LABORATORIO EPICODE

S5_L3

Traccia: Tecniche di scansione con Nmap

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

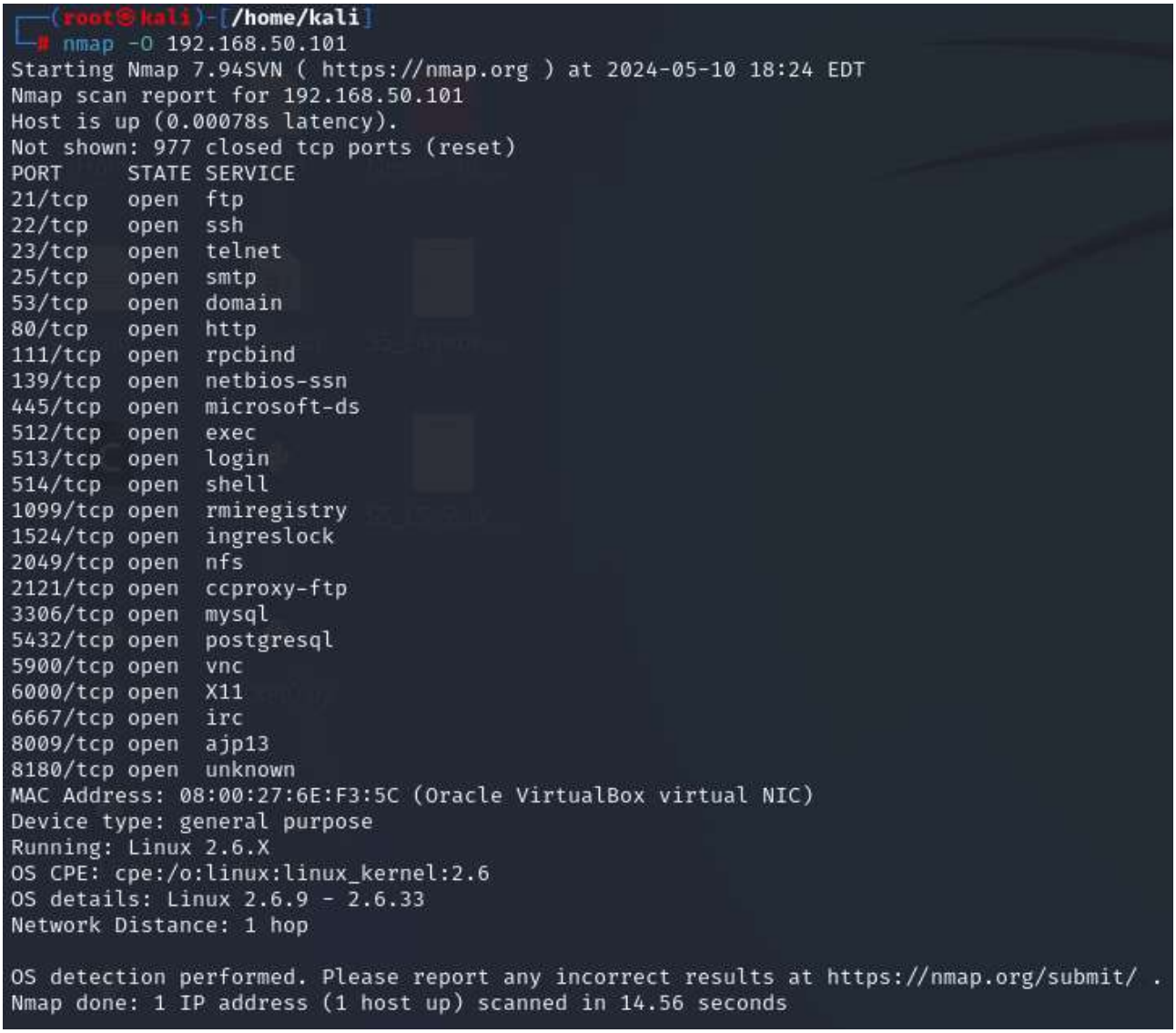
- **OS fingerprint.**
- **Syn Scan.**
- **TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?**
- **Version detection.**

