CHRIST
UNIVERSITY
BENGALURU, INDIA

Declared as Deemed to be University under Section 3 of UGC Act 1956

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING

CYBERSECURITY-ETHICAL HACKING

B. Tech - Computer Science and Engineering
(Artificial Intelligence and Machine Learning)

SCHOOL OF ENGINEERING AND TECHNOLOGY,
CHRIST (Deemed to be University),
Kumbalgodu, Bengaluru-560 074

NAME: SASMITA S

REG NO. : 2462144

CLASS : 3BTCS AIML C

Assignment 1: TCP and UDP Port Discovery using Nmap

TOOL USED: nmap on Kali Linux

TARGET:scanme.nmap.org

Methodology

1. **TCP Port Scan:**

   Command used:

   ```
   nmap -sS scanme.nmap.org -oN tcp_scan.txt
   ```

   > This performed a stealth TCP SYN scan to discover open ports.

   > Output was saved in tcp_scan.txt.

2. **UDP Port Scan:**

   Command used:

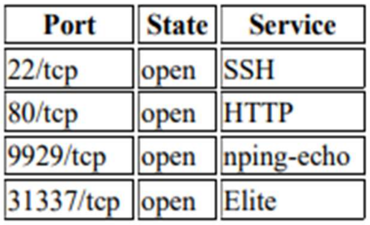
   ```
   sudo nmap -sU scanme.nmap.org -oN udp_scan.txt
   ```

   > This scanned for open UDP ports.

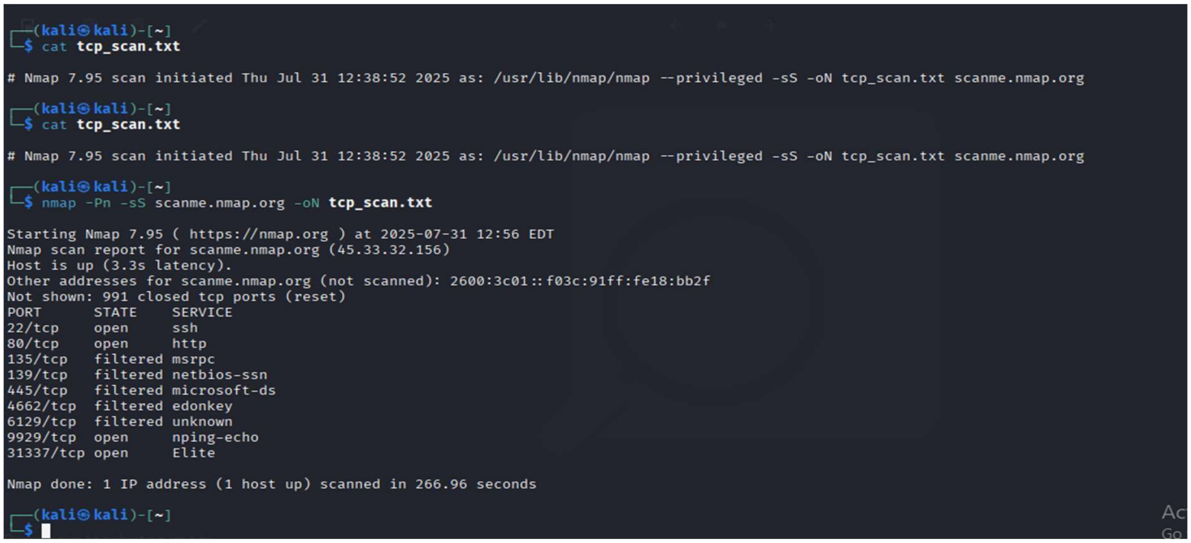
   > Output was saved in udp_scan.txt

Findings

From TCP Scan



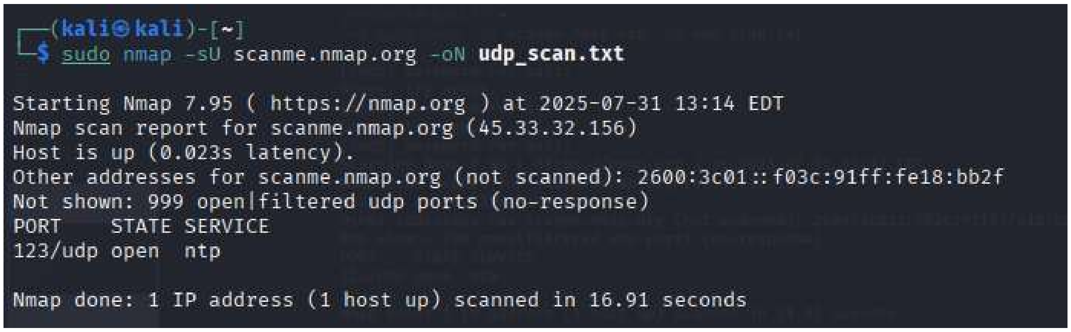
Port	State	Service
22/tcp	open	SSH
80/tcp	open	HTTP
9929/tcp	open	nping-echo
31337/tcp	open	Elite



```
┌──(kali㉿kali)-[~]
└─$ cat tcp_scan.txt

# Nmap 7.95 scan initiated Thu Jul 31 12:38:52 2025 as: /usr/lib/nmap/nmap --privileged -sS -oN tcp_scan.txt scanme.nmap.org

┌──(kali㉿kali)-[~]
└─$ cat tcp_scan.txt

# Nmap 7.95 scan initiated Thu Jul 31 12:38:52 2025 as: /usr/lib/nmap/nmap --privileged -sS -oN tcp_scan.txt scanme.nmap.org

┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sS scanme.nmap.org -oN tcp_scan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 12:56 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (3.3s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
4662/tcp  filtered edonkey
6129/tcp  filtered unknown
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 266.96 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

From UDP Scan

Port	State	Service
123/udp	open	NTP (Time Sync)



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU scanme.nmap.org -oN udp_scan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 13:14 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.023s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 999 open|filtered udp ports (no-response)
PORT    STATE SERVICE
123/udp open  ntp

Nmap done: 1 IP address (1 host up) scanned in 16.91 seconds
```

Conclusion:

TCP is connection-oriented, reliable, and ensures delivery of packets. It's suitable for services like HTTP, SSH.

UDP is connectionless, faster but unreliable — used for lightweight tasks like time sync (NTP).

The scan showed that the host had 4 open TCP ports and 1 open UDP port, with most other ports either closed or filtered.