

# NMAP TryHackMe

Name: Nandakumar K.S

Tryhackme username: [nandu682015](#)

Date: 10th August 2025

## Task 1: deploy the machine

The screenshot shows a browser window with multiple tabs open, including 'tryhackme.com/room/furthernmap'. The main content area displays a task for deploying a machine. It includes a note about pressing a green button, a warning about not logging in or exploiting vulnerabilities, and a 'Start Machine' button. Below this is an 'OpenVPN' interface with a 'Start AttackBox' button highlighted by a green arrow. A section for answering questions is present, with a 'Correct Answer' button. A sidebar on the right lists various tasks related to Nmap, such as 'Task 2 Introduction', 'Task 3 Nmap Switches', and 'Task 4 Scan Types Overview'. At the bottom, there's a 'Feedback' section.

## Task 2: Introduction

The screenshot shows a web browser window with multiple tabs open, including various documentation and tool pages from TryHackMe. The main content area displays a challenge titled "Randomly, I'm gonna ask for server's common ports or windows remote server". It contains several text blocks and questions:

- A text block about standard ports (e.g., port 80 for HTTP, port 443 for HTTPS, port 139 for Windows NETBIOS).
- A text block explaining the use of nmap for port scanning.
- A text block about well-known ports, mentioning port 1024 as an example.
- A section titled "Answer the questions below" with the following questions:
  - "What networking constructs are used to direct traffic to the right application on a server?" (Answer: Ports)
  - "How many of these are available on any network-enabled computer?" (Answer: 65535)
  - "[Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)" (Answer: 1024)

At the bottom, there are navigation links for "Task 3 Nmap Switches" and "Task 4 Firewall/IDS".

## Task 3: Nmap Switches

The screenshot shows a web browser window with multiple tabs open, including documentation and tool pages from TryHackMe. The main content area displays a challenge titled "Answer the questions below" with the following questions:

- "What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?" (Answer: -sS)
- "Which switch would you use for a "UDP scan"?" (Answer: -sU)
- "If you wanted to detect which operating system the target is running on, which switch would you use?" (Answer: -O)
- "Nmap provides a switch to detect the version of the services running on the target. What is this switch?" (Answer: -sV)
- "The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?" (Answer: -v)
- "Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two? (Note: it's highly advisable to always use at least this option)" (Answer: -vv)
- "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?" (Answer: -oA)

At the bottom, there are navigation links for "Task 3 Nmap Switches" and "Task 4 Firewall/IDS".

Room completed (100%)

-oA

✓ Correct Answer

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

-oN

✓ Correct Answer

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

-oG

✓ Correct Answer

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?

-A

✓ Correct Answer

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!

How would you set the timing template to level 5?

-T5

✓ Correct Answer

We can also choose which port(s) to scan.

How would you tell nmap to only scan port 80?

-p 80

✓ Correct Answer

How would you tell nmap to scan ports 1000-1500?

-p 1000-1500

✓ Correct Answer

A very useful option that should not be ignored:

How would you tell nmap to scan all ports?

Room completed (100%)

-T5

✓ Correct Answer

How would you set the timing template to level 5?

-T5

✓ Correct Answer

We can also choose which port(s) to scan.

How would you tell nmap to only scan port 80?

-p 80

✓ Correct Answer

How would you tell nmap to scan ports 1000-1500?

-p 1000-1500

✓ Correct Answer

How would you tell nmap to scan all ports?

-p -

✓ Correct Answer

How would you activate a script from the nmap scripting library (lots more on this later)?

--script

✓ Correct Answer

How would you activate all of the scripts in the "vuln" category?

