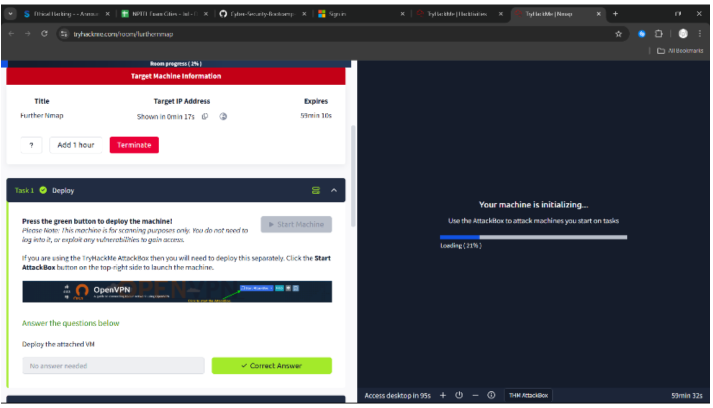
Nmap CTF Walkthrough (with Original Screenshots)

This document provides a detailed walkthrough of the "Further Nmap" room on TryHackMe This creates a complete, step-by-step procedure of how you solved the challenges.



tryhackme.com/room/furthernmap

Room progress (2%)

Target Machine Information

Title	Target IP Address	Expires
Further Nmap	Shown in 0min 17s	59min 10s

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

Your machine is initializing...

Use the AttackBox to attack machines you start on tasks

Loading (21%)

Access desktop in 95s

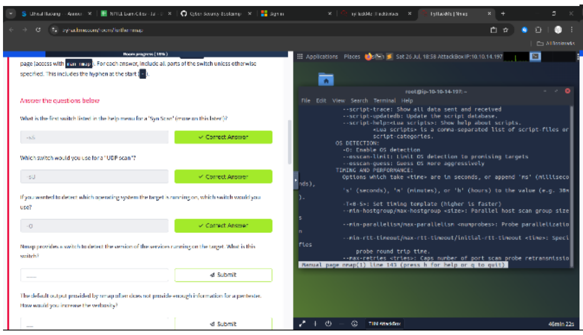
THM AttackBox

59min 32s

Initial Setup

The first step in any TryHackMe room involving a target machine is to deploy the virtual machine.

- **Action:** You clicked the "Start Machine" button.
- **Result:** A target machine with a specific IP address was deployed for you to scan. This is a prerequisite for all subsequent tasks.



Room progress (18%)

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?

-O

✓ Correct Answer

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

___

Submit

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

___

Submit

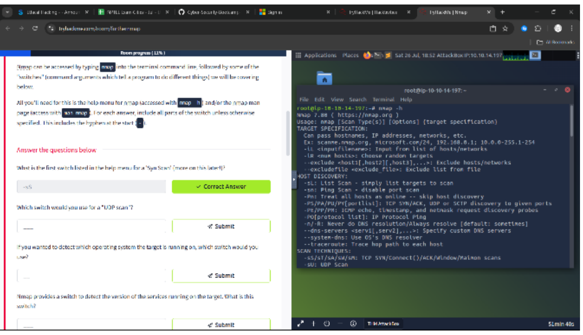
Sat 26 Jul, 18:58 AttackBox IP:10.10.14.197

root@ip-10-10-14-197: ~

```
        --script-trace: Show all data sent and received
        --script-updatedb: Update the script database.
        --script-help=<Lua scripts>: Show help about scripts.
                 <Lua scripts> is a comma-separated list of script-files or
                 script-categories.
      OS DETECTION:
        -O: Enable OS detection
        --osscan-limit: Limit OS detection to promising targets
        --osscan-guess: Guess OS more aggressively
      TIMING AND PERFORMANCE:
        Options which take <time> are in seconds, or append 'ms' (milliseco
nds),
        's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m
).
        -T<0-5>: Set timing template (higher is faster)
        --min-hostgroup/max-hostgroup <size>: Parallel host scan group size
s
        --min-parallelism/max-parallelism <numprobes>: Probe parallelizatio
n
        --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Speci
fies
           probe round trip time.
        --max-retries <tries>: Caps number of port scan probe retransmissio
 Manual page nmap(1) line 143 (press h for help or q to quit)
```

THM AttackBox

46min 22s



Room progress (11%)

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"?

