

# TRYHACKME – FURTHER NMAP

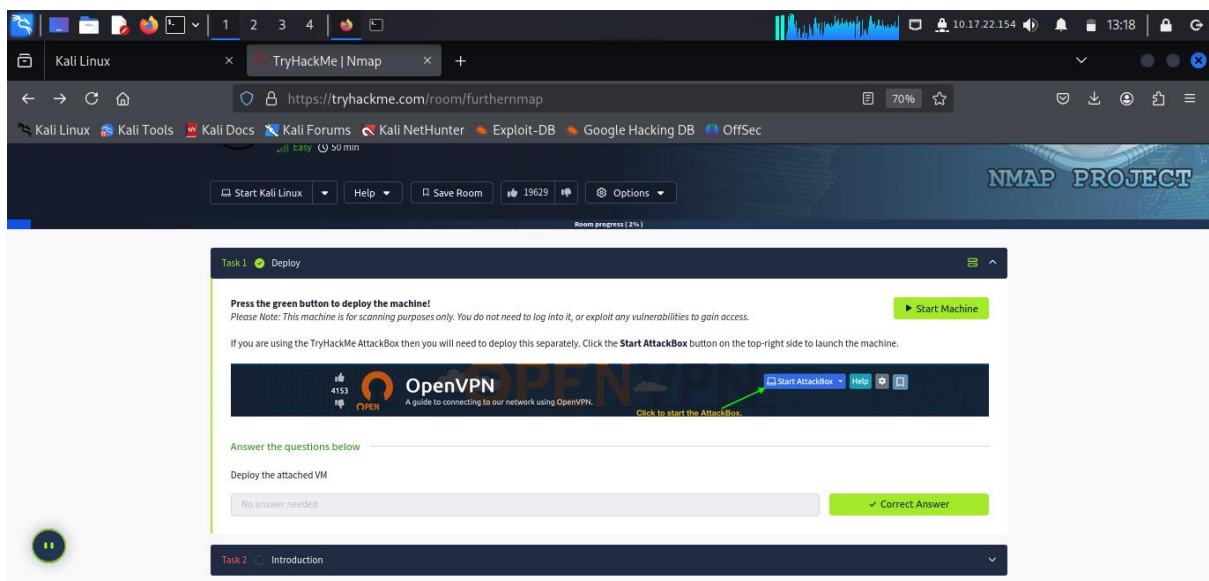
## Task 3: Complete the room furthernmap

Prepared by: NIVEDA S

The furthernmap room on TryHackMe explores advanced scanning techniques in Nmap, covering everything from basic flags to firewall evasion and script usage. The objective is to deepen knowledge of scanning, detection, and enumeration methods beyond a standard nmap - A scan. I completed the room successfully with the help of a YouTube walkthrough video, which clarified certain commands and helped confirm the expected outputs.

## Task1:Deploy

Deploy the target vm



## Task2: Intoduction

Learned the purpose of the room: advanced Nmap usage, scanning techniques, and firewall evasion.

Kali Linux TryHackMe | Nmap

https://tryhackme.com/room/furthernmap

Room progress (6%)

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.

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.

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.

Answer the questions below

What networking constructs are used to direct traffic to the right application on a server?

Ports ✓ Correct Answer

How many of these are available on any network-enabled computer?

65535 ✓ Correct Answer

[Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

Submit Hint

Kali Linux TryHackMe | Nmap how many well known po

https://www.google.com/search?client=firefox-b-e&channel=entpr&q=how+many+well+known+ports+ai

Google

how many well known ports are there

AI Mode All Images Videos News Shopping Web More Tools

AI Overview

Listen

There are **1024** well-known ports, ranging from 0 to 1023. These ports are reserved for commonly used services and protocols.

Explanation:

**Well-Known Ports:**

These ports are pre-assigned by the IANA (Internet Assigned Numbers Authority) for widely used services.

Registered port - Wikipedia

Ports with numbers 0–1023 are called system or well-known ports; ports with numbers 1024–49151 are called user or...

