

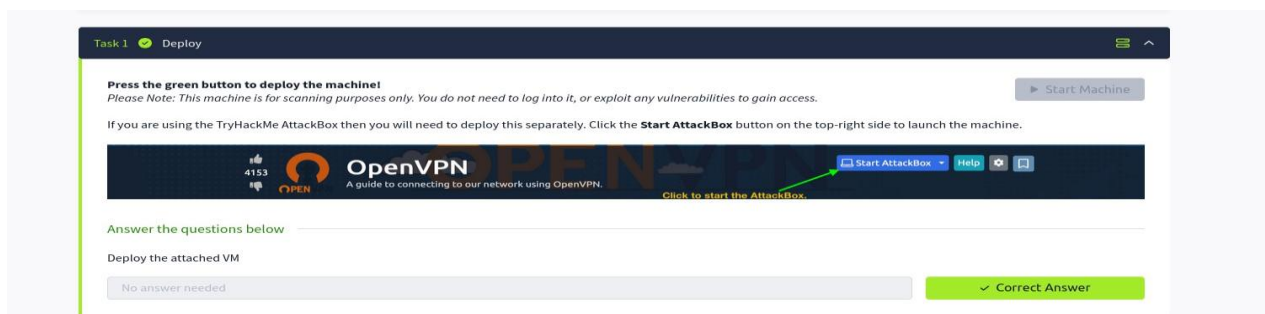
CTF Writeup: Further Nmap

Prepared By: Jestine Thomas Mathew

This writeup details the steps taken to solve the 'Further Nmap' room on TryHackMe. This room is categorized as 'Easy' and focuses on advanced Nmap scanning techniques, including host discovery, port scanning, firewall evasion, and the Nmap Scripting Engine (NSE).

1. Introduction & Connecting to the Network

First, I need to connect to the TryHackMe network to access the target machine. This is done by deploying the machine in the room and connecting to the TryHackMe VPN, for example using OpenVPN. Once connected, the target machine's IP address is provided. For this writeup, the target IP is `10.201.9.199`.



```
root@kali: /home/jesti

2025-08-10 04:56:55 Closing TUN/TAP interface
2025-08-10 04:56:55 net_addr_v4 del: 10.9.0.129 dev tun1
2025-08-10 04:56:55 SIGTERM[soft,exit-with-notification] received, process exiting

(jesti@kali)-[~]
└─$ sudo su
└─(root@kali)-[/home/jesti]
└─# openvpn /home/jesti/Downloads/beta25p.ovpn
2025-08-10 04:57:28 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2025-08-10 04:57:28 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by ovpn-dco, disabling data channel offload.
2025-08-10 04:57:28 OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/TKINTFO] [AEAD] [DCO]
2025-08-10 04:57:28 library versions: OpenSSL 3.5.0 8 Apr 2025, LZO 2.10
2025-08-10 04:57:28 DCO version: N/A
2025-08-10 04:57:28 TCP/UDP: Preserving recently used remote address: [AF_INET]54.76.30.11:1194
2025-08-10 04:57:28 Socket Buffers: R=[212992->425984] S=[212992->425984]
2025-08-10 04:57:28 UDPv4 link local: (not bound)
2025-08-10 04:57:28 UDPv4 link remote: [AF_INET]54.76.30.11:1194
2025-08-10 04:57:28 TLS: Initial packet from [AF_INET]54.76.30.11:1194, sid=54b2c338 f2f704cb
2025-08-10 04:57:29 VERIFY OK: depth=1, CN=ChangeMe
2025-08-10 04:57:29 VERIFY KU OK
2025-08-10 04:57:29 Validating certificate extended key usage
2025-08-10 04:57:29 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-08-10 04:57:29 VERIFY ECU OK
2025-08-10 04:57:29 VERIFY OK: depth=0, CN=server
2025-08-10 04:57:29 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 253 bits X25519
2025-08-10 04:57:29 [server] Peer Connection Initiated with [AF_INET]54.76.30.11:1194
2025-08-10 04:57:29 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-08-10 04:57:29 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-08-10 04:57:30 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-08-10 04:57:30 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route 10.101.0.0 255.255.0.0,route 10.103.0.0 255.255.0.0,route 10.201.0.0 255.255.128.0,route-metric 1000,comp-lzo no,route-gateway 10.9.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.9.0.129 255.255.0.0,peer-id 16'
2025-08-10 04:57:30 OPTIONS IMPORT: --ifconfig/up options modified
2025-08-10 04:57:30 OPTIONS IMPORT: route options modified
2025-08-10 04:57:30 OPTIONS IMPORT: route-related options modified
2025-08-10 04:57:30 Using peer cipher 'AES-256-CBC'
2025-08-10 04:57:30 net_route_v4_best_gw query: dst 0.0.0.0
2025-08-10 04:57:30 net_route_v4_best_gw result: via 192.168.94.2 dev eth0
2025-08-10 04:57:30 ROUTE_GATEWAY 192.168.94.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:6c:79:10
2025-08-10 04:57:30 TUN/TAP device tun1 opened
2025-08-10 04:57:30 net_iface_mtu_set: mtu 1500 for tun1
2025-08-10 04:57:30 net_iface_up: set tun1 up
2025-08-10 04:57:30 net_addr_v4 add: 10.9.0.129/16 dev tun1
2025-08-10 04:57:30 net_route_v4 add: 10.10.0.0/16 via 10.9.0.1 dev [NULL] table 0 metric 1000
2025-08-10 04:57:30 sitnl_send: rtnl: generic error (-17): File exists
```

