

CS0424IT — ESERCITAZIONE S5L3  
SCAN METASPLOITABLE 2 E WINDOWS 7

*Simone La Porta*



---

TRACCIA

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati delle scansioni TCP connect e SYN
- Version detection

E la seguente sul target Windows 7: OS fingerprint.

A valle delle scansioni è prevista la produzione di un report contenente le seguenti informazioni (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione

---

**Quesito extra:** Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

## SVOLGIMENTO

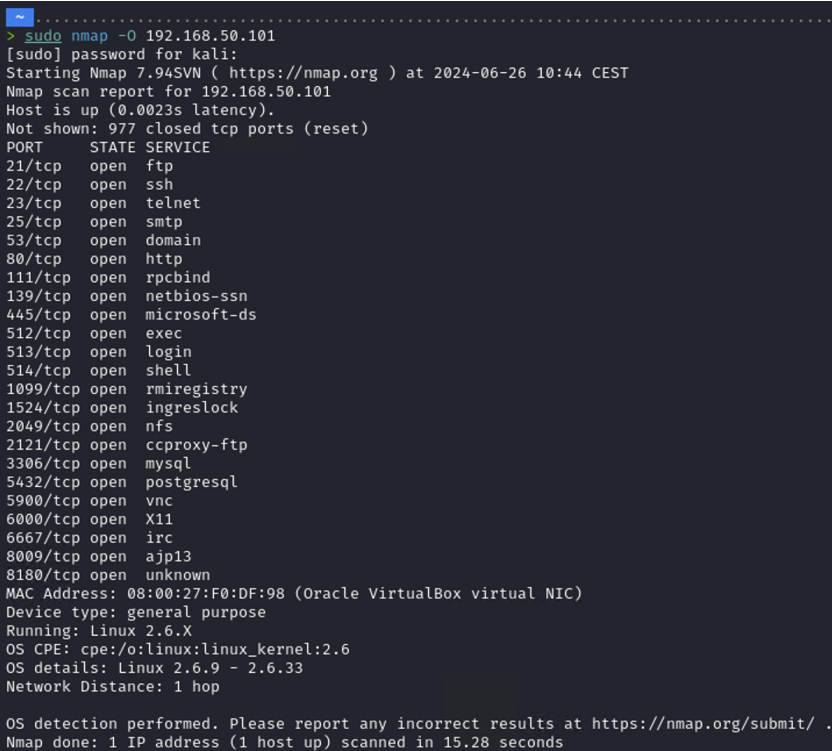
### *Target: Metasploitable 2*

#### OS Fingerprint

Il comando utilizzato è:

```
sudo nmap -O indirizzo_ip
```

Con questo comando si effettua una scansione OS fingerprint. Questa funzionalità stima il sistema operativo target ispezionando i pacchetti di risposta ricevuti. Tali pacchetti sono leggermente differenti per ogni sistema operativo (Windows, Linux, macOS). Confrontando i pacchetti con un database di risposte conosciute per i differenti SO, è possibile identificare il sistema operativo target. Il comando "sudo" viene utilizzato per ottenere i permessi di root.



```
> sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 10:44 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0023s 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:F0:DF:98 (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 15.28 seconds
```

---

## Syn Scan

Il comando utilizzato è:

```
sudo nmap -sS indirizzo_ip
```

Questo comando esegue una scansione delle porte, in particolare lo switch '-sS' indica il cosiddetto SYN scan. Questo metodo sfrutta il *3-way-handshake*, il modo in cui TCP lavora per stabilire una comunicazione. In questo caso viene utilizzato per capire se una porta è attiva o meno. Se dopo una richiesta SYN si riceve in risposta un SYN-ACK, questo significa che la porta è aperta. Il SYN scan non conclude il *3-way-handshake* con una risposta, ma chiude la comunicazione inviando un pacchetto RST (reset).

```
~ .....
> sudo nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 10:51 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00086s 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:F0:DF:98 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

---

## TCP Connect

Il comando utilizzato è:

```
sudo nmap -sT indirizzo_ip
```

Questo comando esegue una scansione delle porte simile a quella descritta sopra nello SYN scan. A differenza del SYN scan, questo metodo è molto più invasivo poiché conclude il *3-way-handshake*, stabilendo un canale di comunicazione. Questo crea più “rumore” a livello di rete e aumenta il rischio di essere identificati.

```
~ .....  
> sudo nmap -sT 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 10:57 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.0060s 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:F0:DF:98 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.93 seconds
```

---

## Version Detection

Il comando utilizzato è:

```
sudo nmap -sV -sS indirizzo_ip
```

Questo comando avvia una scansione con privilegi elevati utilizzando una combinazione di SYN scan e rilevazione delle versioni dei servizi per identificare le porte aperte e i servizi eseguiti su un indirizzo IP specifico. Lo switch '-sV' permette di effettuare il "Service Version Detection". Nmap tenta di determinare quali servizi stanno girando sulle porte aperte e, se possibile, di identificare la versione specifica di quei servizi. Questo include informazioni come il tipo di servizio (es. HTTP, FTP, SSH), il software esatto in esecuzione (es. Apache, OpenSSH), e la versione. Questo tipo di scansione è utile per capire la configurazione di un sistema e identificare potenziali punti deboli, ma dovrebbe essere eseguita solo su sistemi su cui si ha il permesso di fare test di sicurezza o analisi di rete.