___

Submit

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

___

Submit

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

___

Submit

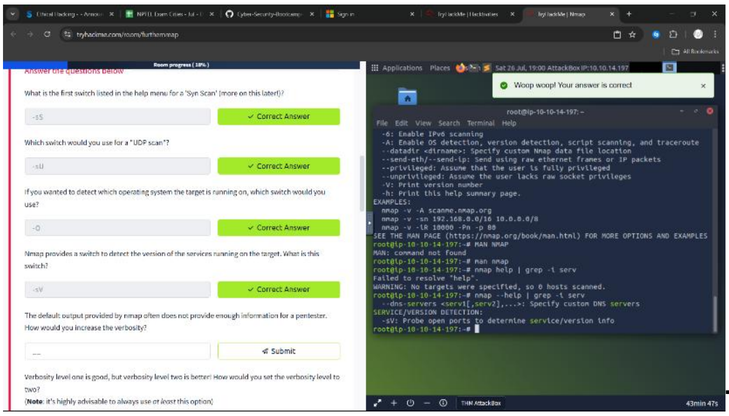
Sat 26 Jul, 18:52 AttackBox IP:10.10.14.197

root@ip-10-10-14-197: ~

```
root@ip-10-10-14-197:~# nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
```

THM AttackBox

51min 40s



tryhackme.com/room/furthernmap

Room progress (18%)

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?

___

Submit

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)

Sat 26 Jul, 19:00 AttackBox IP:10.10.14.197

Woop woop! Your answer is correct

root@ip-10-10-14-197: ~

```
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@ip-10-10-14-197:~# MAN NMAP
MAN: command not found
root@ip-10-10-14-197:~# man nmap
root@ip-10-10-14-197:~# nmap help | grep -i serv
Failed to resolve "help".
WARNING: No targets were specified, so 0 hosts scanned.
root@ip-10-10-14-197:~# nmap --help | grep -i serv
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
root@ip-10-10-14-197:~#
```

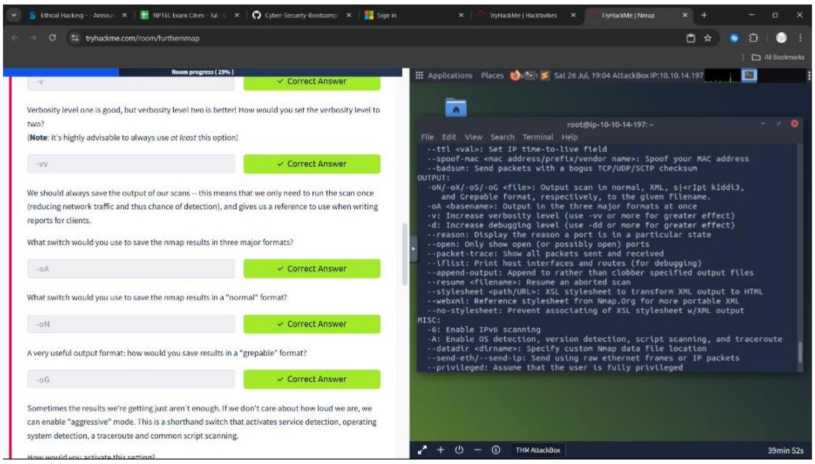
THM AttackBox

43min 47s

Task 2: Scan Types and Basic Enumeration

This section focused on the fundamental scan types and how to gather initial information about the target system.

