

# Memo/Instructions Nmap

Vinci Nicolò

25 October 2021

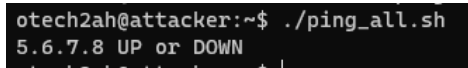
## 1 Host discovery

### 1.1 ICMP scan

A simple bash script has been written to perform an ICMP scan. It is called *ping\_all.sh* and it can be found in the folder *scripts*. It pings any IP address of the network 5.6.7.0/24. The ping command returns 1 if the ping goes bad otherwise 0. Hence, if the IP destination is unreachable or if the ICMP request goes in timeout, the ping command will return the state 1. If an ICMP request goes in timeout, it means that the host is present but there may be a packet filtering. Instead, if the ICMP request returns that the destination is unreachable, it means that the host is not present. Considering this difference, the script checks if there is *Unreachable* in any ping output. To launch the script:

```
$ ./scripts/ping_all.sh
```

A result is shown in figure 1.



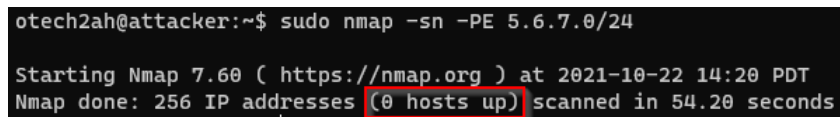
```
otech2ah@attacker:~$ ./ping_all.sh
5.6.7.8 UP or DOWN
```

Figure 1: ping\_all.sh result

Then, all scans performed with *nmap* are written in *command.sh*. The script can be executed and all scans will be executed. Otherwise, a single scan can be copied and executed individually. The first scan is the ICMP scan:

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

*Nmap* is not be able to spot any host, because the ping state is 1 both for unreachable host and ICMP request timed out.



```
otech2ah@attacker:~$ sudo nmap -sn -PE 5.6.7.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-22 14:20 PDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 54.20 seconds
```

Figure 2: ICMP nmap scan result

Then an ACK scan has been performed.

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

Now, *nmap* is able to discover one host.

```
otech2ah@attacker:~$ sudo nmap -sn -PA 5.6.7.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-22 14:24 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00037s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 1.36 seconds
```

Figure 3: ACK nmap scan result

At the end, a multiple probes scan has been launched.

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

*Nmap* discovers one host even in this case.

```
otech2ah@attacker:~$ sudo nmap -sn 5.6.7.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-22 14:26 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00030s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 37.35 seconds
```

Figure 4: Multi probes nmap scan result

Listening on the attacker interface, the probes sent by *nmap* are:

- ICMP request
- TCP SYN packet on port 443
- TCP ACK packet on port 80
- ICMP timestamp query

The host 5.6.7.8 replies back to the TCP ACK packet on port 80 with a TCP RST.

```
13:56:14.349218 IP 1.1.2.4 > 5.6.7.8: ICMP echo request, id 28514, seq 0, length 8
13:56:14.349272 IP 1.1.2.4.52918 > 5.6.7.8.443: Flags [S], seq 4039677371, win 1024, options [mss 1460], length 0
13:56:14.349292 IP 1.1.2.4.52918 > 5.6.7.8.80: Flags [A], ack 4039677371, win 1024, length 0
13:56:14.349312 IP 1.1.2.4 > 5.6.7.8: ICMP time stamp query id 57853 seq 0, length 20
13:56:14.349595 IP 5.6.7.8.80 > 1.1.2.4.52918: Flags [R], seq 4039677371, win 0, length 0
```

Figure 5: Listening on attacker interface

## 2 Port scanning

In the section 1, the host 5.6.7.8 has been discovered. Now, ports will be analyzed performing different port scanning with *nmap*.

## 2.1 TCP half open scan

A TCP half open scan can be launched and it scans by default the most common 1000 ports.

```
$ sudo nmap -sS 5.6.7.8
```

```
otech2ah@attacker:~$ sudo nmap -sS 5.6.7.8
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-22 14:27 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00025s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 18.09 seconds
```

Figure 6: TCP half open scan result

Ports 22 and 80 are discovered as open thanks to this scan. However, if the first 1500 ports are scanned, a new open port will be discovered.

```
$ sudo nmap -sS -p1-1500 5.6.7.8
```

```
otech2ah@attacker:~$ sudo nmap -sS -p1-1500 5.6.7.8
Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-22 14:28 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00025s 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 15.66 seconds
```

Figure 7: TCP half open scan on the first 1500 ports result

The port 1212 is not a common port and with the previous scan has not been discovered.

## 2.2 XMAS scan

A XMAS can be performed to discover new open ports.

```
$ sudo nmap -sX -T4 5.6.7.8
```

```

otech2ah@attacker:~$ sudo nmap -sX -T4 5.6.7.8

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-22 14:29 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00018s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind

Nmap done: 1 IP address (1 host up) scanned in 28.60 seconds

```

Figure 8: XMAS scan result

The previous ports discovered as open, now they are open-filtered. The XMAS scan sends to any port a TCP packet with FIN, PSF and URG flags set to 1. So, if a port does not respond to the XMAS probe even after retransmissions, the port will be reported as open-filtered. Hence, ports 22, 80 and 111 don not respond to XMAS scan.

### 2.3 TCP ACK scan

A TCP ACK scan can be performed to fake an ACK packet of an unexisting ongoing connection.

```
$ sudo nmap -sA -T4 5.6.7.8
```

```

otech2ah@attacker:~$ sudo nmap -sA -T4 5.6.7.8

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-22 14:31 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00017s latency).
All 1000 scanned ports on server-link1 (5.6.7.8) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds

```

Figure 9: ACK scan result

All 1000 scanned ports are reported as unfiltered. It means that all ports respond back with a TCP RST packet. So, there is a stateless firewall, otherwise a stateful firewall would be able to distinguish the ACK packet of a not established TCP connection and it would drop it. A port should not reply or it should reply with an ICMP error with a stateful firewall.

## 3 Service versions and O.S. detection

A new scan can be launched to find service versions and O.S running on the host 5.6.7.8:

```
$ sudo nmap -A -T4 5.6.7.8
```

```
nmap scan report for server-link1 (5.6.7.8)
Host is up (0.0002s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
|_ ssh-hostkey:
|_ 1024 ec:de:ba:cc:c9:20:3e:08:39:b3:a8:b1:f2:53:97:ff (RSA)
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: IT works
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 (99%), Linux 3.2 - 4.8 (94%), Linux 2.6.32 - 3.18 (94%), Linux 3.4 - 3.18 (92%), Synology DiskStation Manager 5.2-5604 (92%), Linux 3.1 (99%), Linux 3.2 (99%), Linux 2.6.32
- 2.6.35 (99%), Linux 2.6.32 - 3.5 (99%), Linux 3.3 (99%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
Hop RTT ADDRESS
1 0.30 ms gateway-lan1 (1.1.2.2)
2 0.20 ms server-link1 (5.6.7.8)

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 20.28 seconds
```

Figure 10: Service versions and O.S. detection scan result

Services:

- port 22: OpenSSH
- port 80: Apache httpd 2.4.9.29

There are 2 hops to reach the host, so the path is:

- gateway-lan1 (1.1.2.2)
- server-link1 (5.6.7.8)