Task 3: Nmap Walkthrough

Maheshwar Anup

July 30, 2025

1 Objective

A walkthrough of the Nmap room on TryHackMe.

2 Steps

2.1 Deploy the target VM

- Go to the Nmap room on TryHackMe.
- Click on the ”Deploy” button to start the target VM.
- Wait for the VM to be deployed and the IP address to be assigned.
- Once the VM is ready, you will see the IP address in the room.
- Make sure to note down the IP address as you will need it for the Nmap scans.
- You can also use the ”Start Attack Box” button to launch an attack box if you prefer to use the web-based terminal.
- Alternatively, you can use your own terminal to connect to the target VM using openvpn, by downloading the corresponding ovpn file from the room.
- Once you have the IP address, you can proceed to the next step.

2.2 Extra insights on nmap and basic networking

- Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing.
- It can be used to discover hosts and services on a computer network, thus creating a ”map” of the network.
- Nmap can be used to perform various types of scans, including TCP connect scans, SYN scans, UDP scans, and more.
- It can also be used to detect operating systems, service versions, and even vulnerabilities in the target systems.
- Nmap is widely used by security professionals, network administrators, and penetration testers to assess the security of networks and systems.
- Understanding basic networking concepts such as IP addresses, ports, and protocols is essential for effectively using Nmap.
- An IP address is a unique identifier assigned to each device on a network, allowing them to communicate with each other.
- Ports are logical endpoints for communication, and they are associated with specific services running on a device.

- Protocols are rules that define how data is transmitted over a network, such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- Nmap can be used to scan a single host, a range of IP addresses, or an entire subnet.
- It can also perform more advanced scans, such as OS detection, version detection, and script scanning.
- Nmap provides various options and flags to customize the scans, such as specifying the scan type, timing options, and output formats.
- It is important to use Nmap responsibly and ethically, as scanning networks without permission can be considered illegal or malicious activity.
- Always ensure you have permission to scan the target network or system before using Nmap.
- Nmap is a versatile tool that can be used for both offensive and defensive security purposes, making it an essential tool in the arsenal of any cybersecurity professional.
- For more information on Nmap, you can refer to the official documentation at Nmap Documentation.
- Computer has a total 65535 ports, but many of them are reserved for specific services and protocols.
- Commonly used ports include:
  - Port 22: SSH (Secure Shell) for secure remote access.
  - Port 80: HTTP (Hypertext Transfer Protocol) for web traffic.
  - Port 443: HTTPS (HTTP Secure) for secure web traffic.
  - Port 21: FTP (File Transfer Protocol) for file transfers.
  - Port 25: SMTP (Simple Mail Transfer Protocol) for email sending.
- Functionality of Nmap can be extended with scripts, which can automate various tasks:
  - *Host Discovery*: Identifying live hosts on a network.
  - *Port Scanning*: Identifying open ports on a host.
  - *Service Version Detection*: Identifying the version of services running on open ports.
  - *OS Detection*: Identifying the operating system running on a host.
  - *Aggressive Scanning*: Combining multiple scan types to gather more information about the target.
  - *Script Scanning*: Running Nmap scripts for detecting vulnerabilities.
  - *Tcp vs Udp Scanning*: TCP scans are more reliable but can be detected, while UDP scans are stealthier but less reliable.
  - *Firewall Evasion Techniques*: Using techniques like fragmenting packets or changing the source port to bypass firewalls.

2.3 Understand the Nmap scan types

- Using the command `nmap --help` or `nmap -h` will display the help menu with available options and scan types.
- Nmap supports various scan types, each with its own purpose and characteristics. Here are some common scan types:
  - **TCP Connect Scan**: Establishes a full TCP connection to the target port. It is reliable but easily detectable.
  - **SYN Scan**: Sends SYN packets to the target ports and analyzes the responses. It is stealthier than a TCP connect scan. Also known as "half-open" scan.
  - **UDP Scan**: Sends UDP packets to the target ports and checks for responses. It is used to discover open UDP ports.