- **SYN Scan (-sS):** This is Nmap's default and most popular scan option. It's a "stealth" scan, also known as a half-open scan, because it never completes the full TCP three-way handshake. It's fast and less likely to be logged by the target system.
- **UDP Scan (-sU):** This switch is used to identify open UDP ports. UDP scanning is generally slower and more difficult than TCP scanning.
- **OS Detection (-O):** This option enables Nmap's operating system detection feature. It sends a series of TCP and UDP packets to the target and analyzes the responses to determine the OS fingerprint.
- **Service/Version Detection (-sV):** This is one of the most useful features. It probes open ports to determine the specific service and version of the software running on them (e.g., Apache httpd 2.4.41, OpenSSH 8.2p1). This is crucial for finding potential vulnerabilities



-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.

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?

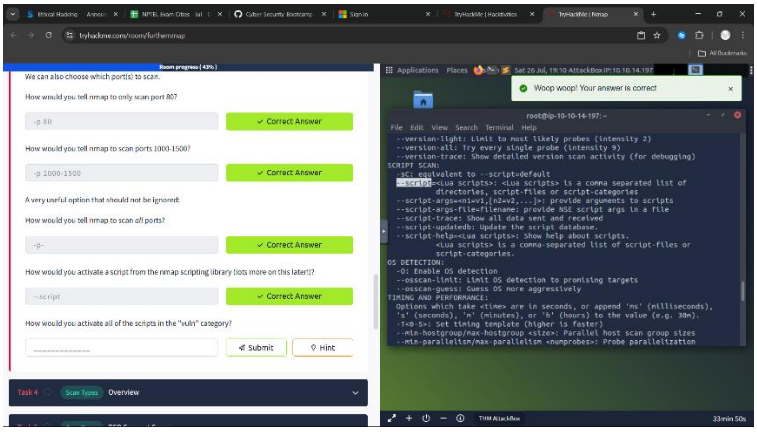
```
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
```

Controlling Output

Effective penetration testing requires proper documentation. This section covered how to control the verbosity and format of Nmap's output.

- **Verbosity (-v and -vv): By default, Nmap's output can be sparse. The verbosity switches provide more detailed information during the scan.**
  - **-v: Sets the verbosity to level one.**
  - **-vv: Sets the verbosity to level two, providing even more detail. It's highly recommended to use at least -v to get real-time feedback.**
- **Output Formats: Saving scan results is essential for reporting. Nmap offers several output formats.**

- **Save in All Formats (-oA): This is a convenient switch that saves the output in Nmap's three main formats at once: Normal (.nmap), Grepable (.gnmap), and XML (.xml).**
- **Normal Output (-oN): Saves the output in a standard, human-readable format.**
- **Grepable Output (-oG): Saves the output in a format that is easy to parse with command-line tools like grep, awk, and cut.**



Room progress (43%)

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?

______________ Submit Hint

Task 4 Scan Types Overview

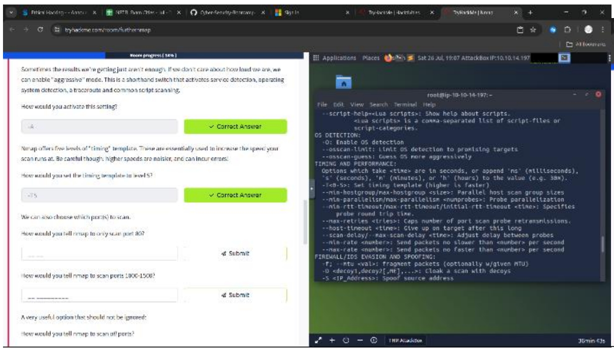
Sat 26 Jul, 19:10 AttackBox IP:10.10.14.197 [redacted]

Woop woop! Your answer is correct

root@ip-10-10-14-197: ~

```
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
```

THM AttackBox 33min 50s



Room progress (38%)

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?

