), UDP scans (-sU), service/version detection (-sV), OS fingerprinting (-O), aggressive scanning (-A), and saving results in multiple formats (-oA).

The enumeration process started with a **quick top-100 port scan** using:

```
sudo nmap -Pn --top-ports 100 -sS -sV -T4 -oN quick-top100.txt <IP>
```

This quickly revealed common open ports and their associated services, allowing an initial understanding of the system. To ensure complete coverage, a **full TCP port sweep** was then performed with:

```
sudo nmap -Pn -p- -sS -T4 -oA scan-allports <IP>
```

This scanned all 65,535 TCP ports, identifying every open service. The number of open ports was calculated using:

```
grep '/open/' scan-allports.gnmap | wc -l
```

ensuring precise answers to the room's questions.

Once all open ports were known, **detailed enumeration** was carried out using:

```
sudo nmap -Pn -sS -sV -O --script=default -oN scan-services-os.txt <IP>
```

and, where needed, the shorthand aggressive mode:

```
sudo nmap -Pn -A -p <open-ports> -oN scan-aggr.txt <IP>
```

This provided service versions, OS guesses, traceroute information, and the results of default NSE scripts, enriching the understanding of the target.

If required by the task, a **UDP scan** of the top 50 ports was performed:

```
sudo nmap -Pn -sU --top-ports 50 -sV -oN scan-udp.txt <IP>
```

Since UDP scanning is slow, limiting to the most common ports provided efficiency while still detecting important UDP services such as SNMP or DNS.

For vulnerability detection, the NSE vuln category was run against discovered services:

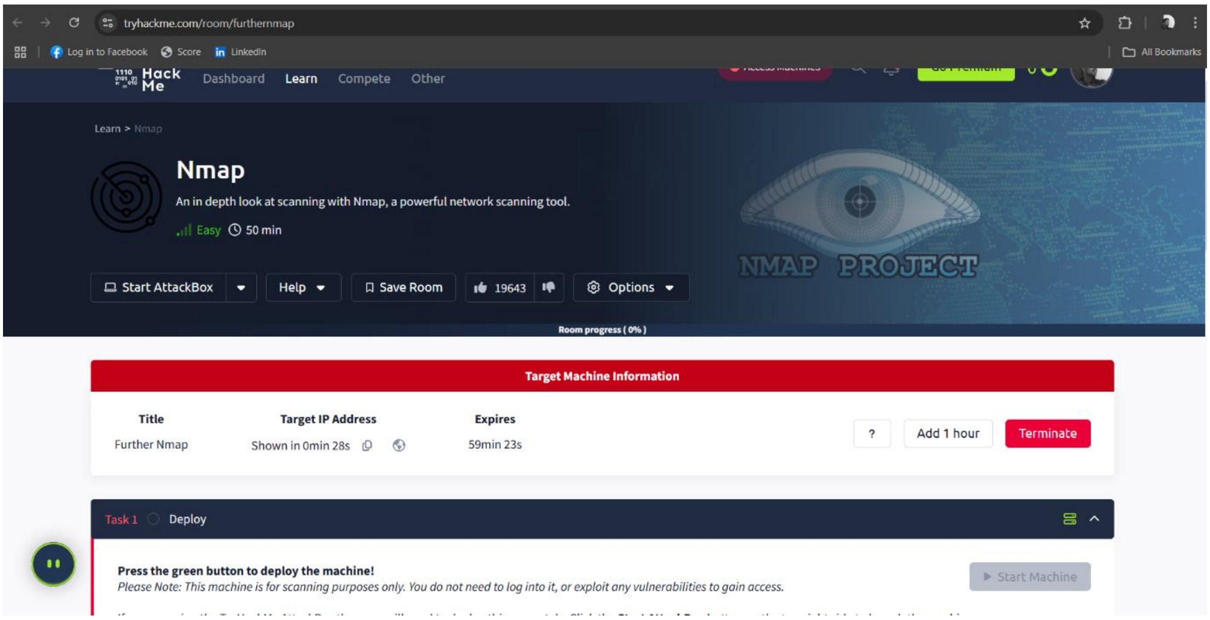
```
sudo nmap -Pn -sV --script=vuln -p <open-ports> -oN vuln-scan.txt <IP>
```

This highlighted potential security flaws like outdated SMB services vulnerable to MS17-010 or misconfigured HTTP servers.

