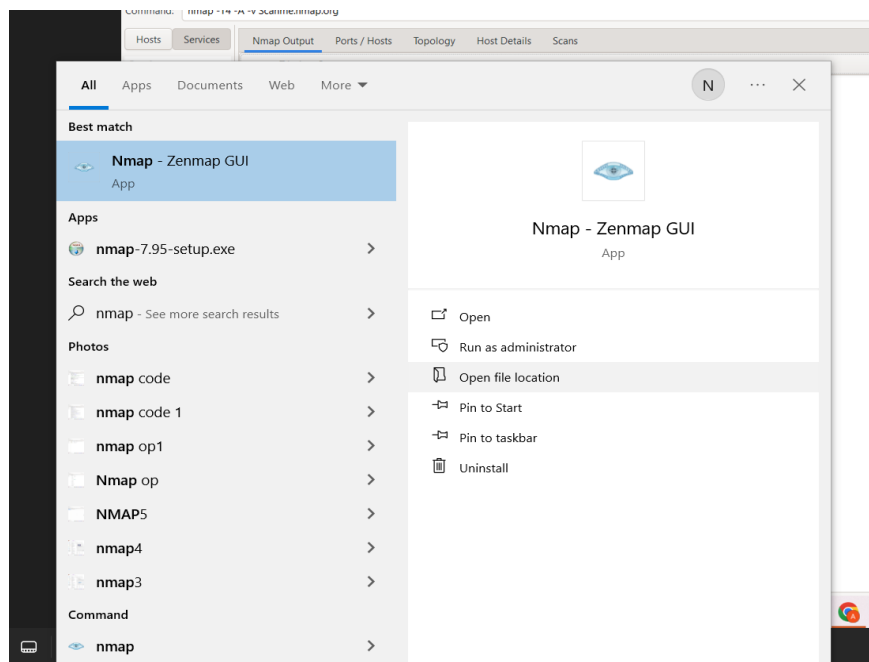
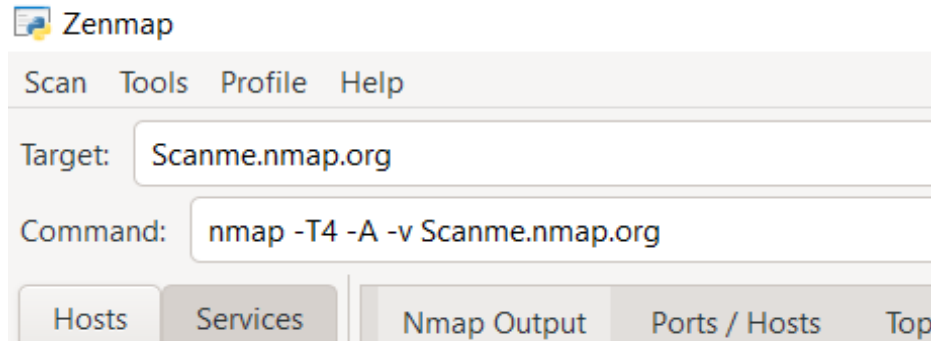


# Nmap (Zenmap):

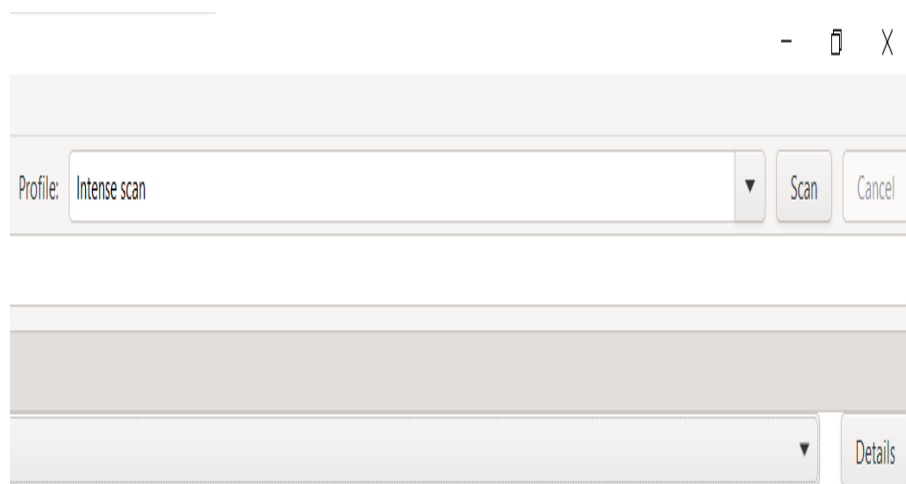
Step 1: Go to search box and type Nmap



Step 2: Open the Nmap and type Scanme.nmap.org in target section.