Wikipedia

What are Network Port Numbers? - UniNets

16 Jul 2025 — There are 3 types of port numbers based on the port number ranges: 1...

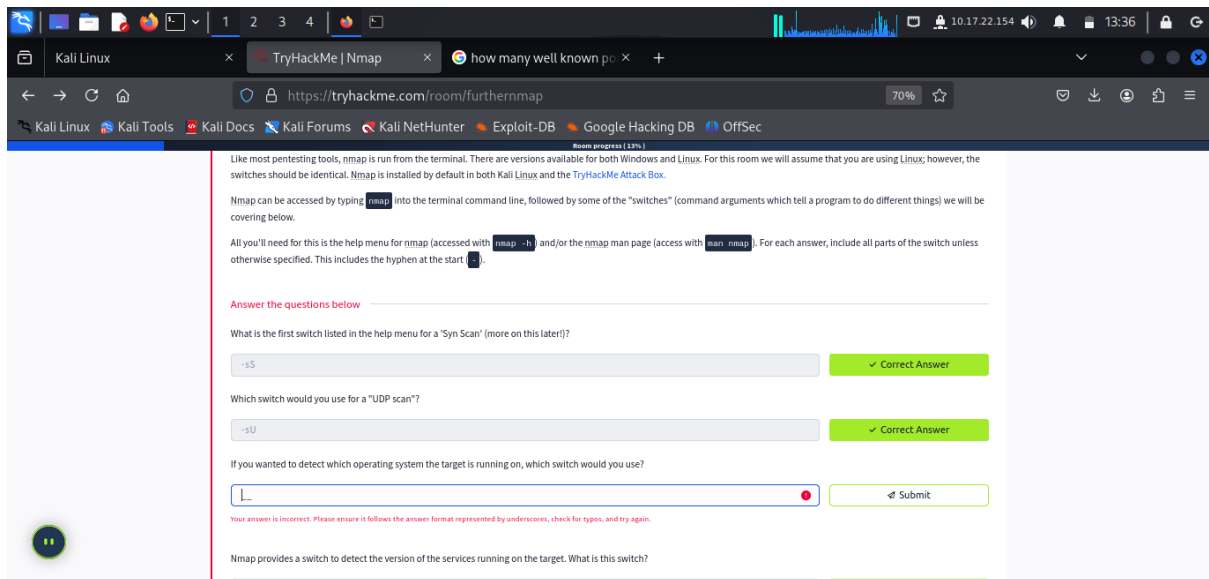
Kali Linux

kali@kali: ~/Downloads

File Actions Edit View Help

kali@kali: ~/Downloads x kali@kali: ~/Downloads x

```
Nmap 7.95 ( 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
  -iI <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/PI[portlist]: TCP SYN, TCP 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
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --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:
Manual page nmap(1) line 70 (press h for help or q to quit)
```

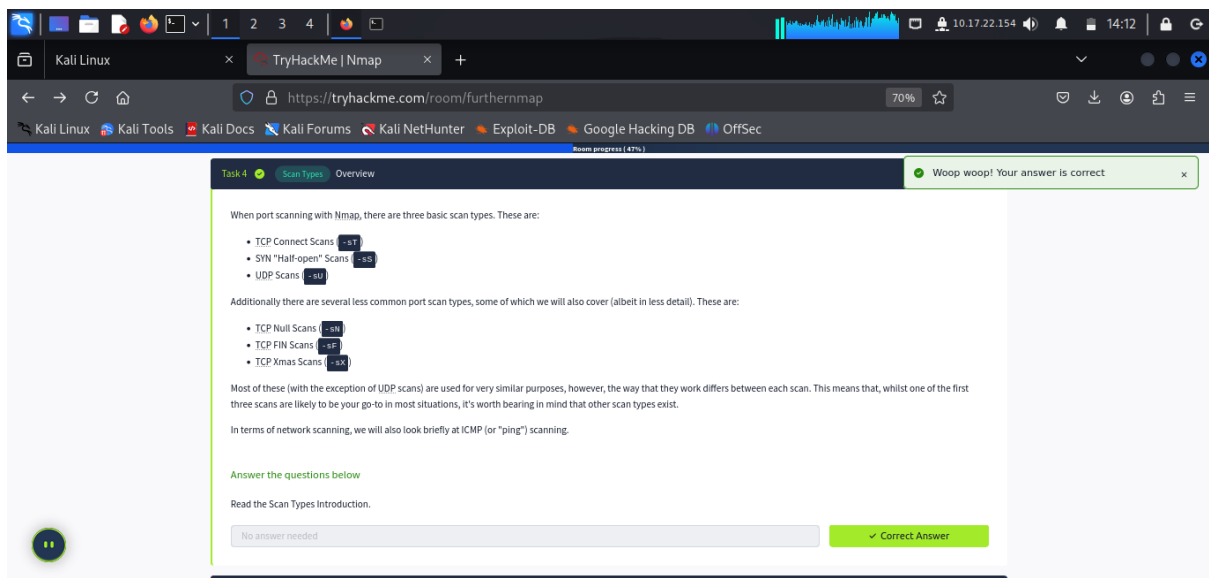


### Task3: Nmap Switches

Studied important flags such as -sS, -sT, -sU, -sV, -O, -A, -p, and -oA.

Learned how to adjust verbosity and timing with -v, -vv, and -T<0-5>.

### Task4:Scantype Overview



### Task5: TCP Connect Scans (-sT)

Ran full TCP handshake scans.