Throughout the process, **screenshots were taken** at key stages: viewing Nmap help, running quick scans, capturing full-port outputs, showing service and OS detection, UDP results, and vulnerability findings. All output files (.nmap, .gnmap, .xml, and .txt) were saved for reporting and verification.

By completing the room, a comprehensive skillset in advanced Nmap usage was reinforced — from identifying relevant switches to executing targeted enumeration and vulnerability assessments. The workflow demonstrated the importance of starting with quick reconnaissance, moving to exhaustive scanning, and finishing with detailed script-based analysis. These steps mirror real-world penetration testing and network auditing methodologies, making the exercise both educational and practical.

Screenshots



Nmap

An in depth look at scanning with Nmap, a powerful network scanning tool.

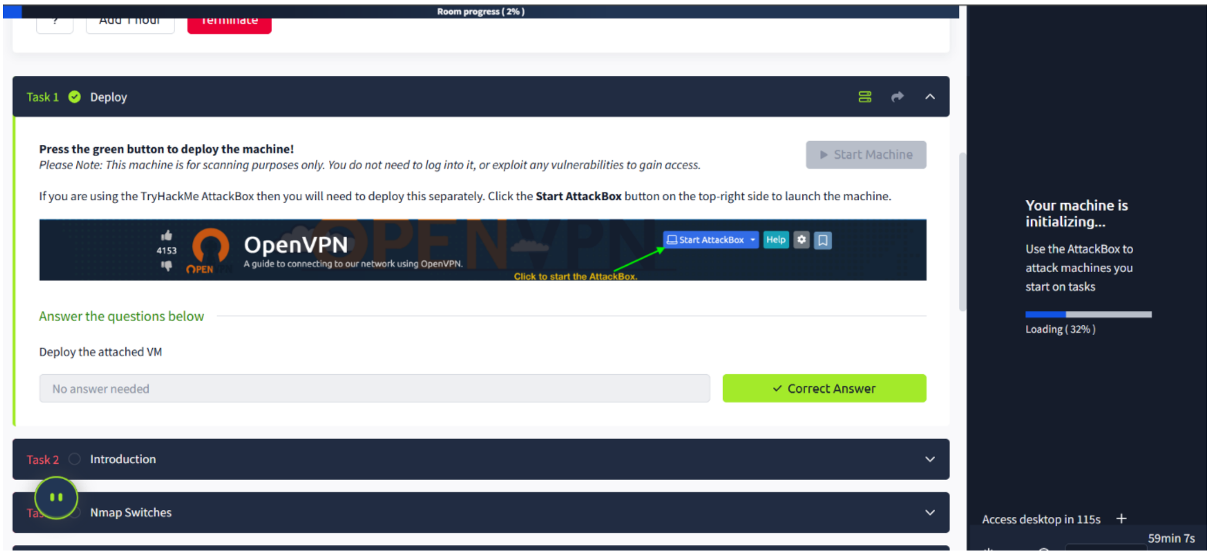
Easy 50 min

Target Machine Information

Title	Target IP Address	Expires
Further Nmap	Shown in 0min 28s	59min 23s

Task 1 Deploy

Press the green button to deploy the machine!
Please Note: This machine is for scanning purposes only. You do not need to log into it, or exploit any vulnerabilities to gain access.


Room progress (2%)
?
Add 1 hour
Terminate
▶ Start Machine
4153
OpenVPN
A guide to connecting to our network using OpenVPN.
Start AttackBox
Help
Click to start the AttackBox.
Your machine is initializing...
Use the AttackBox to attack machines you start on tasks
Loading (32%)
Access desktop in 115s
59min 7s

Task 1 ✓ Deploy

Press the green button to deploy the machine!
Please Note: This machine is for scanning purposes only. You do not need to log into it, or exploit any vulnerabilities to gain access.

If you are using the TryHackMe AttackBox then you will need to deploy this separately. Click the **Start AttackBox** button on the top-right side to launch the machine.

