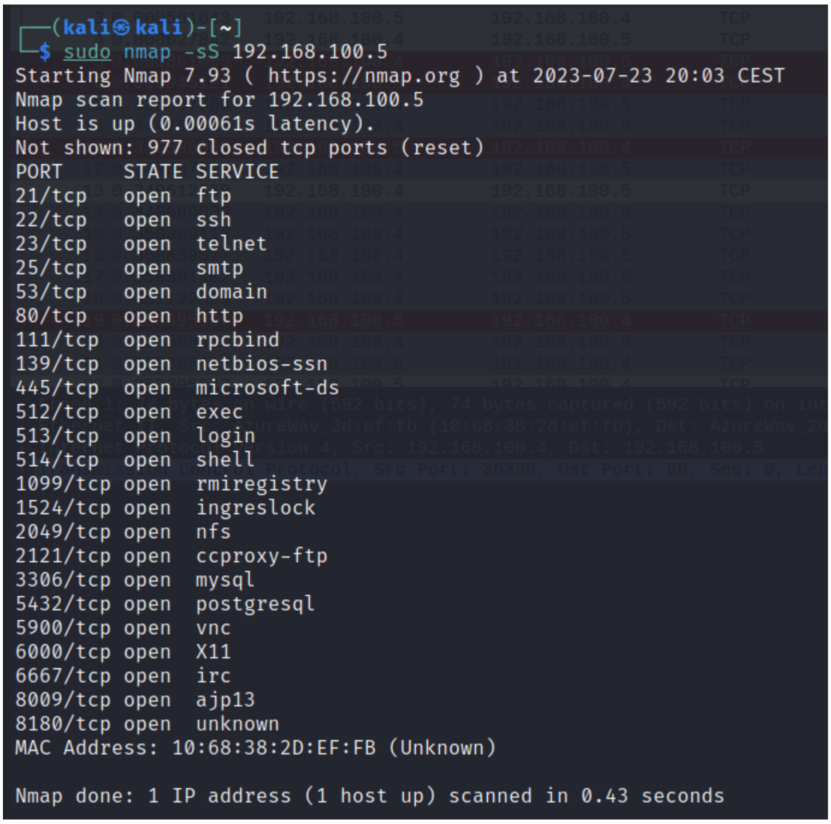
NMAP SCAN

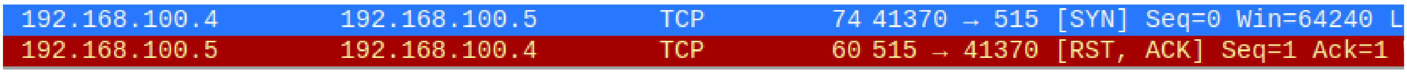
Scan con -sS

-sS: detto anche SYN scan è meno invasivo rispetto a -sT scan in quanto nmap, una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3-way-handshake



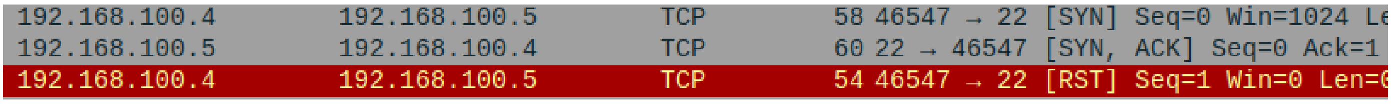
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.100.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 20:03 CEST
Nmap scan report for 192.168.100.5
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 10:68:38:2D:EF:FB (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Laddove la macchina target ci risponde con **[RST,ACK]**, ci conferma che **la porta è chiusa,** in questo caso la porta chiusa è il 515



```
192.168.100.4        192.168.100.5        TCP       74 41370 → 515 [SYN] Seq=0 Win=64240 L
192.168.100.5        192.168.100.4        TCP       60 515 → 41370 [RST, ACK] Seq=1 Ack=1
```