  - **ACK Scan**: Used to map out firewall rules by sending ACK packets to the target ports.
  - **FIN Scan**: Sends FIN packets to the target ports, which can sometimes bypass firewalls.
  - **Null Scan**: Sends packets with no flags set, which can also bypass some firewalls.
  - **Xmas Scan**: Sends packets with the FIN, URG, and PSH flags set, which can confuse some firewalls.

- Further explore other options and scan types by referring to the Nmap documentation or using the `nmap --help` command.
- Nmap also supports various timing options to control the speed and stealthiness of the scans. You can use the `-T` option followed by a number from 0 (paranoid) to 5 (insane) to adjust the timing. For example:

  ```
  nmap -T4 <target_ip>
  ```

  for a faster scan.

  ```
  nmap -T0 <target_ip>
  ```

  for a very slow and stealthy scan.
- Additionally, Nmap allows you to specify the ports to scan using the `-p` option. For example:

  ```
  nmap -p 22,80,443 <target_ip>
  ```

  This command will scan only ports 22, 80, and 443 on the target IP address.
- You can also specify a range of ports using a hyphen:

  ```
  nmap -p 1-1000 <target_ip>
  ```

  This command will scan ports 1 to 1000 on the target IP address.
- Nmap can also perform service version detection using the `-sV` option, which attempts to determine the version of the services running on open ports:

  ```
  nmap -sV <target_ip>
  ```

- Nmap can also perform operating system detection using the `-O` option, which attempts to identify the operating system running on the target host:

  ```
  nmap -O <target_ip>
  ```

- Nmap can output the scan results in various formats, such as plain text, XML, or grepable format. You can use the `-oN`, `-oX`, or `-oG` options to specify the output format:

  ```
  nmap -oN output.txt <target_ip>
  ```

2.4 Perform Nmap scans

- Open your terminal or the attack box provided by TryHackMe.
- Use the following command to perform a basic Nmap scan on the target VM:

  ```
  nmap <target_ip>
  ```

2.5 Deep dive into TCP scan

- To perform a TCP connect scan, use the following command:

  ```
  nmap -sT <target_ip>
  ```

- If the firewall is blocking the scan, the server responds with a TCP RST (reset) packet, indicating that the port is closed.
- If the port is open, the server responds with a SYN-ACK packet, indicating that the port is open and ready to accept connections.

2.6 Deep dive into SYN scan

- To perform a SYN scan, use the following command:

  ```
  nmap –sS <target_ip>
  ```

- SYN scan is also known as a "half-open" scan because it does not complete the TCP handshake.
- If the port is open, the server responds with a SYN-ACK packet, indicating that the port is open and ready to accept connections.
- If the port is closed, the server responds with a TCP RST (reset) packet, indicating that the port is closed.
- If the port is filtered, the server does not respond, indicating that the port is either blocked by a firewall or not reachable.
- The main advantage for using SYN scan is that it is stealthier than a TCP connect scan, as it does not establish a full connection.
- This makes it less likely to be detected by intrusion detection systems (IDS) or firewalls.

2.7 Deep dive into UDP scan

- To perform a UDP scan, use the following command:

  ```
  nmap –sU <target_ip>
  ```

- UDP scans are used to discover open UDP ports on the target host.
- Unlike TCP scans, UDP scans do not establish a connection, making them more challenging to detect.
- If the port is open, the server may respond with a UDP packet, indicating that the port is open and ready to accept data.
- If the port is closed, the server may respond with an ICMP "port unreachable" message, indicating that the port is closed.
- If the port is filtered, the server may not respond at all, indicating that the port is either blocked by a firewall or not reachable.
- UDP scans can be slower than TCP scans because they do not provide reliable feedback like TCP does.

