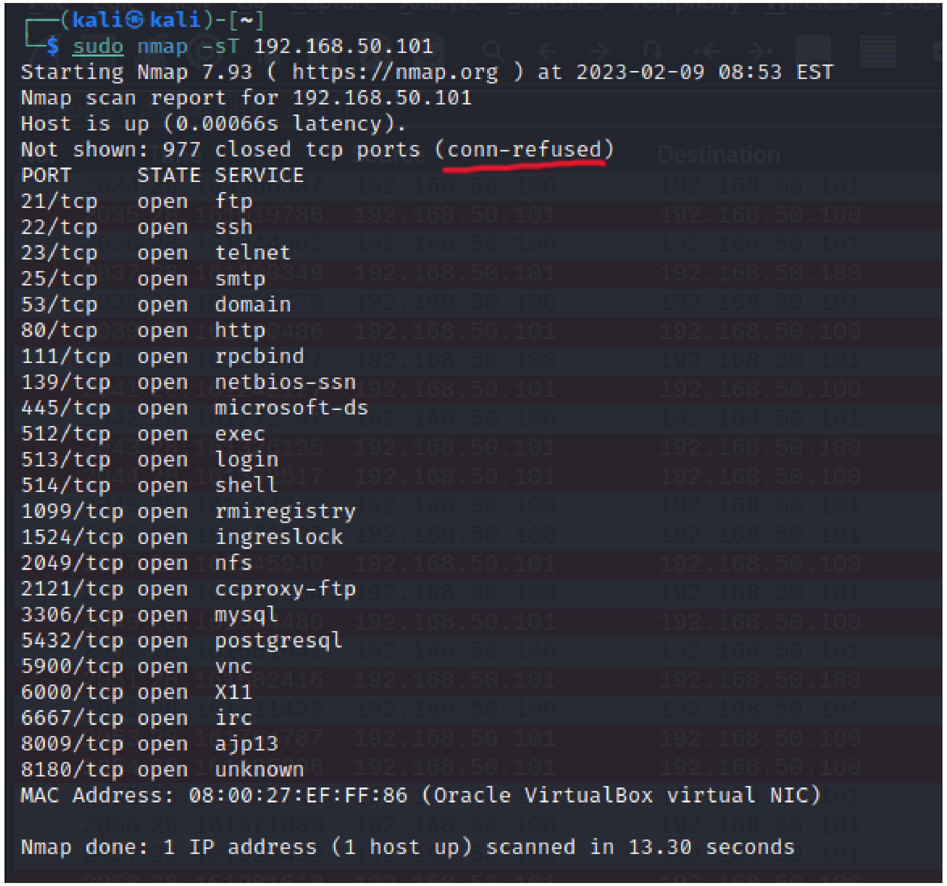
Esercizio 09-02

Traccia: effettuare scansione da Kali a Metasploitable in formato SYN, TCP e con switch -A.

Portare in evidenza differenze notate in Whireshark tra scan SYN e scan TCP

Per ognuno degli scan fare un report con indicati autore, target, metodo e dati ottenuti



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 08:53 EST
Nmap scan report for 192.168.50.101
Host is up (0.00066s 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:EF:FF:86 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

