

## Relazione S5L3 Nmap

La richiesta dell'esercizio è quella di utilizzare Nmap per effettuare delle scansioni sulle macchine target metasploitable2 e windows 7.

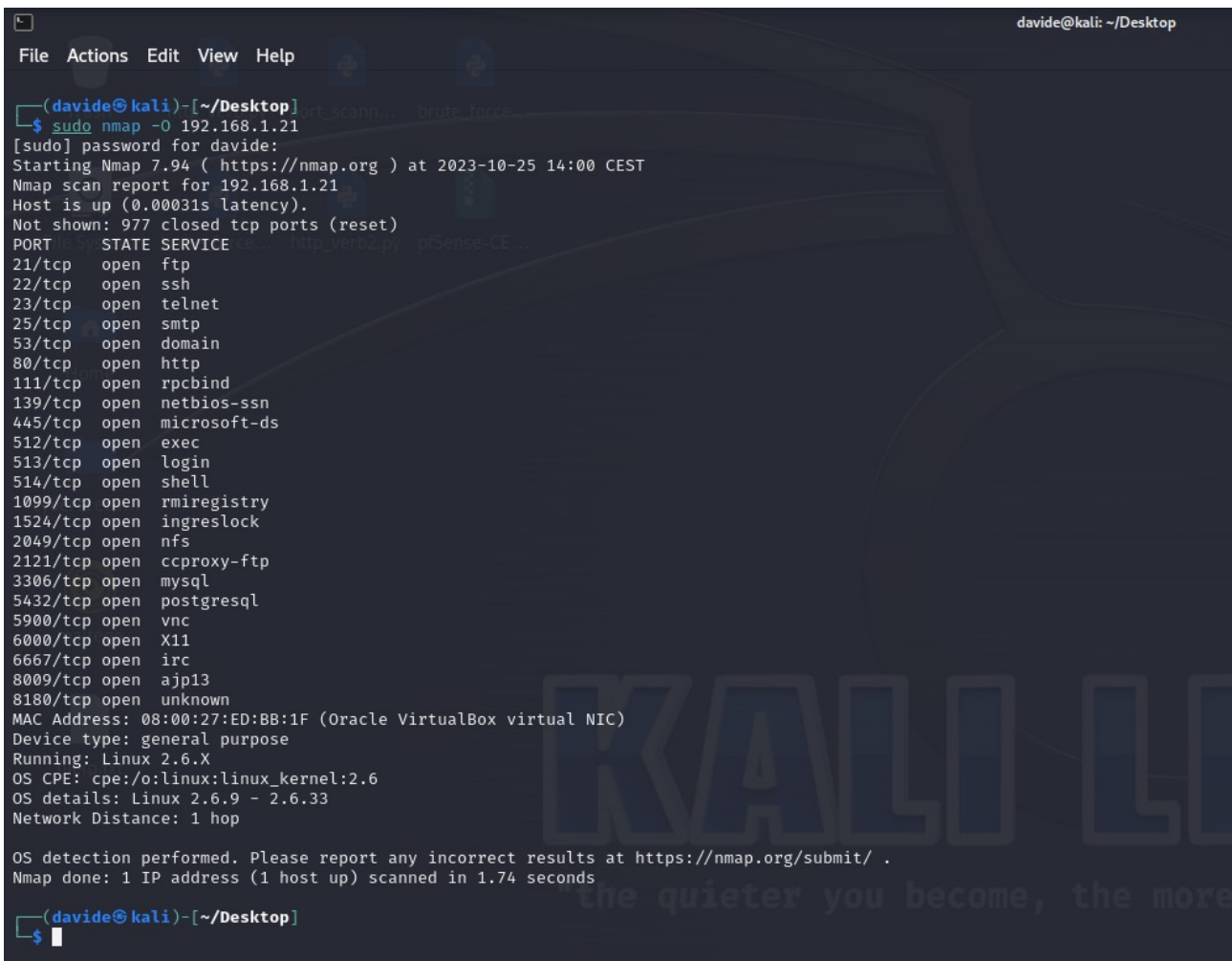
Per metasploitable2 è necessario effettuare:

- OS fingerprint
- Syn scan
- TCP Connect
- Version detection

Per windows 7 invece:

- OS fingerprint

Qui di seguito trovate in allegato i risultati dei comandi per metasploitable2:



```
(davide@kali)-[~/Desktop]
$ sudo nmap -O 192.168.1.21
[sudo] password for davide:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:00 CEST
Nmap scan report for 192.168.1.21
Host is up (0.00031s 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:ED:BB:1F (Oracle VirtualBox virtual NIC)
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 1.74 seconds

(davide@kali)-[~/Desktop]
$
```

Come si può osservare è stato utilizzato il comando **nmap -O <ip\_address>** per identificare il sistema operativo. Questo comando ci restituisce le porte aperte col relativo protocollo associato e alla fine ci indica il tipo di sistema operativo su cui opera la macchina.

```
davide@kali: ~/Desktop
File Actions Edit View Help

(davide@kali)-[~/Desktop]
$ sudo nmap -sS 192.168.1.21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:01 CEST
Nmap scan report for 192.168.1.21
Host is up (0.000067s 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:ED:BB:1F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

(davide@kali)-[~/Desktop]
$
```

Qui invece abbiamo utilizzato il comando **nmap -sS <ip\_address>** che serve per effettuare una scansione stealth e meno invasiva andando ad inviare solamente il SYN. Anche per questo comando possiamo vedere le porte aperte col relativo protocollo e il MAC address alla fine.

```
davide@kali: ~/Desktop
File Actions Edit View Help

(davide@kali)-[~/Desktop]
$ nmap -sT 192.168.1.21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:04 CEST
Nmap scan report for 192.168.1.21
Host is up (0.00041s latency).
Not shown: 977 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Come terza prova invece abbiamo utilizzato il comando **nmap -sT <ip\_address>** che è una scansione più invasiva e l'unica differenza nel nostro caso sta nell'indicazione che le porte chiuse hanno dato un “conn-refused” e con questa scansione il MAC address non viene mostrato.

```
(davide@kali)-[~/Desktop]
$ nmap -sV 192.168.1.21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:06 CEST
Nmap scan report for 192.168.1.21
Host is up (0.00038s latency).
Not shown: 977 closed tcp ports (conn-refused)
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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
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 11.38 seconds
```

Con l'ultimo comando **nmap -sV <ip\_address>** abbiamo ricercato la versione del protocollo per ogni porta aperta. Ci ha messo un bel po' generando molto rumore.

Per quanto riguarda windows 7 invece abbiamo lanciato il comando per identificare il sistema operativo. Questo tuttavia ci ha dato come esito un risultato incerto in quanto le porte non hanno dato una risposta attendibile.

Si può vedere che come device identifica un voip e il pc non compare neanche nelle opzioni. Il sistema operativo invece compare in terza posizione

```
(davide@kali)-[~/Desktop]
$ sudo nmap -O 192.168.1.22
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:25 CEST
Nmap scan report for 192.168.1.22
Host is up (0.00034s latency).
All 1000 scanned ports on 192.168.1.22 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:BD:5F:1D (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specializedVoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_xp:sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley Micrologix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
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 23.75 seconds
```

Sono stati effettuati anche altri tentativi per vedere le porte attive ma il firewall di windows ha bloccato ogni prova.

Davide Lecci