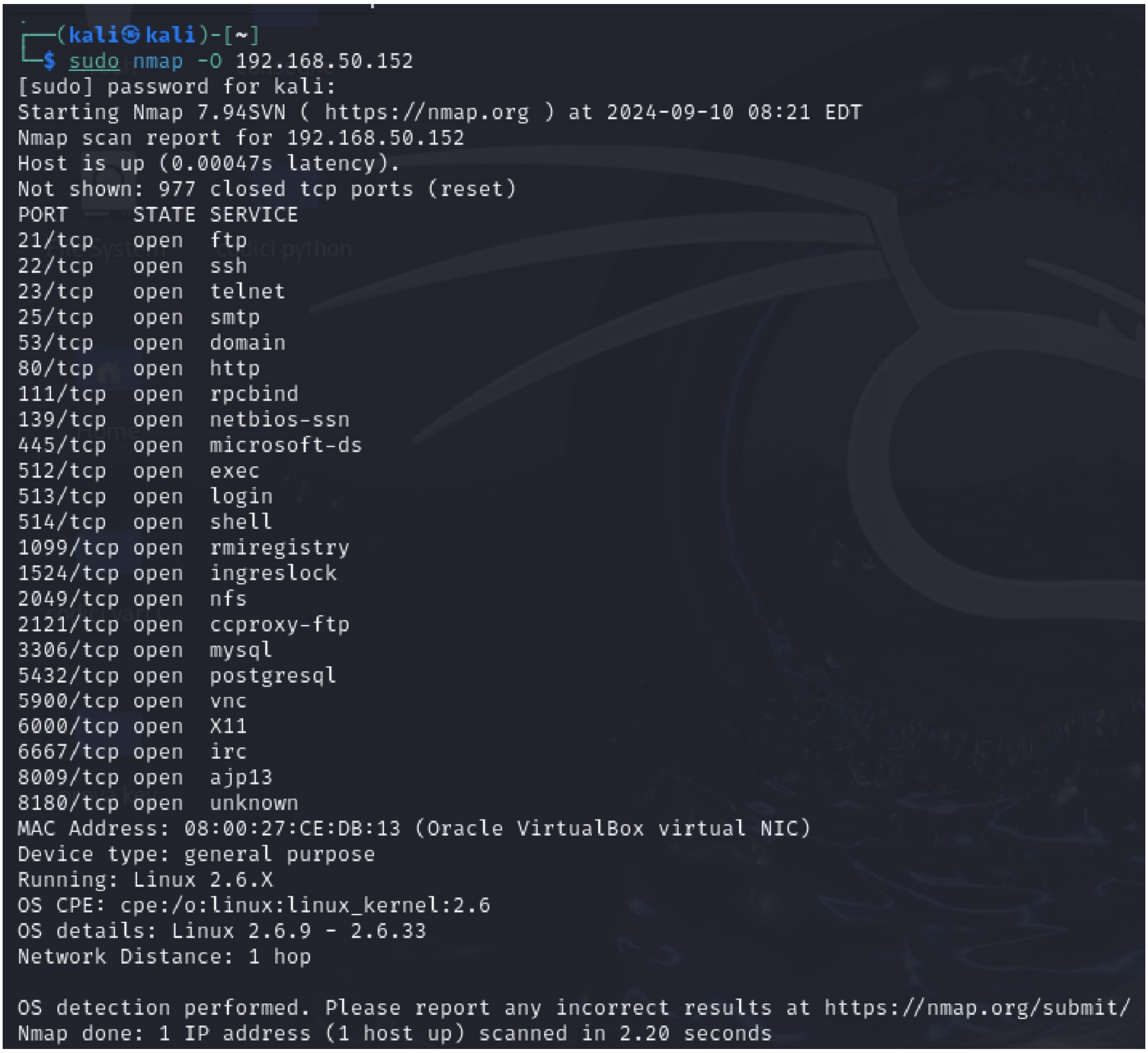
Report Scansioni

Scansione Os Fingerptint verso MetaSploit

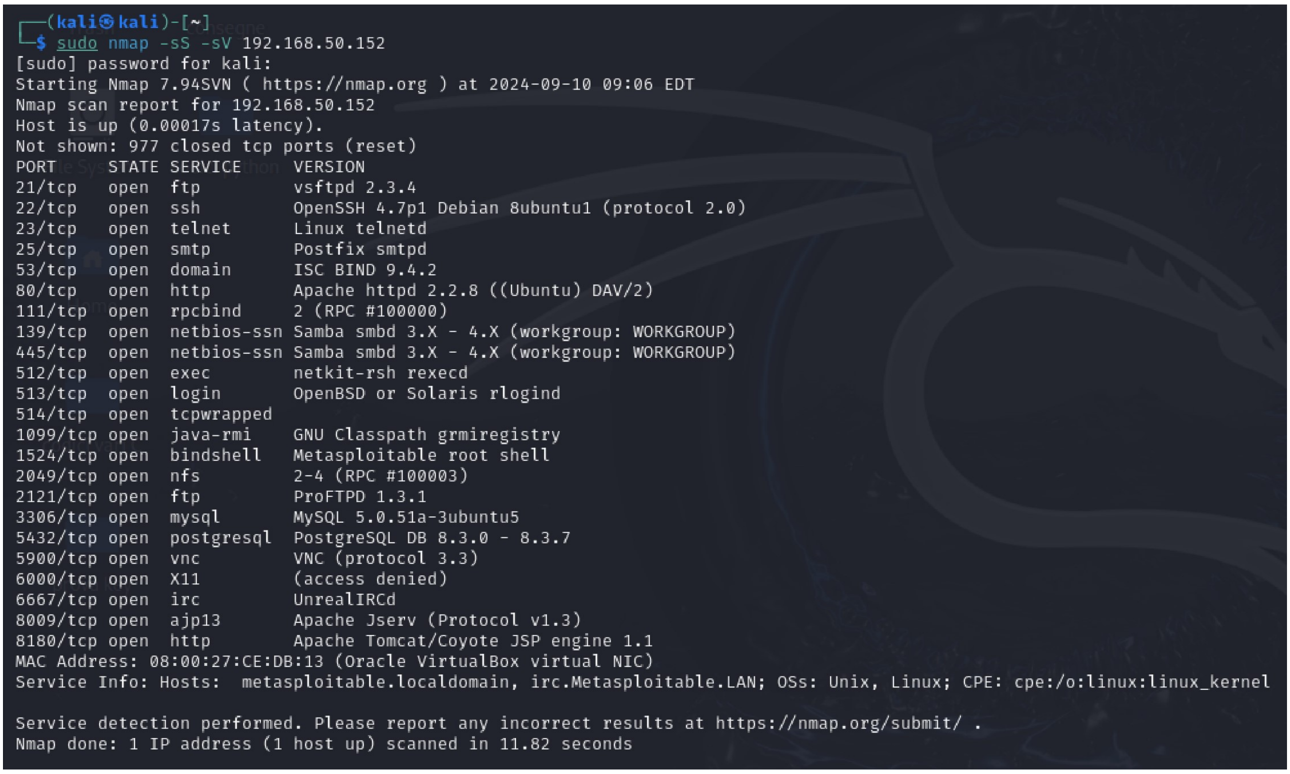


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.152
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 08:21 EDT
Nmap scan report for 192.168.50.152
Host is up (0.00047s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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:CE:DB:13 (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 2.20 seconds
```

La scansione Os (-O) rileva la versione del sistema operativo del target, in questo caso MetaSploit, con ip 192.168.50.152 e sistema operativo Linux 2.6.X.

Scansione SynScan e VersionDetection



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV 192.168.50.152
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 09:06 EDT
Nmap scan report for 192.168.50.152
Host is up (0.00017s 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  tcpwrapped
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:CE:DB:13 (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 11.82 seconds
```