```
> sudo nmap -sV -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 11:03 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00071s 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:F0:DF:98 (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 66.98 seconds
```

---

## Target: Windows 7

### OS Fingerprint

Il comando utilizzato è:

```
sudo nmap -O indirizzo_ip
```

Usando come target Windows 7 è stata effettuata una scansione OS fingerprint. In questo caso si nota una risposta diversa da quella ottenuta su Metasploitable, come mostrato in figura. Lo scan delle porte non è avvenuto correttamente poiché non siamo riusciti a ottenere il loro stato.

```
> sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 11:14 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0039s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:70:E2:8F (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 37.95 seconds
```

### Soluzione al Problema

Per risolvere questa situazione, è stato disattivato il firewall di Windows 7. In questo modo si è riuscito a ottenere uno scan delle porte come fatto prima su Metasploitable. La figura in basso mostra gli output della scansione OS fingerprint.

```
> sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 11:13 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0019s 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: 08:00:27:70:E2:8F (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 14.58 seconds
```

---

## RISPOSTA AL QUESITO EXTRA

L'output ottenuto dalla scansione OS fingerprint su Windows 7 non ha portato a un buon risultato a causa del firewall attivo. Disattivando il firewall, la scansione è andata a buon fine. Tuttavia, questa soluzione è applicabile solo in un ambiente di laboratorio virtuale.

### *Metodi per tentare di eludere il firewall di Windows 7*

#### 1. Utilizzo di Nmap con tecniche di evasione

- **Frammentazione dei pacchetti** (-f): questo metodo tenta di dividere i pacchetti di scansione in frammenti più piccoli.
- **Introduzione di ritardi tra i pacchetti** (--scan-delay): introduce ritardi tra i pacchetti per evitare il rilevamento.
- **Cambiamento della porta di origine** (--source-port): cambia la porta di origine dei pacchetti di scansione per eludere le regole del firewall.

#### **Motivi per cui potrebbe non funzionare:**

- I firewall moderni possono rilevare e bloccare la frammentazione dei pacchetti.
- I ritardi nei pacchetti potrebbero non essere sufficienti per eludere le regole del firewall.
- Cambiare la porta di origine potrebbe essere inefficace se il firewall blocca tutte le porte non autorizzate.

#### 2. Utilizzo di strumenti alternativi per OS Fingerprinting

- **XProbe2**: strumento di fingerprinting passivo.
- **p0f**: strumento di analisi passiva del traffico di rete.

#### **Motivi per cui potrebbe non funzionare:**

- Entrambi gli strumenti richiedono traffico di rete passivo che potrebbe non essere disponibile o sufficiente.
- Il firewall potrebbe comunque bloccare le informazioni necessarie per il fingerprinting.

---

### 3. Utilizzo di Metasploit Framework

- **Modulo di scanner SMB** (`smb_version`): tenta di determinare la versione del sistema operativo tramite SMB.
- **Modulo di enumerazione SMB** (`smb_enum_os`): esegue l'enumerazione del sistema operativo tramite SMB.

#### Motivi per cui potrebbe non funzionare:

- Il firewall potrebbe bloccare le richieste SMB.
- Le impostazioni di sicurezza di Windows 7 potrebbero limitare le risposte SMB.

### 4. Utilizzo di PowerShell Remoting

- **Comando PowerShell** (`Get-WmiObject`): esegue comandi PowerShell remoti per ottenere informazioni sul sistema operativo.

#### Motivi per cui potrebbe non funzionare:

- Richiede credenziali valide per accedere al sistema remoto.
- PowerShell Remoting potrebbe essere disabilitato o limitato dalle politiche di sicurezza.

### 5. Utilizzo di script Python con libreria `impacket`

- **SMBConnection**: utilizza la libreria `impacket` per interagire con il protocollo SMB e raccogliere informazioni sul sistema operativo.

#### Motivi per cui potrebbe non funzionare:

- Il firewall potrebbe bloccare le richieste SMB.
- Le impostazioni di sicurezza di Windows 7 potrebbero limitare le risposte SMB.

Generalmente i firewall semplici sono progettati per consentire o bloccare il traffico a livello del data link. Un mappatore di porte e indirizzi come Nmap non è un programma di hacking definitivo, ma un programma amministrativo utilizzato per il footprinting delle reti. L'uso combinato di diverse tecniche e strumenti può aumentare le probabilità di successo, ma è importante considerare le specifiche configurazioni di sicurezza del target e adattare le strategie di conseguenza.