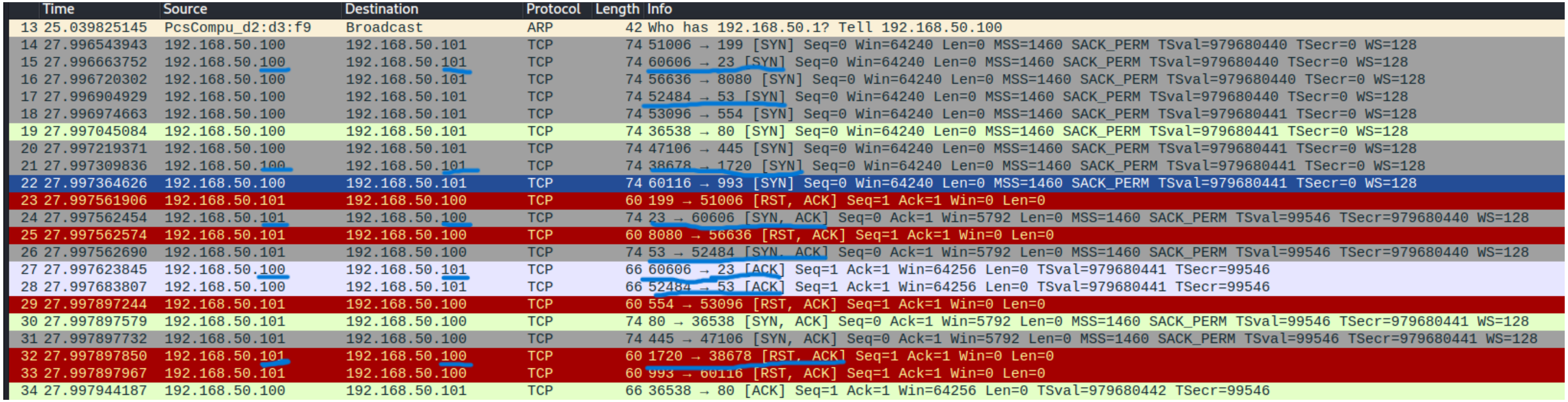
Scan TCP

Autore: IP 192.168.50.100 (Kali)

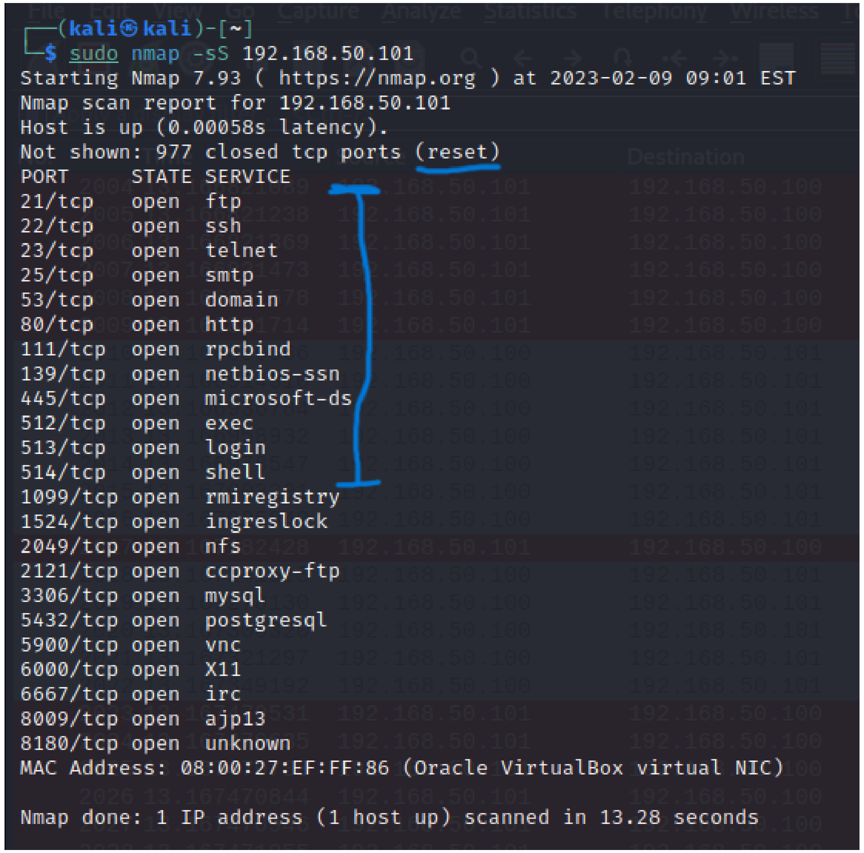
Target: IP 192.168.50.100 Metasploitable

Risultato: ottenuta conoscenza delle porte aperte

Si può notare il tentativo di 3-way-handshake, SYN, SYN-ACK, ACK, andato a buon fine solo con le porte aperte



