Report S5-L3

Studente: Simone Mininni

Obiettivo: Fase di scansione ed enumerazione di due target (Metasploitable e Windows 7).

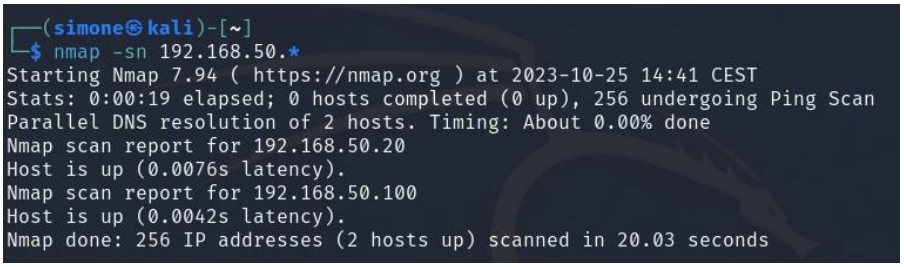
Situazione iniziale:
Tre macchine settate sulla stessa rete con scheda di bridge:
-Kali, ip: 192.168.50.20
-Metasploitable, ip 192.168.50.100
-Windows 7, ip 192.168.50.101

La fase di scansione è stata eseguita con l' utilizzo di nmap sulla macchina kali linux.

Primo target: Metasploitable.

Obiettivi:
- Trovare il sistema operativo della macchina target
- Eseguire una scansione stealth sulla macchina target per trovare porte e servizi attivi attraverso il protocollo tcp.
-Eseguire una scansione completa secondo il protocollo tcp(Syn-Syn/Ack-Ack)
-Trovare la versione dei servizi attivi.

Prima di tutto ho scansionato la rete per trovare i target attraverso un ping sweep.



In questo caso gli indirizzi attivi che rispondono sono solo due, la macchina kali e la metasploitable.

Non vediamo la macchina win7 poiché agisce il firewall software che blocca le request ICMP.

Successivamente ho trovato il sistema operativo del target metasploitable (nmap -O ip target)…

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.92 seconds
```

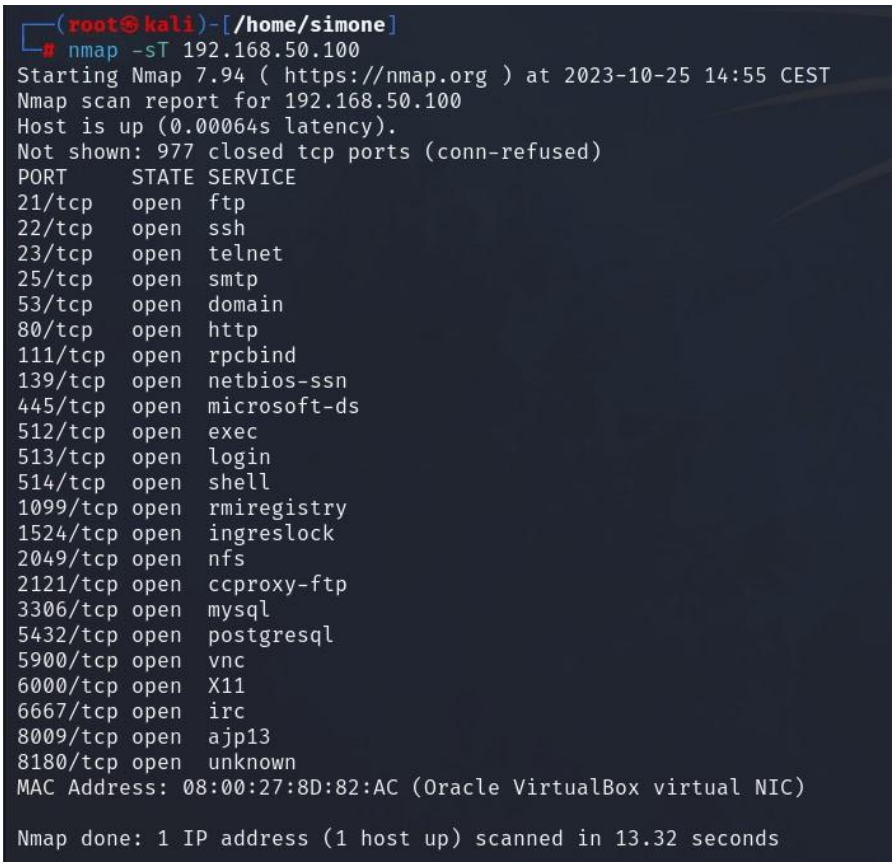
Da qui possiamo dedurre che è una macchina general purpose e si trova un sistema Linux 2.6.9-33

Poi ho effettuato una scansione delle porte e relativi servizi con solo la richiesta di Syn per essere meno invasivi sulla rete.

```
┌──(root㉿kali)-[/home/simone]
└─# nmap -sS 192.168.50.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:55 CEST
Nmap scan report for 192.168.50.100
Host is up (0.00039s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:8D:82:AC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

E ho ripetuta l' operazione eseguendo una richiesta 3 way-handshake completa…



Si può notare che in questo caso il risultato è identico alla scansione stealth, ma in generale la prima situazione può avere un risultato più approssimativo.

Infine ho trovato la versione dei servizi in ascolto sulle porte aperte del target.

```
┌──(root㉿kali)-[/home/simone]
└─# nmap -sV 192.168.50.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:56 CEST
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:57 (0:00:02 remaining)
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:58 (0:00:02 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:58 (0:00:02 remaining)
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:58 (0:00:04 remaining)
Nmap scan report for 192.168.50.100
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:8D:82:AC (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 128.45 seconds
```

Questi risultati potranno essere importanti in una fase di exploit.

Secondo target: Win7

Nel caso di win7 la situazione è un pò differente grazie al firewall software.
Come detto prima le request ICMP sono bloccate quindi non possiamo pingare la macchina con kali.
Per capire se il target è attivo possiamo fare una scansione con nmap escludendo la fase di ping.

```
┌──(simone㉿kali)-[~]
└─$ nmap -Pn 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:42 CEST
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 7.50% done; ETC: 14:46 (0:03:17 remaining)
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 10.50% done; ETC: 14:46 (0:03:08 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 11.00% done; ETC: 14:46 (0:03:06 remaining)
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 30.00% done; ETC: 14:46 (0:02:22 remaining)
Stats: 0:02:50 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 78.00% done; ETC: 14:46 (0:00:45 remaining)
Nmap scan report for 192.168.50.101
Host is up.
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 214.55 seconds
```

Come si può vedere l' host è attivo ma le porte sono filtrate dal firewall, quindi non posso dedurre quali sono aperte e quali chiuse in modo oggettivo.

Anche se vado a eseguire un os footprinting non riesco a determinare particolari informazioni…

```
┌──(root㉿kali)-[/home/simone]
└─# nmap -Pn -O  192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:45 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:B7:32:55 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.10 seconds
```

Di seguito i risultati disattivando il firewall di win7

```
┌──(root㉿kali)-[/home/simone]
└─# nmap  -O  192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:41 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0024s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:B7:32:55 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows
_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.48 seconds
```

Come si può notare riesco a ricavare le informazioni che cercavo come s.o., porte aperte e servizi attivi.

Fine.