E la seguente sul target Windows 7:

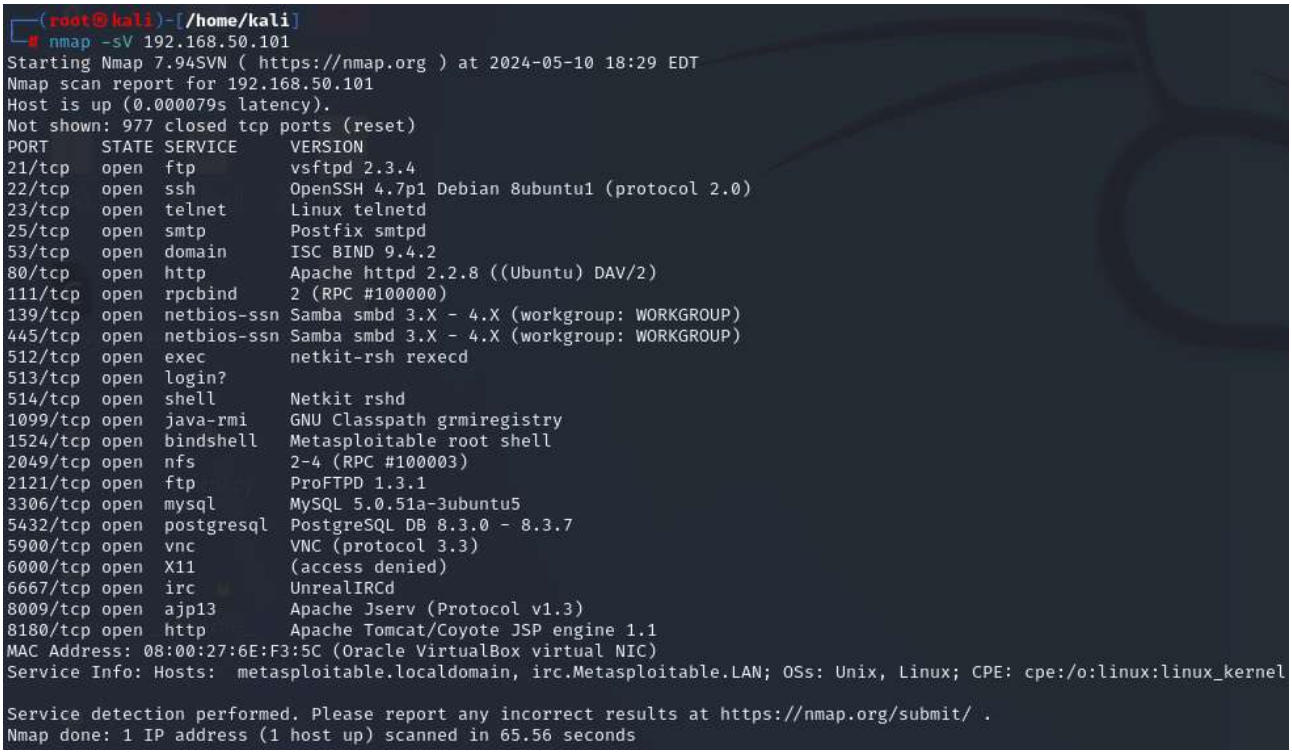
- **OS fingerprint.**

SCAN SU METASPLOITABLE 2

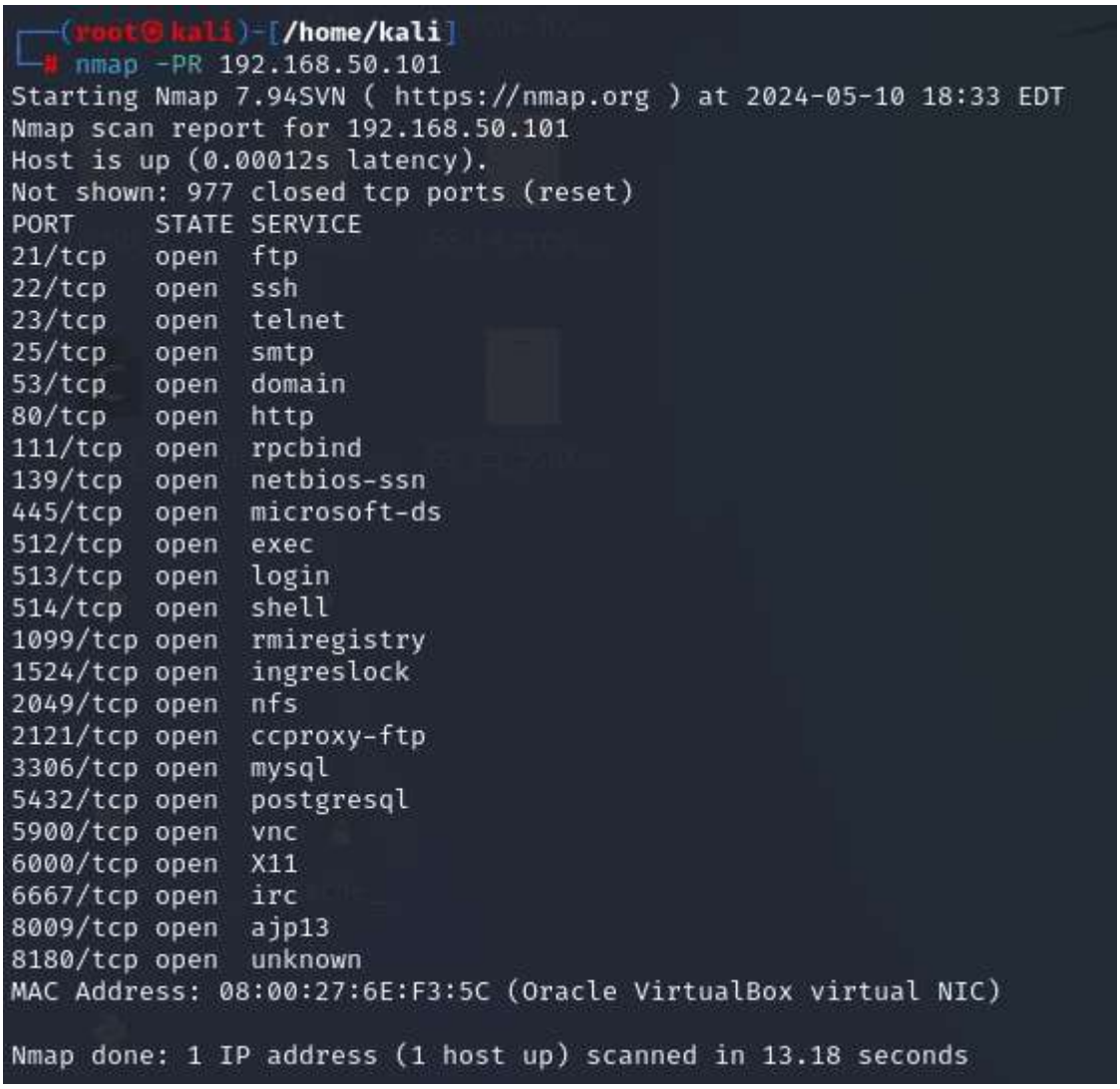
1. **Procediamo con le scansioni di OS Fingerprint con il comando nmap –O per l'identificazione del Sistema Operativo:**



2. **Proseguiamo con le scansioni di OS Fingerprint con il comando nmap –sV per l'identificazione delle versioni disponibili sulle porte scansionate del Sistema Operativo (Version Detection):**