Used when SYN scans are not possible (e.g., restricted permissions).

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 🔍 Hint

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

RST ✓ Correct Answer

## Task6: SYN Scans (-sS)

Performed stealth scans that send SYN packets without completing the handshake.

- It can be used to bypass older Intrusion Detection systems as they are looking out for a full three way handshake. This is often no longer the case with modern IDS solutions; it is for this reason that SYN scans are still frequently referred to as "stealth" scans.
- SYN scans are often not logged by applications listening on open ports, as standard practice is to log a connection once it's been fully established. Again, this plays into the idea of SYN scans being stealthy.
- Without having to bother about completing (and disconnecting from) a three-way handshake for every port, SYN scans are significantly faster than a standard TCP Connect scan.

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?

Half-Open, Stealth ✓ Correct Answer

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

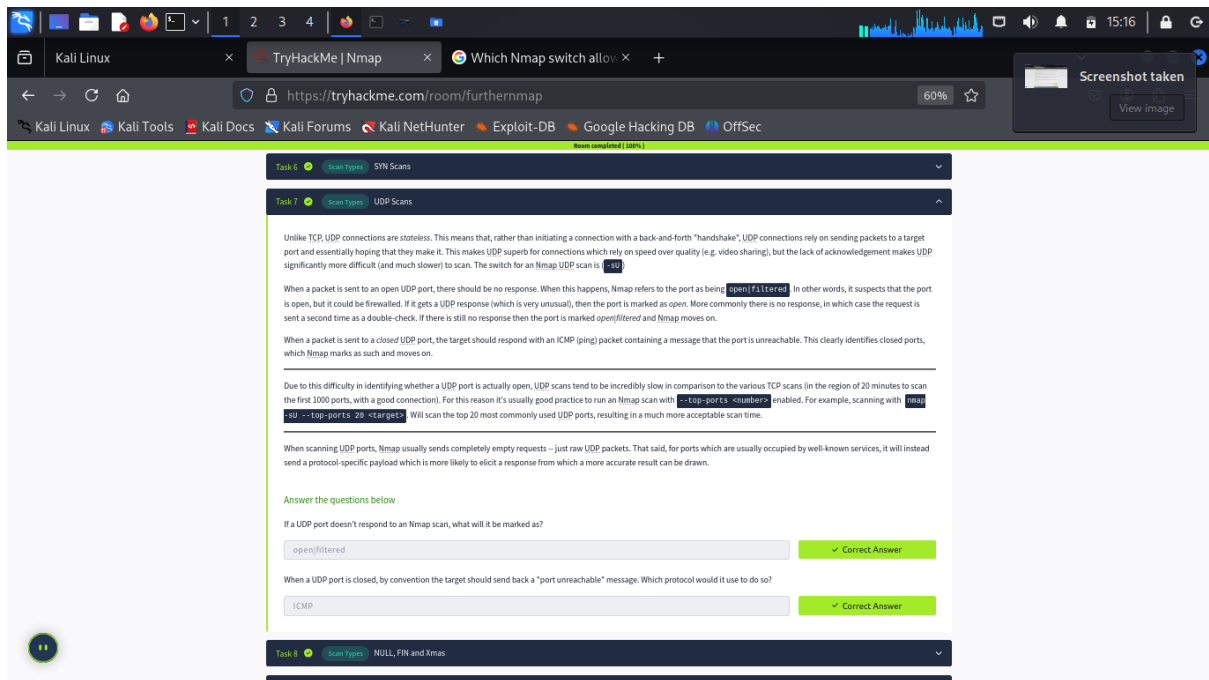
N ✓ Correct Answer

Task 1 🟢 Open type UDP Scans

## Task7: UDP Scans (-sU)

Checked for services running over UDP.

Learned UDP scanning is slower and less reliable than TCP scans.