2.8 Deep dive into FIN,Null and Xmas scans

- To perform a FIN scan, use the following command:

  ```
  nmap –sF <target_ip>
  ```

- FIN scan sends TCP packets with the FIN flag set to the target ports.
- If the port is open, the server does not respond, indicating that the port is open.
- If the port is closed, the server responds with a TCP RST (reset) packet, indicating that the port is closed.
- If the port is filtered, the server does not respond, indicating that the port is either blocked by a firewall or not reachable.
- To perform a Null scan, use the following command:

  ```
  nmap –sN <target_ip>
  ```

- Null scan sends TCP packets with no flags set to the target ports.

- If the port is open, the server does not respond, indicating that the port is open.
- If the port is closed, the server responds with a TCP RST (reset) packet, indicating that the port is closed.
- If the port is filtered, the server does not respond, indicating that the port is either blocked by a firewall or not reachable.
- To perform an Xmas scan, use the following command:

  ```
  nmap -sX <target_ip>
  ```

- Xmas scan sends TCP packets with the FIN, URG, and PSH flags set to the target ports.
- If the port is open, the server does not respond, indicating that the port is open.
- If the port is closed, the server responds with a TCP RST (reset) packet, indicating that the port is closed.
- If the port is filtered, the server does not respond, indicating that the port is either blocked by a firewall or not reachable.
- These scans are often used to bypass firewalls and intrusion detection systems (IDS) because they do not follow the standard TCP handshake process.

2.9 Deep dive into ICMP scans

- To perform a ping sweep using ICMP echo requests, use the following command:

  ```
  nmap -sn <target_ip>
  ```

- Use either CIDR notation or ip address range to specify the target range.
- For example, to scan the entire subnet:

  ```
  nmap -sn <target_ip>/24
  ```

  or

  ```
  nmap -sn <target_ip>-<target_ip>
  ```

2.9.1 Subnetting/CIDR notation

- CIDR (Classless Inter-Domain Routing) notation is a way to represent IP addresses and their associated network masks.
- It is commonly used in networking to define IP address ranges and subnets.
- CIDR notation consists of an IP address followed by a slash (/) and a number that represents the number of bits in the subnet mask.
- Contains 2 parts
  - Host part: The part of the IP address that identifies a specific device on the network.
  - Network part: The part of the IP address that identifies the network to which the device belongs.
  - The number after the slash indicates how many bits are used for the network part of the address.
- To learn more about subneting visit Subnetting Guide.
- To visualize it visit here and download the html page.

2.10 Deep dive into NSE scripts

- Nmap Scripting Engine (NSE) allows users to write scripts to automate various tasks and extend Nmap's functionality.
- NSE scripts can be used for tasks such as service version detection, vulnerability scanning, and more.
- To run a specific NSE script, use the `--script` option followed by the script name:

  ```
  nmap --script <script_name> <target_ip>
  ```

- Script help command can be used to get more information about a specific script:

  ```
  nmap --script-help <script_name>
  ```

- This command will display the description, usage, and options for the specified script.
- To manually search for scripts, you can navigate to the Nmap scripts directory, which is typically located at `/usr/share/nmap/scripts/` on Linux systems.

2.11 Deep dive into Firewall evasion techniques

- Nmap provides various techniques to evade firewalls and intrusion detection systems (IDS) during scans.
- Some common techniques include:
  - **Fragmentation**: Splitting packets into smaller fragments to bypass firewalls that may block larger packets.

    ```
    nmap -f <target_ip>
    ```

  - **Decoy Scanning**: Using decoy IP addresses to confuse intrusion detection systems and make it harder to trace the source of the scan.

    ```
    nmap -D RND:10 <target_ip>
    ```

  - **Source Port Manipulation**: Changing the source port of the scan packets to avoid detection by firewalls.

    ```
    nmap --source-port <port_number> <target_ip>
    ```

  - **Timing Options**: Adjusting the timing of the scan to avoid detection by IDS or firewalls.