--script=vuln

✓ Correct Answer

! Hint

Task 4 Scan Types Overview

Task 5 Scan Types TCP Connect Scans

Task 6 Scan Types SYN Scans

## Task 4: Scan Types - Overview

The screenshot shows a web browser window with multiple tabs open, including 'tryhackme.com/room/furthernmap'. The main content area displays the 'Scan Types - Overview' task. It includes a list of basic scan types (TCP Connect Scans, SYN "Half-open" Scans, UDP Scans) and less common ones (TCP Null Scans, TCP FIN Scans, TCP Xmas Scans). It also discusses the three basic scan types and their differences. A 'Correct Answer' button is visible.

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

Task 6 Scan Types SYN Scans

Task 7 Scan Types UDP Scans

## Task 5: Scan Types - TCP Connect Scan

The screenshot shows a web browser window with multiple tabs open, including 'tryhackme.com/room/furthernmap'. The main content area displays the 'TCP Connect Scan' task. It includes a sequence diagram of a TCP handshake and a note about firewalls. A 'Correct Answer' button is visible.

If, however, the request 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 completes the handshake by sending back a TCP packet with ACK set).

This is all well and good, however, there is a third possibility.

What if the port is open, but hidden behind a **firewall**?

Many firewalls are configured to simply **drop** incoming packets. Nmap sends a TCP SYN request, and receives nothing back. This indicates that the port is being protected 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 would be as follows:

```
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 9 Hint

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

RST ✓ Correct Answer

Task 5 Scan Types SYN Scans

## Task 6: Scan Types - Syn Scans

There are, however, a couple of disadvantages to SYN scans, namely:

- They require **sudo permissions**<sup>[1]</sup> in order to work correctly in Linux. This is because SYN scans require the ability to create raw packets (as opposed to the full TCP handshake), which is a privilege only the root user has by default.
- Unstable services are sometimes brought down by SYN scans, which could prove problematic if a client has provided a production environment for the test.

All in all, the pros outweigh the cons.

For this reason, SYN scans are the default scans used by Nmap *if run with sudo permissions*. If run **without** sudo permissions, Nmap defaults to the TCP Connect scan we saw in the previous task.

When using a SYN scan to identify closed and filtered ports, the exact same rules as with a TCP Connect scan apply.

If a port is closed then the server responds with a RST TCP packet. If the port is filtered by a firewall then the TCP SYN packet is either dropped, or spoofed with a TCP reset.

In this regard, the two scans are identical: the big difference is in how they handle open ports.

[1] SYN scans can also be made to work by giving Nmap the CAP\_NET\_RAW, CAP\_NET\_ADMIN and CAP\_NET\_BIND\_SERVICE capabilities; however, this may not allow many of the NSE scripts to run properly.

Answer the questions below

There are two other names for a SYN scan, what are they?

✓ Correct Answer

Can Nmap use a SYN scan without Sudo permissions (Y/N)?

✓ Correct Answer

Task 7 ✓ Scan Types UDP Scans

Task 8 ✓ Scan Types NULL, FIN and Xmas

## Task 7: Scan Types - UDP scans

Unlike TCP, UDP connections are **stateless**. This means that, rather than initiating a connection with a back-and-forth "handshake", UDP connections rely on sending packets to a target port and essentially hoping that it makes it. This makes UDP superb for connections which rely on speed over quality (e.g. video sharing), but the lack of acknowledgement makes UDP significantly more difficult (and much slower) to scan. The switch for an Nmap UDP scan is `-sU`.

When a packet is sent to an open UDP port, there should be no response. When this happens, Nmap refers to the port as being **open|filtered**. In other words, it suspects that the port is open, but it could be filtered. If it gets a UDP response (which is very unusual), then the port is marked as **open**. More commonly there is no response, in which case the request is sent a second time as a double-check. If there is still no response then the port is marked **open|filtered** and Nmap moves on.

When a packet is sent to a **closed** UDP port, the target should respond with an ICMP (ping) packet containing a message that the port is unreachable. This clearly identifies closed ports, which Nmap marks as such and moves on.

Due to this difficulty in identifying whether a UDP port is actually open, UDP scans tend to be incredibly slow in comparison to the various TCP scans (in the region of 20 minutes to scan the first 1000 ports, with a good connection). For this reason it's usually good practice to run an Nmap scan with `--top-ports <number>` enabled. For example, scanning with `nmap -sU --top-ports 20 <target>` will scan the top 20 most commonly used UDP ports, resulting in a much more acceptable scan time.

When scanning UDP ports, Nmap usually sends completely empty requests – just raw UDP packets. That said, for ports which are usually occupied by well-known services, it will instead send a protocol-specific payload which is more likely to elicit a response from which a more accurate result can be drawn.

Answer the questions below

If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

✓ Correct Answer

When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so?

✓ Correct Answer

Task 8 ✓ Scan Types NULL, FIN and Xmas