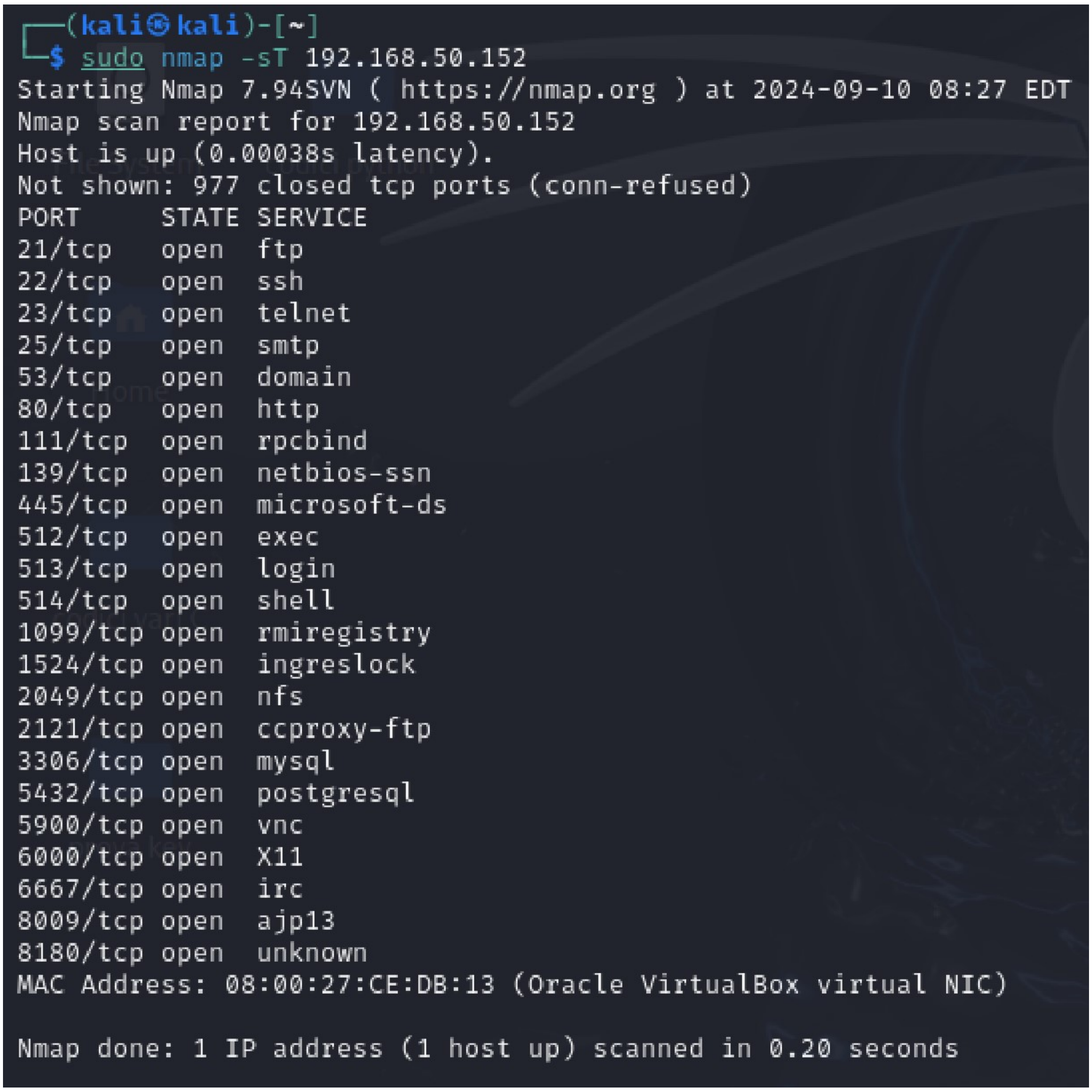
La scansione Syn (-sS) è utilizzata per determinare quali porte sono aperte senza terminare il processo di handshake.

VersionDetection (-sV) è usato per rilevare la versione dei servizi in esecuzione sulle porte aperte.

Unendo i comandi (–sS –sV “ip target) è possibile osservare :

- Porte aperte (21,22,23….)
- Protocollo (tcp)
- Stato delle porte (open/closed)
- Servizio (ftp,telnet,…)
- versione

TCP Connect



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.152
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 08:27 EDT
Nmap scan report for 192.168.50.152
Host is up (0.00038s 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:CE:DB:13 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

