HOST DISCOVERY USING NMAP

Command:

```
sudo nmap -sn 5.6.7.0/24
```

OUTPUT:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 01:06 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00040s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 37.34 seconds
```

OBSERVATION:

If no host discovery options are given, Nmap sends an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request.

HOST DISCOVERY USING ONLY ACK SCAN

COMMAND:

```
sudo nmap -sA 5.6.7.0/24
```

OUTPUT:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 01:08 PDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing Ping Scan
Ping Scan Timing: About 0.49% done
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00018s latency).
All 1000 scanned ports on server-link1 (5.6.7.8) are unfiltered

Nmap done: 256 IP addresses (1 host up) scanned in 34.85 seconds
```

PORT SCAN ON 5.6.7.8 USING HALF OPEN SCAN

COMMAND:

```
sudo nmap -p- -sS 5.6.7.8
```

OUTPUT:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 02:01 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00022s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1212/tcp open  lupa

Nmap done: 1 IP address (1 host up) scanned in 2567.75 seconds
```

SCANNING FIRST 1500 PORTS ON 5.6.7.8

COMMAND:

```
sudo nmap -p 1-1500 -sS 5.6.7.8
```

OUTPUT:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 01:52 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00023s latency).
Not shown: 1497 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1212/tcp open  lupa

Nmap done: 1 IP address (1 host up) scanned in 12.41 seconds
```

OBSERVATION:

No difference can be seen in the two scans. Of course in the first scan all the ports have been scanned and it required much more time. Anyways usually not all the ports are tested but just the most used. This can be done using the –F options of nmap, in this case the port 1212 will not be displayed because is not a port usually used.

SCANNING FIRST 1500 PORTS ON 5.6.7.8 USIN XMAS SCAN

COMMAND:

```
sudo nmap -p 1-1500 -sX 5.6.7.8
```

OUTPUT:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 02:00 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00026s latency).
Not shown: 1496 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
1212/tcp open|filtered lupa

Nmap done: 1 IP address (1 host up) scanned in 146.88 seconds
```

OBSERVATION:

The TCP RFC state that packets sent to open ports without the SYN, RST, or ACK bits set should be dropped and no response send. By performing this scan nmap does not receive an aswer for the open ports meaning that the port can be or open or the traffic filtered.

SCANNING FIRST 1500 PORTS ON 5.6.7.8 USIN TCP ACK SCAN

COMMAND:

```
sudo nmap -p 1-1500 -sA 5.6.7.8
```

#OUTPUT:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 02:05 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00019s latency).
All 1500 scanned ports on server-link1 (5.6.7.8) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

OBSERVATION:

Due to the fact that all the ports are unfiltered we can assume that the firewall apply an "allow per default" policy or that the filter is stateless. A stateful firewall can determine if an incoming ACK packet is part of an established outgoing connection. It only blocks the packet if it is unsolicited as in the case of the the ACK SCAN performed by nmap which would, in the case of blocked packets, label the port as filtered.

SCANNING THE OS OF 5.6.7.8

COMMAND:

```
sudo nmap -O 5.6.7.8
```

OUTPUT:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 02:06 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00026s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 2.6.32 (94%), Linux 3.2 - 4.8 (94%), Linux 2.6.32 - 3.10
(94%), Linux 3.4 - 3.10 (92%), Linux 3.3 (91%), Synology DiskStation Manager 5.2-5644
(91%), Linux 3.1 (90%), Linux 3.2 (90%), Linux 2.6.32 - 2.6.35 (90%), Linux 2.6.32 -
3.5 (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.37 seconds
```

SCANNING THE SERVICE VERSION OF 5.6.7.8

COMMAND:

```
sudo nmap -sV 5.6.7.8
```

OUTPUT:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 02:12 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00021s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.76 seconds
```

OBSERVATION:

I'm able to reach the host inside the network throw the port 80 for http traffic or directly connect to it throw ssh at port 22 which does not require authentication.