# *Scanning and OS Fingerprinting*

First, we need to find the network address of the target. For that, we can check our ifconfig and find the network address from the IP assigned to us.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 1 - Scanning and OS Fingerprinting$ sudo ifconfig
[sudo] password for hades:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.6  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::e7c1:2e43:eb57:cbd2  prefixlen 64  scopeid 0x20<link>
        ether 00:0e:c6:8a:55:c1  txqueuelen 1000  (Ethernet)
        RX packets 402788  bytes 482826983 (460.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 159917  bytes 32652753 (31.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2402  bytes 267918 (261.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2402  bytes 267918 (261.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.142.111.240  netmask 255.255.255.0  broadcast 10.142.111.255
        inet6 fe80::a83f:6fff:fe4f:b0da  prefixlen 64  scopeid 0x20<link>
        ether aa:3f:6f:4f:b0:da  txqueuelen 100  (Ethernet)
        RX packets 70  bytes 5864 (5.7 KiB)
        RX errors 0  dropped 20  overruns 0  frame 0
        TX packets 3885  bytes 166782 (162.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

In this case, we have the IP as 10.142.111.240 and subnet mask is 255.255.255.0, so the network address is 10.142.111.0/24.
Let's do a ping sweep of the network using fping.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 1 - Scanning and OS Fingerprinting$ fping -a -g 10.142.111.0/24 > fping-results.txt
```

We get 6 ip addresses using pingsweep, and we also get our device's ip on the network.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 1 - Scanning and OS Fingerprinting$ cat fping-results.txt
10.142.111.1
10.142.111.6
10.142.111.48
10.142.111.96
10.142.111.99
10.142.111.100
10.142.111.240
```

Now, let's do a ping sweep using nmap.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 1 - Scanning and OS Fingerprinting$ nmap -sn 10.142.111.0/24 > nmap-results.txt
```

Comparing both results, we can see one more ip (10.142.111.213) has been found by nmap. This is probably a host that does not respond to ICMP requests.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 1 - Scanning and OS Fingerprinting$ cat nmap-results.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-14 16:17 IST
Nmap scan report for 10.142.111.1
Host is up (0.27s latency).
Nmap scan report for 10.142.111.6
Host is up (0.53s latency).
Nmap scan report for 10.142.111.48
Host is up (0.33s latency).
Nmap scan report for 10.142.111.96
Host is up (0.27s latency).
Nmap scan report for 10.142.111.99
Host is up (0.27s latency).
Nmap scan report for 10.142.111.100
Host is up (0.27s latency).
Nmap scan report for 10.142.111.213
Host is up (0.32s latency).
Nmap scan report for 10.142.111.240
Host is up (0.00018s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 10.09 seconds
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 1 - Scanning and OS Fingerprinting$ cat fping-results.txt
10.142.111.1
10.142.111.6
10.142.111.48
10.142.111.96
10.142.111.99
10.142.111.100
10.142.111.240
```

Now, we can save all the ips in a separate file for ease of further testing.

Let's do a SYN scan on all ips.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 1 - Scanning and OS Fingerprinting$ sudo nmap -sS -iL all-ips.txt > SYN-scan-results
.txt
```

The result can be found in the SYN-scan-results.txt file in this folder.

Let's also do an OS and service versions check.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 1 - Scanning and OS Fingerprinting$ sudo nmap -sC -sV -O -iL all-ips.txt > version-a
nd-os-check-results.txt
[sudo] password for hades:
```

The result can be found in the version-and-os-check-results.txt file in this folder.