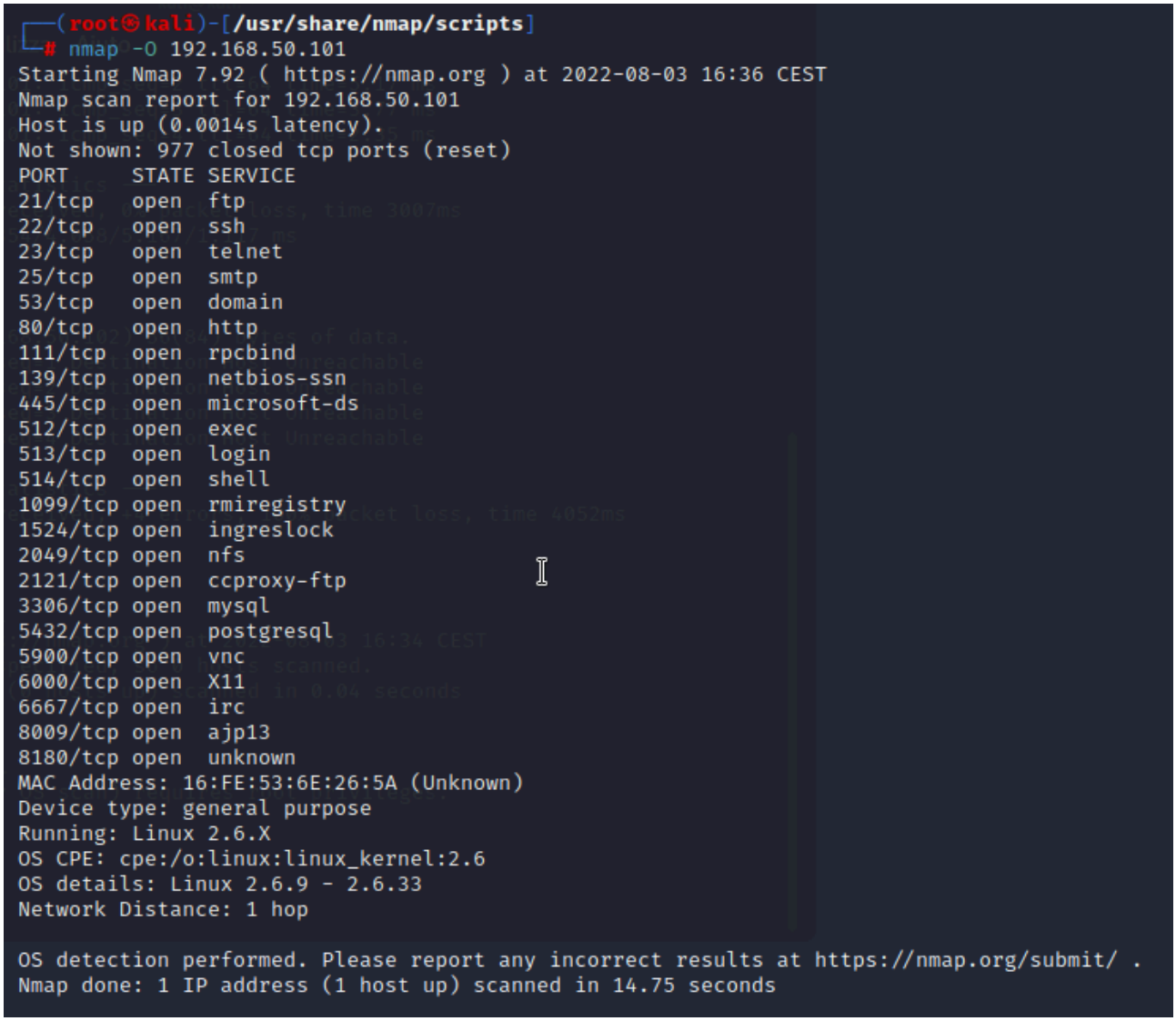
Report

L’esercizio richiede di fare delle scansioni.