	Time	Source	Destination	Protocol	Length	Info
13	25.039825145	PcsCompu_d2:d3:f9	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.100
14	27.996543943	192.168.50.100	192.168.50.101	TCP	74	51006 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=979680440 TSecr=0 WS=128
15	27.996663752	192.168.50.100	192.168.50.101	TCP	74	60606 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=979680440 TSecr=0 WS=128
16	27.996720302	192.168.50.100	192.168.50.101	TCP	74	56636 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=979680440 TSecr=0 WS=128
17	27.996904929	192.168.50.100	192.168.50.101	TCP	74	52484 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=979680440 TSecr=0 WS=128
18	27.996974663	192.168.50.100	192.168.50.101	TCP	74	53096 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=979680441 TSecr=0 WS=128
19	27.997045084	192.168.50.100	192.168.50.101	TCP	74	36538 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=979680441 TSecr=0 WS=128
20	27.997219371	192.168.50.100	192.168.50.101	TCP	74	47106 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=979680441 TSecr=0 WS=128
21	27.997309836	192.168.50.100	192.168.50.101	TCP	74	38678 → 1720 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=979680441 TSecr=0 WS=128
22	27.997364626	192.168.50.100	192.168.50.101	TCP	74	60116 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=979680441 TSecr=0 WS=128
23	27.997561906	192.168.50.101	192.168.50.100	TCP	60	199 → 51006 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	27.997562454	192.168.50.101	192.168.50.100	TCP	74	23 → 60606 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=99546 TSecr=979680440 WS=128
25	27.997562574	192.168.50.101	192.168.50.100	TCP	60	8080 → 56636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	27.997562690	192.168.50.101	192.168.50.100	TCP	74	53 → 52484 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=99546 TSecr=979680440 WS=128
27	27.997623845	192.168.50.100	192.168.50.101	TCP	66	60606 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=979680441 TSecr=99546
28	27.997683807	192.168.50.100	192.168.50.101	TCP	66	52484 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=979680441 TSecr=99546
29	27.997897244	192.168.50.101	192.168.50.100	TCP	60	554 → 53096 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	27.997897579	192.168.50.101	192.168.50.100	TCP	74	80 → 36538 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=99546 TSecr=979680441 WS=128
31	27.997897732	192.168.50.101	192.168.50.100	TCP	74	445 → 47106 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=99546 TSecr=979680441 WS=128
32	27.997897850	192.168.50.101	192.168.50.100	TCP	60	1720 → 38678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	27.997897967	192.168.50.101	192.168.50.100	TCP	60	993 → 60116 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	27.997944187	192.168.50.100	192.168.50.101	TCP	66	36538 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=979680442 TSecr=99546



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 09:01 EST
Nmap scan report for 192.168.50.101
Host is up (0.00058s 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:EF:FF:86 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