    ```
    nmap -T0 <target_ip>  # Very slow and stealthy scan
    ```

  - **Bad sum**: Sending packets with incorrect checksums to bypass some firewalls.

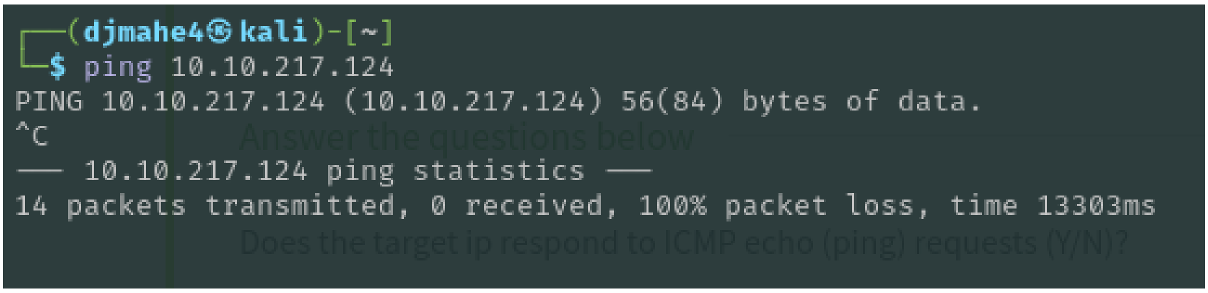
    ```
    nmap --badsum <target_ip>
    ```

  - **Idle Scan**: Using a third-party host to send packets to the target, making it harder to trace the scan back to the source.