Task 9 ✓ Scan Types ICMP Network Scanning

## Task 8: Scan Types - NULL, Fin and Xmas

The expected response for open ports with these scans is also identical, and is very similar to that of a UDP scan. If the port is open then there is no response to the malformed packet. Unfortunately (as with open UDP ports), that is also expected behaviour if the port is protected by a firewall, so NULL, FIN and Xmas scans will only ever identify ports as being open/filterd, closed, or filtered. If a port is identified as filtered with one of these scans then it is usually because the target has responded with an ICMP unreachable packet.

It's also worth noting that while RFC 793 mandates that network hosts respond to malformed packets with a RST TCP packet for closed ports, and don't respond at all for open ports; this is not always the case in practice. In particular Microsoft Windows (and a lot of Cisco network devices) are known to respond with a RST to any malformed TCP packet -- regardless of whether the port is actually open or not. This results in all ports showing up as being closed.

That said, the goal here is, of course, firewall evasion. Many firewalls are configured to drop incoming TCP packets to blocked ports which have the SYN flag set (thus blocking new connection initiation requests). By sending requests which do not contain the SYN flag, we effectively bypass this kind of firewall. Whilst this is good in theory, most modern IDS solutions are savvy to these scan types, so don't rely on them to be 100% effective when dealing with modern systems.

Answer the questions below

Which of the three shown scan types uses the URG flag?

xmas ✓ Correct Answer

Why are NULL, FIN and Xmas scans generally used?

Firewall Evasion ✓ Correct Answer

Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

Microsoft Windows ✓ Correct Answer

Task 9 Scan Types ICMP Network Scanning

Task 10 NSE Scripts Overview

Task 11 NSE Scripts Working with the NSE

## Task 9: Scan Types - ICMP Network Scanning

The `-sn` switch tells Nmap not to scan any ports – forcing it to rely primarily on ICMP echo packets (or ARP requests on a local network, if run with sudo or directly as the root user) to identify targets. In addition to the ICMP echo requests, the `-sn` switch will also cause nmap to send a TCP SYN packet to port 443 of the target, as well as a TCP ACK (or TCP SYN if not run as root) packet to port 80 of the target.

Answer the questions below

How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

`nmap -sn 172.16.0.0/16` ✓ Correct Answer 💡 Hint

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

## Task 10: NSE Scripts - Overview

The screenshot shows a web browser window with multiple tabs open, including 'tryhackme.com/room/furthernmap'. The main content area displays the 'NSE Scripts - Overview' task. It includes a list of NSE script categories: safe, intrusive, vuln, exploit, auth, brute, and discovery. Below this is a note about running scripts in a production environment and a section for answering questions. A sidebar on the right lists completed tasks: Task 11 (Working with the NSE), Task 12 (Searching for Scripts), Task 13 (Firewall Evasion), and Task 14 (Practical). A green circular icon with a question mark is visible on the left.

There are many categories available. Some useful categories include:

- 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).

A more exhaustive list can be found [here](#).

In the next task we'll look at how to interact with the NSE and make use of the scripts in these categories.

Answer the questions below

What language are NSE scripts written in?

Lua ✓ Correct Answer

Which category of scripts would be a very bad idea to run in a production environment?

intrusive ✓ Correct Answer

Task 11 NSE Scripts Working with the NSE

Task 12 NSE Scripts Searching for Scripts

Task 13 Firewall Evasion

Task 14 Practical

## Task 11: NSE Scripts - Working with the NSE

The screenshot shows a web browser window with multiple tabs open, including 'tryhackme.com/room/furthernmap'. The main content area displays the 'Working with the NSE' task. It provides instructions on using the --script switch to run specific scripts or multiple scripts simultaneously. It also explains how to use --script-args to provide arguments to scripts like http-put. Examples and notes are included. A sidebar on the right lists completed tasks: Task 12 (Searching for Scripts) and Task 13 (Firewall Evasion). A green circular icon with a question mark is visible on the left.

In Task 3 we looked very briefly at the `--script` switch for activating NSE scripts from the `vuln` category using `--script=vuln`. It should come as no surprise that the other categories work in exactly the same way. If the command `--script=safe` is run, then any applicable safe scripts will be run against the target (Note: only scripts which target an active service will be activated).

To run a specific script, we would use `--script=<script-name>`, e.g. `--script=http-fileupload-exploiter`

Multiple scripts can be run simultaneously in this fashion by separating them by a comma. For example, `--script=smb-enum-users,smb-enum-shares`.

Some scripts require arguments (for example, credentials, if they're exploiting an authenticated vulnerability). These can be given with the `--script-args` Nmap switch. An example of this would be with the `http-put` script (used to upload files using the PUT method). This takes two arguments: the URL to upload the file to, and the file's location on disk. For example:

```
nmap -p 80 --script http-put --script-args http-put.url='/dav/shell.php',http-put.file='./shell.php'
```

Note that the arguments are separated by commas, and connected to the corresponding script with periods (i.e. `<script-name>.<argument>`).

A full list of scripts and their corresponding arguments (along with example use cases) can be found [here](#).

Nmap scripts come with built-in help menus, which can be accessed using `nmap --script-help <script-name>`. This tends not to be as extensive as in the link given above, however, it can still be useful when working locally.

Answer the questions below

What optional argument can the `ftp-anon.nse` script take?

maxlist ✓ Correct Answer

Task 12 NSE Scripts Searching for Scripts

Task 13 Firewall Evasion

## Task 12: NSE Scripts - Searching for scripts

The screenshot shows a web browser window with multiple tabs open, including 'tryhackme.com/room/furthernmap'. The main content area displays Nmap's NSE script documentation. It includes code snippets for 'ajp-methods.nse', 'ajp-request.nse', and 'allseingeye-info.nse'. Below this, there's a section titled 'Installing New Scripts' with instructions on how to update local scripts from the Nmap website. A note about Lua knowledge is present. A question asks to search for 'smb' scripts in the '/usr/share/nmap/scripts/' directory, with a correct answer being 'smb-os-discovery.nse'. Another question asks what determines the OS of an SMB server, with a correct answer being 'smb-brute'. At the bottom, there are links to 'Task 13 Firewall Evasion', 'Task 14 Practical', and 'Task 15 Conclusion'.

## Task 13: Firewall evasion

The screenshot shows a web browser window with multiple tabs open, including 'tryhackme.com/room/furthernmap'. The main content area discusses Nmap switches for firewall evasion. It lists several switches: '-f', '-mtu <numbers>', '-scan-delay <time>', '-badsum', and '--data-length'. A question asks which protocol is often blocked, with a correct answer being 'ICMP'. Another question asks which switch allows appending random data, with a correct answer being '--data-length'. At the bottom, there are links to 'Task 14 Practical', 'Task 15 Conclusion', and a recommendation rating scale from 1 to 10.

## Task 14: Practical

The screenshot shows a browser window with multiple tabs open, including various Kali Linux tools and documentation. The main content area is titled "Room completed (100%)". It contains several questions and their answers:

- Does the target ip respond to ICMP echo (ping) requests (Y/N)? Answer: N (Correct Answer)
- Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered? Answer: 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!) Answer: No Response (Correct Answer, Hint available)
- Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open? Answer: 5 (Correct Answer)
- Open Wireshark (see [Crylllic'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) Answer: Y (Correct Answer)

Below the questions is a "Conclusion" section for Task 15, which includes a recommendation scale from 1 to 10.

## Task 15: Conclusion

The screenshot shows a browser window with multiple tabs open, including various Kali Linux tools and documentation. The main content area is titled "Room completed (100%)". It lists the completed tasks:

- Task 11 (NSE Scripts) Working with the NSE
- Task 12 (NSE Scripts) Searching for Scripts
- Task 13 (Firewall Evasion)
- Task 14 (Practical)
- Task 15 (Conclusion)

Below the tasks is a message: "You have now completed the Further Nmap room – hopefully you enjoyed it, and learnt something new! There are lots of great resources for learning more about Nmap on your own. Front and center are Nmap's own (highly extensive) [docs](#) which have already been mentioned several times throughout the room. These are a superb resource, so, whilst reading through them line-by-line and learning them by rote is entirely unnecessary, it would be highly advisable to use them as a point of reference, should you need it."

Answer the questions below

Read the conclusion.

No answer needed (Correct Answer)

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

Submit now

The screenshot shows a Firefox browser window with the URL [tryhackme.com/room/furthernmap](https://tryhackme.com/room/furthernmap). The page displays a vertical list of 13 tasks, each with a sub-section selected. A circular progress bar at the bottom left indicates 86% completion.

- Task 1: Deploy
- Task 2: Introduction
- Task 3: Nmap Switches
- Task 4: Scan Types Overview
- 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

A circular progress bar at the bottom left shows 86% completion.

midax@kali: ~ [midax@kali: ~]