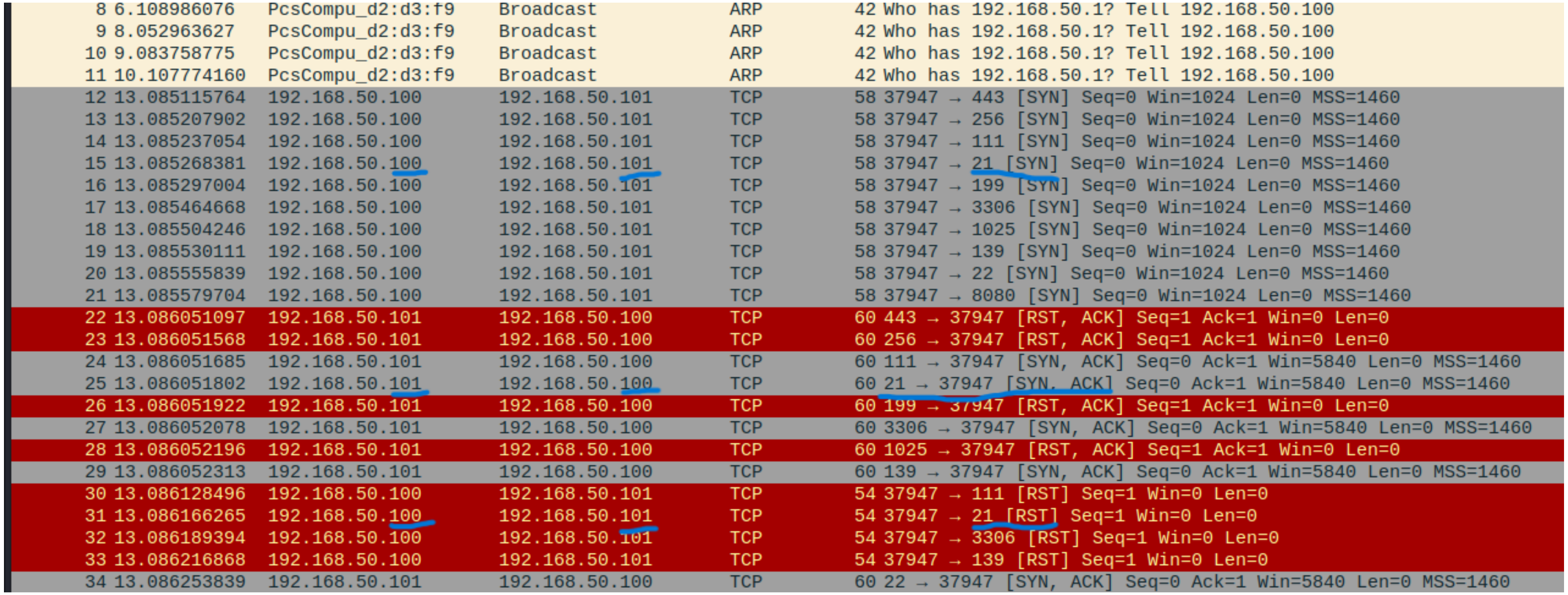
Scan SYN

Autore: IP 192.168.50.100 (Kali)

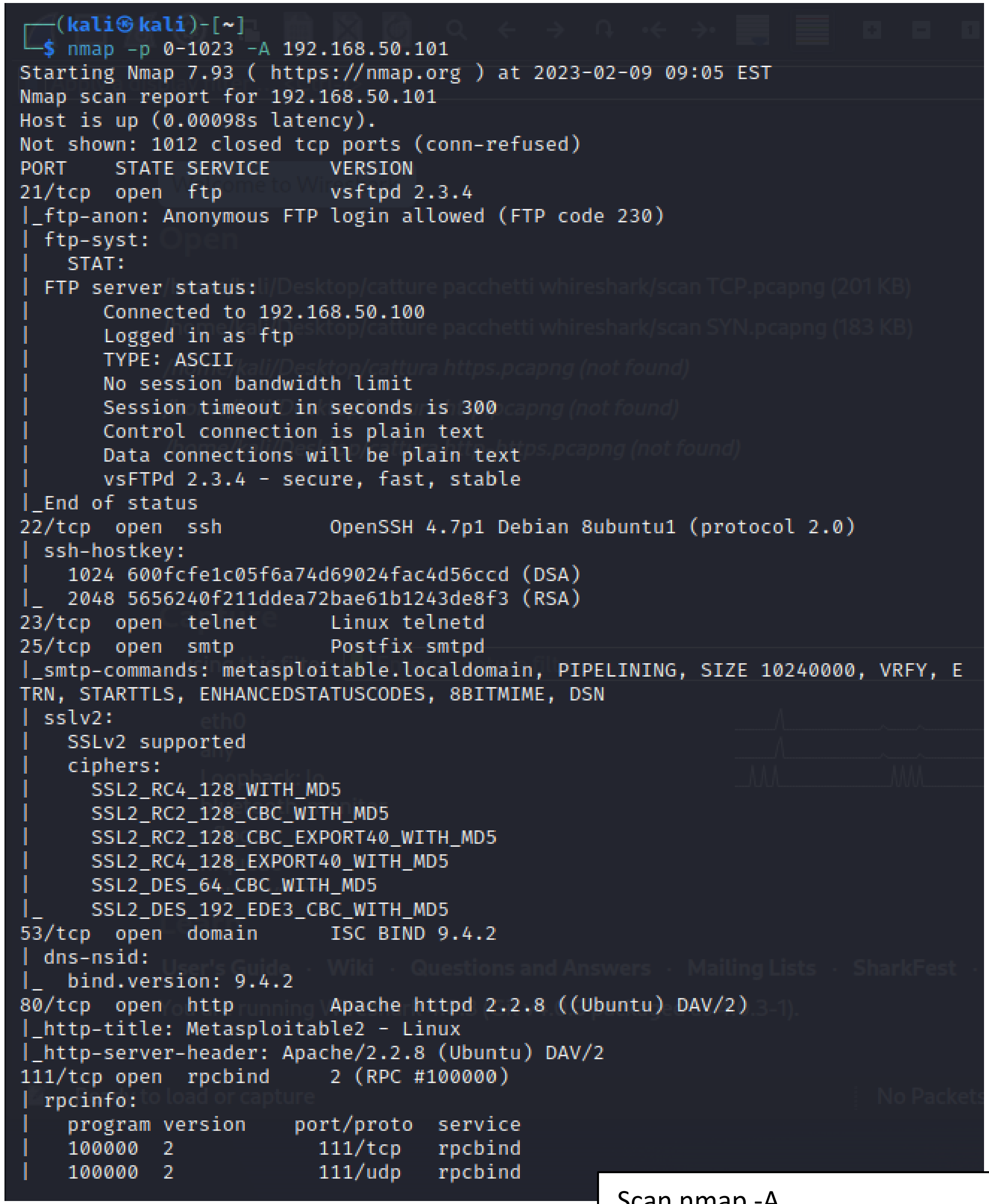
Target: IP 192.168.50.100 (Metasploitable)