TryHackMe | Nmap

https://tryhackme.com/room/furthernmap

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB TryHackMe | Nmap

Access Machines Go Premium 1

Learn > Nmap

Nmap
An in depth look at scanning with Nmap, a powerful network scanning tool.
Easy 50 min

Share your achievement Start AttackBox Help Save Room 19643 Options

Room completed (100%)

Target Machine Information		
Title	Target IP Address	Expires
Further Nmap	10.201.9.199	9min 18s

? Add 1 hour Terminate

Stuck on a question? I am here to help you with real-time guidance, personalized hints, and explanations.

Task 1 Introduction

Task 2 Introduction

Task 3 Nmap Switches

To confirm connectivity, a simple `ping` command can be used.

```
ping 10.201.9.199
```

```
(jesti@kali)-[~]
└─$ sudo su
[sudo] password for jesti:
(jesti@kali)-[~]
└─# ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data:
64 bytes from 10.10.10.10: icmp_seq=1 ttl=63 time=189 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=63 time=292 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=63 time=189 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=63 time=189 ms
64 bytes from 10.10.10.10: icmp_seq=5 ttl=63 time=193 ms
64 bytes from 10.10.10.10: icmp_seq=6 ttl=63 time=189 ms
64 bytes from 10.10.10.10: icmp_seq=7 ttl=63 time=195 ms
64 bytes from 10.10.10.10: icmp_seq=8 ttl=63 time=188 ms
64 bytes from 10.10.10.10: icmp_seq=9 ttl=63 time=189 ms
64 bytes from 10.10.10.10: icmp_seq=10 ttl=63 time=189 ms
64 bytes from 10.10.10.10: icmp_seq=11 ttl=63 time=189 ms
^C
--- 10.10.10.10 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10008ms
rtt min/avg/max/mdev = 188.180/199.148/292.345/29.539 ms
```

2. Answering the Initial Questions

The initial tasks involve answering theoretical questions about Nmap and networking.

- **Task 2 & 3:** These tasks cover basic networking concepts like ports and the different Nmap switches.

