

Report S5/L2

Indice:

1) Introduzione

2) Scansioni su Metasploitable

3) Scansione su Windows

4) Conclusioni

```
root@kali:~/home/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.150)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned):
Not shown: 987 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
          Version: 1.1.0ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
1080/tcp  filtered instl_bootc
4444/tcp  filtered krb524
5800/tcp  filtered vnc-https
5900/tcp  filtered vnc
9929/tcp  open     nping-echo
31337/tcp open     tcptrapped
Service Info: OS: Linux; CPE: cpe:/o: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 29.39 seconds
```



NMAP

1) Introduzione:

Introduzione

Questa esercitazione ha l'obiettivo di eseguire una serie di scansioni di rete utilizzando Nmap per identificare host attivi, rilevare sistemi operativi, analizzare porte aperte e individuare servizi in esecuzione su due target distinti: Metasploitable (macchina vulnerabile per test di sicurezza) e Windows.

Le tecniche di scansione applicate includeranno:

- OS Fingerprint → Identificazione del sistema operativo
- SYN Scan → Scansione stealth per rilevare porte aperte
- TCP Connect Scan → Scansione completa delle porte
- Version Detection → Identificazione delle versioni dei servizi in ascolto

Strumenti utilizzati

- Nmap → Strumento open-source per la scansione di rete e sicurezza
- Kali Linux → Sistema operativo utilizzato come macchina attaccante
- Metasploitable → Macchina virtuale vulnerabile utilizzata come target
- Windows (7/10) → Secondo target per il fingerprinting del sistema operativo

L'esercitazione sarà eseguita in ambiente isolato utilizzando macchine virtuali collegate tramite rete Host-Only, per garantire sicurezza e controllo sul traffico generato

2) Scansioni su metasploitable:

Innanzitutto scopriamo l' IP di metasploitable simulando che non lo sappiamo:

```
(kali㉿kali)-[~]
$ nmap -sn 192.168.56.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 17:17 CET
Nmap scan report for 192.168.56.101
Host is up (0.0054s latency).
Nmap scan report for 192.168.56.102
Host is up (0.016s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 24.36 seconds

(kali㉿kali)-[~]
```

Cosa fa? Questo comando esegue un Ping Scan su tutta la subnet 192.168.56.0/24, elencando solo gli host attivi senza scansionare le porte.

```
(kali㉿kali)-[~]
$ ip a
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    qlen 1000
    link/ether 08:00:27:35:30:e3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic no
        link-layer
        valid_lft 517sec preferred_lft 517sec
    inet6 fe80::a00:27ff:fe35:30e3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Sapendo che kali è sulla .102 possiamo essere sicuri che l'IP di metasploitable è 192.168.56.102.

Adesso che sappiamo l'indirizzo IP iniziamo l'OS fingerprint.

comando usato: sudo nmap -O 192.168.56.102

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.56.102

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 17:27 CET
Nmap scan report for 192.168.56.102
Host is up (0.0086s 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
```

Nmap -O non è riuscito a identificare con certezza il sistema operativo.

Possibile Soluzione: Usare --osscan-guess.

comando sudo nmap -O --oscan-guess 192.168.56.102

```
Aggressive OS guesses: Linux 2.6.9 - 2.6.24 (97%), Linux 2.6.9 - 2.6.30 (97%),
Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linux 2.6.9 (97%),
Linux 2.6.18 - 2.6.32 (96%), Linux 2.6.22 - 2.6.23 (96%), Linux 2.6.18 (Debian 4, VMware) (96%), Linksys RV042 router (96%), Linux 2.6.24 - 2.6.28 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org
```

Grazie a questo comando abbiamo il 97% che è Linux.

-Syn scan (-sS)

comando utilizzato: sudo nmap -sS 192.168.56.102

```
L$ sudo nmap -sS 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 17:39 CET
Nmap scan report for 192.168.56.102
Host is up (0.014s 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: 08:00:27:62:12:BB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.64 seconds
```

Risultato:

22 porte aperte rilevate

Scansione stealth: non completando il 3-way handshake, è meno rilevabile da firewall e IDS.

