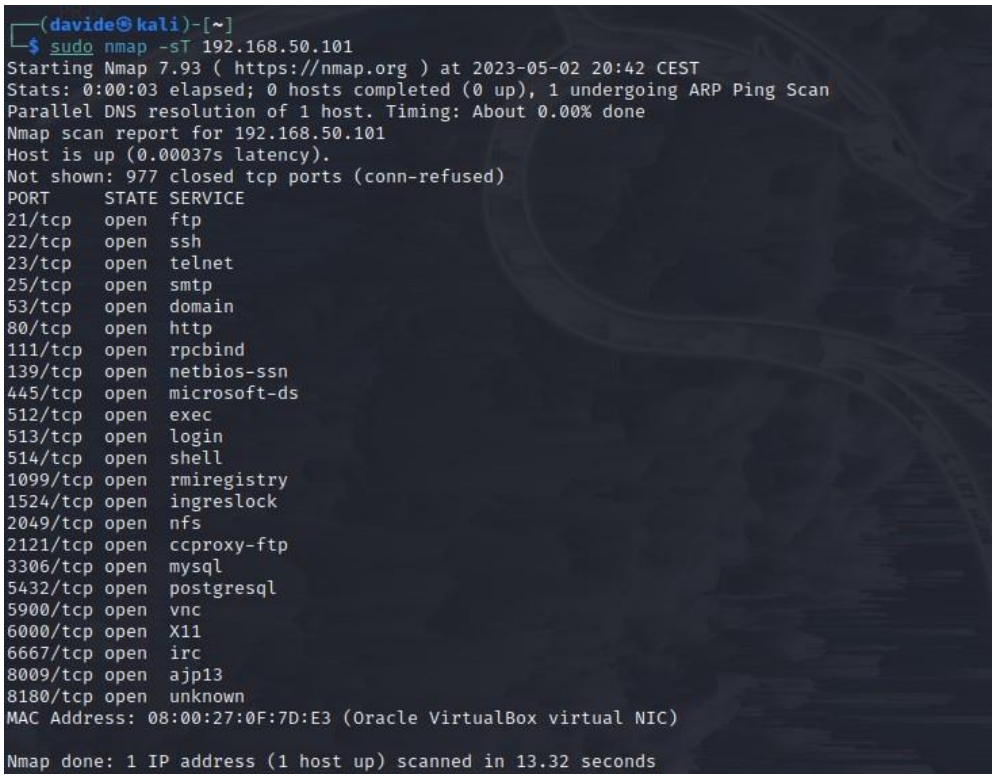
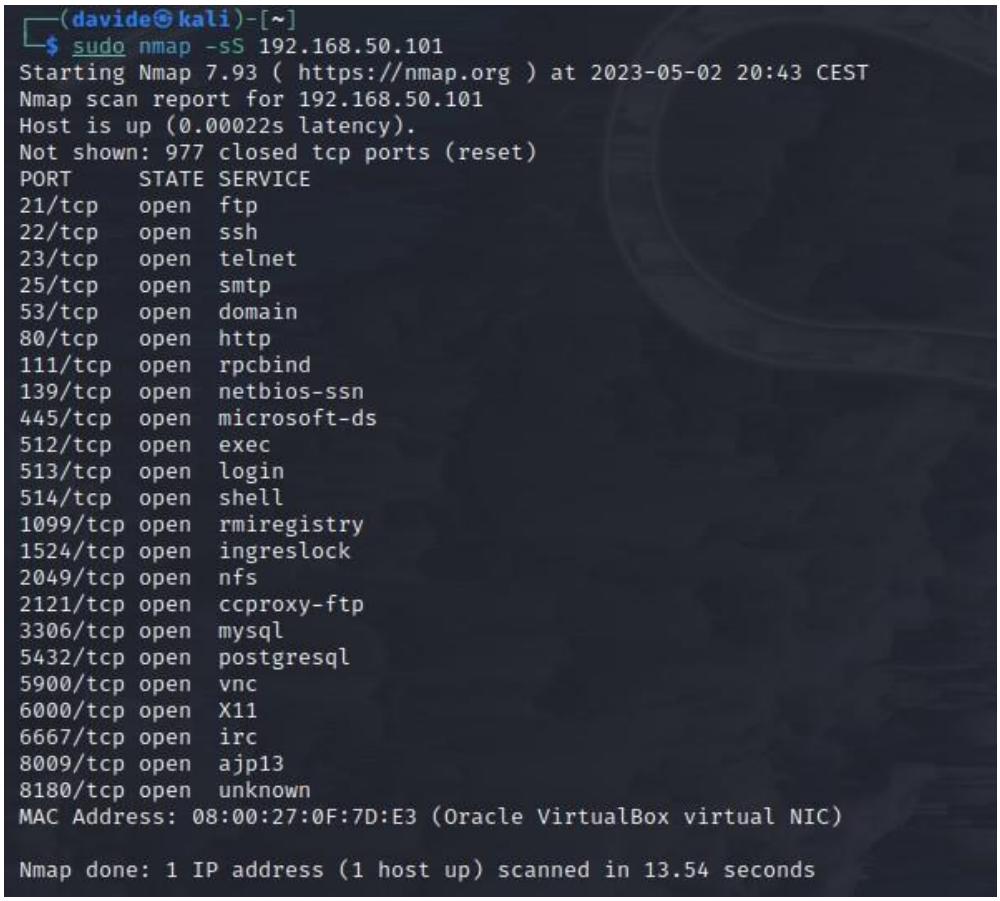
Sequenza di scansioni su Metasploitable:

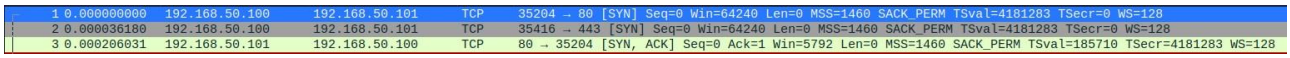
-sT



-sS



La differenza fra la scansione -sS e -sT non è visibile “ad occhio nudo”. Abbiamo bisogno di Wireshark che intercetta i pacchetti rispettivamente SYN – SYN ACK – RST e SYN – SYN ACK – ACK.



