Esercizio 22-02

Traccia: effettuazione di scansioni su Metasploitable, quali:

- OS fingerprint
- SYN Scan
- TCP connect - evidenziare le differenze tra scan TCP e SYN
- Version detection

Scansione su Windows 7:

- OS fingerprint

Produrre un report che contenga queste informazioni dei due target:

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Spiegazione dei servizi

Extra: indicare la ragione dietro alla diversità dei risultati ottenuti dalla scansione su Windows e proporre una soluzione per continuare le scansioni

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 08:45 EST
Nmap scan report for 192.168.50.101
Host is up (0.00081s 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:EF:FF:86 (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 14.84 seconds
```

r individuare il
get (Metasploitable).

```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 08:58 EST
Nmap scan report for 192.168.50.101
Host is up (0.0017s 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:EF:FF:86 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

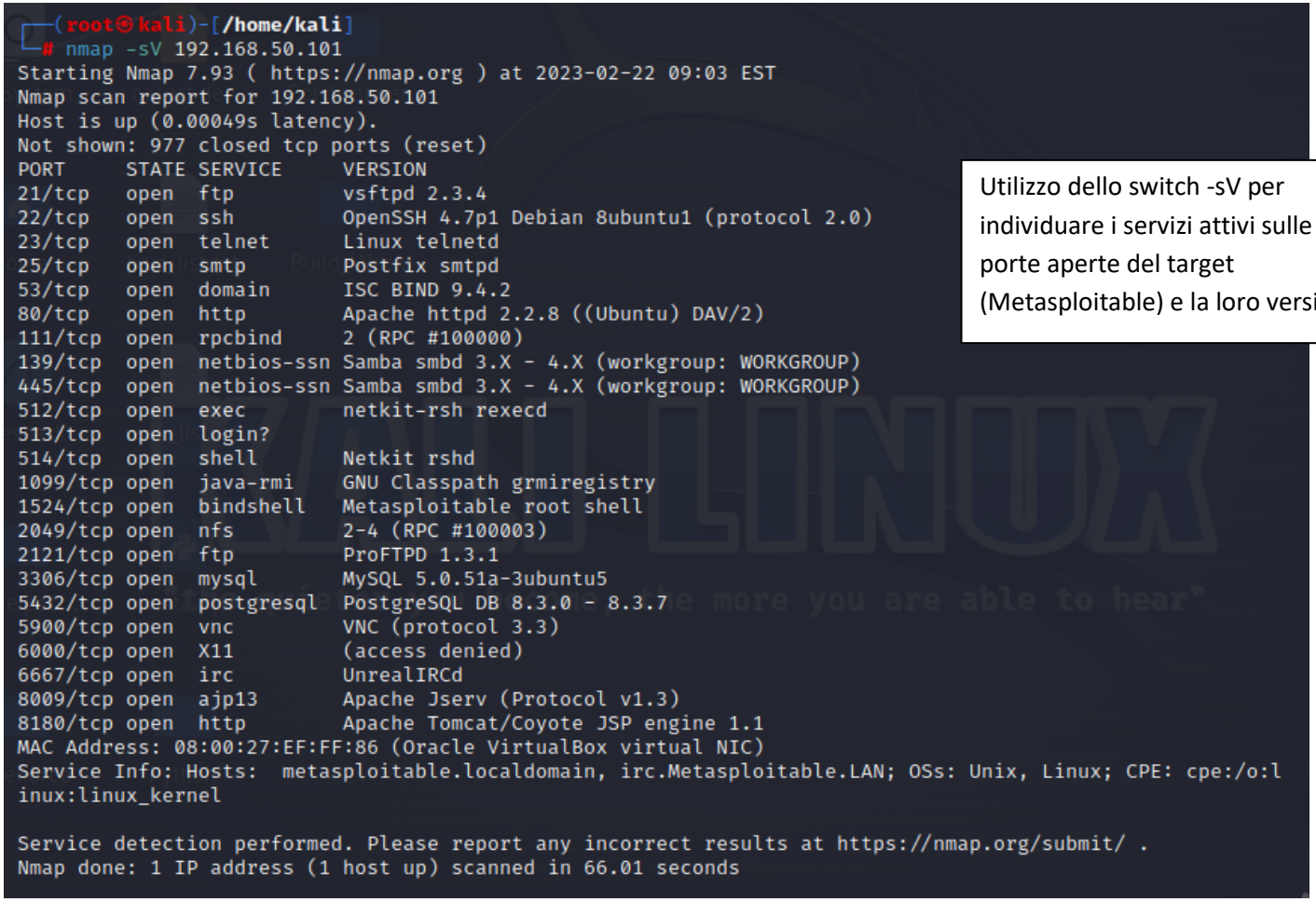
Utilizzo dello switch -sS per individuare le porte aperte del target (Metasploitable) con una scansione di tipo SYN.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 08:59 EST
Nmap scan report for 192.168.50.101
Host is up (0.0016s 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:EF:FF:86 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

Utilizzo dello switch -sT per individuare le porte aperte del target (Metasploitable) con una scansione di tipo TCP.

Si può notare come differenza in output tra scan di tipo SYN e TCP che il primo tipo reputa le porte chiuse come porte a cui è stato inviato un “reset”, mentre nel secondo la stessa tipologia di porte viene definita con “conn-refused”, ovvero le porte che hanno rifiutato la connessione TCP impedendo il completamento del 3-handway-shake



Utilizzo dello switch -sV per individuare i servizi attivi sulle porte aperte del target (Metasploitable) e la loro versione

```
┌──(kali㉿kali)-[~/Desktop/Scan]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 09:22 EST
Nmap scan report for 192.168.50.102
Host is up (0.00078s 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:E8:14:FD (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 36.79 seconds
```

Utilizzo dello switch -O per individuare il Sistema Operativo di Windows, non riuscito.

Extra: non riuscito