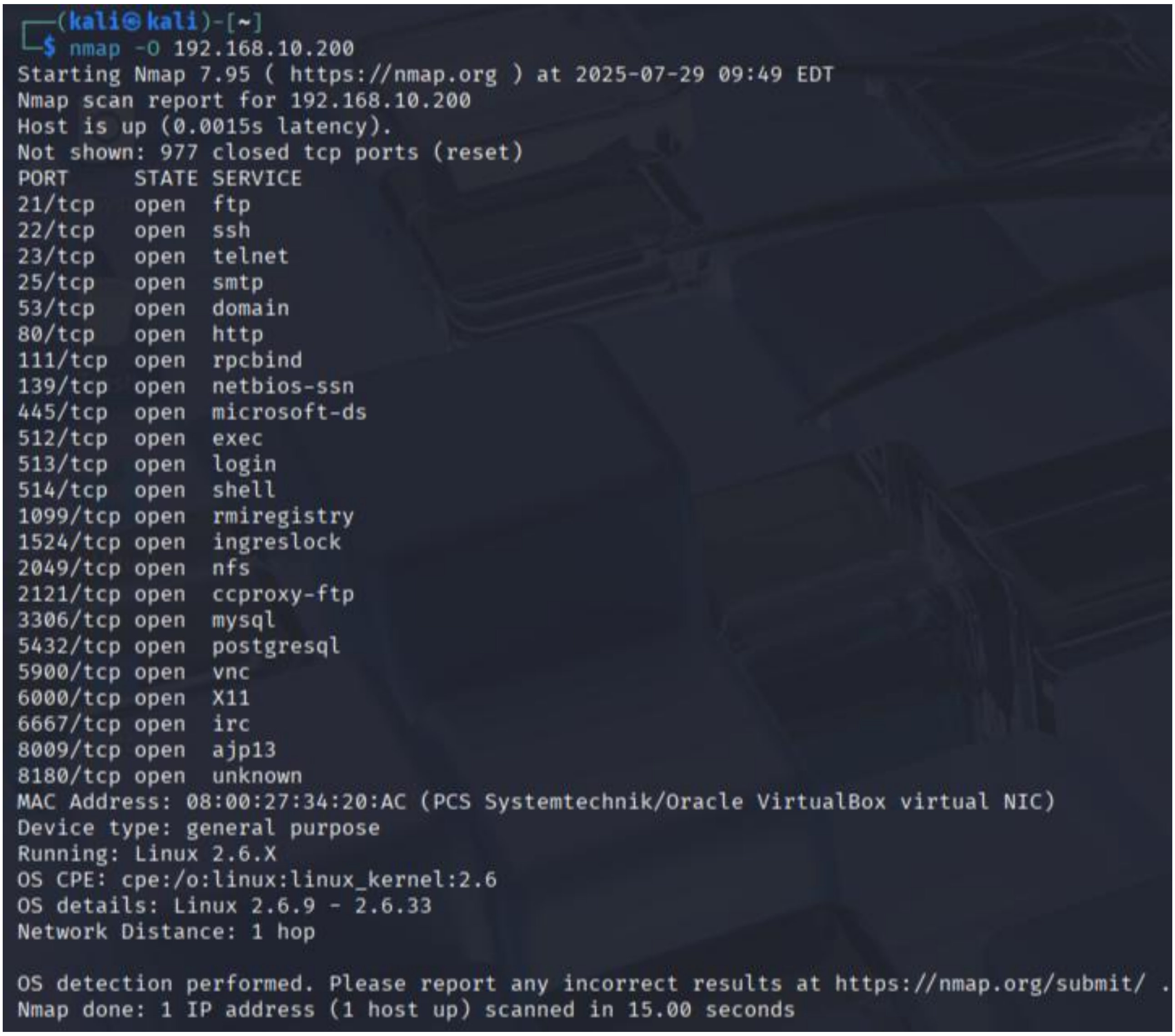
Pratica S5/L2

L'obbiettivo di questo esercizio è di effettuare diverse tipologie di scansioni Nmap dul target Metasploitable2 per identificare il sistema operativo, le porte aperte, i servizi in ascolto e le loro versioni.