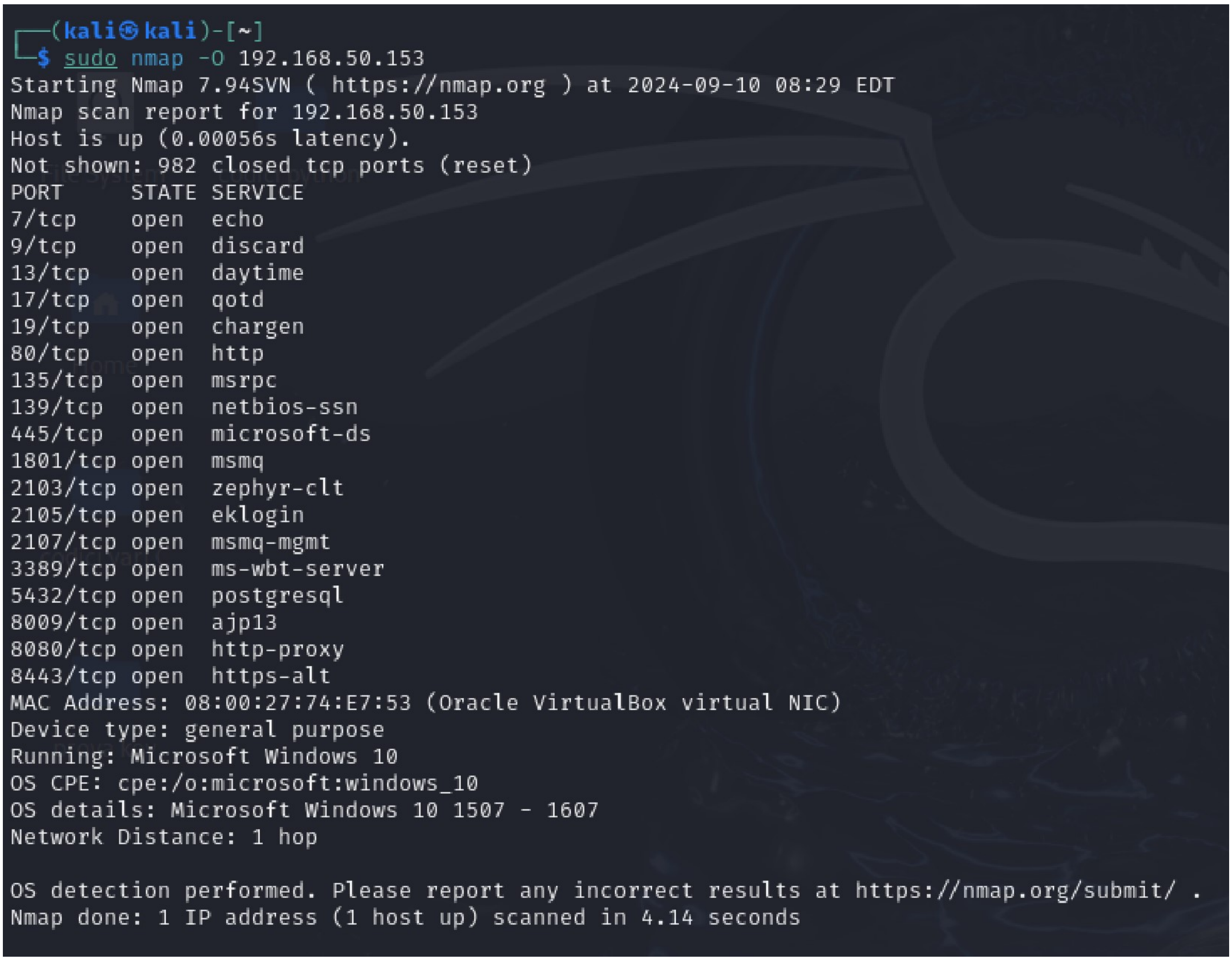
La scansione TCP (-sT) è usata per visualizzare lo stato delle porte completando il processo di handshake.

Differenza tra SYN e TCP

La scansione SYN è preferita per la sua furtività, in quanto non completando il processo 3-way handshake rispondendo con un pacchetto RST (reset) per chiudere la connessione. Poiché la connessione non viene completamente stabilita risulta essere meno rilevabile.

La scansione TCP invia pacchetti ad una porta e se risulta aperta completa il processo di handshake, ciò fa si che questa scansione sia sia più facile da rilevare.

OS fingerprint su Windows



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 08:29 EDT
Nmap scan report for 192.168.50.153
Host is up (0.00056s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:74:E7:53 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 4.14 seconds
```

- Versione windows 10
- Ip 192.168.50.153