Answer the questions below

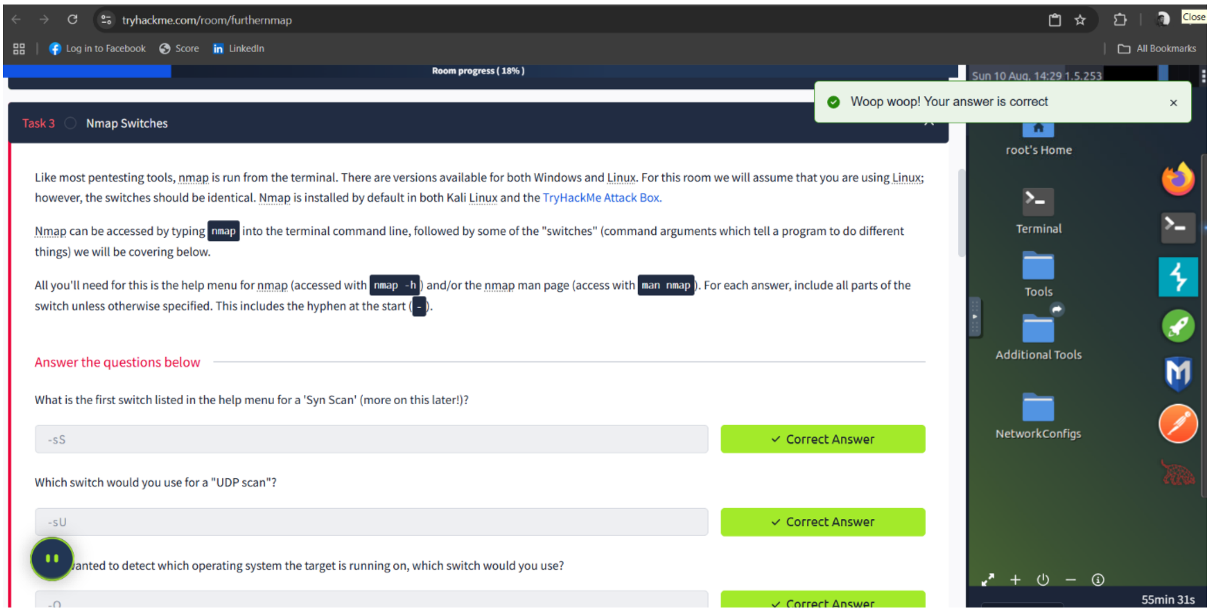
Deploy the attached VM

No answer needed

✓ Correct Answer

Task 2 ○ Introduction

Task 3 ○ Nmap Switches



Woop woop! Your answer is correct

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"?

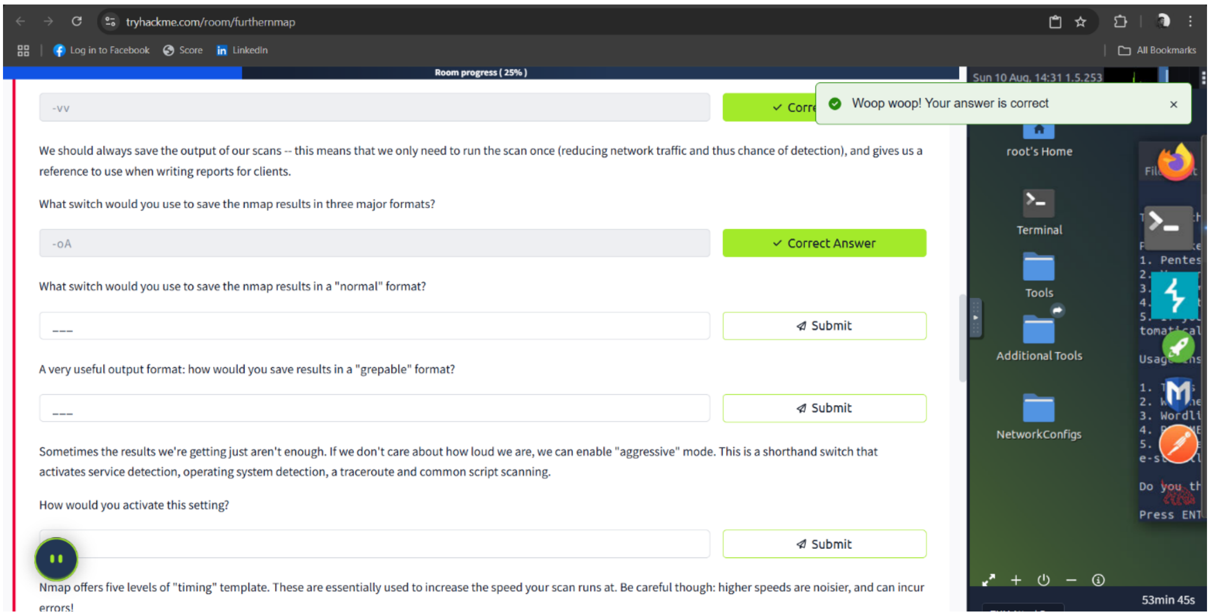
-sU

✓ Correct Answer

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

-O

✓ Correct Answer



Woop woop! Your answer is correct

-vv

✓ Corr

We should always save the output of our scans -- this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients.