    ```
    nmap -sI <zombie_ip> <target_ip>
    ```

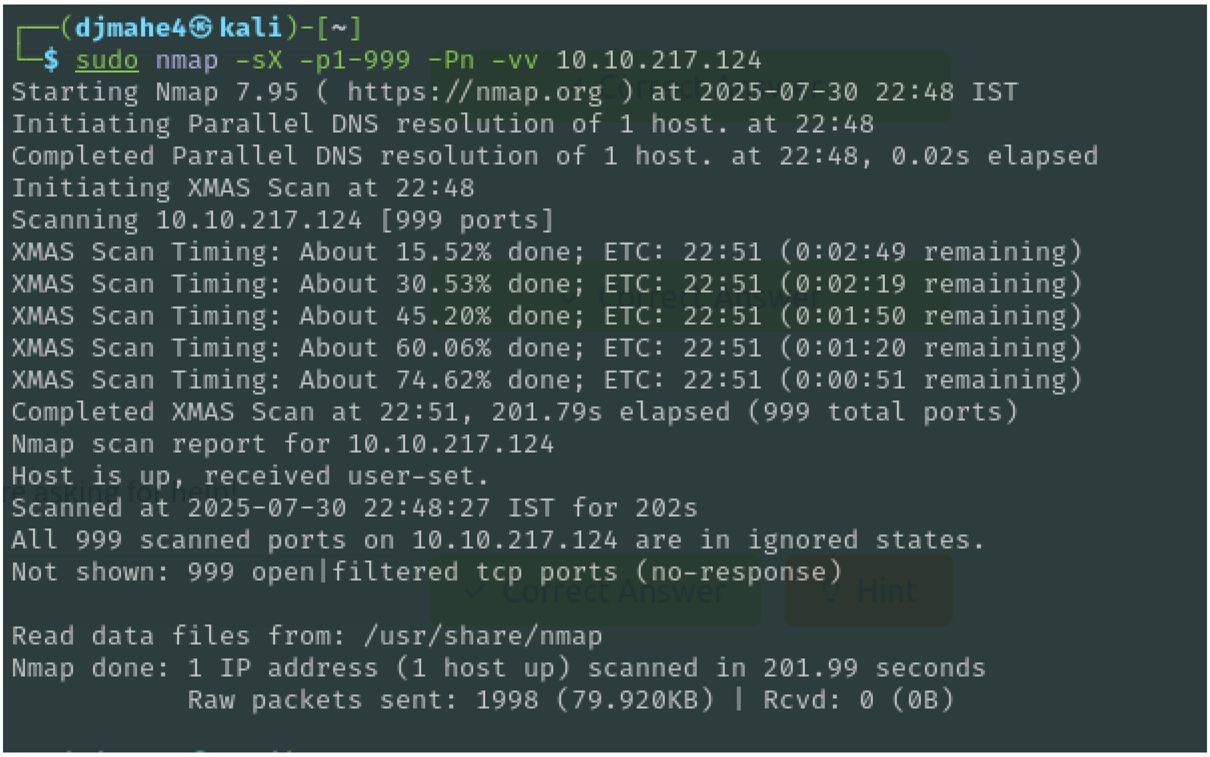
2.12 Practical Application

- Now that you have learned about Nmap and its various scan types, you can apply your knowledge to perform scans on the target VM.



```
┌──(djmahe4㉿kali)-[~]
└─$ ping 10.10.217.124
PING 10.10.217.124 (10.10.217.124) 56(84) bytes of data.
^C
--- 10.10.217.124 ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 13303ms
```

Figure 1: Pinging the target machine.



```
┌──(djmahe4㉿kali)-[~]
└─$ sudo nmap -sX -p1-999 -Pn -vv 10.10.217.124
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 22:48 IST
Initiating Parallel DNS resolution of 1 host. at 22:48
Completed Parallel DNS resolution of 1 host. at 22:48, 0.02s elapsed
Initiating XMAS Scan at 22:48
Scanning 10.10.217.124 [999 ports]
XMAS Scan Timing: About 15.52% done; ETC: 22:51 (0:02:49 remaining)
XMAS Scan Timing: About 30.53% done; ETC: 22:51 (0:02:19 remaining)
XMAS Scan Timing: About 45.20% done; ETC: 22:51 (0:01:50 remaining)
XMAS Scan Timing: About 60.06% done; ETC: 22:51 (0:01:20 remaining)
XMAS Scan Timing: About 74.62% done; ETC: 22:51 (0:00:51 remaining)
Completed XMAS Scan at 22:51, 201.79s elapsed (999 total ports)
Nmap scan report for 10.10.217.124
Host is up, received user-set.
Scanned at 2025-07-30 22:48:27 IST for 202s
All 999 scanned ports on 10.10.217.124 are in ignored states.
Not shown: 999 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.99 seconds
           Raw packets sent: 1998 (79.920KB) | Rcvd: 0 (0B)
```

Figure 2: Xmas scan on the target.