I servizi attivi includono FTP, SSH, HTTP, MySQL e altri potenzialmente vulnerabili su Metasploitable.

Scansione TCP Connect (-sT) e confronto con SYN Scan.

Con il comando sudo nmap -sT 192.168.56.102

```
└$ sudo nmap -sT 192.168.56.102

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 17:43 CET
Nmap scan report for 192.168.56.102
Host is up (0.021s 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
MAC Address: 08:00:27:62:12:BB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds
```

Il risultato è praticamente lo stesso la differenza vera tra i due è che in confronto al SYN SCAN questo tipo di scansione è meno stealth, perché il 3-way handshake viene completato, generando log sui server target.

Version Detection (-sV) per scoprire le versioni dei servizi in ascolto.

comando utilizzato sudo nmap -sV 192.168.56.102

```
L$ sudo nmap -sV 192.168.56.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 17:49 CET
Nmap scan report for 192.168.56.102
Host is up (0.012s 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        OpenBSD or Solaris rlogind
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: 08:00:27:62:12:BB (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.24 seconds
```

Abbiamo ottenuto un elenco delle porte aperte e dei servizi in ascolto con le relative versioni.

3) Scansione di windows

Usiamo il comando visto in precedenza per metasploitable per capire l'IP (sudo nmap -sn 192.168.56.0/24) , noto che questa volta oltre a kali sulla .101 vi sono altri 2 indirizzi uno sulla .100 e l'altro sulla .103

```
(kali㉿kali)-[~]
$ sudo nmap -sn 192.168.56.0/24

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 18:00 CET
Nmap scan report for 192.168.56.1
Host is up (0.00068s latency).
MAC Address: 0A:00:27:00:00:11 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00047s latency).
MAC Address: 08:00:27:FE:A0:9F (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.00087s latency).
MAC Address: 08:00:27:26:87:A7 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.76 seconds
```

Proprio per questo decido di usare OS Fingerprint su entrambi gli indirizzi perchè almeno vedo se sono entrambi windows oppure uno è diverso, in quest'ultimo caso avrei la conferma dell'IP del bersaglio.

-comando utilizzato sudo nmap -O 192.168.56.100 e poi .103

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.56.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 18:09 CET
Nmap scan report for 192.168.56.100
Host is up (0.00067s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:FE:A0:9F (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 16.05 seconds

(kali㉿kali)-[~]
$ sudo nmap -O 192.168.56.103

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 18:11 CET
Nmap scan report for 192.168.56.103
Host is up (0.00074s latency).
All 1000 scanned ports on 192.168.56.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:26:87:A7 (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 42.89 seconds
```

Purtroppo entrambi non mi danno accesso, penso ad un eventuale firewall ma molto strano visto che pfSense è spenta ed è la prima volta che accendo la VM di windows 7, potrebbe essere che ne abbia uno di default.

Utilizzerò una tecnica meno aggressiva con il comando:

sudo nmap -Pn -A 192.168.56.100 e poi su .103

il quale con -Pn disabilita il ping (utile se il firewall di Windows sta bloccando le richieste ICMP).

Mentre con -A esegue OS detection, version detection e traceroute, aumentando le possibilità di riconoscere Windows.

Purtroppo il risultato è deludente, devo trovare un altro modo per agire il firewall.

- **Se vogliamo essere stealth** e ridurre il rischio di essere bloccati, usiamo una scansione SYN (-sS). Questo metodo non completa la connessione TCP (lasciando la stretta di mano a metà) e quindi è più difficile da rilevare dai firewall.

comando usato : **sudo nmap -sS -Pn 192.168.56.103**

```
(kali㉿kali)-[~]
$ sudo nmap -sS -Pn 192.168.56.103

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 18:28 CET
Nmap scan report for 192.168.56.103
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.56.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:26:87:A7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 40.88 seconds
```

Probabilmente il firewall blocca in SYN quindi non ha funzionato.

- **Scansione lenta e furtiva con -T0 o -T1**

comando usato: **sudo nmap -sS -Pn -T1 192.168.56.103**

✓ **Vantaggio:**

Simula il comportamento di un utente normale, evitando di attirare l'attenzione.

✗ **Svantaggio:**

Molto lenta, potrebbe richiedere diversi minuti per completarsi.