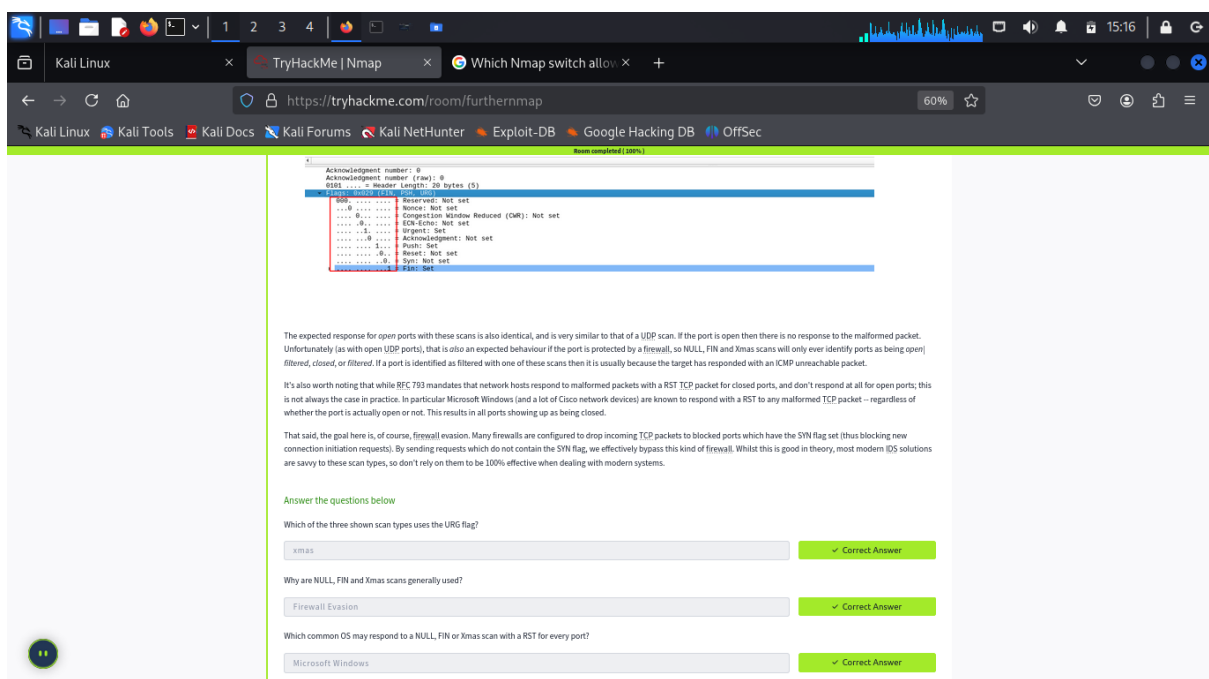


## Task8: Null,FIN and Xmas Scans

-sN (Null) Sent packets with no flags set to detect open/closed ports based on RFC-compliant responses.

-sF (Fin) Sent packets with only the FIN flag set to identify closed ports without full connection attempts.

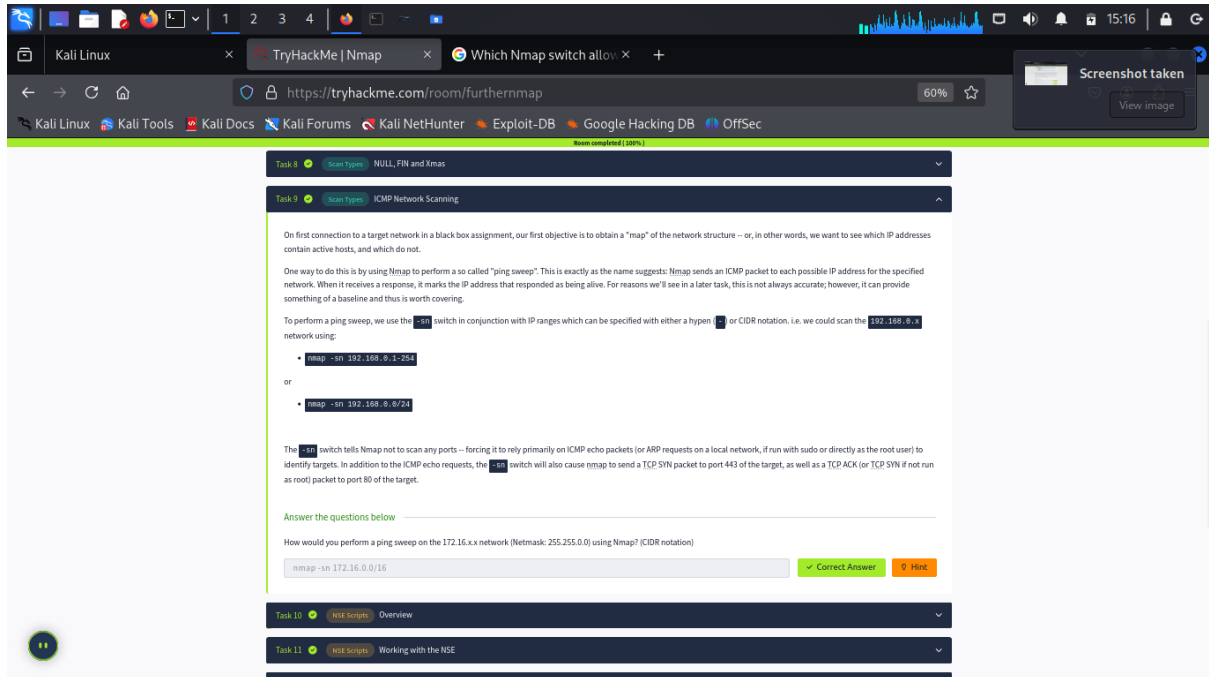
-sX (Xmas) Sent packets with FIN, PSH, and URG flags set to bypass some firewalls and detect port states.