Submit

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

Submit

A very useful option that should not be ignored:

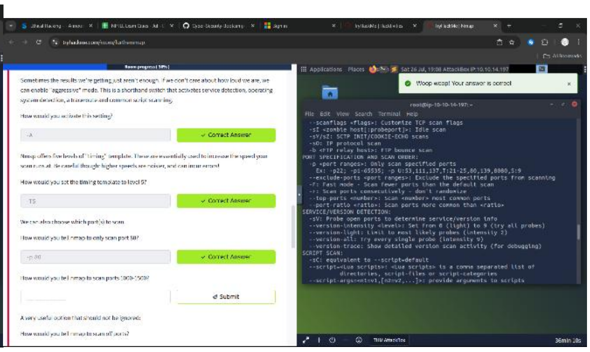
How would you tell nmap to scan *all* ports?

Sat 26 Jul, 19:07 AttackBox IP:10.10.14.197 [redacted]

root@ip-10-10-14-197: ~

```
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
```

THM AttackBox 36min 43s



Room progress (38%)

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?

Submit

A very useful option that should not be ignored:

How would you tell nmap to scan *all* ports?

Sat 26 Jul, 19:08 AttackBox IP:10.10.14.197 [redacted]

Woop woop! Your answer is correct

root@ip-10-10-14-197: ~

```
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
```

THM AttackBox 36min 10s

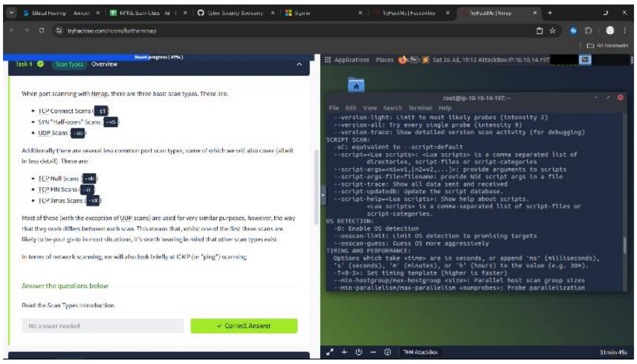
Scan Timing, Port Specification, and NSE

This section explores how to fine-tune scans for speed, target specific ports, and leverage the Nmap Scripting Engine (NSE).

- **Aggressive Mode (-A):** A powerful, "loud" option that enables OS detection (-O), version detection (-sV), default script scanning (-sC), and traceroute (--traceroute).
- **Timing Template (-T5):** Controls the speed of the scan. -T5 (insane) is the fastest setting, trading stealth and some accuracy for speed.
- **Port Specification (-p):** Allows you to define which ports to scan.
  - -p 80: Scans a single port.
  - -p 1000-1500: Scans a range of ports.

    - -p-: Scans all 65,535 TCP ports.

- **Nmap Scripting Engine (NSE):** Automates tasks by using Lua scripts.
    - --script: The switch to enable script scanning.
    - --script "vuln": Runs all scripts within the vuln category to check for known vulnerabilities.



tryhackme.com/room/furthernmap
Room progress (47%)
Task 4
Scan Types
Overview
Applications
Places
Sat 26 Jul, 19:12 AttackBox IP:10.10.14.197 [redacted]
root@ip-10-10-14-197: ~
File Edit View Search Terminal Help
THM AttackBox
31min 45s

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.

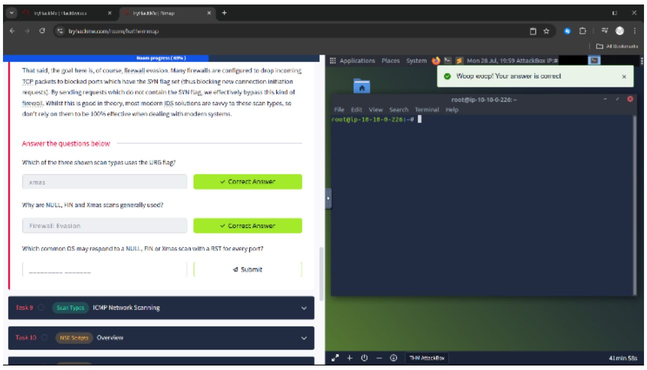
In terms of network scanning, we will also look briefly at ICMP (or "ping") scanning.

Answer the questions below

Read the Scan Types Introduction.

No answer needed ✓ Correct Answer

```
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
```



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?

