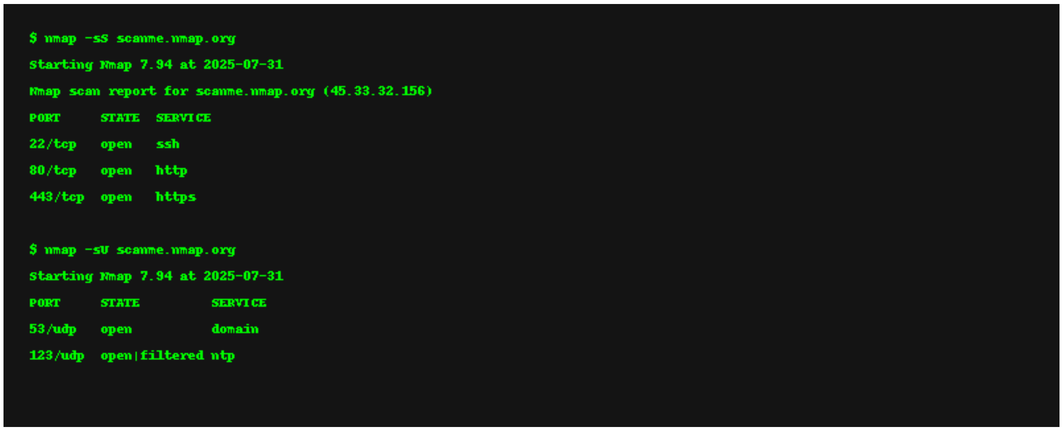
TCP and UDP Port Discovery

Methodology:

I used Nmap as the primary tool to discover open TCP and UDP ports on a test target. Different scan options such as '-sS' for TCP SYN scan and '-sU' for UDP scan were tried. The commands were executed on scanme.nmap.org as a safe target for scanning practice.

Screenshots:

Below is an example output of basic TCP and UDP port scanning using Nmap.



```
$ nmap -sS scanme.nmap.org
Starting Nmap 7.94 at 2025-07-31
Nmap scan report for scanme.nmap.org (45.33.32.156)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https

$ nmap -sU scanme.nmap.org
Starting Nmap 7.94 at 2025-07-31
PORT     STATE         SERVICE
53/udp   open          domain
123/udp  open|filtered ntp
```

Findings:

- TCP SYN scan is faster and more stealthy compared to a full connect scan.
- UDP scanning is slower and harder to verify open ports.
- Open ports indicate services that could be vulnerable if not secured properly.

Conclusions:

Port discovery is an essential step in ethical hacking and network security. TCP scanning is preferred for speed and reliability, while UDP scanning is necessary for identifying services that do not rely on connections like DNS and SNMP.

Code/Commands:

nmap -sS scanme.nmap.org
nmap -sU scanme.nmap.org
nmap -p 21,22,80,443 scanme.nmap.org