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

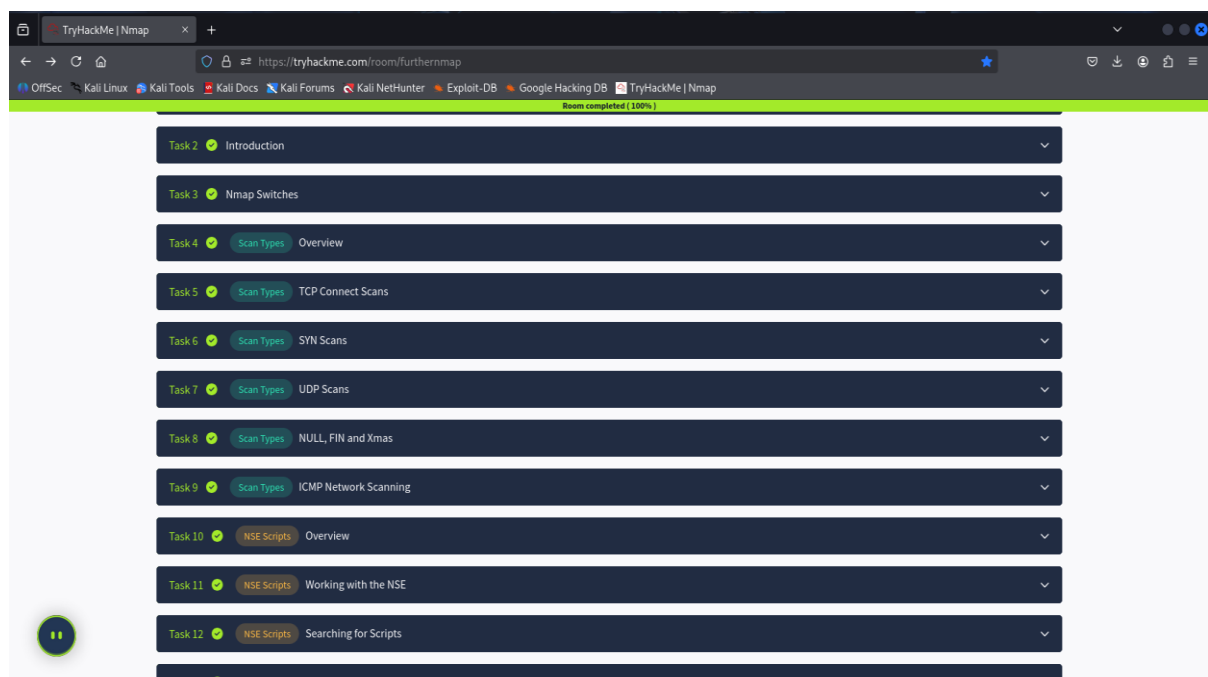
✓ Correct Answer

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

1024

✓ Correct Answer ? Hint

- **Task 4-9:** These tasks go over different scan types like TCP Connect, SYN, UDP, NULL, FIN, and Xmas scans, and ICMP network scanning.



- **Task 10-13:** These tasks introduce the Nmap Scripting Engine (NSE), how to work with scripts, and firewall evasion techniques.

TryHackMe | Nmap

https://tryhackme.com/room/furthernmap

Room progress (10%)

something or a machine and this 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

Hey, Congratulations! You submitted the correct answer for task 9 question 1. Keep it up!

king with the NSE

Task 12

NSE Scripts

Searching for Scripts

Apps

Places

Aug 10 3:59 AM

10.9.0.129

25%

59%

0.2 kB

0.2 kB

TryHackMe | Nmap

https://tryhackme.com/room/furthernmap

Room progress (81%)

`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 14

Practical

Hey, Congratulations! You submitted the correct answer for task 12 question 2. Keep it up!

How likely are you to recommend this room to others?

12345678910

(root@kali)-[/home/jesti]

cat /usr/share/nmap/scripts/smb-os-discovery.nse | grep "dependencies ="

dependencies = {"smb-brute"}

(root@kali)-[/home/jesti]

nmap --help | grep "random"

-iR <num hosts>: Choose random targets

-r: Scan ports sequentially - don't randomize

--data-length <num>: Append random data to sent packets

(root@kali)-[/home/jesti]


```

-P[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:
-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 sequentially - 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
--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).