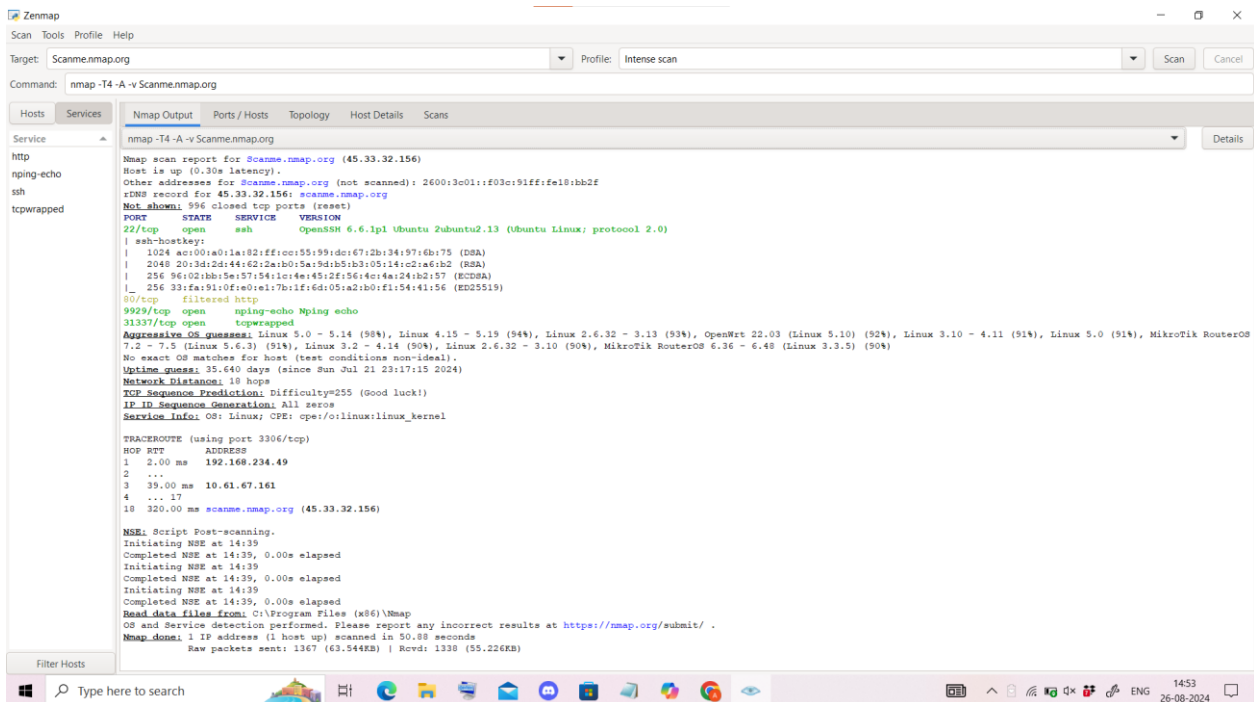


Step 3: And in profile, select intense scan and click on Scan



## Output:

- You will get all the information regarding the website

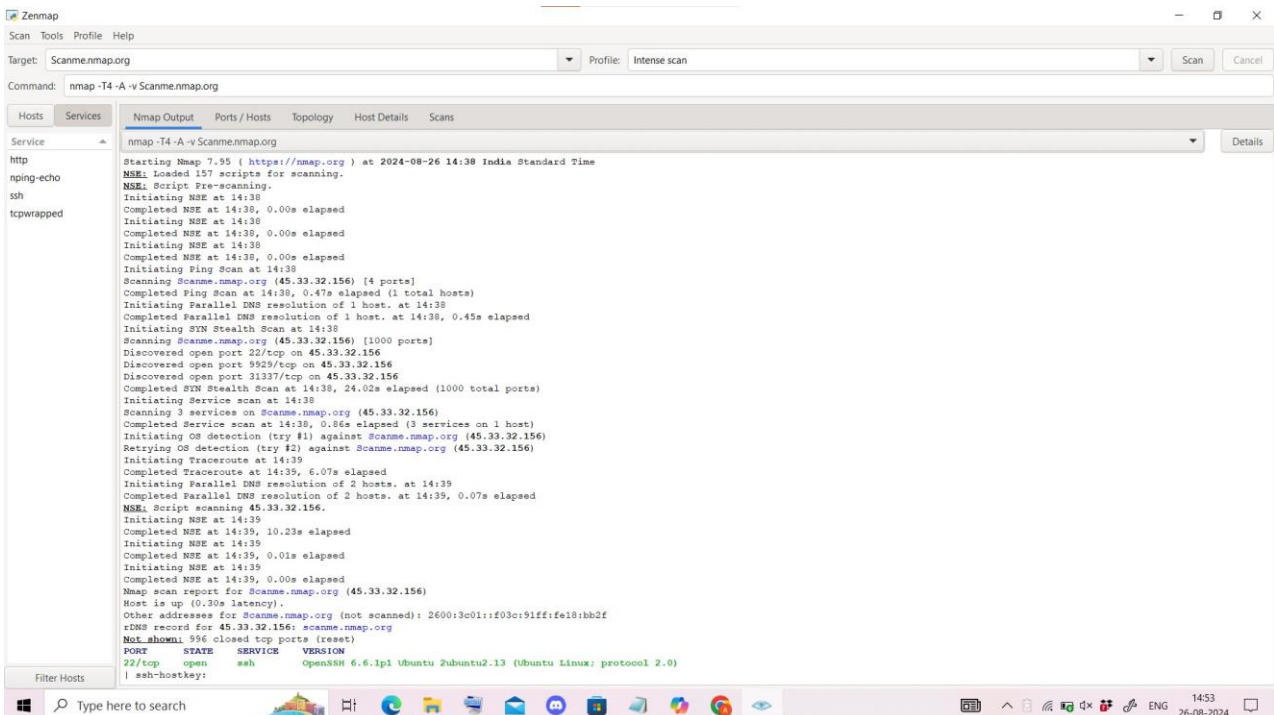


The screenshot shows the Zenmap application window with the target set to Scanme.nmap.org and the command nmap -T4 -A -v Scanme.nmap.org. The Nmap Output pane displays the following information:

```
Nmap scan report for Scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Other addresses for Scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 596 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 ac:00:a0:1a:82:ff:ce:55:99:de:67:2b:34:97:6b:75 (DSA)
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4e:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:el:7b:1f:6d:05:a2:b0:fi:54:41:56 (ED25519)
9929/tcp  filtered http
31337/tcp open  tcpwrapped
Aggressive OS guesses: Linux 5.0 - 5.14 (98%), Linux 4.15 - 5.19 (94%), Linux 2.6.32 - 3.13 (93%), OpenWrt 22.03 (Linux 5.10) (92%), Linux 3.10 - 4.11 (91%), Linux 5.0 (91%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (91%), Linux 3.2 - 4.14 (90%), Linux 2.6.32 - 3.10 (90%), MikroTik RouterOS 6.36 - 6.48 (Linux 3.3.5) (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 35.640 days (since Sun Jul 21 23:17:15 2024)
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3306/tcp)
HOP RTT ADDRESS
1 2.00 ms 192.168.234.49
2 ...
3 39.00 ms 10.61.67.161
4 ... 17
10 320.00 ms scanme.nmap.org (45.33.32.156)

NSE: Script Post-scanning.
Initiating NSE at 14:39
Completed NSE at 14:39, 0.00s elapsed
Initiating NSE at 14:39
Completed NSE at 14:39, 0.00s elapsed
Initiating NSE at 14:39
Completed NSE at 14:39, 0.00s elapsed
Initiating NSE at 14:39
Completed NSE at 14:39, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.88 seconds
Raw packets sent: 1367 (63.544KB) | Rcvd: 1330 (55.226KB)
```



