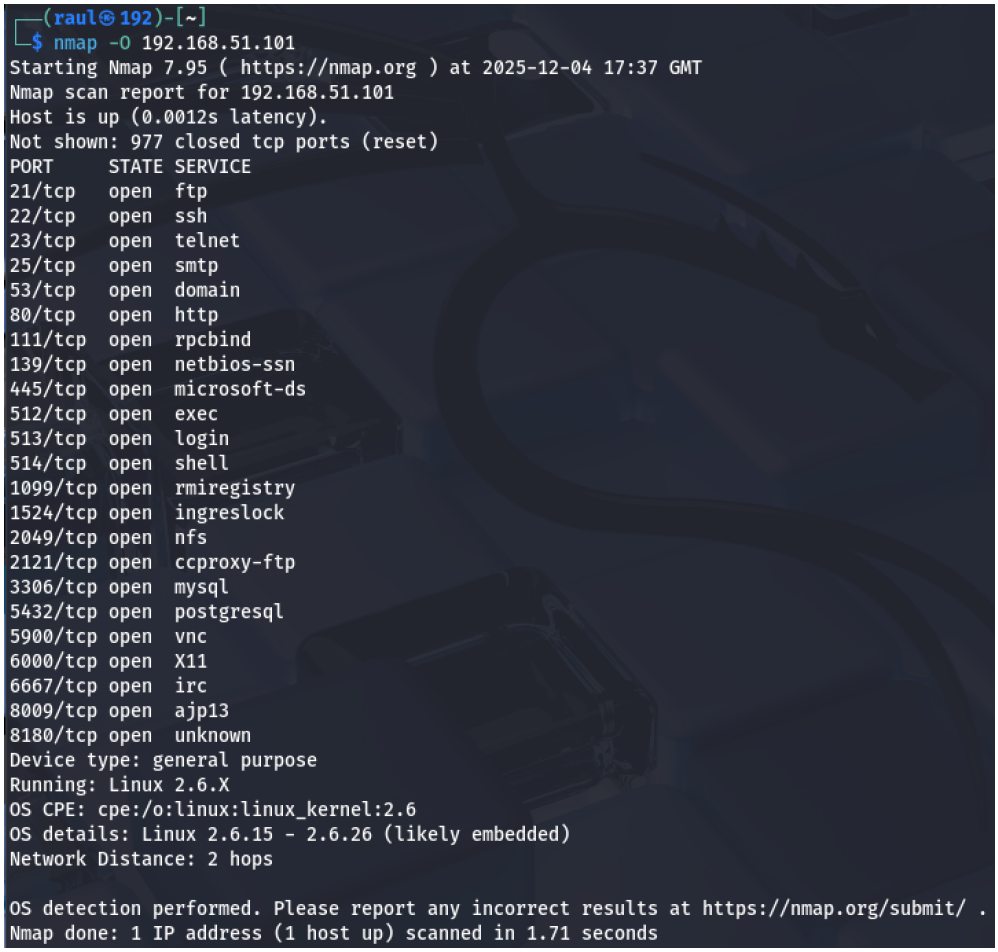
Raul Pastor

Nmap

L’esercizio di oggi riguarda la creazione di un report con i dettagli di 4 tipi di scansioni sul target Metasploitable(su reti diverse).

La prima scansione è la scansione del sistema operativo, la seconda il syn scan, la terza il tcp scan e l’ultima la version scan.

1)