```

Manual page nmap(1) line 81 (press h for help or q to quit)

```

root@kali: /home/jesti
nmap --script-help ftp-anon
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 04:42 EDT

ftp-anon
Categories: default auth safe
https://nmap.org/nse/doc/scripts/ftp-anon.html
  Checks if an FTP server allows anonymous logins.

  If anonymous is allowed, gets a directory listing of the root directory
  and highlights writable files.

root@kali: /home/jesti
cat /usr/share/nmap/scripts/script.db | grep "anon"
Entry { filename = "ftp-anon.nse", categories = { "auth", "default", "safe", } }

root@kali: /home/jesti
cat /usr/share/nmap/scripts/script.db | grep "smb"
Entry { filename = "smb-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "smb-double-pulsar-backdoor.nse", categories = { "malware", "safe", "vuln", } }
Entry { filename = "smb-enum-domains.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-groups.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-processes.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-services.nse", categories = { "discovery", "intrusive", "safe", } }
Entry { filename = "smb-enum-sessions.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-shares.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-users.nse", categories = { "auth", "intrusive", } }
Entry { filename = "smb-flood.nse", categories = { "dos", "intrusive", } }
Entry { filename = "smb-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-mbenum.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-os-discovery.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb-print-text.nse", categories = { "intrusive", } }
Entry { filename = "smb-protocols.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-psexec.nse", categories = { "intrusive", } }
Entry { filename = "smb-remote-exec.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb-server-stats.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-system-info.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-vuln-conficker.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-cve-2017-7494.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-vuln-cve2009-3103.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms06-025.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms07-029.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms08-067.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms10-054.nse", categories = { "dos", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms10-061.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms17-010.nse", categories = { "safe", "vuln", } }
Entry { filename = "smb-vuln-regsvc-dos.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-webexec.nse", categories = { "intrusive", "vuln", } }

```

3. Practical Scanning and Exploitation

Task 14 is the practical part of the room, where I use the learned Nmap techniques to scan the deployed machine and answer a series of questions.

Task 14 Practical

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 10.201.9.199

(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

- **Does the target respond to ICMP echo (ping) requests?** The answer is **N** (No), which I can determine because a standard ping fails, or by using `nmap -Pn` to assume the host is up.
- ♦ **Perform an Xmas scan on the first 999 ports. How many ports are shown to be open or filtered?** The command `nmap -sX -p 1-999 10.201.9.199` is used. The result shows **999** ports are `open|filtered`.

```
(root@kali)-[/home/jesti]
# nmap -nmap -vv -sX -Pn -p 0-999 10.201.9.199
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Warning: The -m option is deprecated. Please use -oG
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 04:08 EDT
Initiating XMAS Scan at 04:08
Scanning 10.201.9.199 [1000 ports]
```



```

(root@kali)-[/home/jesti]
# nmap -nmap -vv -sX -Pn -p 0-999 10.201.9.199
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Warning: The -m option is deprecated. Please use -oG
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 04:08 EDT
Initiating XMAS Scan at 04:08
Scanning 10.201.9.199 [1000 ports]
XMAS Scan Timing: About 15.50% done; ETC: 04:12 (0:02:49 remaining)
XMAS Scan Timing: About 30.50% done; ETC: 04:12 (0:02:19 remaining)
XMAS Scan Timing: About 45.00% done; ETC: 04:12 (0:01:51 remaining)
XMAS Scan Timing: About 60.00% done; ETC: 04:12 (0:01:21 remaining)
XMAS Scan Timing: About 75.00% done; ETC: 04:12 (0:00:50 remaining)
Completed XMAS Scan at 04:12, 201.33s elapsed (1000 total ports)
Nmap scan report for 10.201.9.199
Host is up, received user-set.
Scanned at 2025-08-10 04:08:57 EDT for 202s
All 1000 scanned ports on 10.201.9.199 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.38 seconds
Raw packets sent: 2000 (80.000KB) | Rcvd: 0 (0B)