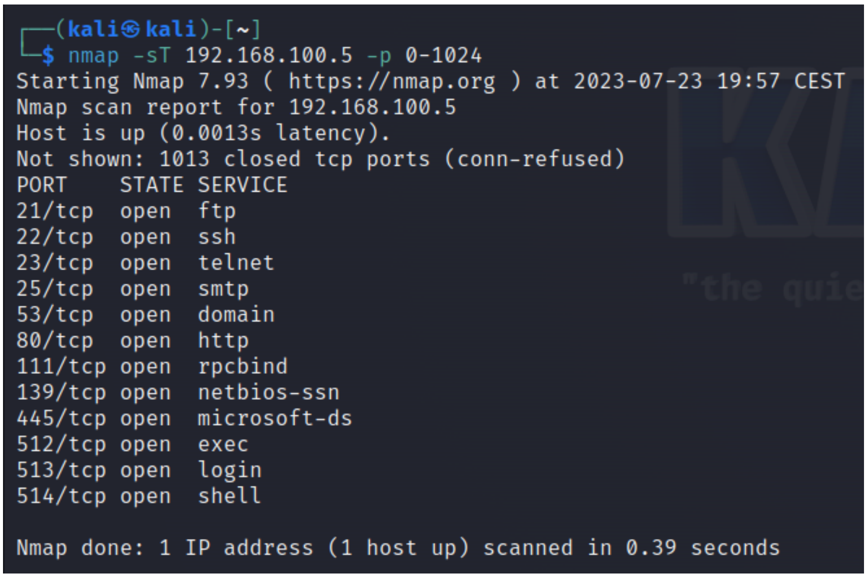
Laddove invece la macchina target ci risponde con **[SYN, ACK]**, ci conferma che **la porta (22) è aperta** Dopo aver ricevuto il pacchetto [SYN, ACK] la macchina attaccante chiuderà la connessione con un pacchetto [RST] evitando la conclusione del 3-way-handshake.



```
192.168.100.4        192.168.100.5        TCP       58 46547 → 22 [SYN] Seq=0 Win=1024 Le
192.168.100.5        192.168.100.4        TCP       60 22 → 46547 [SYN, ACK] Seq=0 Ack=1
192.168.100.4        192.168.100.5        TCP       54 46547 → 22 [RST] Seq=1 Win=0 Len=0
```

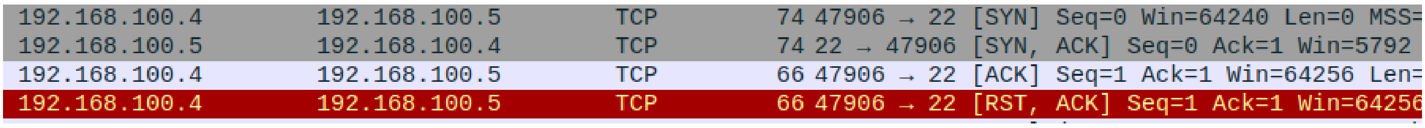
Scan con -sT

-sT: è un metodo più invasivo rispetto al SYN scan, in quanto stabilisce un canale completando tutti i passaggi del 3-way-handshake in modo tale da controllare se una porta è aperta o meno e recuperare le informazioni del servizio in ascolto



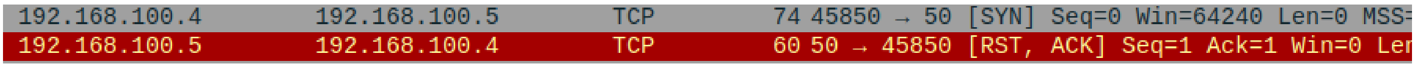
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.100.5 -p 0-1024
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 19:57 CEST
Nmap scan report for 192.168.100.5
Host is up (0.0013s latency).
Not shown: 1013 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  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

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

3-way-handshake completato sulla porta 22 in quanto è aperta



```
192.168.100.4       192.168.100.5       TCP        74 47906 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=
192.168.100.5       192.168.100.4       TCP        74 22 → 47906 [SYN, ACK] Seq=0 Ack=1 Win=5792
192.168.100.4       192.168.100.5       TCP        66 47906 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=
192.168.100.4       192.168.100.5       TCP        66 47906 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256
```

3-way-handshake non completato in quanto la porta 50 risulta chiusa



```
192.168.100.4       192.168.100.5       TCP        74 45850 → 50 [SYN] Seq=0 Win=64240 Len=0 MSS=
192.168.100.5       192.168.100.4       TCP        60 50 → 45850 [RST, ACK] Seq=1 Ack=1 Win=0 Len
```