What switch would you use to save the nmap results in three major formats?

-oA

✓ Correct Answer

What switch would you use to save the nmap results in a "normal" format?

___

Submit

A very useful output format: how would you save results in a "grepable" format?

___

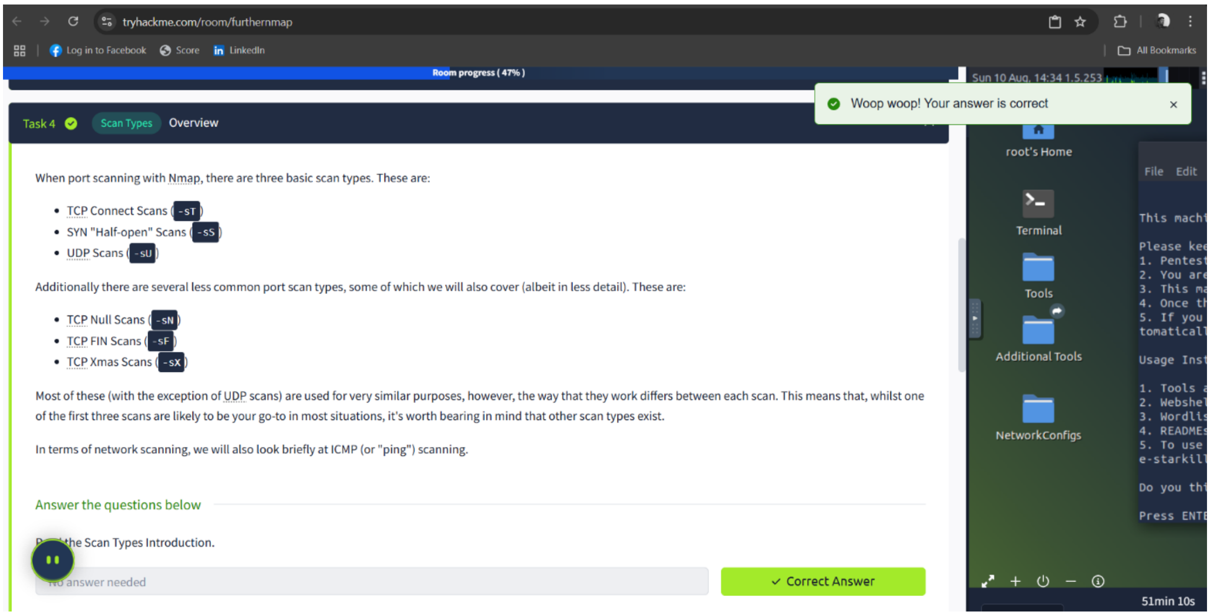
Submit

Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning.

How would you activate this setting?

Submit

Nmap offers five levels of "timing" template. These are essentially used to increase the speed your scan runs at. Be careful though: higher speeds are noisier, and can incur errors!



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.