Risultato: ottenuta conoscenza delle porte aperte

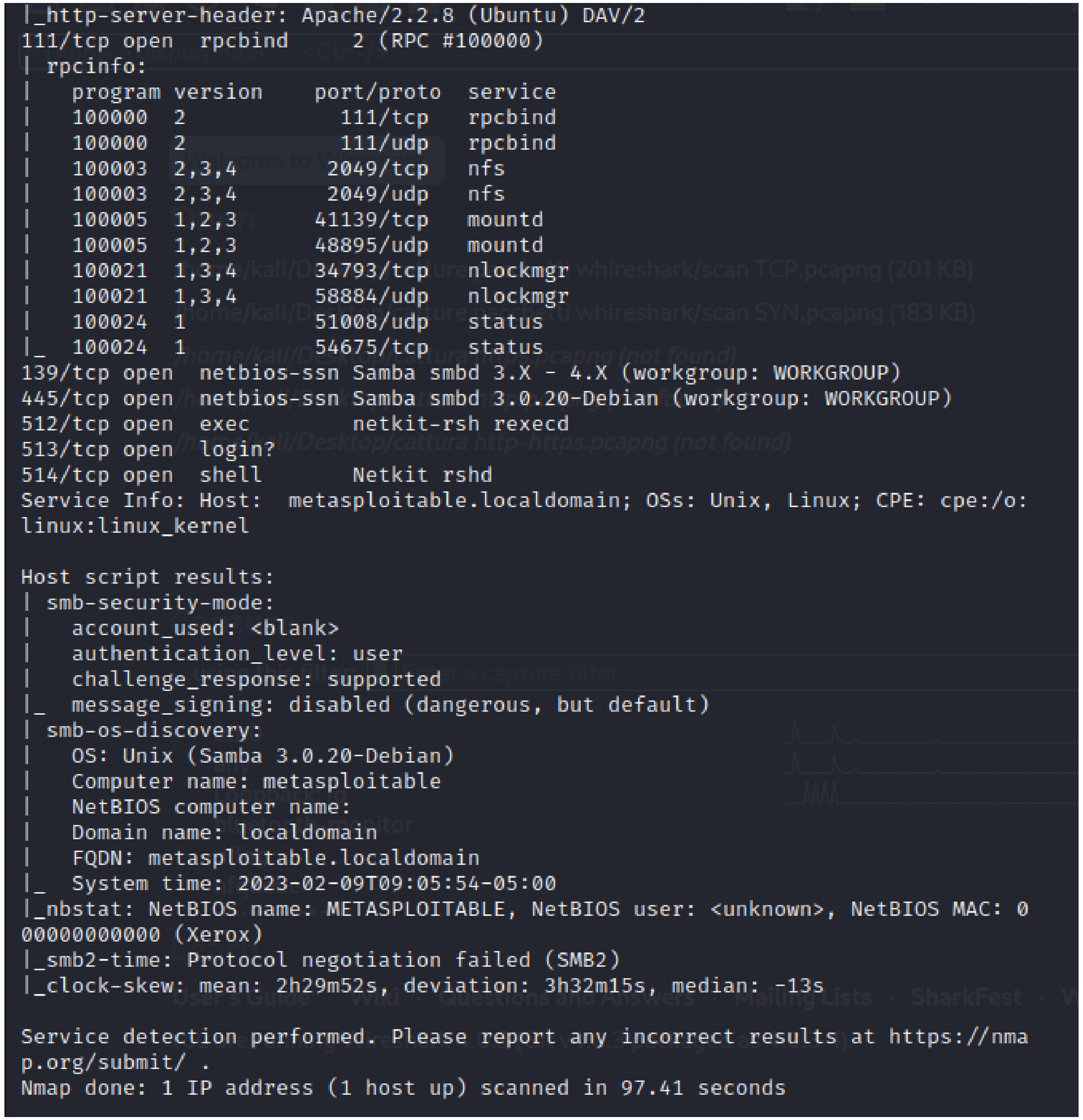
Si può notare che a differenza dello scan TCP invece di inviare ACK alle porte che hanno accettato SYN, l'autore dello scan invia un reset RST



```
 8 6.108986076   PcsCompu_d2:d3:f9   Broadcast        ARP   42 Who has 192.168.50.1? Tell 192.168.50.100
 9 8.052963627   PcsCompu_d2:d3:f9   Broadcast        ARP   42 Who has 192.168.50.1? Tell 192.168.50.100
10 9.083758775   PcsCompu_d2:d3:f9   Broadcast        ARP   42 Who has 192.168.50.1? Tell 192.168.50.100
11 10.107774160  PcsCompu_d2:d3:f9   Broadcast        ARP   42 Who has 192.168.50.1? Tell 192.168.50.100
12 13.085115764  192.168.50.100      192.168.50.101   TCP   58 37947 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13 13.085207902  192.168.50.100      192.168.50.101   TCP   58 37947 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14 13.085237054  192.168.50.100      192.168.50.101   TCP   58 37947 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15 13.085268381  192.168.50.100      192.168.50.101   TCP   58 37947 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16 13.085297004  192.168.50.100      192.168.50.101   TCP   58 37947 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17 13.085464668  192.168.50.100      192.168.50.101   TCP   58 37947 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18 13.085504246  192.168.50.100      192.168.50.101   TCP   58 37947 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19 13.085530111  192.168.50.100      192.168.50.101   TCP   58 37947 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20 13.085555839  192.168.50.100      192.168.50.101   TCP   58 37947 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21 13.085579704  192.168.50.100      192.168.50.101   TCP   58 37947 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22 13.086051097  192.168.50.101      192.168.50.100   TCP   60 443 → 37947 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 13.086051568  192.168.50.101      192.168.50.100   TCP   60 256 → 37947 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 13.086051685  192.168.50.101      192.168.50.100   TCP   60 111 → 37947 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
25 13.086051802  192.168.50.101      192.168.50.100   TCP   60 21 → 37947 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