```
(kali㉿kali)-[~]
$ sudo nmap -sS -Pn -T1 192.168.56.103

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 18:33 CET
Stats: 0:06:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.20% done; ETC: 03:17 (8:37:20 remaining)
```

Ennesimo buco nell'acqua più che altro per una questione di tempistica, il comando funziona ma ha un tempo di attesa di 8 ore e 37 minuti. eccessiva

- Se il firewall blocca le SYN scans, possiamo provare una TCP Connect Scan, che usa il metodo standard di connessione, unico neo è che può essere registrata nei file di log di windows.

comando utilizzato **sudo nmap -sT -Pn 192.168.56.103**

```
(kali㉿kali)-[~]
└─$ sudo nmap -sT -Pn 192.168.56.103

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 18:43 CET
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 15.50% done; ETC: 18:47 (0:03:00 remaining)
Stats: 0:01:40 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 42.00% done; ETC: 18:46 (0:02:02 remaining)
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 43.00% done; ETC: 18:46 (0:01:59 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.50% done; ETC: 18:46 (0:01:12 remaining)
Nmap scan report for 192.168.56.103
Host is up.
All 1000 scanned ports on 192.168.56.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 220.08 seconds
```

Firewall molto resistente, anche questa ha fallito.

- Ultima idea Invece di scansionare tutte le 1000 porte, possiamo concentrarci su quelle più comuni per Windows: da una ricerca su internet le ho trovate.

comando **sudo nmap -sS -Pn -p 135,139,445,3389 192.168.56.103**

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS -Pn -p 135,139,445,3389 192.168.56.103

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 18:49 CET
Nmap scan report for 192.168.56.103
Host is up (0.0013s latency).

PORT      STATE      SERVICE
135/tcp    filtered  msrpc
139/tcp    filtered  netbios-ssn
445/tcp    filtered  microsoft-ds
3389/tcp   filtered  ms-wbt-server
MAC Address: 08:00:27:26:87:A7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
```

Nonostante abbiamo provato parecchie strade, **anche se per principio volevamo vedere se con le nuove tecniche di nmap si riusciva a eludere il firewall, non siamo riusciti** a rilevare il sistema operativo di Windows con Nmap a causa della configurazione del firewall, che ha filtrato tutte le richieste di scansione. Per proseguire con l'esercitazione e ottenere il fingerprint, abbiamo temporaneamente

disattivato il firewall e rieseguito la scansione.

```
[Kali㉿Kali)-[~]$ sudo nmap -O 192.168.56.103

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 19:03 CET
Nmap scan report for 192.168.56.103
Host is up (0.0016s 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: 08:00:27:26:87:A7 (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 16.09 seconds
```

Ovviamente, rimuovendo i firewall siamo riusciti subito con **OS fingerprint** ad avere le informazioni sul sistema operativo che è **windows 7**.

4) Conclusioni

L'esercitazione ha dimostrato come Nmap sia uno strumento potente per la scansione di rete, ma anche quanto un firewall ben configurato possa limitarne l'efficacia.

- Su Metasploitable, le scansioni hanno rilevato facilmente porte aperte, servizi e sistema operativo, evidenziando la vulnerabilità della macchina.
- Su Windows, il firewall ha bloccato tutte le rilevazioni, impedendo di ottenere informazioni utili fino alla sua disattivazione.

Lezioni apprese:

- La SYN Scan (-sS) è più furtiva, ma inefficace contro firewall restrittivi.
- La TCP Connect Scan (-sT) è più rumorosa e rilevabile.

- La Version Detection (-sV) è utile per scoprire dettagli sui servizi attivi.
- Un firewall ben configurato è essenziale per proteggere un sistema da ricognizioni non autorizzate.
- Nmap è utile sia per gli attaccanti che per i difensori. Sapere quali informazioni sono esposte aiuta a migliorare la sicurezza di una rete.