```
$ nmap -sT -Pn -o 0-5000 10.10.239.162 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 18:46 IST
Stats: 0:00:10 elapsed; 1 hosts completed (1 up), 1 undergoing Connect Scan
Completed: 1 hosts up, 0 hosts down; ETC: 18:47 (0:00:35 remaining)
Nmap scan report for 10.10.239.162
Host is up (0.19s latency).
Not shown: 4996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
1337/tcp  open  msrpc
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 27.42 seconds
```

(midax@kali: ~)

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

292

Anticipate the questions below

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

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

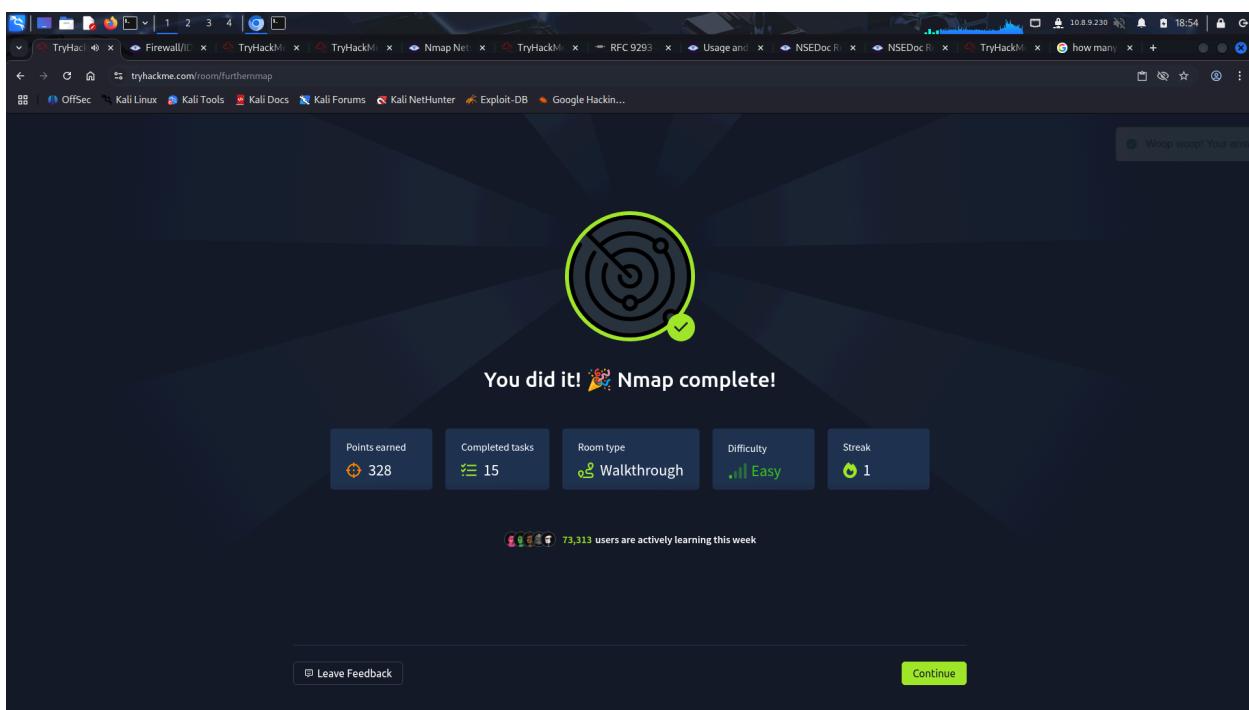
-

Open Wireshark (see Cryville'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 `lfi.py` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

-

d. Submit

How likely are you to recommend this room to others?



