Definition

Nmap, short for Network Mapper, is an open-source tool used for network discovery and security auditing.

Ping Scanning

Ping scanning is a technique used to determine the reachability of hosts on a network. It involves sending ICMP (Internet Control Message Protocol) Echo Request packets (commonly known as "ping" packets) to a target IP address or range of IP addresses and waiting for ICMP Echo Reply packets in return.

```
┌──(hiki8man㉿Kali)-[~]
└─$ ping 75.2.96.41
PING 75.2.96.41 (75.2.96.41) 56(84) bytes of data.
64 bytes from 75.2.96.41: icmp_seq=1 ttl=128 time=30.5 ms
64 bytes from 75.2.96.41: icmp_seq=2 ttl=128 time=30.1 ms
64 bytes from 75.2.96.41: icmp_seq=3 ttl=128 time=30.4 ms
64 bytes from 75.2.96.41: icmp_seq=4 ttl=128 time=29.3 ms
64 bytes from 75.2.96.41: icmp_seq=5 ttl=128 time=30.4 ms
64 bytes from 75.2.96.41: icmp_seq=6 ttl=128 time=29.7 ms
64 bytes from 75.2.96.41: icmp_seq=7 ttl=128 time=30.1 ms
64 bytes from 75.2.96.41: icmp_seq=8 ttl=128 time=29.9 ms
64 bytes from 75.2.96.41: icmp_seq=9 ttl=128 time=29.5 ms
64 bytes from 75.2.96.41: icmp_seq=10 ttl=128 time=30.8 ms
64 bytes from 75.2.96.41: icmp_seq=11 ttl=128 time=30.1 ms
64 bytes from 75.2.96.41: icmp_seq=12 ttl=128 time=30.3 ms
64 bytes from 75.2.96.41: icmp_seq=13 ttl=128 time=30.1 ms
64 bytes from 75.2.96.41: icmp_seq=14 ttl=128 time=30.3 ms
64 bytes from 75.2.96.41: icmp_seq=15 ttl=128 time=30.4 ms
64 bytes from 75.2.96.41: icmp_seq=16 ttl=128 time=29.9 ms
64 bytes from 75.2.96.41: icmp_seq=17 ttl=128 time=30.5 ms
64 bytes from 75.2.96.41: icmp_seq=18 ttl=128 time=29.7 ms
64 bytes from 75.2.96.41: icmp_seq=19 ttl=128 time=31.3 ms
64 bytes from 75.2.96.41: icmp_seq=20 ttl=128 time=30.6 ms
```

SYN Scan

- A SYN scan is a common and efficient scanning technique used to determine the open ports on a target system. It sends SYN packets to target ports and analyzes the responses to infer the port's status.
- Here is the command to perform a SYN scan using Nmap on Kali Linux:

```
sudo nmap -sS [target]
```

```
┌──(hiki8man㉿Kali)-[~]
└─$ sudo nmap -sS 75.2.96.41
[sudo] password for hiki8man:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-07 12:22 EDT
Nmap scan report for a65596dcef46cf45f.awsglobalaccelerator.com (75.2.96.41)
Host is up (0.012s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 14.90 seconds
```