```

```

(root@kali)-[/home/jesti]
# 
(root@kali)-[/home/jesti]
# nmap -nmap -vv -sX -Pn -p 0-999 10.201.9.199
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Warning: The -m option is deprecated. Please use -oG
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 04:08 EDT
Initiating XMAS Scan at 04:08
Scanning 10.201.9.199 [1000 ports]
XMAS Scan Timing: About 15.50% done; ETC: 04:12 (0:02:49 remaining)
XMAS Scan Timing: About 30.50% done; ETC: 04:12 (0:02:19 remaining)
XMAS Scan Timing: About 45.00% done; ETC: 04:12 (0:01:51 remaining)
XMAS Scan Timing: About 60.00% done; ETC: 04:12 (0:01:21 remaining)
XMAS Scan Timing: About 75.00% done; ETC: 04:12 (0:00:50 remaining)
Completed XMAS Scan at 04:12, 201.33s elapsed (1000 total ports)
Nmap scan report for 10.201.9.199
Host is up, received user-set.
Scanned at 2025-08-10 04:08:57 EDT for 202s
All 1000 scanned ports on 10.201.9.199 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.38 seconds
Raw packets sent: 2000 (80.000KB) | Rcvd: 0 (0B)

```

- ♦ There is a reason given for this – what is it? The reason given in the Nmap output is **no-response**.
- ♦ Perform a TCP SYN scan on the first 5000 ports. How many ports are shown to be open? Using the command `nmap -sS -p 1-5000 -Pn 10.201.9.199`, I found **5** open ports.

```

(root@kali)-[/home/jesti]
# nmap -nmap -vv -sS -Pn -p 0-5000 10.201.9.199
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Warning: The -m option is deprecated. Please use -oG
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 04:14 EDT
Initiating SYN Stealth Scan at 04:14
Scanning 10.201.9.199 [5001 ports]
Discovered open port 21/tcp on 10.201.9.199
Discovered open port 53/tcp on 10.201.9.199
Discovered open port 135/tcp on 10.201.9.199
Discovered open port 80/tcp on 10.201.9.199
Discovered open port 3389/tcp on 10.201.9.199

```

```
(root@kali)~/home/jesti
# nmap -nmap -vv -sS -Pn -p 0-5000 10.201.9.199
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Warning: The -m option is deprecated. Please use -oG
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 04:16 EDT
Initiating SYN Stealth Scan at 04:16
Scanning 10.201.9.199 [5001 ports]
Discovered open port 53/tcp on 10.201.9.199
Discovered open port 135/tcp on 10.201.9.199
Discovered open port 21/tcp on 10.201.9.199
Discovered open port 80/tcp on 10.201.9.199
Discovered open port 3389/tcp on 10.201.9.199
Completed SYN Stealth Scan at 04:17, 56.24s elapsed (5001 total ports)
Nmap scan report for 10.201.9.199
Host is up, received user-set (0.27s latency).
Scanned at 2025-08-10 04:16:44 EDT for 56s
Not shown: 4996 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 125
53/tcp    open  domain       syn-ack ttl 125
80/tcp    open  http         syn-ack ttl 125
135/tcp   open  msrpc        syn-ack ttl 125
3389/tcp  open  ms-wbt-server syn-ack ttl 125

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 56.30 seconds
Raw packets sent: 10032 (441.408KB) | Rcvd: 40 (1.760KB)
```

4. Conclusion

The "Further Nmap" room provides a solid, hands-on understanding of Nmap's more advanced capabilities. It effectively demonstrates how different scan types can be used to bypass firewall rules and how to leverage the Nmap Scripting Engine for deeper enumeration. The practical challenge reinforces the importance of choosing the right Nmap switches for a given scenario.

TryHackMe | Nmap
PLAYING

+

https://tryhackme.com/room/furthermap

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Woop woop! Your answer is correct

You did it! 🎉 Nmap complete!

Points earned
328

Completed tasks
15

Room type
Walkthrough

Difficulty
Easy

Streak
1

73,450 users are actively learning this week

Leave Feedback

Continue