Raul Pastor

2)

```
┌──(raul㉿192)-[~]
└─$ nmap -sS 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 17:38 GMT
Nmap scan report for 192.168.51.101
Host is up (0.0016s 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

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

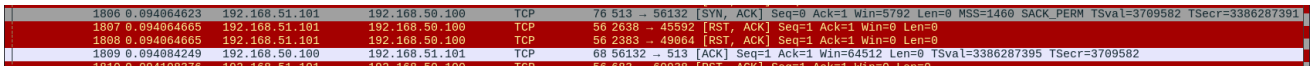
1	0.000000000	192.168.50.100	192.168.51.101	ICMP	44 Echo (ping) request id=0x1376, seq=0/0, ttl=41 (reply in 5)
2	0.000016712	192.168.50.100	192.168.51.101	TCP	60 52416 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.000019296	192.168.50.100	192.168.51.101	TCP	56 52416 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
4	0.000021505	192.168.50.100	192.168.51.101	ICMP	56 Timestamp request id=0xe885, seq=0/0, ttl=48
5	0.001187222	192.168.51.101	192.168.50.100	ICMP	44 Echo (ping) reply id=0x1376, seq=0/0, ttl=63 (request in 1)
6	0.001187305	192.168.51.101	192.168.50.100	TCP	56 443 → 52416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.001187347	192.168.51.101	192.168.50.100	ICMP	56 Timestamp reply id=0xe885, seq=0/0, ttl=63
8	0.059515489	192.168.50.100	192.168.50.1	DNS	89 Standard query 0x0e26 PTR 101.51.168.192.in-addr.arpa
9	0.060481829	192.168.50.1	192.168.50.100	DNS	148 Standard query response 0x0e26 No such name PTR 101.51.168.192.in-addr.arpa SOA localhost
10	0.084083062	192.168.50.100	192.168.51.101	TCP	60 52672 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.084093564	192.168.50.100	192.168.51.101	TCP	60 52672 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.084096440	192.168.50.100	192.168.51.101	TCP	60 52672 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.084098274	192.168.50.100	192.168.51.101	TCP	60 52672 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.084100108	192.168.50.100	192.168.51.101	TCP	60 52672 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.084101608	192.168.50.100	192.168.51.101	TCP	60 52672 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.084103400	192.168.50.100	192.168.51.101	TCP	60 52672 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	0.084104900	192.168.50.100	192.168.51.101	TCP	60 52672 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	0.084106484	192.168.50.100	192.168.51.101	TCP	60 52672 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	0.084108026	192.168.50.100	192.168.51.101	TCP	60 52672 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	0.085020270	192.168.51.101	192.168.50.100	TCP	56 1723 → 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	0.085020395	192.168.51.101	192.168.50.100	TCP	56 199 → 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	0.085020395	192.168.51.101	192.168.50.100	TCP	60 3306 → 52672 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
23	0.085124877	192.168.50.100	192.168.51.101	TCP	56 52672 → 3306 [RST] Seq=1 Win=0 Len=0
24	0.085152966	192.168.51.101	192.168.50.100	TCP	56 8080 → 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.085153008	192.168.51.101	192.168.50.100	TCP	56 113 → 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	0.085153008	192.168.51.101	192.168.50.100	TCP	60 111 → 52672 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
27	0.085153049	192.168.51.101	192.168.50.100	TCP	56 1025 → 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.085153049	192.168.51.101	192.168.50.100	TCP	56 554 → 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	0.085153091	192.168.51.101	192.168.50.100	TCP	56 443 → 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	0.085153091	192.168.51.101	192.168.50.100	TCP	56 587 → 52672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	0.085160259	192.168.50.100	192.168.51.101	TCP	56 52672 → 111 [RST] Seq=1 Win=0 Len=0
32	0.085190349	192.168.50.100	192.168.51.101	TCP	60 52672 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
33	0.085292039	192.168.50.100	192.168.51.101	TCP	60 52672 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	0.085294539	192.168.50.100	192.168.51.101	TCP	60 52672 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35	0.085296039	192.168.50.100	192.168.51.101	TCP	60 52672 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36	0.085297581	192.168.50.100	192.168.51.101	TCP	60 52672 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
37	0.085298915	192.168.50.100	192.168.51.101	TCP	60 52672 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Raul Pastor

3)

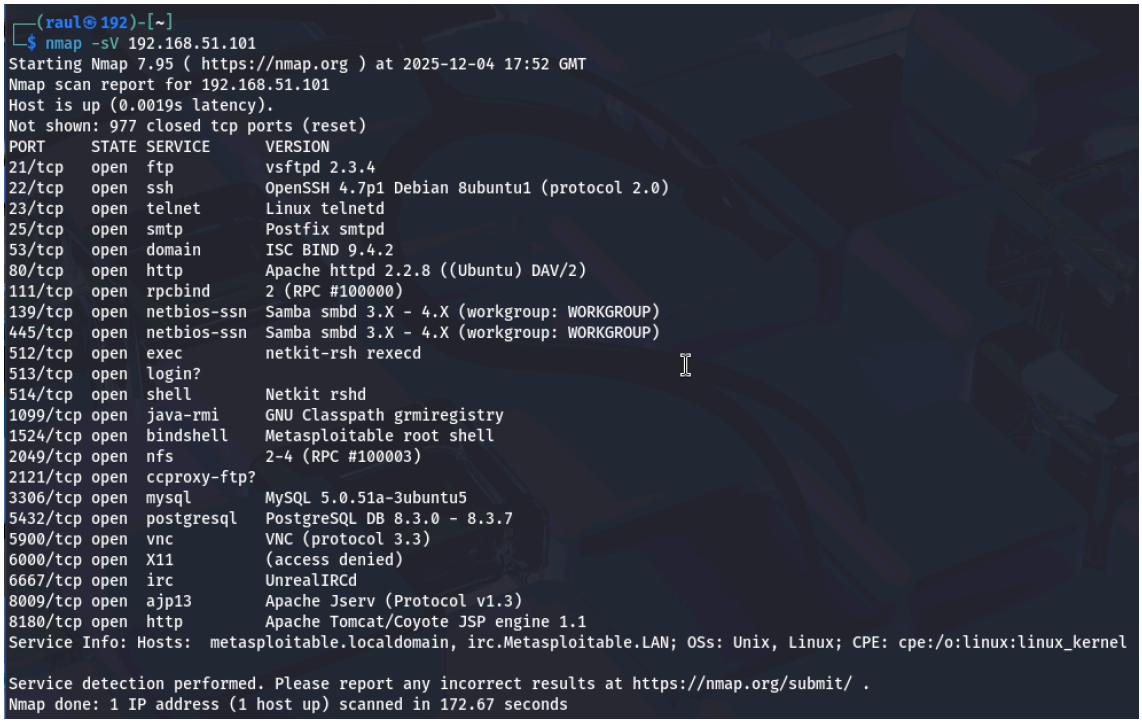
```
┌──(raul㉿192)-[~]
└─$ nmap -sT 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 17:38 GMT
Nmap scan report for 192.168.51.101
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```