2.12.1 Step1: Tried to ping the machine

2.12.2 Step2: Performed Xmas scan on the target

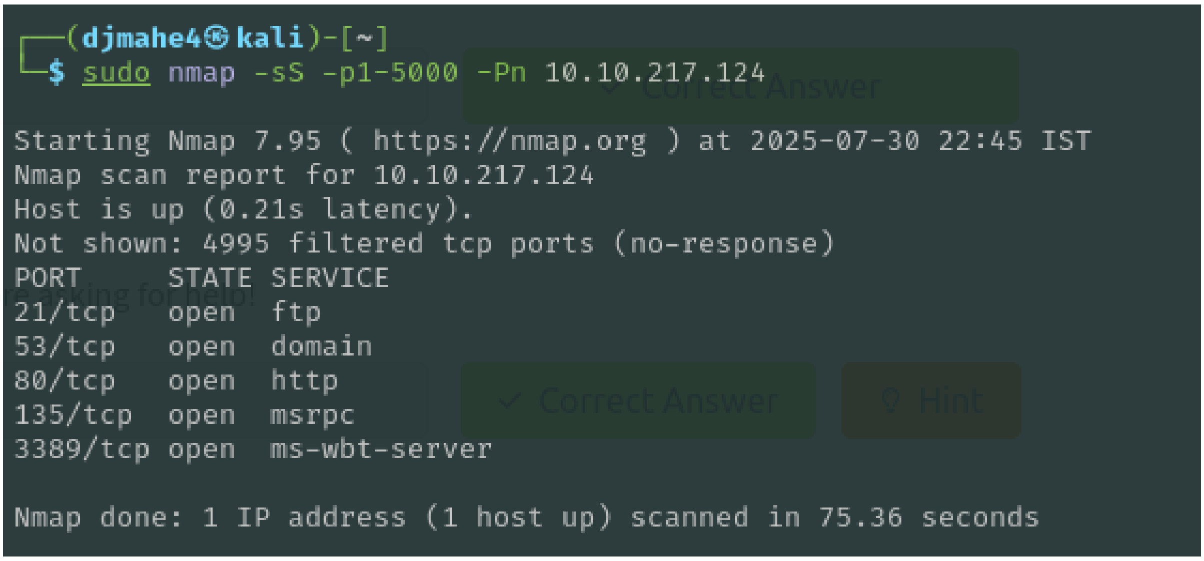
- Performed an Xmas scan
- Host down reply indicate that the ports are closed or filtered.
- This is because the target VM is configured to block certain types of scans, including Xmas scans.

2.12.3 Step3: Performed a TCP SYN scan

- Performed a TCP SYN scan for first 5000 ports

2.12.4 Step4: Performed a TCP connect scan

- Wireshark shows that the target VM is responding to the TCP connect scan.
- Anonymous login is allowed while scanned with `ftp-anon.nse` script.

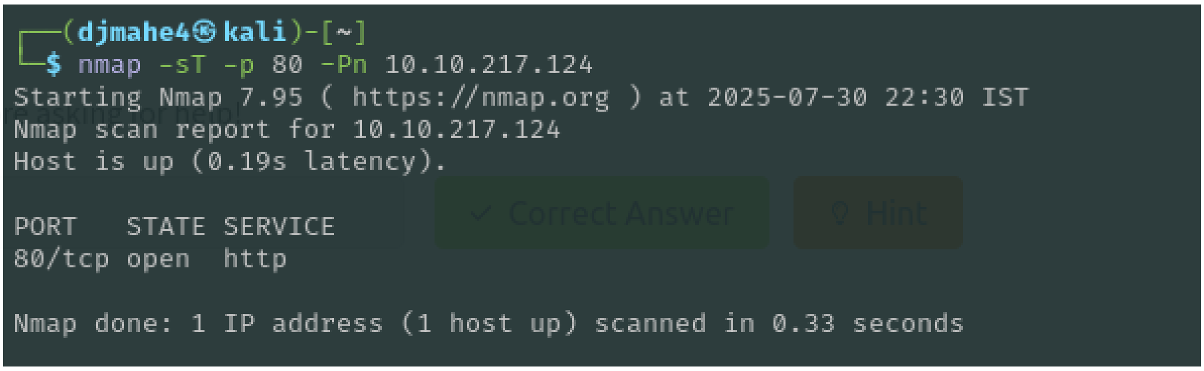


```
┌──(djmahe4㉿kali)-[~]
└─$ sudo nmap -sS -p1-5000 -Pn 10.10.217.124

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 22:45 IST
Nmap scan report for 10.10.217.124
Host is up (0.21s latency).
Not shown: 4995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 75.36 seconds
```

Figure 3: TCP SYN scan for first 5000 ports.