ACK Scan

- An ACK scan is a type of network scan performed using Nmap that is primarily used to map out firewall rulesets and determine whether ports are filtered.
- Here is the command to perform a ACK scan using Nmap on Kali Linux:

```
sudo nmap -sA [target]
```

```
┌──(hiki8man㉿Kali)-[~]
└─$ sudo nmap -sA 75.2.96.41
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-07 12:26 EDT
Nmap scan report for 41.96.2.75.in-addr.arpa (75.2.96.41)
Host is up (0.000074s latency).
All 1000 scanned ports on 41.96.2.75.in-addr.arpa (75.2.96.41) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

FIN Scan

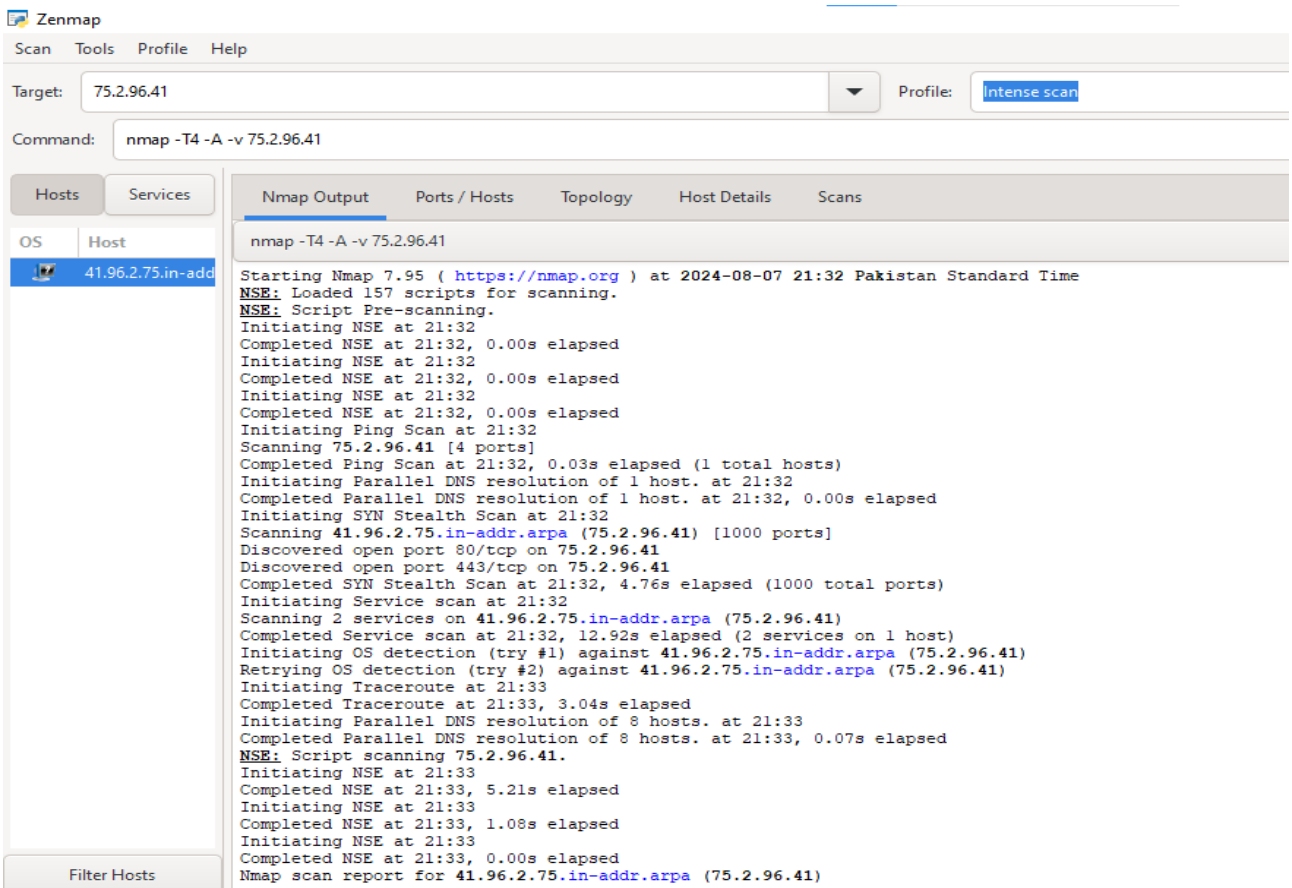
- A FIN scan is a type of network scanning technique used to determine the status of TCP ports on a target system. It is particularly useful for bypassing certain firewalls and packet filtering systems that might block standard scanning methods.
- Here is the command to perform a ACK scan using Nmap on Kali Linux:

```
sudo nmap -sF [target]
```

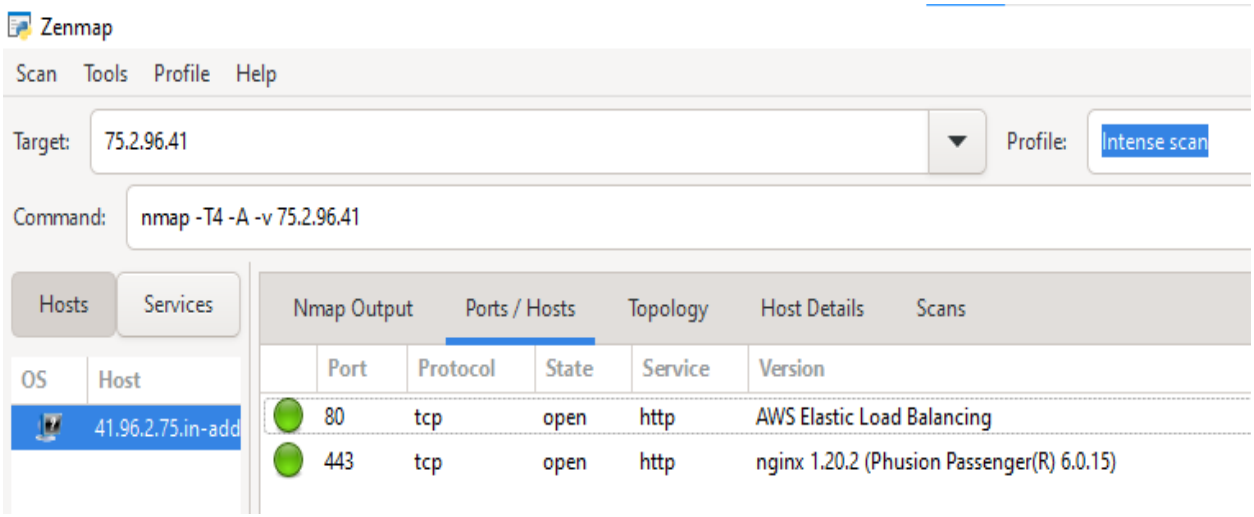
```
┌──(hiki8man㉿Kali)-[~]
└─$ sudo nmap -sF 75.2.96.41
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-07 12:31 EDT
Nmap scan report for a65596dcef46cf45f.awsglobalaccelerator.com (75.2.96.41)
Host is up (0.00049s latency).
All 1000 scanned ports on a65596dcef46cf45f.awsglobalaccelerator.com (75.2.96.41) are
in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
```

Zenmap

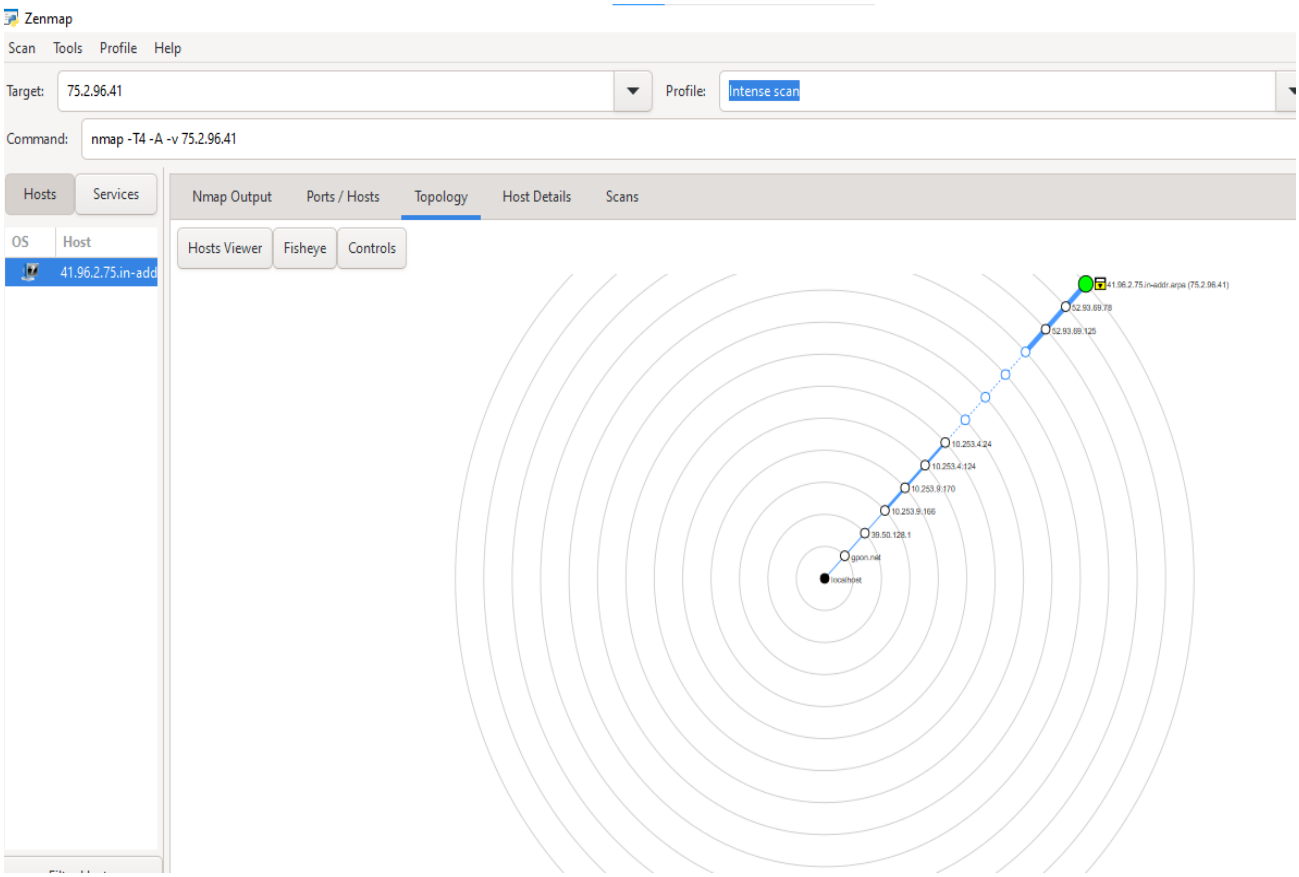
It is a Graphical User Interface (GUI) for Nmap, to perform a network scan.



Ports/Hosts



Topology



Host Details