Target: Metasploitable2 (IP: 192.168.10.200)

Scanner: Kali Linux (IP: 192.168.10.100)

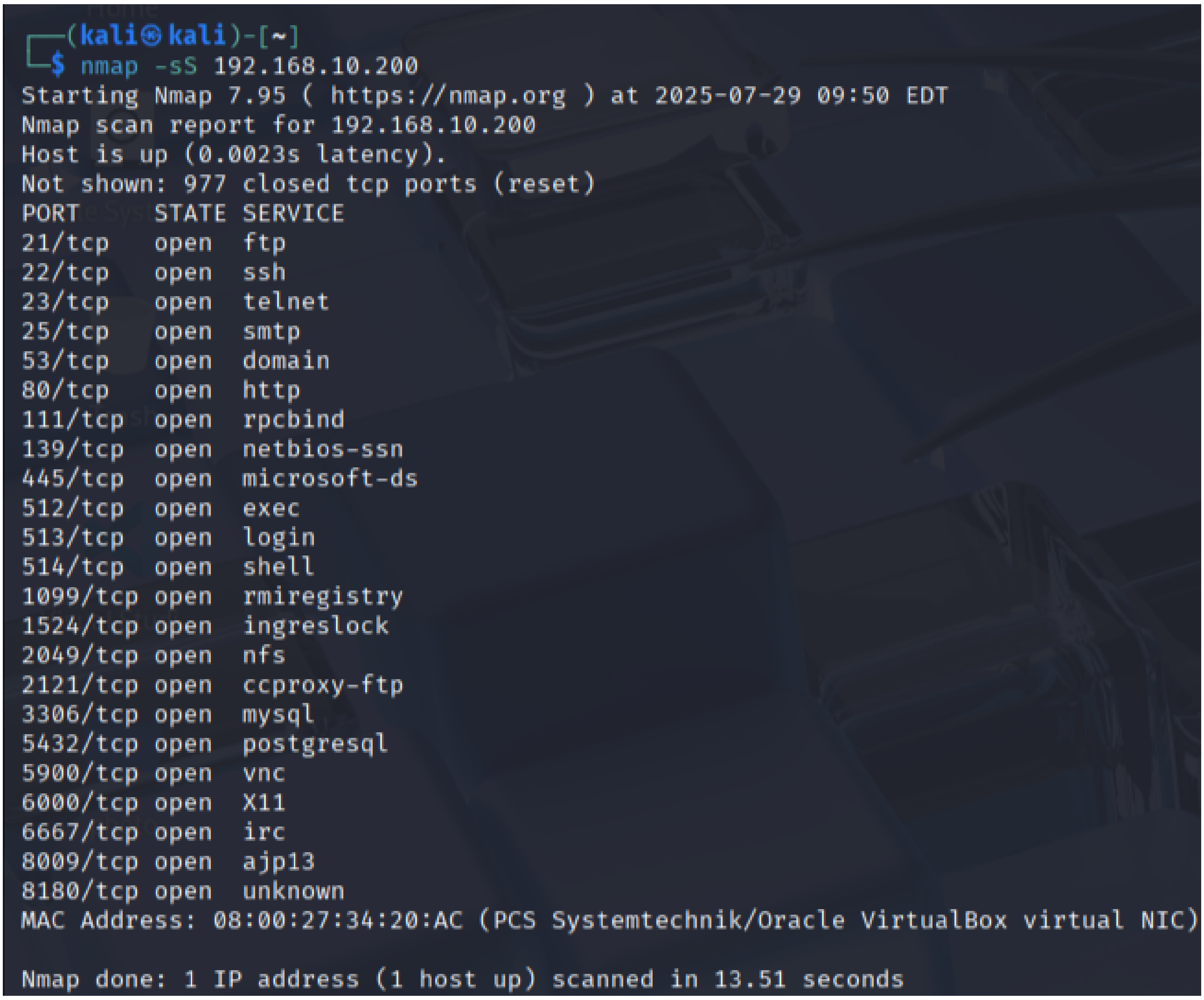
1. OS Fingerprint (Rilevamento del sistema operativo)
   Questo comando, basandosi sulle risposte TCP/IP, identifica il sistema operativo del taget.