_______ ______ Submit

Woop woop! Your answer is correct

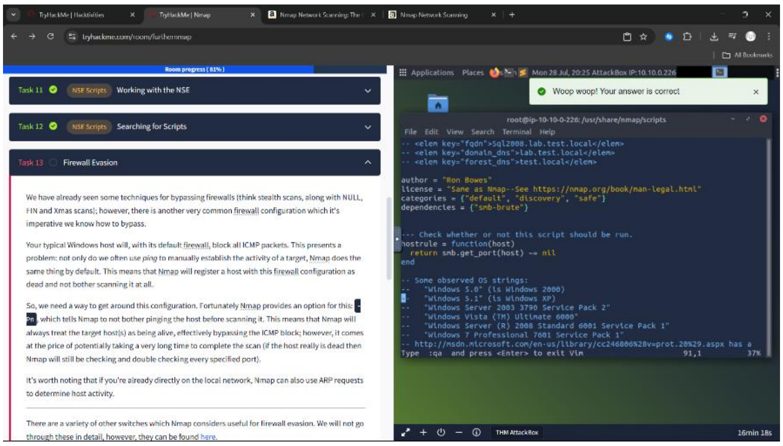
```
root@ip-10-10-0-226:~#
```

Firewall Evasion with Stealth Scans

This task introduces scan types that are less common than the standard SYN scan but are useful for bypassing certain firewall rules. These are the **NULL**, **FIN**, and **Xmas** scans.

These scans work by sending TCP packets with unusual flag combinations:

- **NULL Scan (-sN):** Sends a packet with no flags set.
- **FIN Scan (-sF):** Sends a packet with only the FIN flag set.
- **Xmas Scan (-sX):** Sends a packet with the FIN, PSH, and URG flags set, making it "light up like a Christmas tree."



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.

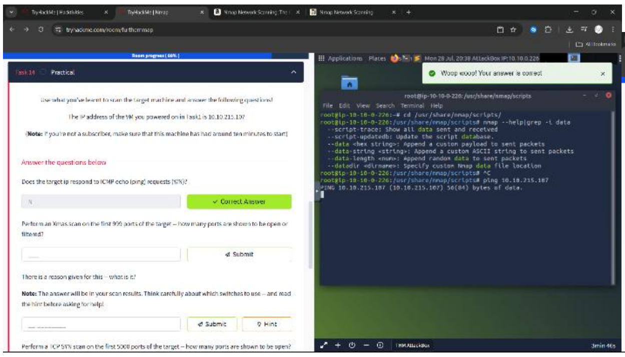
root@ip-10-10-0-226: /usr/share/nmap/scripts

```
-- <elem key="fqdn">Sql2008.lab.test.local</elem>
-- <elem key="domain_dns">lab.test.local</elem>
-- <elem key="forest_dns">test.local</elem>

author = "Ron Bowes"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "safe"}
dependencies = {"smb-brute"}


--- Check whether or not this script should be run.
hostrule = function(host)
  return smb.get_port(host) ~= nil
end

-- Some observed OS strings:
--   "Windows 5.0" (is Windows 2000)
--   "Windows 5.1" (is Windows XP)
--   "Windows Server 2003 3790 Service Pack 2"
--   "Windows Vista (TM) Ultimate 6000"
--   "Windows Server (R) 2008 Standard 6001 Service Pack 1"
--   "Windows 7 Professional 7601 Service Pack 1"
-- http://msdn.microsoft.com/en-us/library/cc246806%28v=prot.20%29.aspx has a
Type  :qa  and press <Enter> to exit Vim                      91,1          37%
```

Firewall Evasion - Bypassing Ping

Sometimes, a target will not respond to ICMP echo requests (pings), often due to a firewall rule. By default, Nmap will assume the host is offline if it doesn't get a ping response and will not proceed with a port scan.

To get around this, you can use the -Pn switch. This tells Nmap to **skip the host discovery (ping) phase** and scan every specified port as if the host were confirmed to be online.