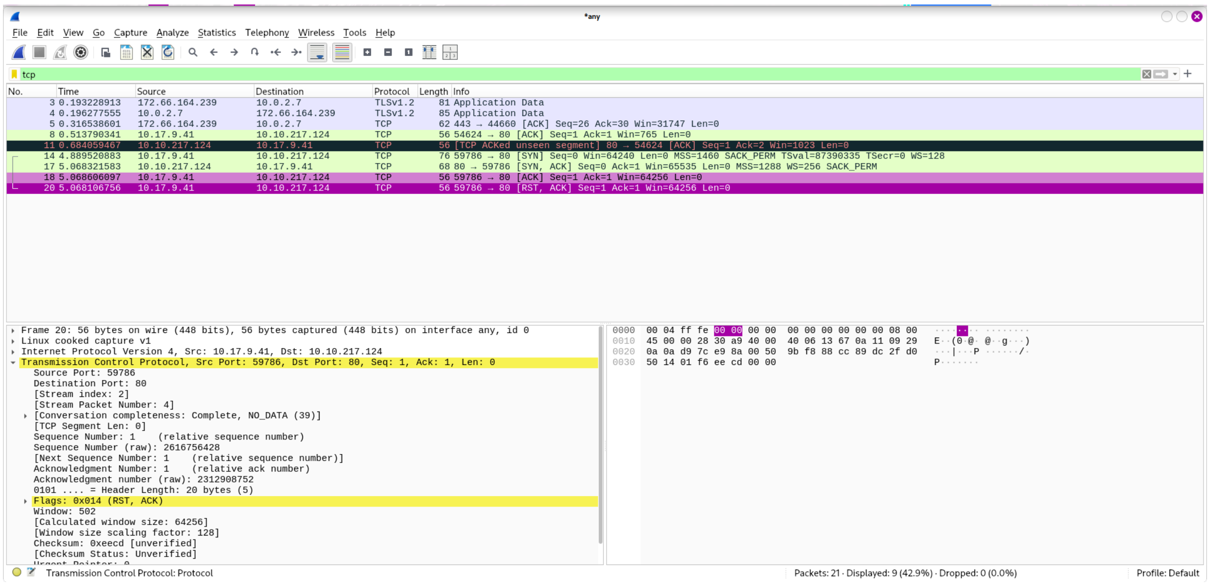


```
┌──(djmahe4㉿kali)-[~]
└─$ nmap -sT -p 80 -Pn 10.10.217.124
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 22:30 IST
Nmap scan report for 10.10.217.124
Host is up (0.19s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Figure 4: TCP connect scan.


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

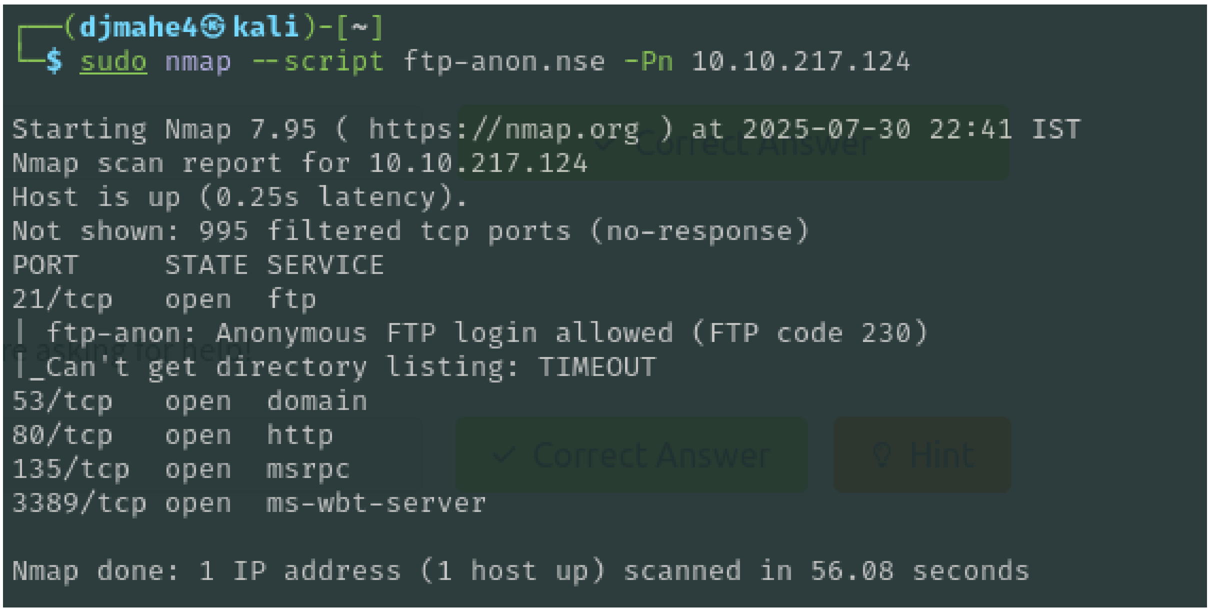
```
No.  Time         Source          Destination    Protocol Length Info
   3 0.193228913  172.66.164.239  10.0.2.7       TLSv1.2  81 Application Data
   4 0.196277555  10.0.2.7        172.66.164.239 TLSv1.2  85 Application Data
   5 0.316538601  172.66.164.239  10.0.2.7       TCP      62 443 → 44660 [ACK] Seq=26 Ack=30 Win=31747 Len=0
   8 0.513790341  10.17.9.41      10.10.217.124  TCP      56 54624 → 80 [ACK] Seq=1 Ack=1 Win=765 Len=0
  11 0.684059467  10.10.217.124   10.17.9.41     TCP      56 [TCP ACKed unseen segment] 80 → 54624 [ACK] Seq=1 Ack=2 Win=1023 Len=0
  14 4.889520883  10.17.9.41      10.10.217.124  TCP      76 59786 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=87390335 TSecr=0 WS=128
  17 5.068321583  10.10.217.124   10.17.9.41     TCP      68 80 → 59786 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1288 WS=256 SACK_PERM
  18 5.068606097  10.17.9.41      10.10.217.124  TCP      56 59786 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
  20 5.068106756  10.17.9.41      10.10.217.124  TCP      56 59786 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
```