## Task9: ICMP Network Scanning

Learned ping sweeps and how to detect live hosts.

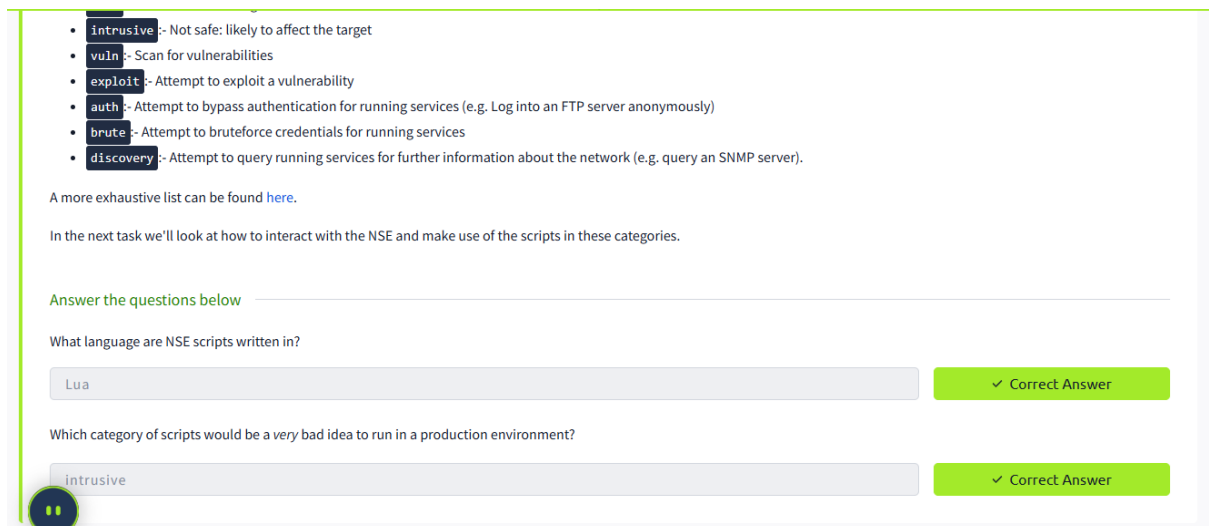
Used -Pn when ICMP was blocked.



## Task10: NSE Scripts Overview

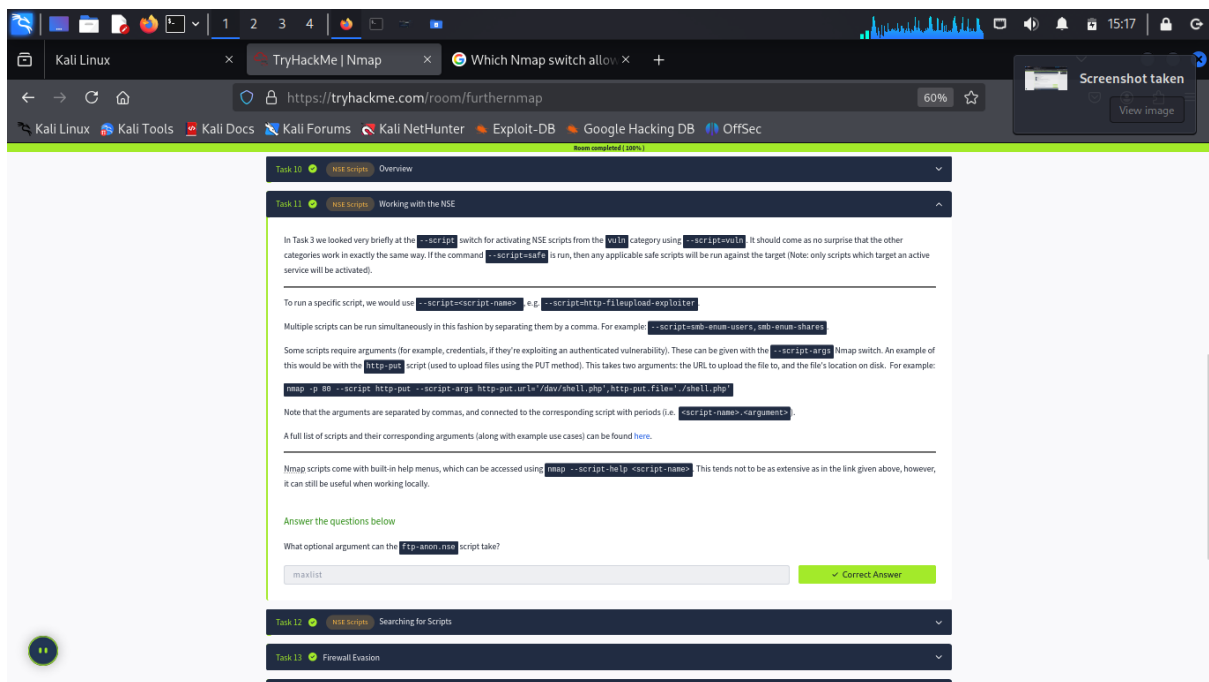
Introduction to the Nmap Scripting Engine (NSE).