Raul Pastor

4)



Notiamo attraverso una cattura con wireshark che nella seconda scansione (syn-scan) con nmap il threeway handshake non viene completato mentre nella terza (tcp-scan) viene completato.

REPORT

Indirizzo ip target: 192.168.51.101

Sistema operativo: Linux 2.6

Informazioni sulle porte:

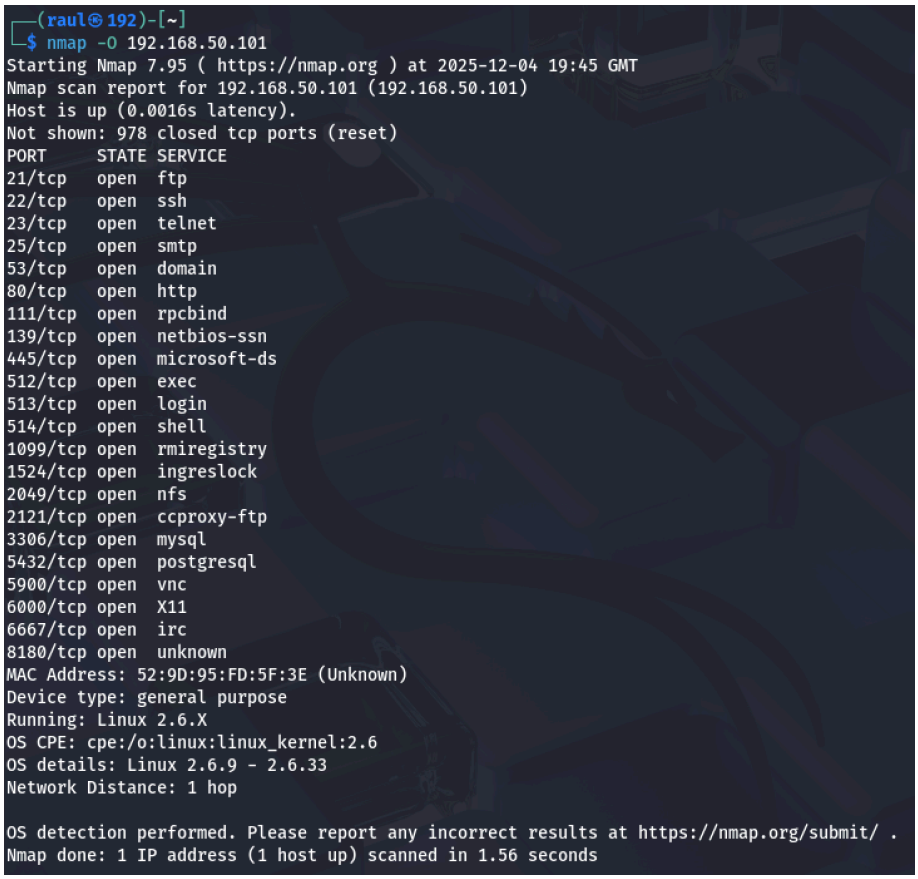
PORTA	STATO	SERVIZIO	VERSIONE
21	open	ftp	vsftpd 2.3.4
22	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	open	telnet	Linux telnetd
25	open	smtp	Postfix smtpd
53	open	domain	ISC BIND 9.4.2
80	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	open	rpcbind	2 (RPC #100000)
139	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	open	exec	netkit-rsh rexecd
513	open	login?	—
514	open	shell	Netkit rshd
1099	open	java-rmi	GNU Classpath grmiregistry

