Host Reconnaissance & Fingerprinting

We are going to utilise tools like Hping3, Nmap for host discovery, live status and their open ports, services running & their server versions.

```
└─$ nmap -v -sT -Pn 104.18.39.38
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 12:37 IST
Initiating Parallel DNS resolution of 1 host. at 12:37
Completed Parallel DNS resolution of 1 host. at 12:37, 0.03s elapsed
Initiating Connect Scan at 12:37
Scanning 104.18.39.38 [1000 ports]
Discovered open port 443/tcp on 104.18.39.38
Discovered open port 8080/tcp on 104.18.39.38
Discovered open port 80/tcp on 104.18.39.38
Completed Connect Scan at 12:37, 6.21s elapsed (1000 total ports)
Nmap scan report for 104.18.39.38
Host is up (0.025s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.26 seconds
```

In this Nmap scan, we are using **-Pn** and **-sT** options to perform a "**TCP connect**" scan, attempting to establish a connection with the target on open ports and ignoring ping sweep altogether, making Nmap skip the initial host discovery step, making it fast and relatively stealthy since it doesn't send many packets.

Next, let's do a more comprehensive scan, which includes version detection (the "**-sV**" flag) and operating system guessing ("**-sN**" stands for "No Ping", used to skip the initial ping sweep). The verbose mode ("**-v**") provides additional output, making it easier to follow.

```
└─$ nmap -v -sV -sN 104.18.39.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 12:29 IST
NSE: Loaded 47 scripts for scanning.
Initiating Ping Scan at 12:29
Scanning 104.18.39.38 [4 ports]
Completed Ping Scan at 12:29, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:29
Completed Parallel DNS resolution of 1 host. at 12:29, 0.03s elapsed
Initiating NULL Scan at 12:29
Scanning 104.18.39.38 [1000 ports]
Completed NULL Scan at 12:30, 4.54s elapsed (1000 total ports)
Initiating Service scan at 12:30
Scanning 996 services on 104.18.39.38
Discovered open port 80/tcp on 104.18.39.38
Discovered open|filtered port 80/tcp on 104.18.39.38 is actually open
Discovered open port 443/tcp on 104.18.39.38
Discovered open|filtered port 443/tcp on 104.18.39.38 is actually open
Service scan Timing: About 12.30% done; ETC: 12:34 (0:03:41 remaining)
```

Next let's explore Hping3,

In this we are doing a basic ICMP scan using ***sudo hping3 -1 xx.xx.xx.xx***.

```
HPING 192.168.1.5 (eth0 192.168.1.5): icmp mode set, 28 headers + 0 data bytes
len=28 ip=192.168.1.5 ttl=127 id=53706 icmp_seq=0 rtt=10.0 ms
len=28 ip=192.168.1.5 ttl=127 id=53707 icmp_seq=1 rtt=10.0 ms
len=28 ip=192.168.1.5 ttl=127 id=53708 icmp_seq=2 rtt=19.8 ms
len=28 ip=192.168.1.5 ttl=127 id=53709 icmp_seq=3 rtt=19.9 ms
^C
--- 192.168.1.5 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 10.0/14.9/19.9 ms
```

-1 --icmp (ICMP mode): Specifies the source IP address to use only use the first (lowest) fragment of an ICMP packet, which can be useful in scenarios where firewalls or other network configurations may drop higher fragments.

```
└─$ sudo hping3 -S -p 80 104.18.39.38
HPING 104.18.39.38 (eth0 104.18.39.38): S set, 40 headers + 0 data bytes
len=44 ip=104.18.39.38 ttl=56 DF id=0 sport=80 flags=SA seq=0 win=65535 rtt=39.8 ms
len=44 ip=104.18.39.38 ttl=56 DF id=0 sport=80 flags=SA seq=1 win=65535 rtt=39.5 ms
len=44 ip=104.18.39.38 ttl=57 DF id=0 sport=80 flags=SA seq=2 win=65535 rtt=39.3 ms
len=44 ip=104.18.39.38 ttl=57 DF id=0 sport=80 flags=SA seq=3 win=65535 rtt=39.1 ms
len=44 ip=104.18.39.38 ttl=56 DF id=0 sport=80 flags=SA seq=4 win=65535 rtt=38.9 ms
len=44 ip=104.18.39.38 ttl=56 DF id=0 sport=80 flags=SA seq=5 win=65535 rtt=38.8 ms
^C
--- 104.18.39.38 hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 38.8/39.2/39.8 ms
```

-S --syn (SYN flag): Sends SYN packets to simulate a connection request. This option is useful in detecting firewall rules or identifying open ports.

```
└─$ sudo hping3 -A -p 80 104.18.39.38
HPING 104.18.39.38 (eth0 104.18.39.38): A set, 40 headers + 0 data bytes
len=40 ip=104.18.39.38 ttl=56 DF id=0 sport=80 flags=R seq=0 win=0 rtt=30.0 ms
len=40 ip=104.18.39.38 ttl=56 DF id=0 sport=80 flags=R seq=1 win=0 rtt=29.7 ms
len=40 ip=104.18.39.38 ttl=56 DF id=0 sport=80 flags=R seq=2 win=0 rtt=29.3 ms
len=40 ip=104.18.39.38 ttl=56 DF id=0 sport=80 flags=R seq=3 win=0 rtt=28.5 ms
len=40 ip=104.18.39.38 ttl=56 DF id=0 sport=80 flags=R seq=4 win=0 rtt=68.1 ms
^C
--- 104.18.39.38 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 28.5/37.1/68.1 ms
```

-A --ack (ACK flag): This option specifies the target IP address or hostname to which you want to send ICMP echo requests.

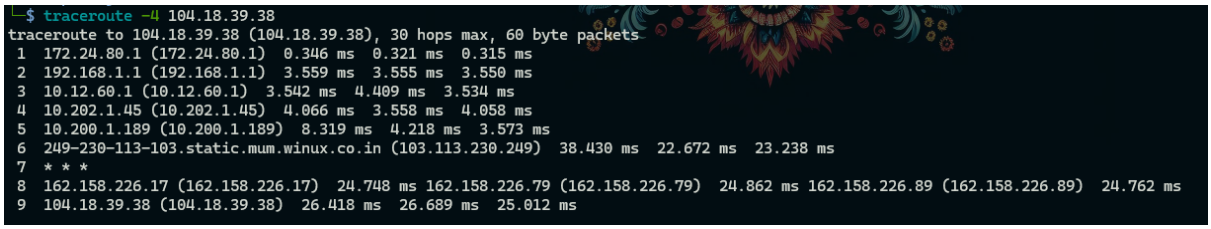
Next we will do fingerprinting of the IP address for information database, using tools and websites like whois, nslookup, traceroute.

nslookup

```
└─$ nslookup serverfault.com
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
Name:   serverfault.com
Address: 172.64.148.218
Name:   serverfault.com
Address: 104.18.39.38
```

whois



traceroute

nslookup: It focuses primarily on DNS (Domain Name System) records.

whois : This command is used to query databases that stores information on IP addresses or domain names (such as DNS servers) and return detailed information about them.

Traceroute : This command is used to display the route (path) that packets take from your computer to a specific destination.