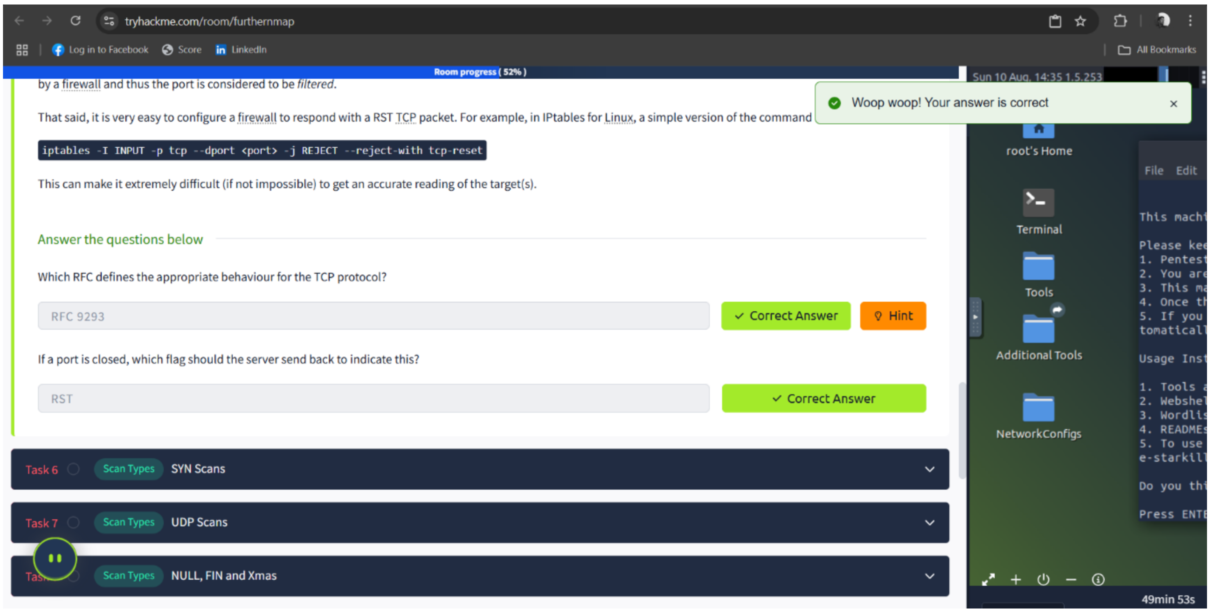
In terms of network scanning, we will also look briefly at ICMP (or "ping") scanning.

Answer the questions below

Read the Scan Types Introduction.

No answer needed ✓ Correct Answer

```
This mach
Please kee
1. Pentest
2. You are
3. This ma
4. Once th
5. If you
tomaticall
Usage Inst
1. Tools a
2. Webshel
3. Wordlis
4. READMEs
5. To use
e-starkill
Do you thi
Press ENTE
```



by a firewall and thus the port is considered to be *filtered*.

That said, it is very easy to configure a firewall to respond with a RST TCP packet. For example, in IPtables for Linux, a simple version of the command

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

This can make it extremely difficult (if not impossible) to get an accurate reading of the target(s).

Answer the questions below

Which RFC defines the appropriate behaviour for the TCP protocol?

RFC 9293 ✓ Correct Answer Hint

If a port is closed, which flag should the server send back to indicate this?

