

S5-L2

Scansione dei servizi con nMap

Presented By:
Mattia Di Donato



TRACCIA:

Mi è stato richiesto di effettuare le seguenti scansione:

- OS Fingerprint per l s.o. Metasploitable2 e Windows7
- Syn Scan per s.o. Meta2
- TCP Connect per s.o. Meta2 & differenze tra la scansione syn e quest'ultima.
- Version Detection per s.o. Meta2

1

**OS Fingerprint
Meta2 e Win7**

2

Syn Scan: Meta2

3

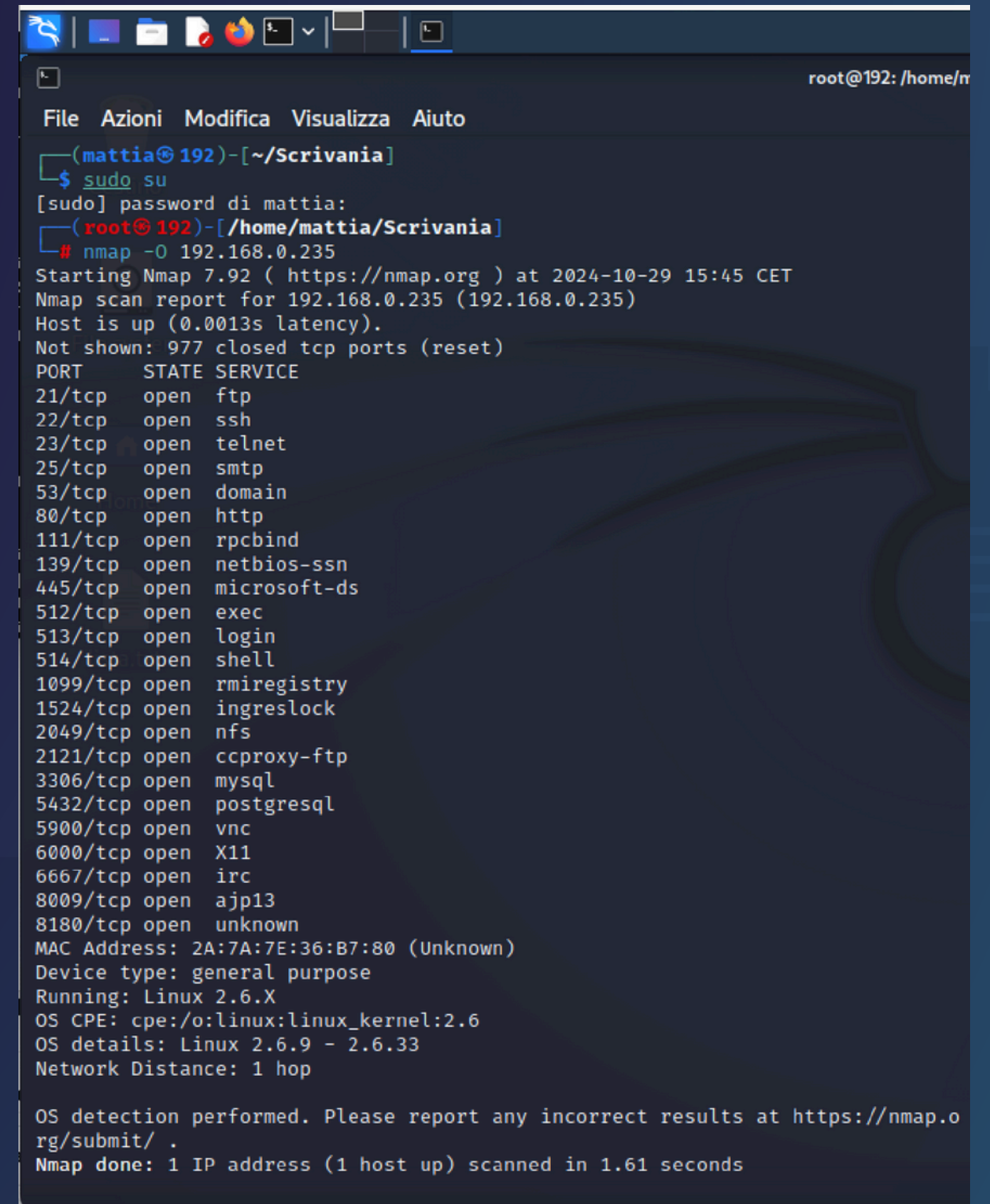
**TCP Connect:
Meta2**

4

**Version
Detection: Meta2**

1.1 OS FINGERPRINT (META2)

Per la scansione con nmap per verificare il sistema operativo in uso, ho utilizzato il comando Nmap -O seguito dall'IP del sistema operativo di riferimento (in questo caso Metasploitable2). Essendo un sistema operativo fragile e facilmente attaccabile, metasploit mi ha dato subito riscontro senza dover effettuare operazioni preliminari.