```
(midax㉿kali)-[~] $ nmap -sX -Pn -p 0-999 10.10.239.162
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 18:43 IST
Nmap scan report for 10.10.239.162
Host is up.
All 1000 scanned ports on 10.10.239.162 are in ignored states.
Not shown: 1000 open/filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.37 seconds

(midax㉿kali)-[~] $ nmap -sX -Pn -p 1-999 10.10.239.162
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 18:48 IST
Nmap scan report for 10.10.239.162
Host is up.
All 999 scanned ports on 10.10.239.162 are in ignored states.
Not shown: 1000 open/filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.35 seconds

(midax㉿kali)-[~] $ nmap -Pn --script:ftp-anon -p 21 -vv 10.10.239.162
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 18:53 IST
NSE: Loaded 1 scripts for scanning.
NSE: Starting pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
NSE: Starting Parallel DNS resolution of 1 host. at 18:53
Completed Parallel DNS resolution of 1 host. at 18:53. 0.00s elapsed
NSE: Initiating Parallel DNS resolution of 1 host. at 18:53
Completed Parallel DNS resolution of 1 host. at 18:53. 0.02s elapsed
NSE: Starting Stealth Scan on 10.10.239.162
Scanning 10.10.239.162 [1 port]
Discovered open port 21/tcp on 10.10.239.162
Completed Stealth Scan at 18:53, 0.26s elapsed (1 total ports)
NSE: Script scanning 10.10.239.162
NSE: Starting runlevel 1 (of 1) scan.
NSE: Starting NSE at 18:53
NSE: Script Post-scanning.
Completed NSE at 18:53, 31.07s elapsed
Nmap scan report for 10.10.239.162
Host is up, received user-set (0.18s latency).
Scanned at 2025-08-10 18:53:19 IST for 32s

PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 127
|_ftponr: Anonymous FTP login allowed (FTP code 230)
|_Cant get directory listing: TIMEOUT

NSE: Script Post-scanning.
Completed NSE at 18:53, 31.07s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Read data Files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) Scanned in 31.38 seconds
Raw packets sent: 1 (44B) | Rcvd: 1 (44B)

(midax㉿kali)-[~]
```