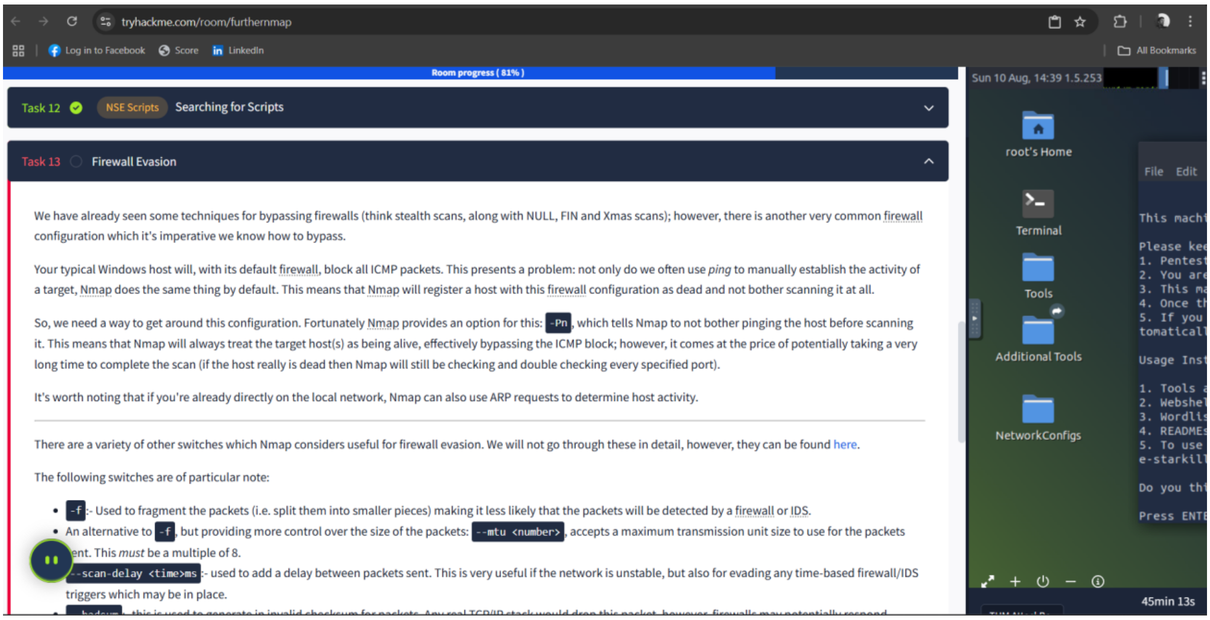
RST ✓ Correct Answer

Task 6 Scan Types SYN Scans

Task 7 Scan Types UDP Scans

Tas Scan Types NULL, FIN and Xmas

```
This mach
Please kee
1. Pentest
2. You are
3. This ma
4. Once th
5. If you
tomaticall
Usage Inst
1. Tools a
2. Webshel
3. Wordlis
4. READMEs
5. To use
e-starkill
Do you thi
Press ENTE
```



Task 12 ✓ NSE Scripts Searching for Scripts

Task 13 ○ Firewall Evasion

We have already seen some techniques for bypassing firewalls (think stealth scans, along with NULL, FIN and Xmas scans); however, there is another very common firewall configuration which it's imperative we know how to bypass.

Your typical Windows host will, with its default firewall, block all ICMP packets. This presents a problem: not only do we often use *ping* to manually establish the activity of a target, Nmap does the same thing by default. This means that Nmap will register a host with this firewall configuration as dead and not bother scanning it at all.

So, we need a way to get around this configuration. Fortunately Nmap provides an option for this: `-Pn`, which tells Nmap to not bother pinging the host before scanning it. This means that Nmap will always treat the target host(s) as being alive, effectively bypassing the ICMP block; however, it comes at the price of potentially taking a very long time to complete the scan (if the host really is dead then Nmap will still be checking and double checking every specified port).

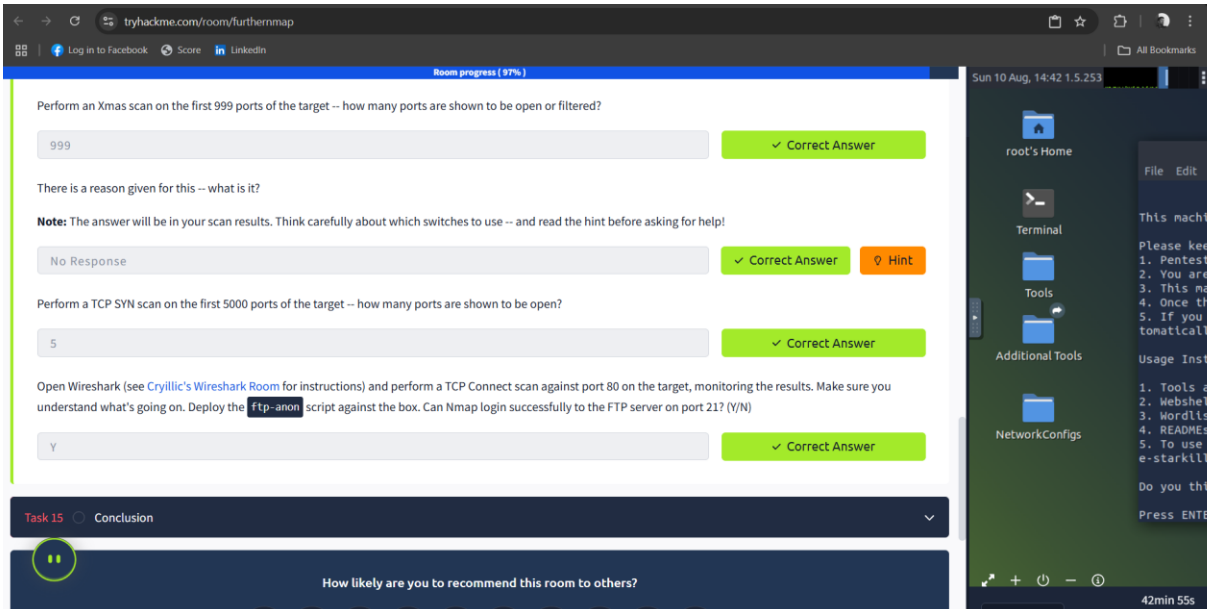
It's worth noting that if you're already directly on the local network, Nmap can also use ARP requests to determine host activity.