```
▸ Frame 20: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 10.17.9.41, Dst: 10.10.217.124
▾ Transmission Control Protocol, Src Port: 59786, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 59786
    Destination Port: 80
    [Stream index: 2]
    [Stream Packet Number: 4]
  ▸ [Conversation completeness: Complete, NO_DATA (39)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2616756428
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2312908752
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x014 (RST, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0xeecd [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

```
0000  00 04 ff fe 00 00 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 28 30 a9 40 00  40 06 13 67 0a 11 09 29   E··(0·@· @··g···)
0020  0a 0a d9 7c e9 8a 00 50  9b f8 88 cc 89 dc 2f d0   ···|···P ······/·
0030  50 14 01 f6 ee cd 00 00                            P·······
```

```
Transmission Control Protocol: Protocol     Packets: 21 · Displayed: 9 (42.9%) · Dropped: 0 (0.0%)     Profile: Default
```

Figure 5: Wireshark capture of the TCP connect scan.



```
┌──(djmahe4㉿kali)-[~]
└─$ sudo nmap --script ftp-anon.nse -Pn 10.10.217.124

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 22:41 IST
Nmap scan report for 10.10.217.124
Host is up (0.25s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 56.08 seconds
```

Figure 6: Anonymous FTP login allowed.

2.12.5 Bonus: `-Pn` option

- The `-Pn` option in Nmap is used to skip host discovery and treat all specified hosts as online.
- This option is useful when you know that the target hosts are online but do not want to perform a ping sweep or other host discovery methods.

3 Conclusion

In this walkthrough, we explored the Nmap room on TryHackMe and learned about various Nmap scan types, including TCP connect scans, SYN scans, UDP scans, FIN scans, Null scans, Xmas scans, ICMP scans, NSE scripts, and firewall evasion techniques. We also applied our knowledge by performing practical scans on the target VM. Nmap is a powerful tool for network discovery and security auditing, and understanding its capabilities is essential for any cybersecurity professional.