Offensive technologies - NMAP exercise

Claudio Facchinetti [claudio.facchinetti@studenti.unitn.it]

October 23, 2021

Abstract

In this document it is presented the work done in order to solve the "SYN Flood" exercise on DeterLab.

1 Solving tasks

In this section it will be discussed how the various tasks has been solved.

1.1 Host discovery

First on the list was to write a simple bash script to scan the `5.6.7.0/24` network and find out the hosts on that network. The script to do so is the following.

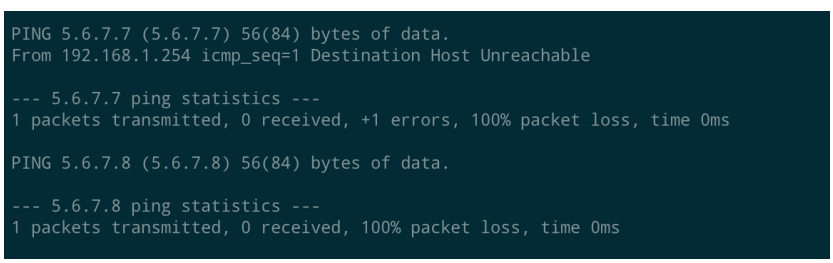
```
#!/bin/sh

LAST_BIT=1
LAST_BIT_MAX=254

echo "" > result.txt

while [ $LAST_BIT -le $LAST_BIT_MAX ]; do
  ping -c 1 5.6.7.${LAST_BIT} >> result.txt
  LAST_BIT=$((LAST_BIT + 1))
done;
```

This script simply iterates over all possible addres and tries to ping every single address.
As we can see from the picture we can notice that the only address available is `5.6.7.8`, because it is the only one which does not return an ICMP error.



```
PING 5.6.7.7 (5.6.7.7) 56(84) bytes of data.
From 192.168.1.254 icmp_seq=1 Destination Host Unreachable

--- 5.6.7.7 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

PING 5.6.7.8 (5.6.7.8) 56(84) bytes of data.

--- 5.6.7.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Figure 1: Result of the ICMP script

After this we it is asked to perform an ACK scan using NMAP; to do this it has been used the following command: `sudo nmap -sn -PA 5.6.7.0/24`.

This once again confirms the hypothesis that the only host listening on the network is `5.6.7.8`. Moving forward it is asked to perform a scan using NMAP with different probes. In order to this the previous command was simply repeated omitting the `-PA` flag: `sudo nmap -sn -PA 5.6.7.0/24`.

Yet again the hypothesis is confirmed.

```
otech2aj@attacker:~$ sudo nmap -sn -PA 5.6.7.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 09:20 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00038s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 1.35 seconds
otech2aj@attacker:~$
```

Figure 2: Result of running NMAP ACK scan

```
otech2aj@attacker:~$ sudo nmap -sn 5.6.7.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 09:25 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00025s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 35.30 seconds
otech2aj@attacker:~$
```

Figure 3: Running NMAP scan with different probes

1.2 Port scanning

Next on the list is to perform port scanning using different techniques, the first being the TCP Half Open scan without specifying a port range. To do this the following command has been issued: `sudo nmap -sS 5.6.7.8`.

```
otech2aj@attacker:~$ sudo nmap -sS 5.6.7.8

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 09:27 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00027s 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 10.17 seconds
otech2aj@attacker:~$
```

Figure 4: Result of the Half Scan with no flags

The result shows that ports 80 and 22 are open on the host, corresponding to the http and to the ssh service.
After it is asked to perform again a TCP Half Open scan on the first 1500 ports; to do this the following command has been issued: `sudo nmap -sS -p 1-1500 5.6.7.8`.

The result is quite interesting: we notice that the server is exposing a service o port 1212. This was not present in the previous scan because by default Nmap scans the first 1000 ports.

Next on the scanning list is to perform a XMAS scan; to do this the following command has been used: `sudo nmap -sX 5.6.7.8`.

From this we can notice that all the ports now appear with the status `open|filtered` and that also port 111 appeared.

Last thing on the scan list was to perform an ACK scan by faking a response to an already existing TCP connection; this was done using Nmap issueing the following command: `sudo nmap -sA 5.6.7.8`.

The result is what we expect: the ports on that host result to be all unfiltered, therefore we can also state that the firewall is a stateless one, otherwise it would have blocked our ACKs.

```
otech2aj@attacker:~$ sudo nmap -sS -p 1-1500 5.6.7.8

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 09:28 PDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.37% done
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00022s 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 15.08 seconds
otech2aj@attacker:~$
```

Figure 5: Result of the Half Scan with the top 1500 ports

```
otech2aj@attacker:~$ sudo nmap -sX 5.6.7.8

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 09:29 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00019s 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 95.87 seconds
```

Figure 6: Result of the XMAS scan

1.3 OS and service version detection

Last on the list was to perform OS and service version detection using Nmap. To do so the following command has been used `sudo nmap -sV -O -A -sC 5.6.7.8`.

As we can see from the figure the host is running Ubuntu, but it is not 100% sure of the version. As for the version of the services we can notice that the web server is hosted using Apache 2.4.49 and the ssh daemon running OpenSSH 7.6p1.

```
otech2aj@attacker:~$ sudo nmap -sA 5.6.7.8

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 09:33 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00015s 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
otech2aj@attacker:~$
```

Figure 7: Reult of the ACK scan faking the response

```
otech2aj@attacker:~$ sudo nmap -sV -O -A -sC 5.6.7.8

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-23 09:38 PDT
Nmap scan report for server-link1 (5.6.7.8)
Host is up (0.00019s 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)
| ssh-hostkey:
|   1024 4d:de:0a:0c:c0:20:3e:40:39:b3;a8:b1:f2:53:57:ff (RSA)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_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 (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%), Li
nux 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).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT    ADDRESS
1   0.13 ms gateway-lan1 (1.1.2.2)
2   0.17 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 21.62 seconds
otech2aj@attacker:~$
```

Figure 8: Result of the OS and service version detection