3. **Proseguiamo con le scansioni di OS Fingerprint con il comando nmap –PR per l'identificazione delle richieste ARP sul Sistema Operativo in esame:**



4. **Proseguiamo con le scansioni di OS Fingerprint con il comando nmap –sS per effettuare un SYN SCAN, un metodo di Scannerizzazione mono-invasivo che non completa il 3 Way Handshake:**

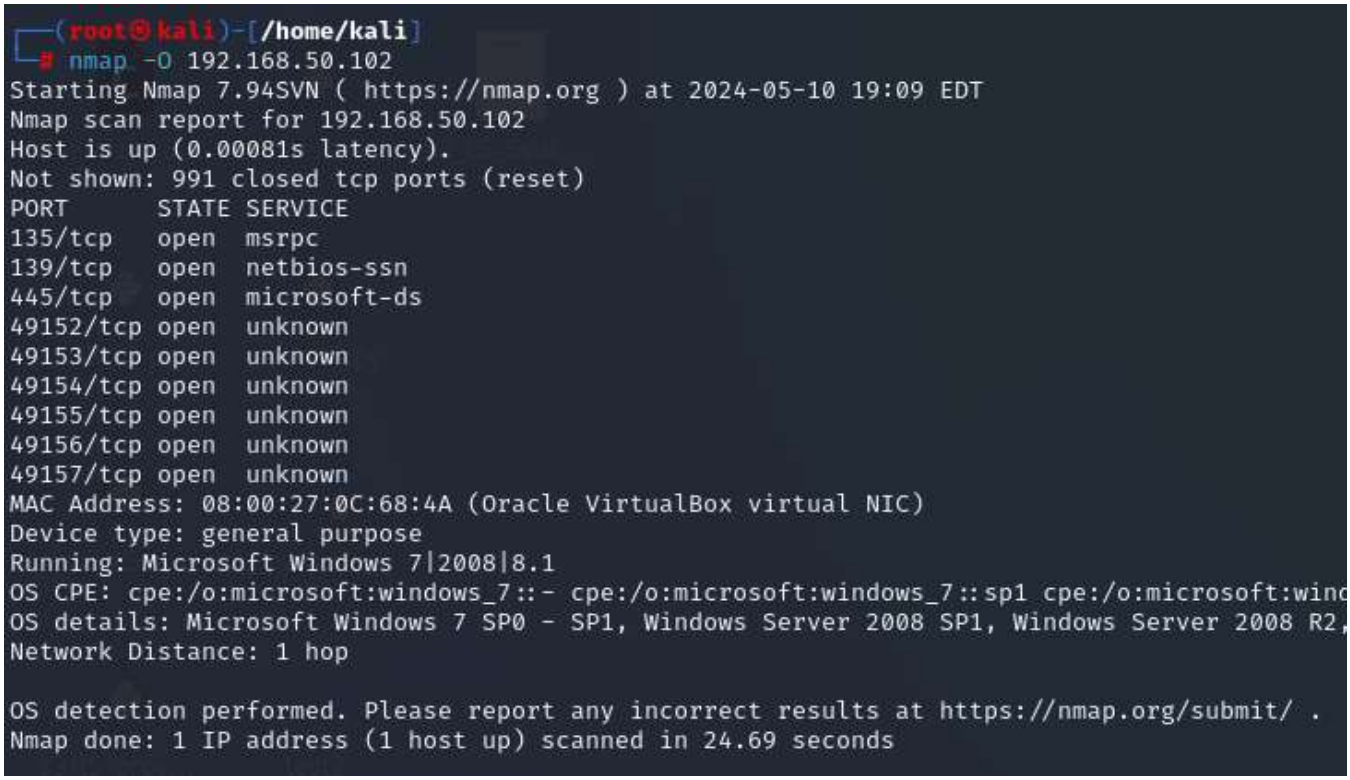
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 18:42 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000069s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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: 08:00:27:6E:F3:5C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