```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.10.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:49 EDT
Nmap scan report for 192.168.10.200
Host is up (0.0015s 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: 08:00:27:34:20:AC (PCS Systemtechnik/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 15.00 seconds
```

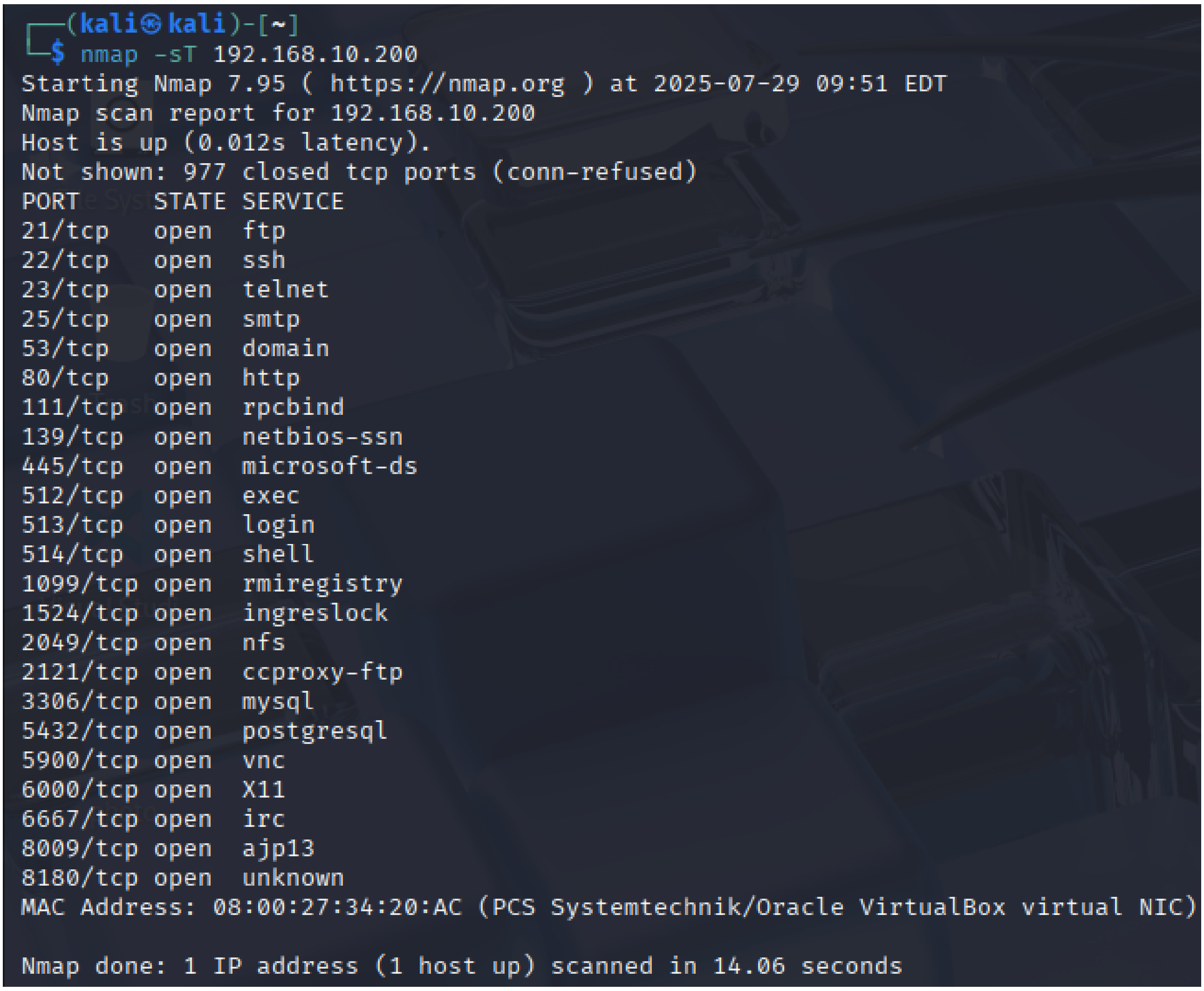
2. Syn Scan (Scansione TCP SYN / Stealth)
   La scansione SYN è stealth perché non completa il three-way handshake TCP. Invia un SYN, e se riceve un SYN/ACK, invia un RST (reset) senza stabilire una connessione completa.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.10.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:50 EDT
Nmap scan report for 192.168.10.200
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: 08:00:27:34:20:AC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds
```

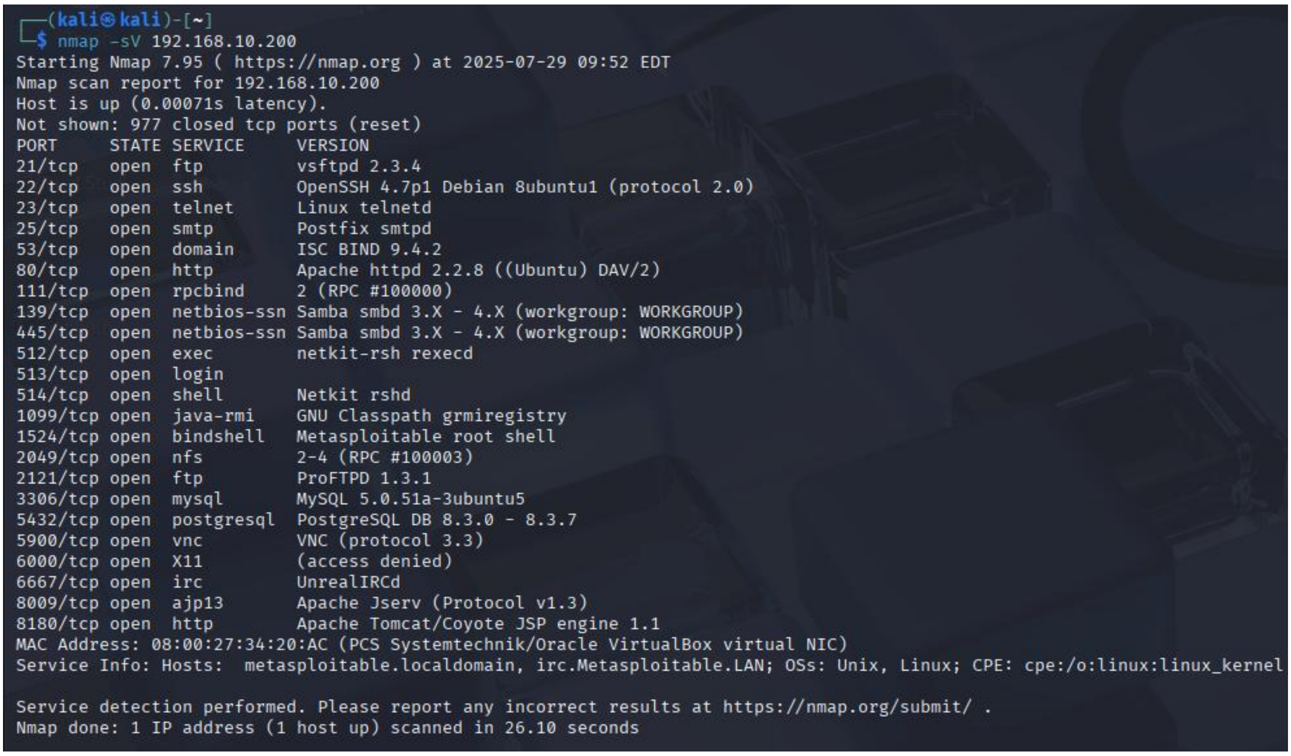
3. TCP Connect Scan (Scansione TCP completa)
   La scansione TCP Connect completa il three-way handshake TCP per ogni porta. A differenza della scansione stealth, questa è più facile da rilevare.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.10.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:51 EDT
Nmap scan report for 192.168.10.200
Host is up (0.012s 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: 08:00:27:34:20:AC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.06 seconds
```

4. Version Detection (Rilevamento della versione dei servizi)
   Questa scansione tenta di identificare il nome e la versione del software in ascolto su ogni porta aperta. Questo è fondamentale per la fase di enumerazione e per identificare vulnerabilità note.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.10.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:52 EDT
Nmap scan report for 192.168.10.200
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: 08:00:27:34:20:AC (PCS Systemtechnik/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 26.10 seconds
```