Categories: discovery, safe, intrusive, vuln, exploit, brute.



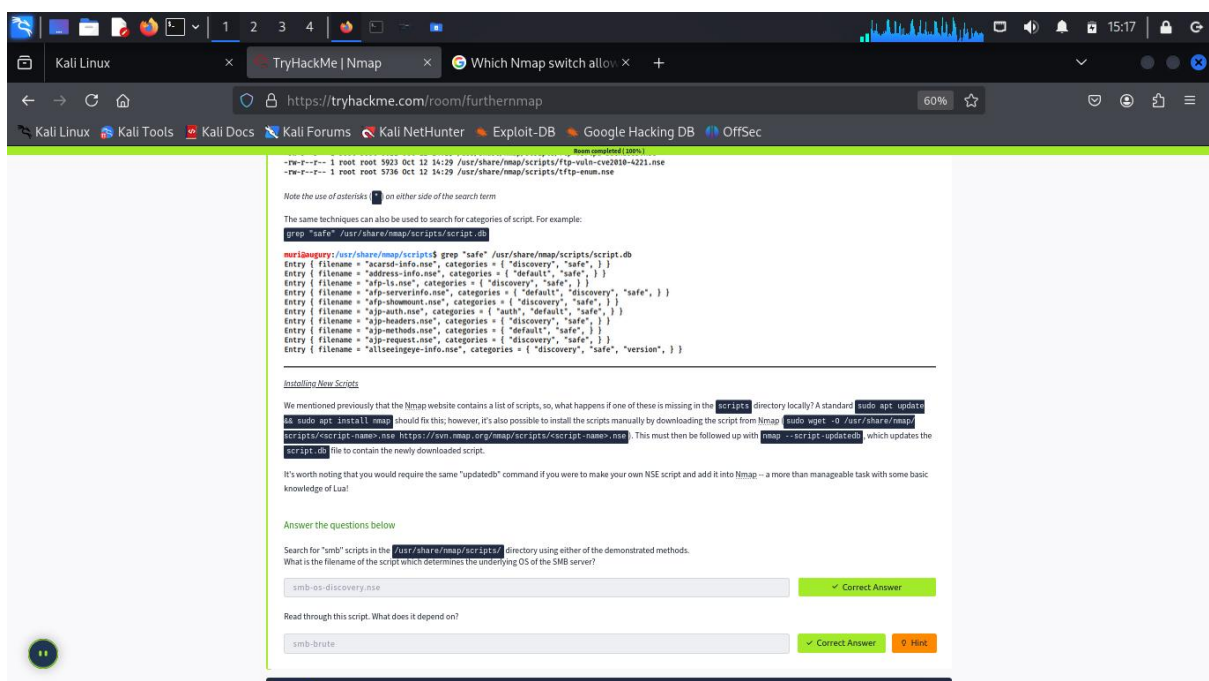
## Task11: Working with NSE

Ran scripts like ftp-anon to check for anonymous FTP logins.