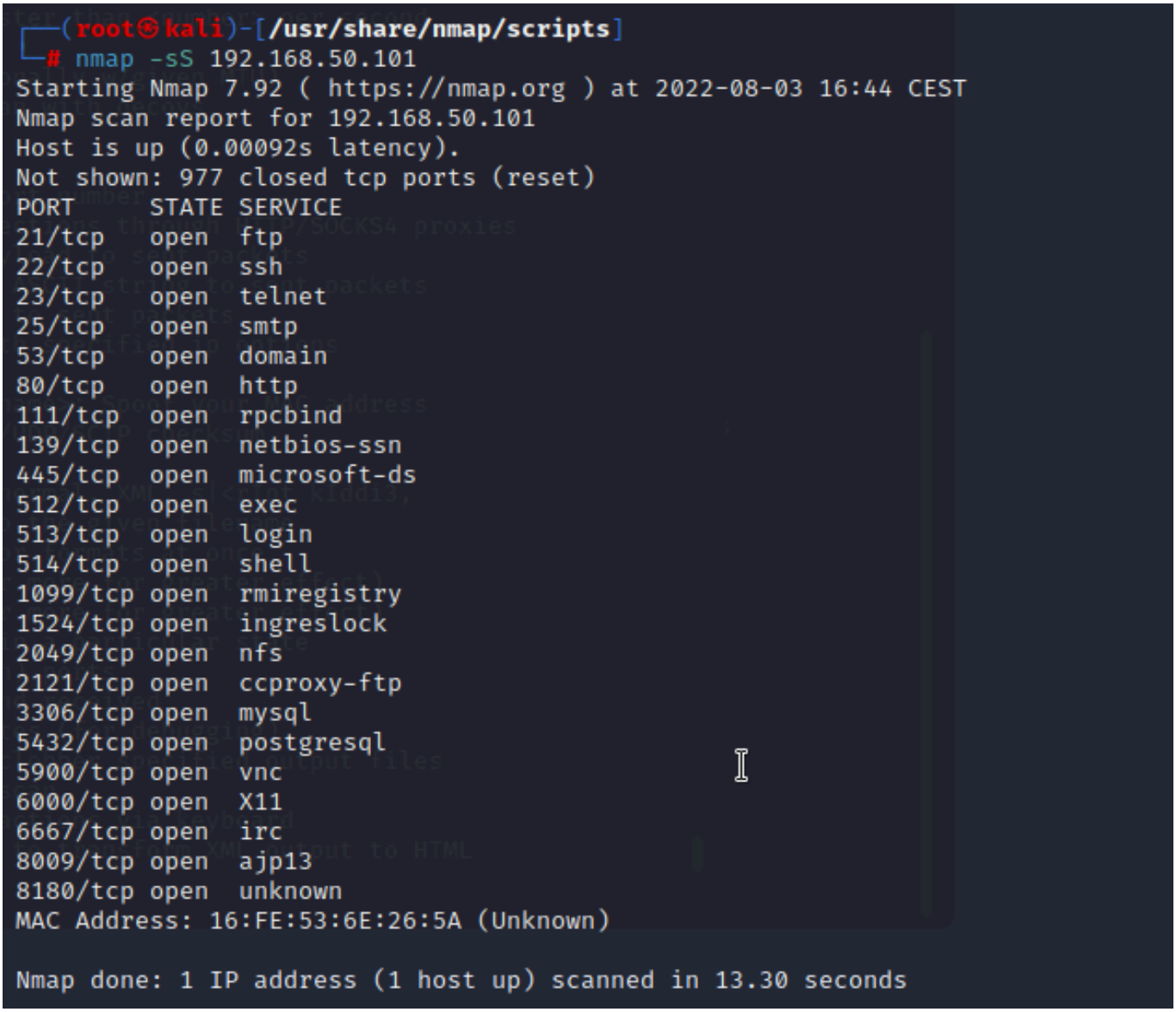
Come richiesto sono state eseguite le scansioni sul target Metasploitable.

Con il comando nmap -O, questo ci permette di stimare il sistema operativo del target.