TABELLA

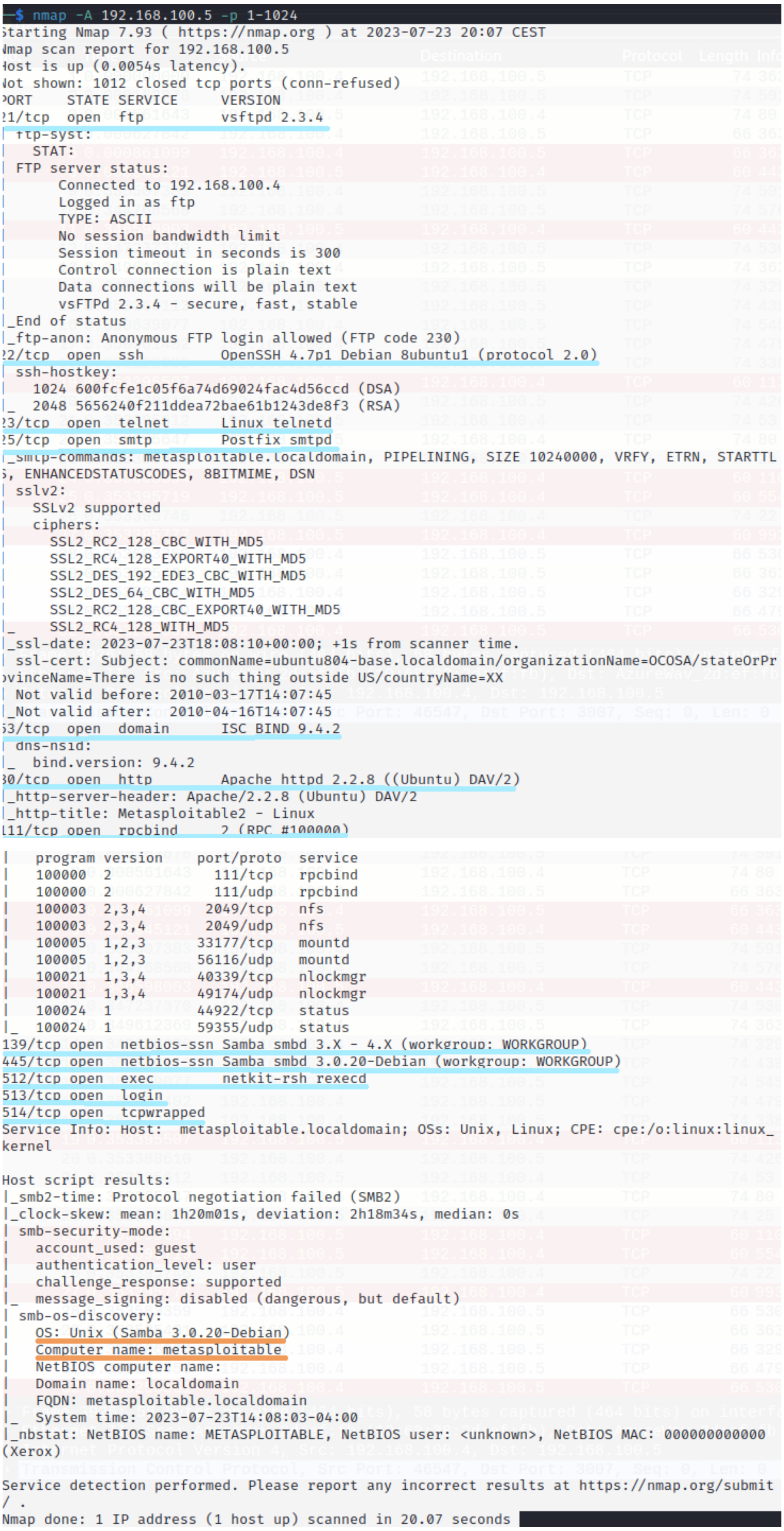
Fonte dello scan	Target dello scan	Tipo di scan	Risultati
Kali Linux 192.168.100.4	**Metasploitable** 192.168.100.5	**-sS**	porta 21 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 22 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 23 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 53 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 80 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 111 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 139 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 445 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 512 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 513 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 514 aperta [SYN] – [SYN, ACK] – [RST] Seq=1
			porta 515 chiusa || 515 [SYN] Seq=0 || 515 [RST, ACK] Seq=1 Ack=1

Fonte dello scan	Fonte dello scan	Tipo di scan	Risultati
Kali Linux 192.168.100.4	**Metasploitable** 192.168.100.5	**-sT**	porta 21 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 22 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 23 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 50 chiusa [SYN] || [RST, ACK] Seq=1 Ack=1
			porta 53 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 80 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 111 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 139 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 445 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 512 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 513 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1
			porta 514 aperta [SYN] || [SYN, ACK] Seq=0 Ack=1 || [ACK] Seq=1 Ack=1 || [RST, ACK] Seq=1 Ack=1

Scansione con switch -A

Ci permette di recuperare informazioni sull’ip target come:

- versione del sistema operativo
- servizi disponibili in ascolto sulle porte aperte



```
─$ nmap -A 192.168.100.5 -p 1-1024
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 20:07 CEST
Nmap scan report for 192.168.100.5
Host is up (0.0054s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.100.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTL
S, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_ssl-date: 2023-07-23T18:08:10+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrPr
ovinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind     2 (RPC #100000)

|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33177/tcp   mountd
|   100005  1,2,3      56116/udp   mountd
|   100021  1,3,4      40339/tcp   nlockmgr
|   100021  1,3,4      49174/udp   nlockmgr
|   100024  1          44922/tcp   status
|_  100024  1          59355/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login
514/tcp open  tcpwrapped
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h20m01s, deviation: 2h18m34s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-07-23T14:08:03-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000
(Xerox)

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 20.07 seconds
```