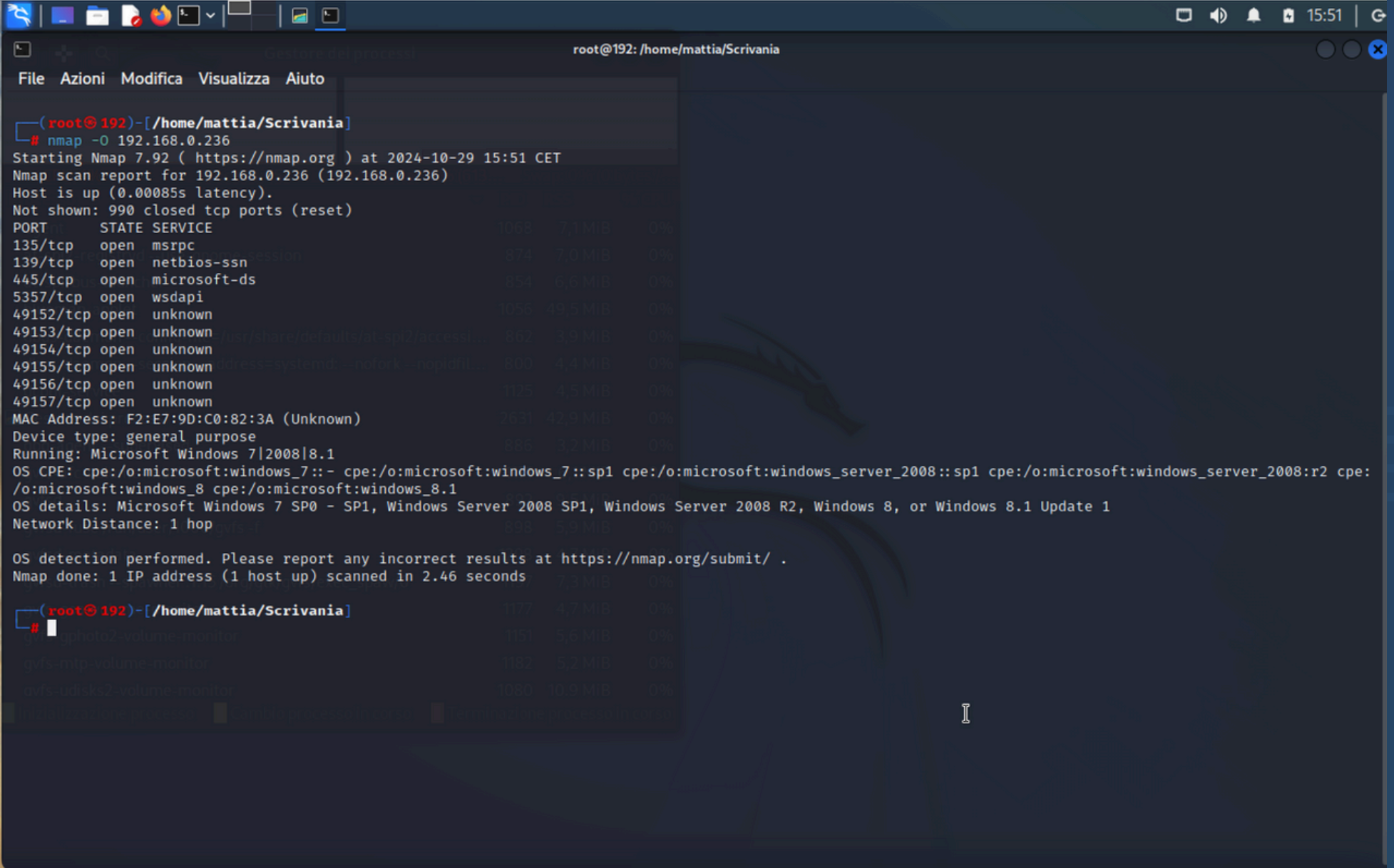


```
root@192: /home/n
File Azioni Modifica Visualizza Aiuto
(mattia@192)-[~/Scrivania]
$ sudo su
[sudo] password di mattia:
(root@192)-[/home/mattia/Scrivania]
# nmap -O 192.168.0.235
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-29 15:45 CET
Nmap scan report for 192.168.0.235 (192.168.0.235)
Host is up (0.0013s 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: 2A:7A:7E:36:B7:80 (Unknown)
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 1.61 seconds
```

