

TASK-3

TRYHACKME - FURTHER NMAP

TASK - 1 DEPLOY:

The screenshot shows the TryHackMe interface for the 'Further Nmap' room. At the top, there's a 'Target Machine Information' section with a table:

Title	Target IP Address	Expires
Further Nmap	Shown in 0min 43s	59min 41s

Buttons for '?', 'Add 1 hour', and 'Terminate' are next to the table.

Below this is 'Task 1: Deploy'. It instructs the user to 'Press the green button to deploy the machine!' and includes a 'Start Machine' button. A note states: 'Please Note: This machine is for scanning purposes only. You do not need to log into it, or exploit any vulnerabilities to gain access.'

Further instructions mention using the 'Start AttackBox' button on the top-right side. An advertisement for OpenVPN is shown with a 'Start AttackBox' button and a 'Click to start the AttackBox' link.

The task question is: 'Deploy the attached VM'. The answer field contains 'No answer needed', and a green 'Correct Answer' button is visible.

'Task 2: Introduction' is partially visible at the bottom.

TASK - 2 INTRODUCTION:

The screenshot shows the 'Introduction' task in the 'Further Nmap' room. It begins with a paragraph: 'Every computer has a total of 65535 available ports; however, many of these are registered as standard ports. For example, a HTTP Webservice can nearly always be found on port 80 of the server. A HTTPS Webservice can be found on port 443. Windows NETBIOS can be found on port 139 and SMB can be found on port 445. It is important to note; however, that especially in a CTF 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.'

The next paragraph explains the importance of port scanning: 'If we 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. This can be 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 most common 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 can be determined 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 - either manually, or more commonly using nmap.'

Another paragraph states: 'So, why 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 newcomers are now 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 even perform the exploit directly! Once again, this will be covered more in upcoming tasks.'

The final paragraph says: 'For now, 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.'

The task question is: 'What networking constructs are used to direct traffic to the right application on a server?'. The answer field contains 'Ports', and a green 'Correct Answer' button is visible.

The next question is: 'How many of these are available on any network-enabled computer?'. The answer field contains '65535', and a green 'Correct Answer' button is visible.

The final question is: '[Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)'. The answer field contains '1024', and green 'Correct Answer' and orange 'Hint' buttons are visible.

TASK - 3 NMAP SWITCHES:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

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?

-O

✓ Correct Answer

Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV

✓ Correct Answer

The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

-v

✓ Correct Answer

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)

-vv

✓ Correct Answer

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.

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

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?

-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?

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

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?

`-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 - 4 OVERVIEW:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

Task 3 ✓ Nmap Switches

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

TASK - 5 TCP CONNECT SCANS:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

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?

✓ Correct Answer

🔍 Hint

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

✓ Correct Answer

Task 6 ✓ Scan Types SYN Scans

Task 7 ✓ Scan Types UDP Scans

TASK - 6 SYN SCANS:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

- 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 UDP SCANS:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

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 firewalled. 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 - 8 NULL, FIN AND XMAS:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

Unfortunately (as with open TCP ports), there is also unexpected behaviour in the ports processed by a firewall, so NULL, FIN and Xmas scans will only ever identify ports as being `open`, `filtered`, `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?

✓ Correct Answer

Why are NULL, FIN and Xmas scans generally used?

✓ Correct Answer

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

✓ Correct Answer

Task 9 ✓ Scan Types

ICMP Network Scanning

Task 10 ✓ NSE Scripts

Overview

TASK - 9 ICMP NETWORK SCANNING:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

On first connection to a target network in a black box assignment, our first objective is to obtain a "map" of the network structure -- or, in other words, we want to see which IP addresses contain active hosts, and which do not.

One way to do this is by using Nmap to perform a so called "ping sweep". This is exactly as the name suggests: Nmap sends an ICMP packet to each possible IP address for the specified network. When it receives a response, it marks the IP address that responded as being alive. For reasons we'll see in a later task, this is not always accurate; however, it can provide something of a baseline and thus is worth covering.

To perform a ping sweep, we use the `-sn` switch in conjunction with IP ranges which can be specified with either a hyphen (`-`) or CIDR notation. i.e. we could scan the `192.168.0.x` network using:

- `nmap -sn 192.168.0.1-254`

or

- `nmap -sn 192.168.0.0/24`

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 - 10 OVERVIEW:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

The `Nmap Scripting Engine (NSE)` is an incredibly powerful addition to Nmap, extending its functionality quite considerably. NSE Scripts are written in the `Lua` programming language, and can be used to do a variety of things: from scanning for vulnerabilities, to automating exploits for them. The NSE is particularly useful for reconnaissance, however, it is well worth bearing in mind how extensive the script library is.

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 - 11 WORKING WITH THE NSE:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

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 - 12 SEARCHING FOR SCRIPTS:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

```
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-methods.nse", categories = { "default", "safe", } }
Entry { filename = "ajp-request.nse", categories = { "discovery", "safe", } }
Entry { filename = "allseeingeys-info.nse", categories = { "discovery", "safe", "version", } }
```

Installing New Scripts

We mentioned previously that the Nmap website contains a list of scripts, so, what happens if one of these is missing in the `scripts` directory locally? A standard `sudo apt update && sudo apt install nmap` should fix this; however, it's also possible to install the scripts manually by downloading the script from Nmap (`sudo wget -O /usr/share/nmap/scripts/<script-name>.nse https://svn.nmap.org/nmap/scripts/<script-name>.nse`). This must then be followed up with `nmap --script-updatedb`, which updates the `script.db` file to contain the newly downloaded script.

It's worth noting that you would require the same "updatedb" command if you were to make your own NSE script and add it into Nmap -- a more than manageable task with some basic knowledge of Lua!

Answer the questions below

Search for "smb" scripts in the `/usr/share/nmap/scripts/` directory using either of the demonstrated methods. What is the filename of the script which determines the underlying OS of the SMB server?

smb-os-discovery.nse

✓ Correct Answer

Read through this script. What does it depend on?

smb-brute

✓ Correct Answer

🔍 Hint

Task 13

Firewall Evasion

TASK - 13 FIREWALL EVASION:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

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 sent. 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 an invalid checksum for packets. Any real TCP/IP stack would drop this packet, however, firewalls may potentially respond automatically, without bothering to check the checksum of the packet. As such, this switch can be used to determine the presence of a firewall/IDS.

Answer the questions below

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the `-Pn` switch?

ICMP

✓ Correct Answer

[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

--data-length

✓ Correct Answer

Task 14 ✓ Practical

TASK - 14 PRACTICAL:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

Answer the questions below

Does the target ip respond to ICMP echo (ping) requests (Y/N)?

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?

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 [Cryllic'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

TASK - 15 CONCLUSION:

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Room completed (100%)

Task 14 Practical

Task 15 Conclusion

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 Nmaps 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

TryHackMe | Nmap

tryhackme.com/room/furthernmap



Congratulations on completing Nmap!!! 🎉

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

This room counted toward joining the league 🎯

Leave Feedback

Continue