1	0.000000000	192.168.50.100	192.168.50.101	TCP	35204 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4181283 TSecr=0 WS=128
2	0.000036180	192.168.50.100	192.168.50.101	TCP	35416 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4181283 TSecr=0 WS=128
3	0.000206031	192.168.50.101	192.168.50.100	TCP	80 → 35204 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=185710 TSecr=4181283 WS=128

2	3.000574885	192.168.50.100	192.168.50.101	TCP	41639 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	3.000734635	192.168.50.101	192.168.50.100	TCP	21 → 41639 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
4	3.000752985	192.168.50.100	192.168.50.101	TCP	41639 → 21 [RST] Seq=1 Win=0 Len=0

-O

```
┌──(davide㉿kali)-[~]
└─$ nmap -O 192.168.50.101
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

┌──(davide㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
[sudo] password di davide:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 20:41 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00023s 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: 08:00:27:0F:7D:E3 (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 15.35 seconds
```

-sV

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 20:44 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000096s 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: 08:00:27:0F:7D:E3 (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 65.95 seconds
```

Fonte - Kali Linux	Target - Metasploitable	MAC	Tipo di scan	Porta	Servizio	Versione	Risultato
192.168.50.100	192.168.50.101	08:00:27:0F:7D:E3	sT, sS, sV	21	FTP	vsftpd 2.3.4	Open
192.168.50.101	192.168.50.102	08:00:27:0F:7D:E4	sT, sS, sV	22	SSH	OpenSSH 4.7p1 Debian	Open
192.168.50.102	192.168.50.103	08:00:27:0F:7D:E5	sT, sS, sV	23	Telnet	Linux telnetd	Open
192.168.50.103	192.168.50.104	08:00:27:0F:7D:E6	sT, sS, sV	25	SMTP	Postfix smtpd	Open
192.168.50.104	192.168.50.105	08:00:27:0F:7D:E7	sT, sS, sV	53	Domain	ISC BIND 9.4.2	Open
192.168.50.105	192.168.50.106	08:00:27:0F:7D:E8	sT, sS, sV	80	HTTP	Apache httpd	Open
192.168.50.106	192.168.50.107	08:00:27:0F:7D:E9	sT, sS, sV	111	RPCBind	RPC #100000	Open
192.168.50.107	192.168.50.108	08:00:27:0F:7D:E10	sT, sS, sV	139	Netbios-ssn	Samba smbd 3.X - 4.X	Open
192.168.50.108	192.168.50.109	08:00:27:0F:7D:E11	sT, sS, sV	445	Netbios-ssn	Samba smbd 3.X - 4.X	Open
192.168.50.109	192.168.50.110	08:00:27:0F:7D:E12	sT, sS, sV	512	Exec	netkit-rsh rexecd	Open
192.168.50.110	192.168.50.111	08:00:27:0F:7D:E13	sT, sS, sV	513	Login	OpenBSD or Solaris logind	Open
192.168.50.111	192.168.50.112	08:00:27:0F:7D:E14	sT, sS, sV	514	Shell	Netkit-rsh	Open
192.168.50.112	192.168.50.113	08:00:27:0F:7D:E15	sT, sS, sV	1099	Java-rmi	GNU Classpath grmiregistry	Open
192.168.50.113	192.168.50.114	08:00:27:0F:7D:E16	sT, sS, sV	1524	Bindshell	Metasploitable root shell	Open
192.168.50.114	192.168.50.115	08:00:27:0F:7D:E17	sT, sS, sV	2049	NFS	2-4 RPC #100003	Open
192.168.50.115	192.168.50.116	08:00:27:0F:7D:E18	sT, sS, sV	2121	FTP	ProFTPD 1.3.1	Open
192.168.50.116	192.168.50.117	08:00:27:0F:7D:E19	sT, sS, sV	3306	MySQL	MySQL 5,0 51a-3ubuntu5	Open
192.168.50.117	192.168.50.118	08:00:27:0F:7D:E20	sT, sS, sV	5432	PostgreSQL	PostgreSQL DB 8.3.0 - 8.3.7	Open
192.168.50.118	192.168.50.119	08:00:27:0F:7D:E21	sT, sS, sV	5900	VNC	VNC (protocol v1.3)	Open
192.168.50.119	192.168.50.120	08:00:27:0F:7D:E22	sT, sS, sV	6000	X11		Open
192.168.50.120	192.168.50.121	08:00:27:0F:7D:E23	sT, sS, sV	6667	IRC	UnrealIRCd	Open
192.168.50.121	192.168.50.122	08:00:27:0F:7D:E24	sT, sS, sV	8009	AJP13	Apache Jserv (Protocol 1.3)	Open
192.168.50.122	192.168.50.123	08:00:27:0F:7D:E25	sT, sS, sV	8180	HTTP	Apache Tomcat/Coyote JSP engine 1.1	Open