5. **Proseguiamo con le scansioni di OS Fingerprint con il comando nmap –sT, effettua uno scan più invasivo completando il 3 Way Handshake creando il canale di comunicazione:**

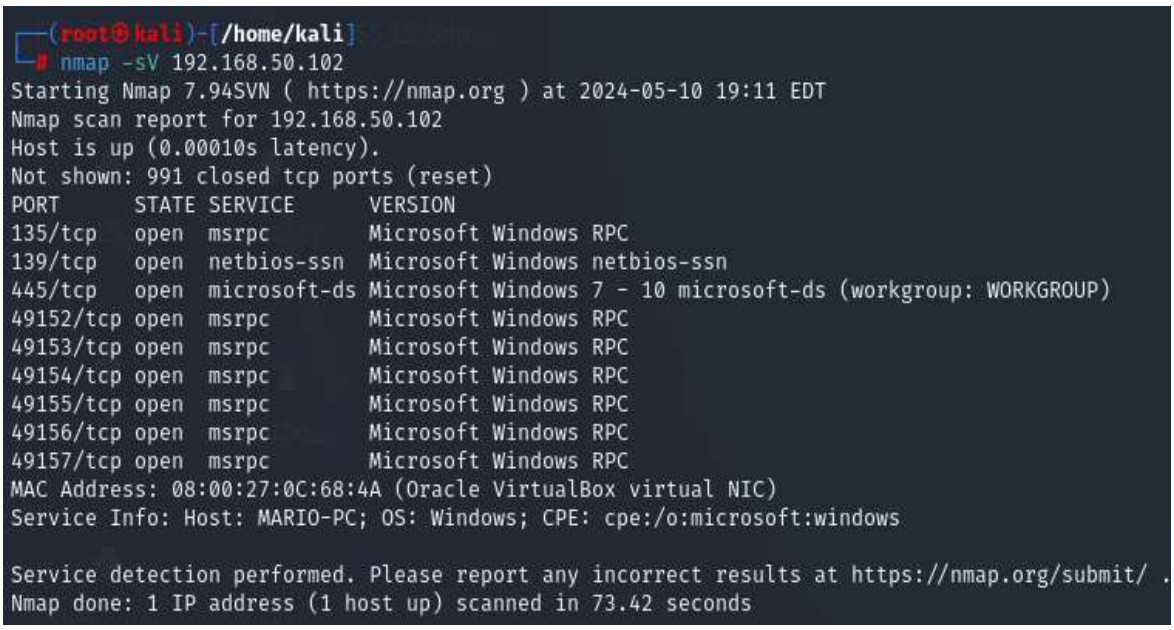
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 18:45 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
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: 08:00:27:6E:F3:5C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

SCAN SU WIN 7

1. **Procediamo ora con le scansioni di OS Fingerprint con il comando nmap –O per l'identificazione del Sistema Operativo di Win 7:**



2. **Proseguiamo con le scansioni di OS Fingerprint con il comando nmap –sV per l'identificazione delle versioni disponibili sulle porte scansionate del Sistema Operativo (Version Detection):**



3. **Proseguiamo con le scansioni di OS Fingerprint con il comando nmap –PR per l'identificazione delle richieste ARP sul Sistema Operativo in esame:**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PR 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 19:14 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00092s 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: 08:00:27:0C:68:4A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.57 seconds
```

4. **Proseguiamo con le scansioni di OS Fingerprint con il comando nmap –sS per effettuare un SYN SCAN, un metodo di Scannerizzazione mono-invasivo che non completa il 3 Way Handshake:**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 19:16 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00086s 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: 08:00:27:0C:68:4A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.45 seconds
```

5. **Proseguiamo con le scansioni di OS Fingerprint con il comando nmap –sT, effettua uno scan più invasivo completando il 3 Way Handshake creando il canale di comunicazione:**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 19:19 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00062s latency).
Not shown: 991 closed tcp ports (conn-refused)
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: 08:00:27:0C:68:4A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.16 seconds
```