1524	open	bindshell	Metasploitable root shell
2049	open	nfs	2-4 (RPC #100003)
2121	open	ccproxy-ftp?	—
3306	open	mysql	MySQL 5.0.51a-3ubuntu5
5432	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	open	vnc	VNC (protocol 3.3)
6000	open	X11	access denied
6667	open	irc	UnrealIRCd
8009	open	ajp13	Apache Jserv (Protocol v1.3)
8180	open	http	Apache Tomcat/Coyote JSP engine 1.1

PARTE FACOLTATIVA:

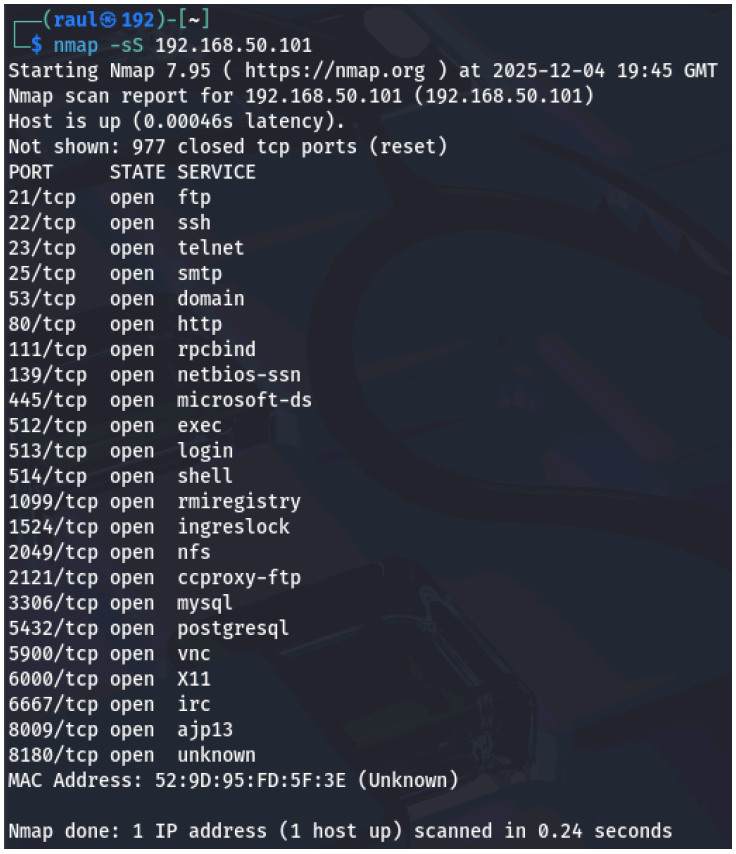
La parte facoltativa prevedeva di estendere le 4 scansioni sulla macchina Metasploitable presente nella stessa rete di Kali e verificarne le differenze.