26 13.086051922  192.168.50.101      192.168.50.100   TCP   60 199 → 37947 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27 13.086052078  192.168.50.101      192.168.50.100   TCP   60 3306 → 37947 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
28 13.086052196  192.168.50.101      192.168.50.100   TCP   60 1025 → 37947 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29 13.086052313  192.168.50.101      192.168.50.100   TCP   60 139 → 37947 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
30 13.086128496  192.168.50.100      192.168.50.101   TCP   54 37947 → 111 [RST] Seq=1 Win=0 Len=0
31 13.086166265  192.168.50.100      192.168.50.101   TCP   54 37947 → 21 [RST] Seq=1 Win=0 Len=0
32 13.086189394  192.168.50.100      192.168.50.101   TCP   54 37947 → 3306 [RST] Seq=1 Win=0 Len=0
33 13.086216868  192.168.50.100      192.168.50.101   TCP   54 37947 → 139 [RST] Seq=1 Win=0 Len=0
34 13.086253839  192.168.50.101      192.168.50.100   TCP   60 22 → 37947 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 0-1023 -A 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 09:05 EST
Nmap scan report for 192.168.50.101
Host is up (0.00098s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      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
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, E
TRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
```



```
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   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      41139/tcp   mountd
|   100005  1,2,3      48895/udp   mountd
|   100021  1,3,4      34793/tcp   nlockmgr
|   100021  1,3,4      58884/udp   nlockmgr
|   100024  1          51008/udp   status
|_  100024  1          54675/tcp   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  shell       Netkit rshd
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:
linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   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: 2023-02-09T09:05:54-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 0
00000000000 (Xerox)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h29m52s, deviation: 3h32m15s, median: -13s

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.41 seconds
```

Scan nmap -A

Autore: IP 192.168.50.100 (Kali)

Target: IP 192.168.50.100 Metasploitable

Risultato: ottenuta conoscenza delle porte aperte, versione e tipo di servizio che offrono