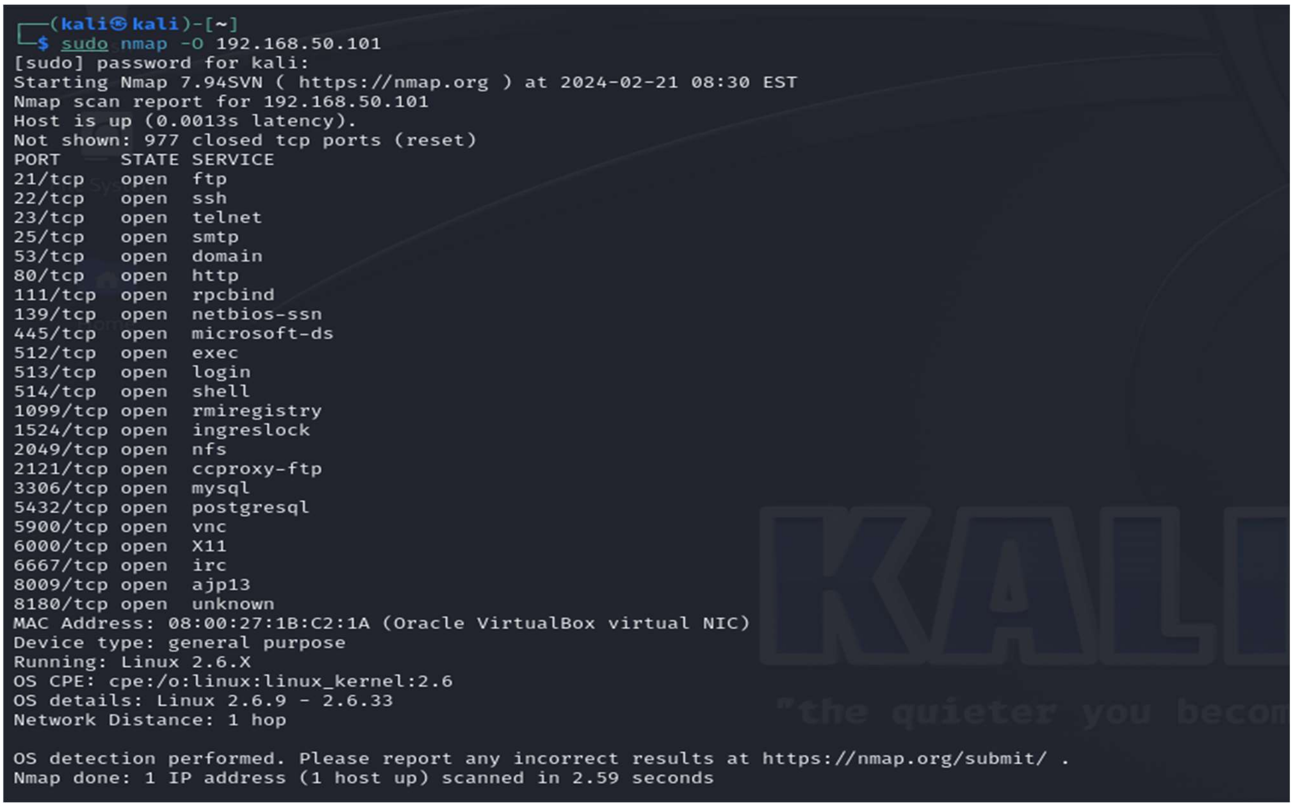
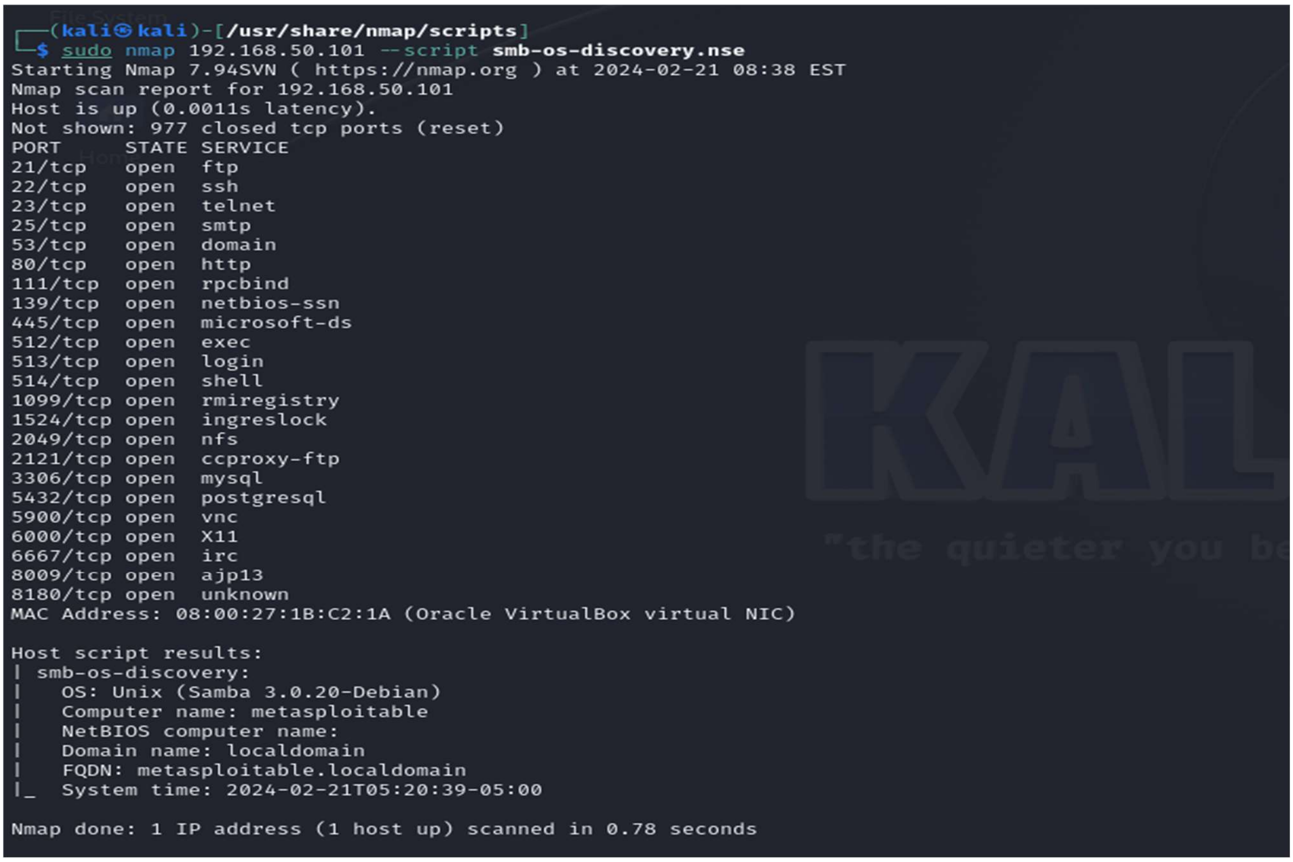
Per **Metaspoitable**:

Possiamo effettuare la scansione OS fingerprint tramite il comando da terminale **sudo nmap -O 192.168.50.101** oppure utilizzando lo script nmap **smb-os-discovery.nse** già installato su Kali Linux presente nella cartella **/usr/share/nmap/scripts**.

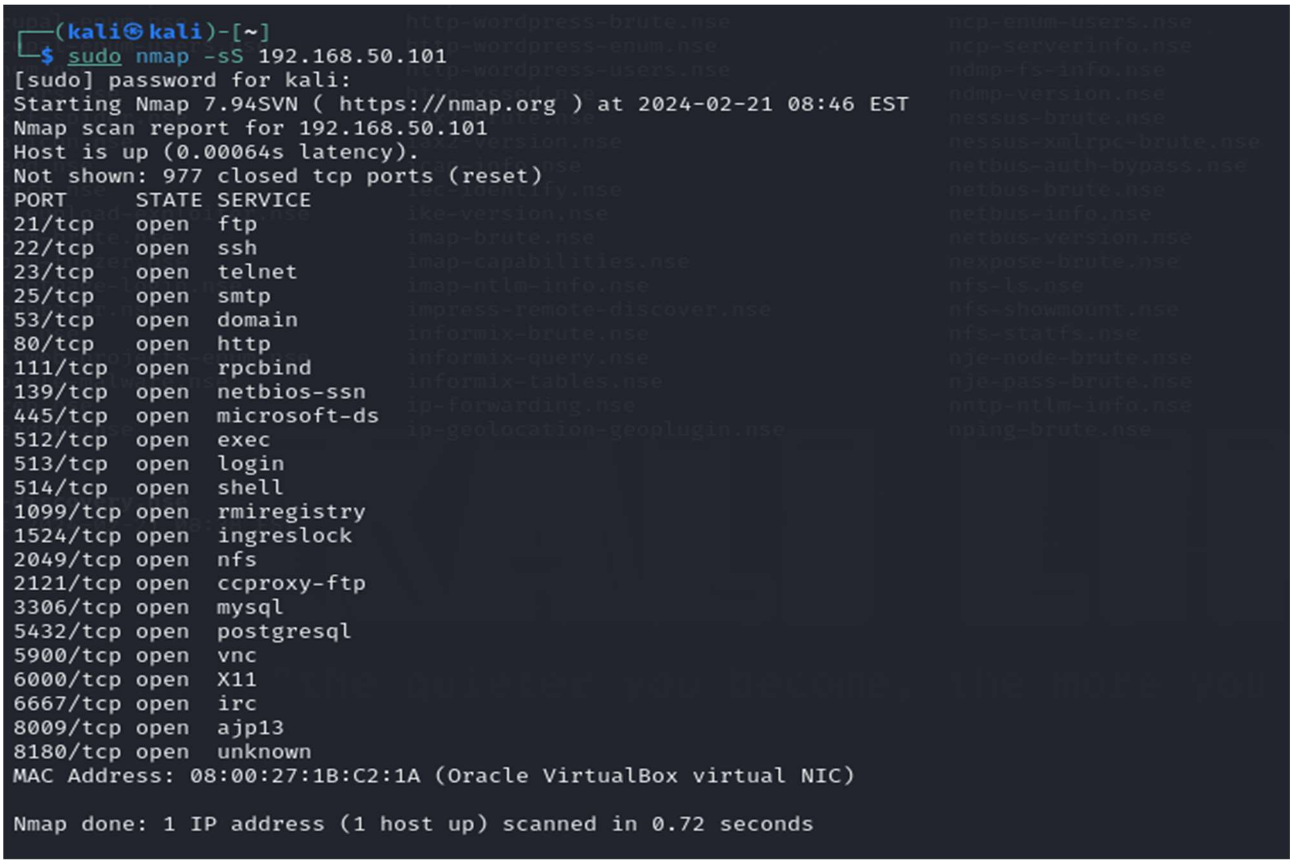


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 08:30 EST
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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: 08:00:27:1B:C2:1A (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 2.59 seconds
```