The screenshot shows the Zenmap application window with the target set to Scanme.nmap.org and the command nmap -T4 -A -v Scanme.nmap.org. The Nmap Output pane displays the following information:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-26 14:38 India Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:38
Completed NSE at 14:38, 0.00s elapsed
Initiating NSE at 14:38
Completed NSE at 14:38, 0.00s elapsed
Initiating NSE at 14:38
Completed NSE at 14:38, 0.00s elapsed
Initiating Ping Scan at 14:38
Completed Ping Scan at 14:38, 0.47s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:38
Completed Parallel DNS resolution of 1 host. at 14:38, 0.45s elapsed
Initiating SYN Stealth Scan at 14:38
Scanning Scanme.nmap.org (45.33.32.156) [4 ports]
Completed SYN Stealth Scan at 14:38, 24.02s elapsed (1000 total ports)
Initiating Service scan at 14:38
Scanning 3 services on Scanme.nmap.org (45.33.32.156)
Completed Service scan at 14:38, 0.86s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against Scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against Scanme.nmap.org (45.33.32.156)
Initiating Traceroute at 14:39
Completed Traceroute at 14:39, 6.07s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 14:39
Completed Parallel DNS resolution of 2 hosts. at 14:39, 0.07s elapsed
NSE: Script scanning 45.33.32.156.
Initiating NSE at 14:39
Completed NSE at 14:39, 10.23s elapsed
Initiating NSE at 14:39
Completed NSE at 14:39, 0.01s elapsed
Initiating NSE at 14:39
Completed NSE at 14:39, 0.00s elapsed
Nmap scan report for Scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Other addresses for Scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 596 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 ac:00:a0:1a:82:ff:ce:55:99:de:67:2b:34:97:6b:75 (DSA)
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4e:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:el:7b:1f:6d:05:a2:b0:fi:54:41:56 (ED25519)
```

