NAME: VEDANT JOSHI

REG NO: 2462168

Assignment

TCP and UDP Port Discovery on scanme.nmap.org

Index

Introduction:

The goal of this assignment is to perform TCP and UDP port discovery on scanme.nmap.org using Nmap, document the steps, findings, and lessons learned. This reinforces skills in network reconnaissance and ethical hacking.

Methodology:

A. TCP SYN SCAN

- **Command :** `nmap -sS scanme.nmap.org -oN tcp_results.txt`
- **Purpose :** Stealthy scan to detect open TCP ports.

B. UDP TOP 100 SCAN

- **Command :** `sudo nmap -sU --top-ports 100 scanme.nmap.org -oN udp_results.txt`
- **Purpose :** Find open UDP services among the 100 most common UDP ports.

SCAN RESULTS:

A. TCP Scan Output

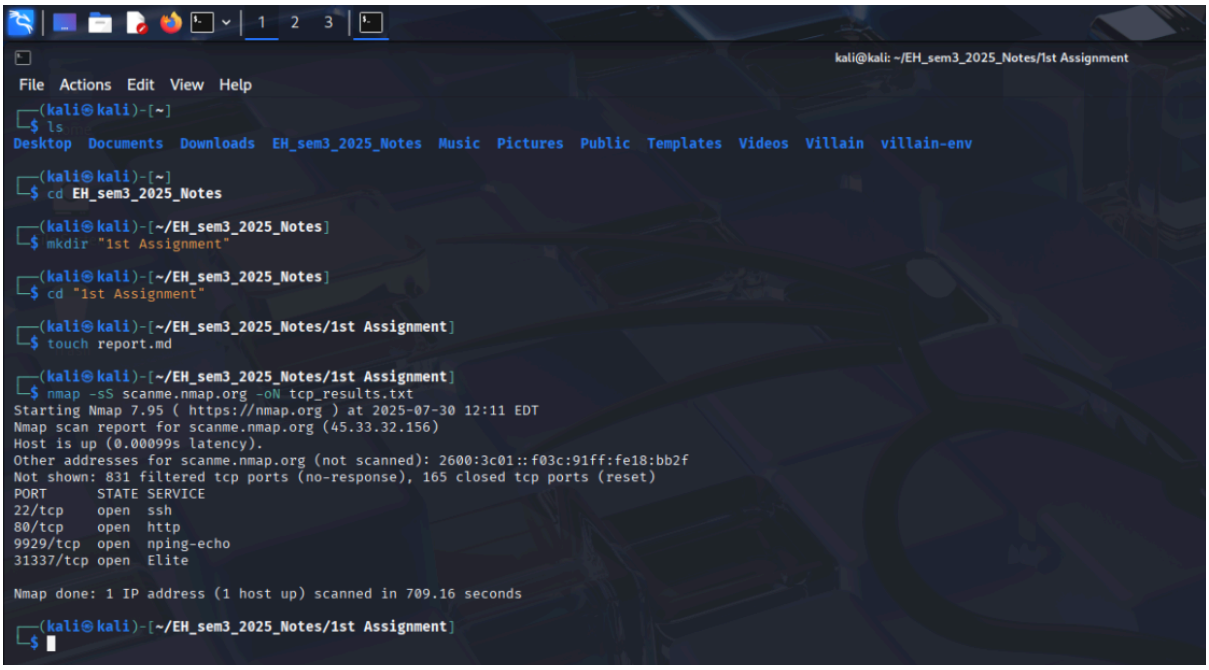
Port	State	Service
22	open	ssh
80	open	http

B. UDP Scan Output

All 100 scanned ports showed as:
> `open|filtered` – No response received; Nmap cannot distinguish between open and filtered due to the nature of UDP scanning.

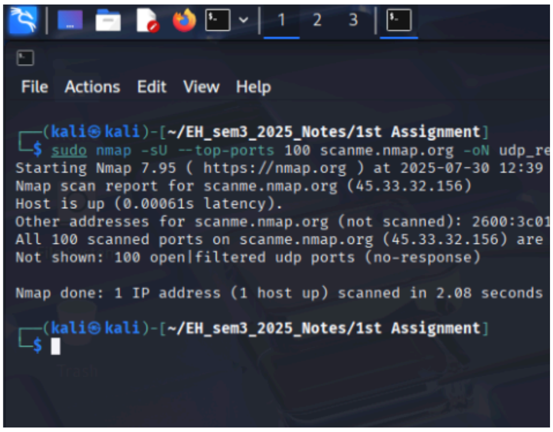
Visual Evidence:

TCP Scan Terminal Output


1 2 3
kali@kali: ~/EH_sem3_2025_Notes/1st Assignment
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  EH_sem3_2025_Notes  Music  Pictures  Public  Templates  Videos  Villain  villain-env

┌──(kali㉿kali)-[~]
└─$ cd EH_sem3_2025_Notes

┌──(kali㉿kali)-[~/EH_sem3_2025_Notes]
└─$ mkdir "1st Assignment"

┌──(kali㉿kali)-[~/EH_sem3_2025_Notes]
└─$ cd "1st Assignment"

┌──(kali㉿kali)-[~/EH_sem3_2025_Notes/1st Assignment]
└─$ touch report.md

┌──(kali㉿kali)-[~/EH_sem3_2025_Notes/1st Assignment]
└─$ nmap -sS scanme.nmap.org -oN tcp_results.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 12:11 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00099s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 831 filtered tcp ports (no-response), 165 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 709.16 seconds

┌──(kali㉿kali)-[~/EH_sem3_2025_Notes/1st Assignment]
└─$ 
```

UDP Scan Terminal Output



```
┌──(kali㉿kali)-[~/EH_sem3_2025_Notes/1st Assignment]
└─$ sudo nmap -sU --top-ports 100 scanme.nmap.org -oN udp_re
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 12:39
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00061s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01
All 100 scanned ports on scanme.nmap.org (45.33.32.156) are
Not shown: 100 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds

┌──(kali㉿kali)-[~/EH_sem3_2025_Notes/1st Assignment]
└─$ 
```

TCP VS UDP:

TCP (Transmission Control Protocol):

- Connection-oriented protocol; establishes a handshake before transmitting data.
- Ensures reliable delivery: packets arrive in order and are re-transmitted if lost.
- Commonly used for services like web (HTTP), email (SMTP), and file transfers (FTP).
- Easier to scan for open ports, as TCP responds reliably.

UDP (User Datagram Protocol):

- Connectionless protocol; sends packets without checking if the receiver is ready or even present.
- No guarantees for order or delivery—packets may arrive out of order or get lost without notice.
- Used for services requiring speed and low overhead, like DNS, VoIP, and streaming.
- Harder to scan: many UDP ports don’t respond to probes, and firewall rules often block or silently drop UDP traffic, resulting in ambiguous scan results (open|filtered).

Conclusion:

This assignment successfully demonstrated the practical application of Nmap for TCP and UDP port discovery on the target scanme.nmap.org. The investigation yielded distinct results that underscore the fundamental differences between the two protocols.

The TCP SYN scan effectively and reliably identified two open ports: 22 (SSH) and 80 (HTTP). This outcome highlights the definitive nature of TCP scanning, made possible by the protocol's connection-oriented design which provides clear responses.

In contrast, the UDP scan resulted in an open|filtered state for all 100 scanned ports. This ambiguity is a direct reflection of the challenges inherent in UDP scanning. Due to its connectionless nature, services often don't respond to probes, and firewalls commonly drop unexpected UDP packets, making it difficult to distinguish an open port from a filtered one.