1)

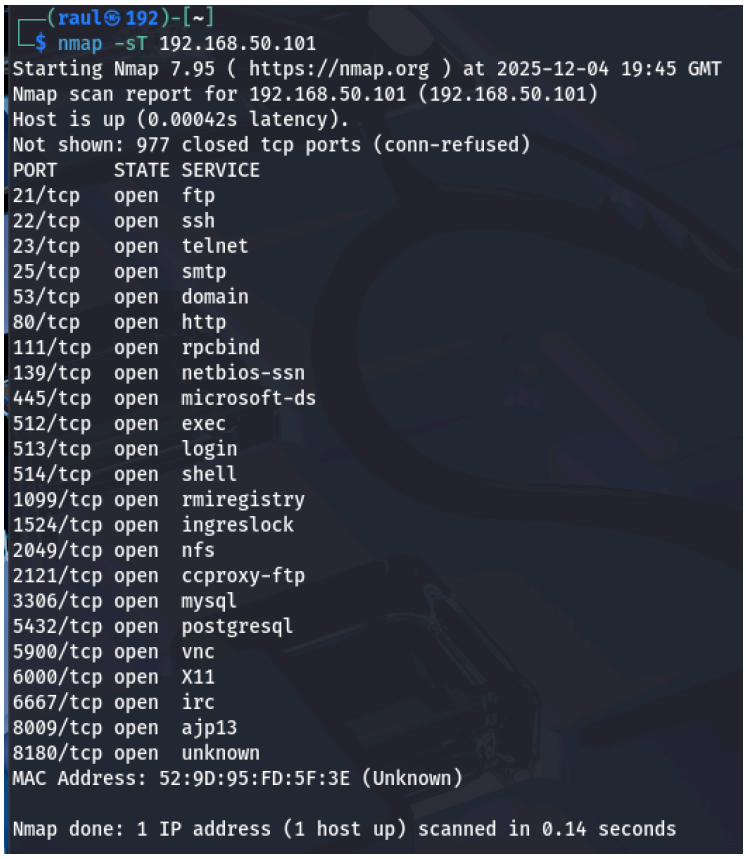


Raul Pastor

2)

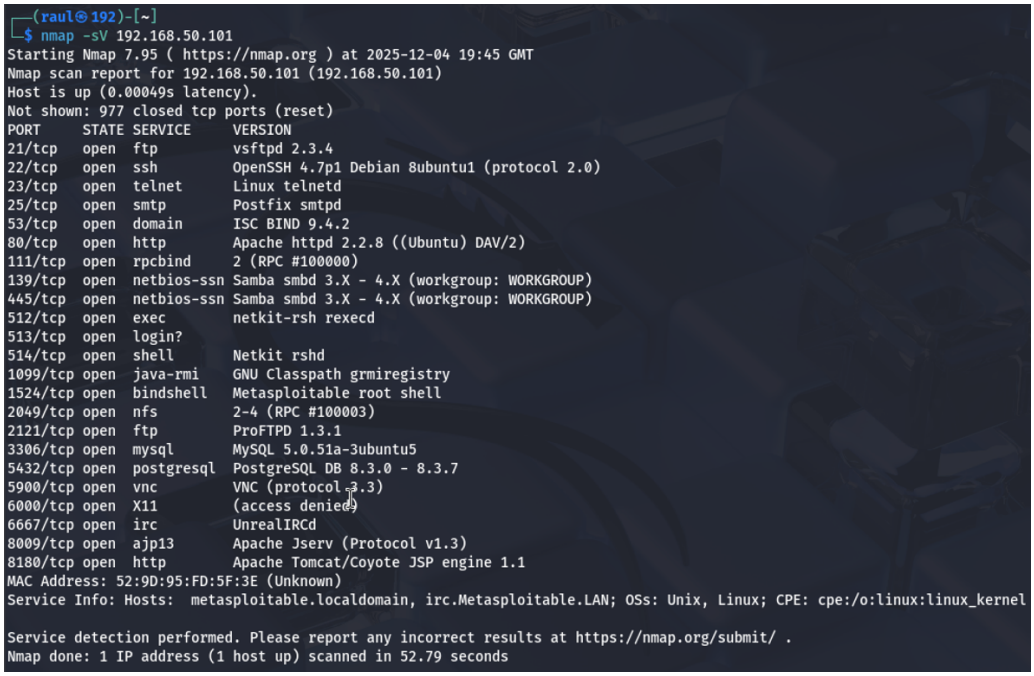


3)



Raul Pastor

4)



Le differenze principali sono:

- Nella prima scansione (OS scan), diversamente da quanto previsto, viene trovata una porta aggiuntiva nella versione scan su 2 reti diverse.
- Nelle restanti scansioni la versione sulla stessa rete ci ha impiegato relativamente molto meno tempo e ha indicato il mac address della macchina target, diversamente dalla scansione su reti diverse.