1.2 OS FINGERPRINT WIN7

Anche per quest'ultimo, per verificare il sistema operativo in uso ho utilizzato il comando `nmap -O` seguito dall'ip del sistema operativo di riferimento ovvero Windows 7. In questo caso per poter avviare la procedura, ho dovuto disabilitare il firewall in quanto altrimenti avrebbe bloccato qualsiasi tentativo di comunicazione. Esso può infatti, filtrare pacchetti, limitare le porte aperte o attuare politiche di sicurezza che impediscono la risposta ai tentativi di scansione come quelli di Nmap. Questo può rendere più difficile per gli scanner ottenere informazioni accurate sui dispositivi.



```
(root@192)-[/home/mattia/Scrivania]
# nmap -O 192.168.0.236
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-29 15:51 CET
Nmap scan report for 192.168.0.236 (192.168.0.236)
Host is up (0.00085s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
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: F2:E7:9D:C0:82:3A (Unknown)
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 2.46 seconds

(root@192)-[/home/mattia/Scrivania]
#
```


2. SYN SCAN

Ci è stata poi richiesta la TCP SYN SCAN ovvero una scansione “Half-open” inviando pacchetti SYN e attendendo risposte SYN/ACK. Tramite il comando `nmap -sS` viene effettuata la scansione.

Essa è conosciuta anche come “Stealth Scan”.

Invia un pacchetto SYN (sincronizzazione) per iniziare la connessione TCP, ma non completa il 3 way handshake. Se la porta è aperta, il target risponde con un pacchetto SYN-ACK, mentre se la porta è chiusa, risponde con un pacchetto RST (reset).

Questa scansione è meno evidente e può passare inosservata dai sistemi di rilevamento delle intrusioni (IDS), poiché non stabilisce una connessione completa, inoltre è spesso utilizzata dagli attaccanti proprio per questa sua peculiarità.

```
File Azioni Modifica Visualizza Aiuto

(root@192)-[/home/mattia/Scrivania]
# nmap -sS 192.168.0.235
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-29 15:48 CET
Nmap scan report for 192.168.0.235 (192.168.0.235)
Host is up (0.00060s 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: 2A:7A:7E:36:B7:80 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

(root@192)-[/home/mattia/Scrivania]
#
```

3. TCP COMPLETO

Tuttavia per poter effettuare una scansione completa dobbiamo necessariamente utilizzare la scansione TCP completa. Essa viene effettuata tramite il comando `nmap -sT`.

Questa modalità completa il processo del 3 way handshake (SYN-SYN/ACK-ACK) per stabilire una connessione. Diversamente dalla scansione syn scan essa è più evidente e può essere registrata dai normali sistemi sicurezza poichè stabilisce una connessione completa. Un'attaccante, quindi, che volesse optare per questa soluzione potrebbe facilmente essere rilevato.

```
File Azioni Modifica Visualizza Aiuto

(root@192)-[/home/mattia/Scrivania]
# nmap -sT 192.168.0.235
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-29 15:46 CET
Nmap scan report for 192.168.0.235 (192.168.0.235)
Host is up (0.0089s 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: 2A:7A:7E:36:B7:80 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds

(root@192)-[/home/mattia/Scrivania]
#
```


4. VERSION DETECT

Infine il Version Detect viene utilizzato per eseguire non solo la scansione delle porte aperte su un host ma tenta anche di identificare i servizi in esecuzione su quelle porte e le relative versioni.

Il comando per eseguirlo è `nmap -sV` seguito dall'ip da scansione.

Nmap invia richieste specifiche ai servizi in esecuzione e analizza le risposte per determinare il tipo di servizio e la sua versione. Questo può fornire informazioni preziose per valutare la sicurezza di un sistema in quanto versioni specifiche di software possono avere vulnerabilità note che un'attaccante potrebbe facilmente sfruttare

THANK YOU

MATTIA DI DONATO