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 10.10.215.107

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

Answer the questions below

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

N

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

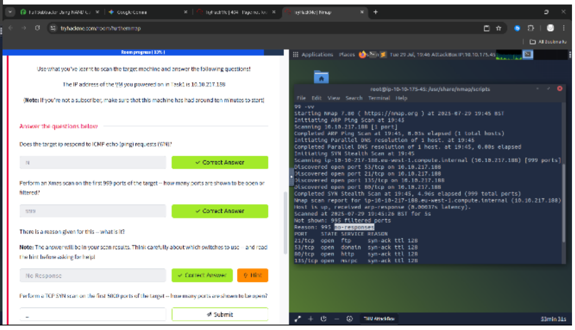
There is a reason given for this -- what is it?

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

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

root@ip-10-10-0-226: /usr/share/nmap/scripts

```
root@ip-10-10-0-226:~# cd /usr/share/nmap/scripts/
root@ip-10-10-0-226:/usr/share/nmap/scripts# nmap --help|grep -i data
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --datadir <dirname>: Specify custom Nmap data file location
root@ip-10-10-0-226:/usr/share/nmap/scripts# ^C
root@ip-10-10-0-226:/usr/share/nmap/scripts# ping 10.10.215.107
PING 10.10.215.107 (10.10.215.107) 56(84) bytes of data.
```



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 10.10.217.188

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

Answer the questions below

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

N

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

999

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

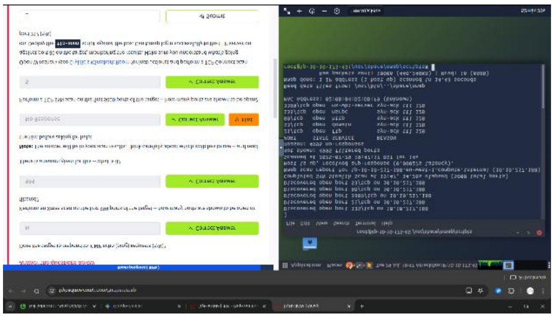
Note: The answer will be in your scan results. Think carefully about which switches to use -- and read the hint before asking for help!

No Response

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

root@ip-10-10-175-45: /usr/share/nmap/scripts

```
99 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-29 19:45 BST
Initiating ARP Ping Scan at 19:45
Scanning 10.10.217.188 [1 port]
Completed ARP Ping Scan at 19:45, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:45
Completed Parallel DNS resolution of 1 host. at 19:45, 0.00s elapsed
Initiating SYN Stealth Scan at 19:45
Scanning ip-10-10-217-188.eu-west-1.compute.internal (10.10.217.188) [999 ports]
Discovered open port 53/tcp on 10.10.217.188
Discovered open port 21/tcp on 10.10.217.188
Discovered open port 135/tcp on 10.10.217.188
Discovered open port 80/tcp on 10.10.217.188
Completed SYN Stealth Scan at 19:45, 4.96s elapsed (999 total ports)
Nmap scan report for ip-10-10-217-188.eu-west-1.compute.internal (10.10.217.188)
Host is up, received arp-response (0.00037s latency).
Scanned at 2025-07-29 19:45:26 BST for 5s
Not shown: 995 filtered ports
Reason: 995 no-responses
PORT     STATE SERVICE REASON
21/tcp   open  ftp     syn-ack ttl 128
53/tcp   open  domain  syn-ack ttl 128
80/tcp   open  http    syn-ack ttl 128
135/tcp  open  msrpc   syn-ack ttl 128
```



Answer the questions below

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

N

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

999

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?