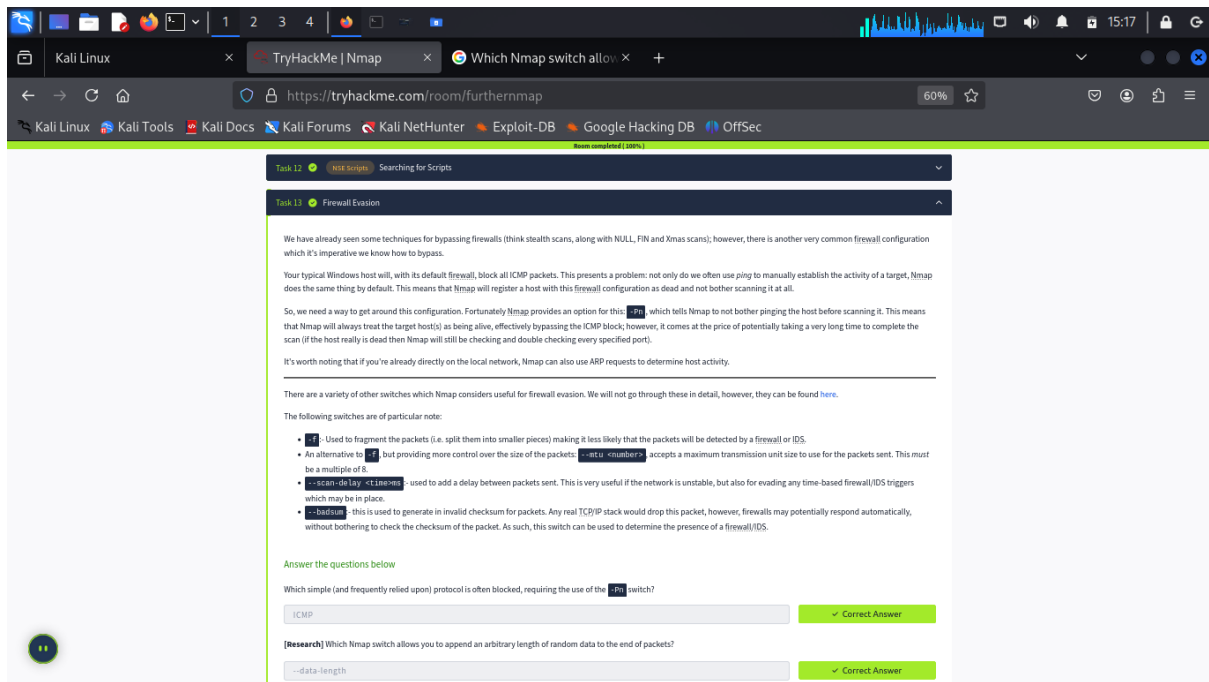
## Task12: Searching for Scripts

Used `ls /usr/share/nmap/scripts/` and `--script-help=<script>` to find and understand available NSE scripts.



## Task13: Firewall Evasion

Techniques: packet fragmentation (-f), custom MTU, bad checksums (--badsum), delays (--scan-delay).



The screenshot shows the 'Task 13: Firewall Evasion' page on TryHackMe. The page explains that Windows firewalls block ICMP packets by default, which prevents Nmap from pinging a host before scanning. It introduces the `-Pn` switch to bypass this. A list of other switches is provided: `-f` (fragmentation), `-x` (Xmas scan), `-sS` (SYN scan), `-sZ` (Zombie scan), `-sV` (version scan), `-sO` (OS detection), `-sC` (script scan), `-sI` (invalid checksum), `-sM` (Maimonides scan), `-sT` (TCP scan), `-sU` (UDP scan), `-sX` (Xmas scan), `-sY` (Yankel scan), `-sZ` (Zombie scan), `-sV` (version scan), `-sO` (OS detection), `-sC` (script scan), `-sI` (invalid checksum), `-sM` (Maimonides scan), `-sT` (TCP scan), `-sU` (UDP scan), `-sX` (Xmas scan), `-sY` (Yankel scan).

Answer the questions below

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

ICMP ✓ Correct Answer

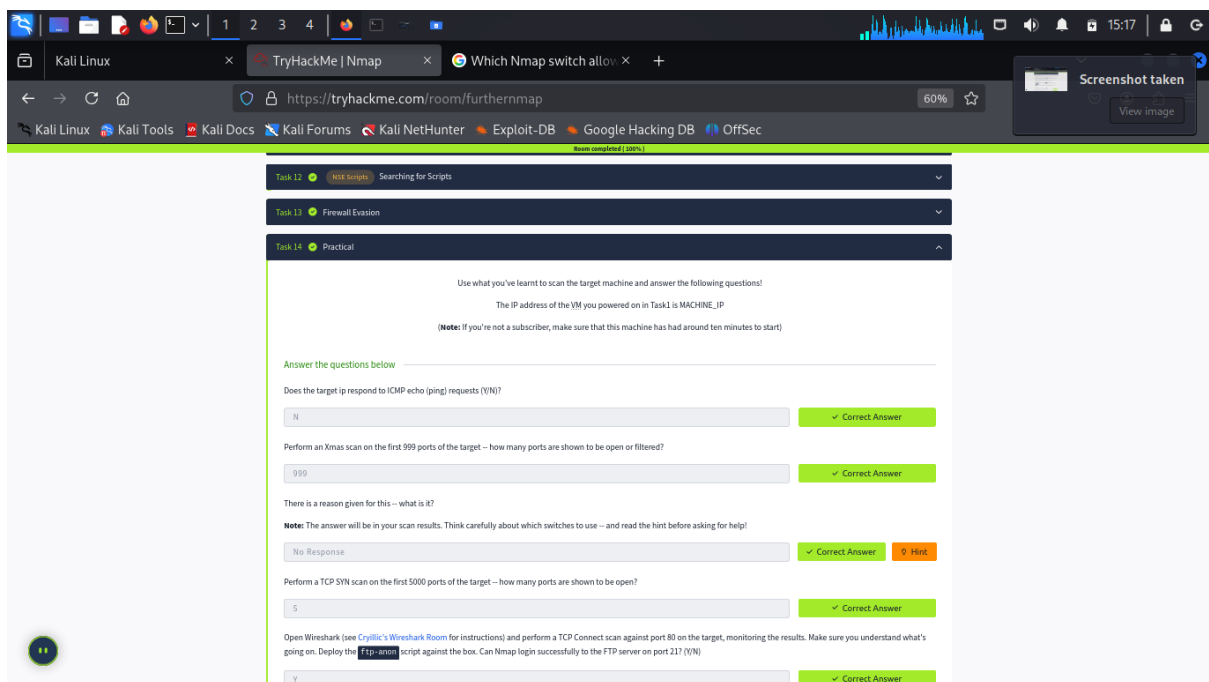
[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