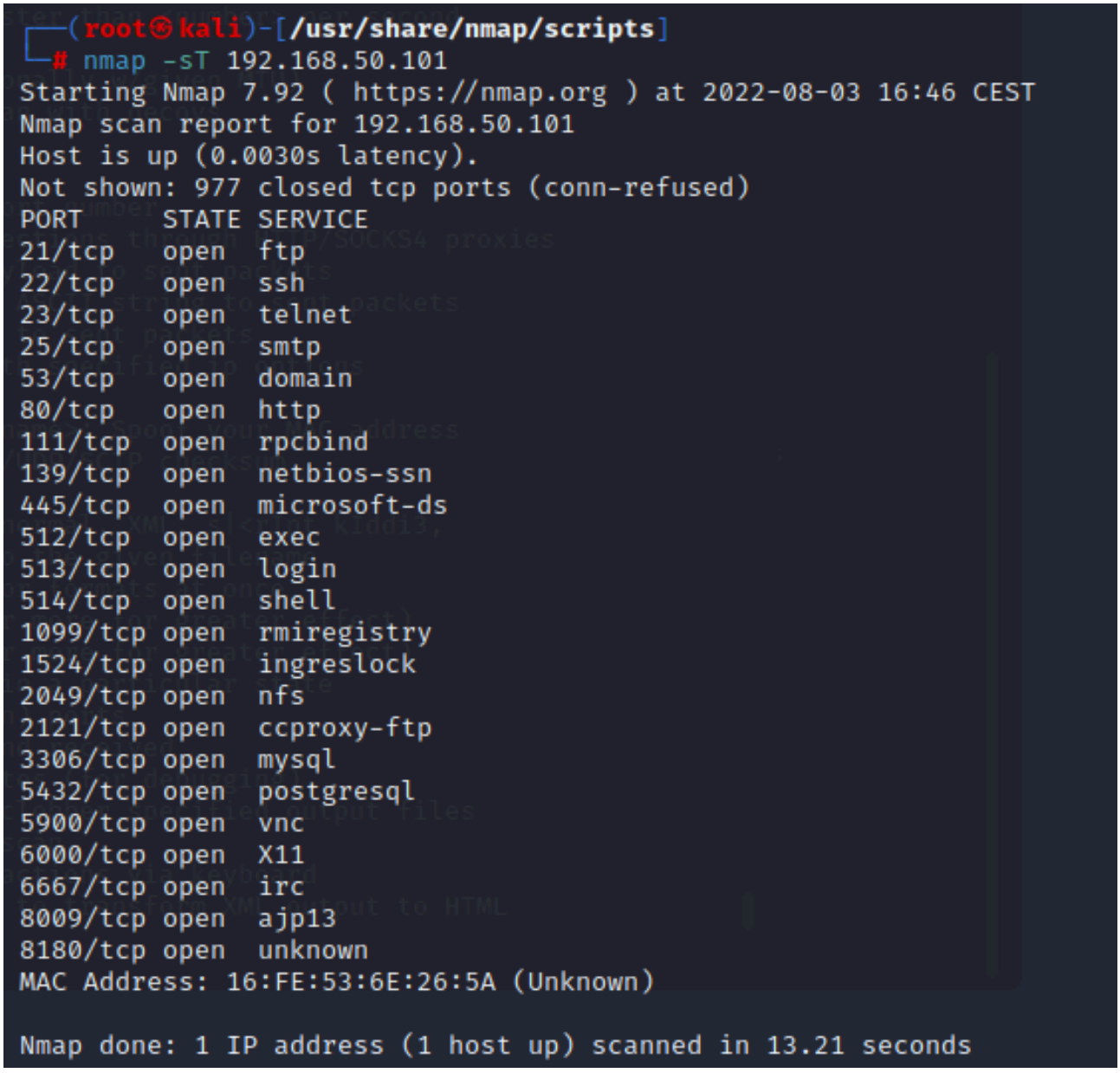
Syn Scan

Con il comando sS di nmap andiamo a fare un scansione poco invasiva sul target segue una scansione Syn che non va a chiudere il 3 way handshake.



TPC Connect

Con il comando sT di nmap andiamo a fare un scansioneinvasiva sul target segue una scansione completa sul tcp eseguendo il 3 way handshake.



Version Detection

Con il comando sV di nmap andiamo a fare un scansione molto invasiva sul target simile a quella che fa sT, ma con l'aggiunta di test specifici che rilevano i servizi in ascolto su un target.

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:48 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0011s 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: HWORKGROUP)
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  unknown
MAC Address: 16:FE:53:6E:26:5A (Unknown)
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 186.98 seconds
```

Scansioni su Windows 7

Le non hanno riportato nessuna risposta.
Scansione con il comando nmap -O:

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -O 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:18 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.74 seconds
```

Scansione con il comando nmap -Pn -O, si usa per un host ch'è attivo ma che non risponde al ping.

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -Pn -O 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:19 CEST
Nmap done: 1 IP address (0 hosts up) scanned in 1.72 seconds
```

Scansione con il comando nmap -sS:

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sS 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:32 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.55 seconds

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -Pn -sS 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:32 CEST
Nmap done: 1 IP address (0 hosts up) scanned in 1.54 seconds
```

Scansione con il comando nmap -sT:

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sT 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:35 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.56 seconds

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -Pn -sT 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:35 CEST
Nmap scan report for 192.168.50.102
Host is up (0.045s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 990 filtered tcp ports (no-response), 10 filtered tcp ports (host-unreach)

Nmap done: 1 IP address (1 host up) scanned in 19.00 seconds
```

Scansione con il comando nmap -sV:

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sV 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:37 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.76 seconds

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -Pn -sV 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 18:37 CEST
Nmap done: 1 IP address (0 hosts up) scanned in 1.66 seconds
```