5

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)

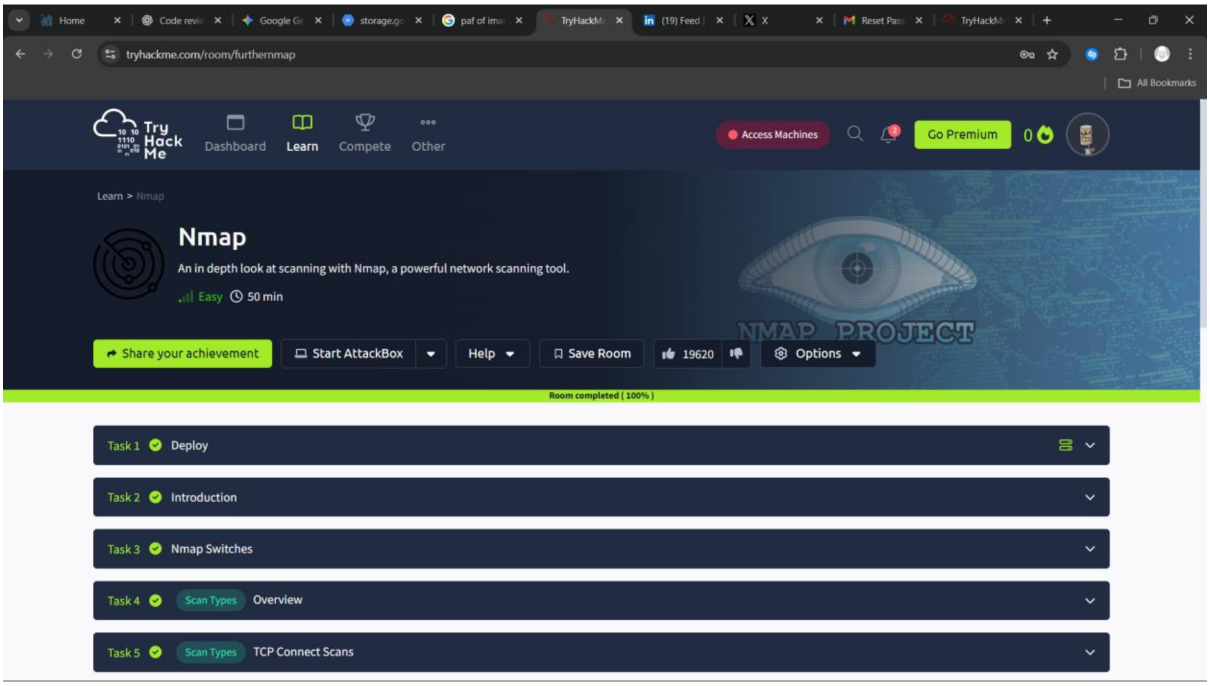
root@ip-10-10-175-45: /usr/share/nmap/scripts

```
]
Discovered open port 135/tcp on 10.10.217.188
Discovered open port 21/tcp on 10.10.217.188
Discovered open port 3389/tcp on 10.10.217.188
Discovered open port 80/tcp on 10.10.217.188
Discovered open port 53/tcp on 10.10.217.188
Completed SYN Stealth Scan at 19:47, 14.28s elapsed (5000 total ports)
Nmap scan report for ip-10-10-217-188.eu-west-1.compute.internal (10.10.217.188)
Host is up, received arp-response (0.00021s latency).
Scanned at 2025-07-29 19:47:17 BST for 14s
Not shown: 4995 filtered ports
Reason: 4995 no-responses
PORT     STATE SERVICE       REASON
21/tcp   open  ftp           syn-ack ttl 128
53/tcp   open  domain        syn-ack ttl 128
80/tcp   open  http          syn-ack ttl 128
135/tcp  open  msrpc         syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
MAC Address: 02:08:84:02:00:F9 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.43 seconds
           Raw packets sent: 10006 (440.248KB) | Rcvd: 16 (0000)
root@ip-10-10-175-45:/usr/share/nmap/scripts#
```

Practical Application

This final task requires you to apply the learned techniques to a target machine to answer a series of questions. The target IP for this task was **10.10.217.188**.

With that nmap ctf is solved.



tryhackme.com/room/furthernmap

Learn > Nmap

Nmap

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

Easy 50 min

Room completed (100%)

Task 1 Deploy

Task 2 Introduction

Task 3 Nmap Switches

Task 4 Scan Types Overview

Task 5 Scan Types TCP Connect Scans