--data-length ✓ Correct Answer

## Task14:Practical

Applied all learned techniques to a hands-on scan challenge.

Exported results in normal, greppable, and XML formats using `-oA`.



The screenshot shows the 'Task 14: Practical' page on TryHackMe. It instructs the user to use what they've learned to scan the target machine and answer the following questions:

The IP address of the VM you powered on in Task1 is MACHINE\_IP

(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 ✓ 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

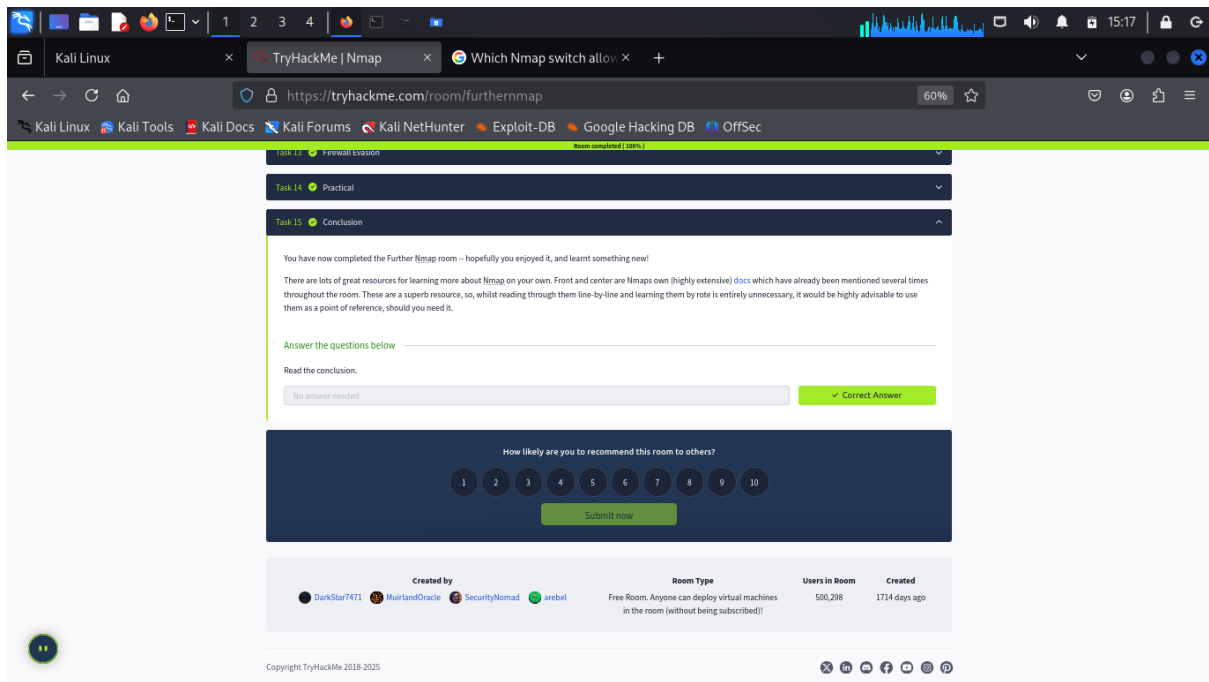
Perform a TCP SYN scan on the first 5000 ports of the target – how many ports are shown to be open?

5 ✓ Correct Answer

Open Wireshark (see [Cryllie'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-scan` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Y ✓ Correct Answer





## Conclusion:

Completed the Further Nmap room, gaining hands-on experience with TCP connect, SYN, UDP, Null, FIN, and Xmas scans, as well as NSE scripting and firewall evasion techniques. Nmap's official documentation remains an excellent reference for expanding these skills further.