There are a variety of other switches which Nmap considers useful for firewall evasion. We will not go through these in detail, however, they can be found here.

The following switches are of particular note:

- `-f`:- Used to fragment the packets (i.e. split them into smaller pieces) making it less likely that the packets will be detected by a firewall or IDS.
- An alternative to `-f`, but providing more control over the size of the packets: `--mtu <number>`, accepts a maximum transmission unit size to use for the packets ent. This *must* be a multiple of 8.
- `--scan-delay <time>ms`:- used to add a delay between packets sent. This is very useful if the network is unstable, but also for evading any time-based firewall/IDS triggers which may be in place.
- `--badsum`:- this is used to generate in invalid checksum for packets. Any real TCP/IP stack would drop this packet, however, firewalls may potentially respond

```
This mach
Please kee
1. Pentest
2. You are
3. This ma
4. Once th
5. If you
tomaticall
Usage Inst
1. Tools a
2. Webshe
3. Wordlis
4. README
5. To use
e-starkill
Do you th
Press ENTE
```



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

999 ✓ Correct Answer

There is a reason given for this -- what is it?

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

No Response ✓ Correct Answer Hint

Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

5 ✓ Correct Answer

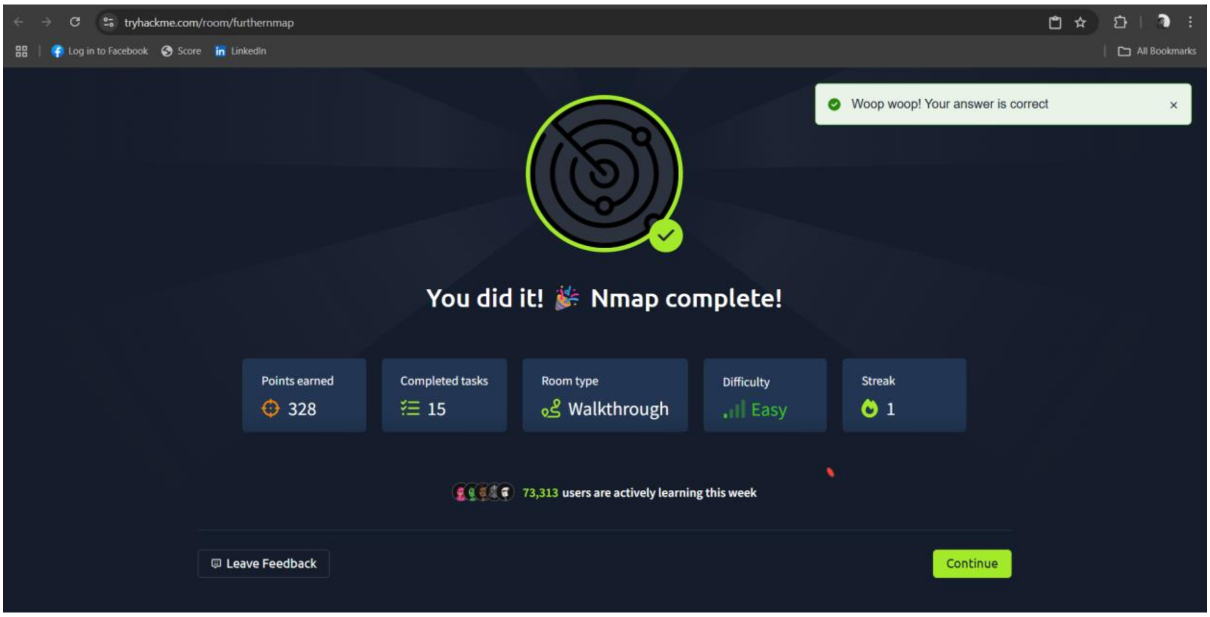
Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Y ✓ Correct Answer

Task 15 ○ Conclusion

How likely are you to recommend this room to others?

```
This mach
Please kee
1. Pentest
2. You are
3. This ma
4. Once th
5. If you
tomaticall
Usage Inst
1. Tools a
2. Webshe
3. Wordlis
4. README
5. To use
e-starkill
Do you th
Press ENTE
```



Woop woop! Your answer is correct

You did it! 🎉 Nmap complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
328	15	Walkthrough	Easy	1

73,313 users are actively learning this week