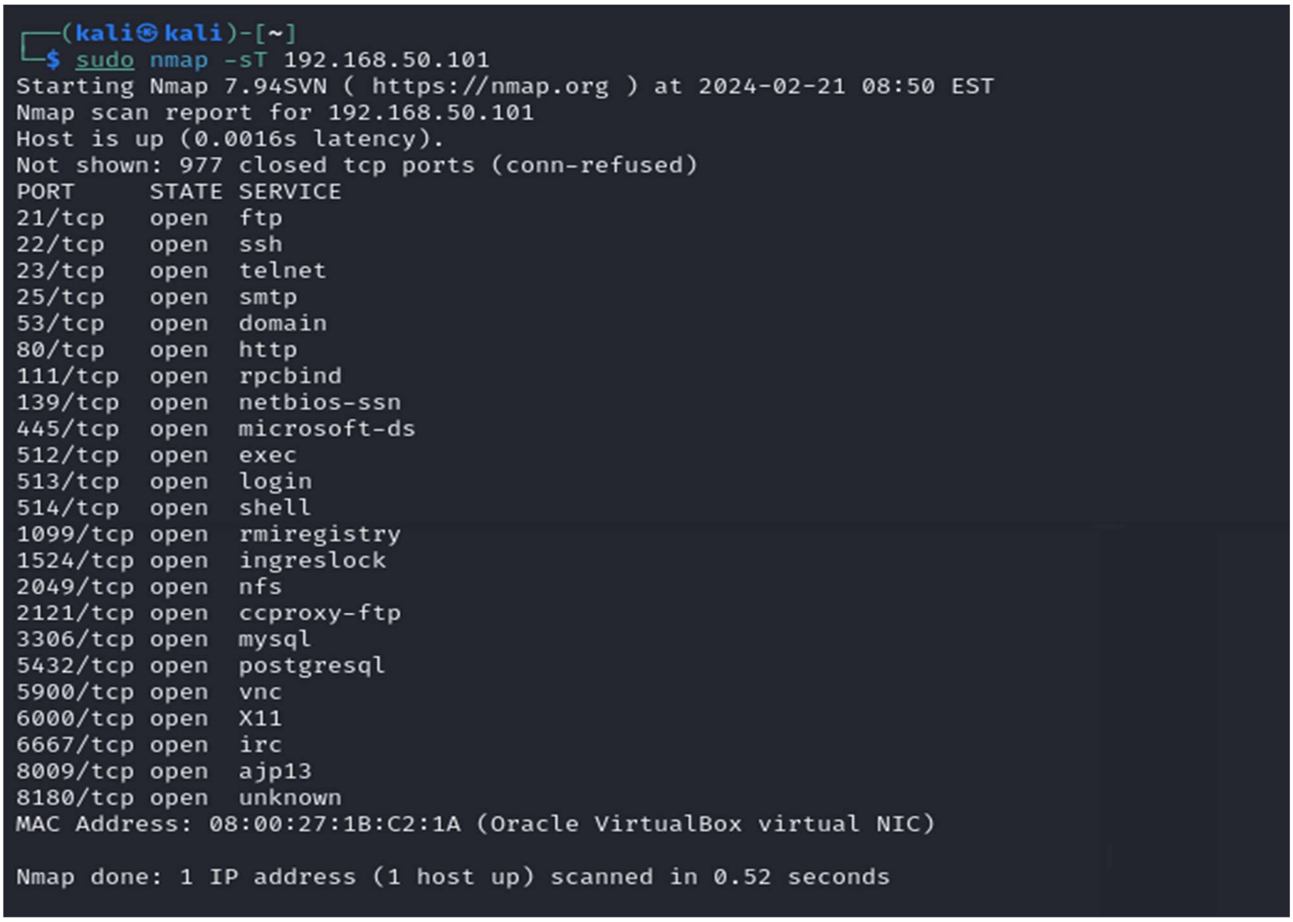


```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap 192.168.50.101 --script smb-os-discovery.nse
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 08:38 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   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: 08:00:27:1B:C2:1A (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-02-21T05:20:39-05:00

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```

Eseguiamo la SYN scan con **sudo nmap -sS 192.168.50.101** mentre la TCP connect con **sudo nmap -sT 192.168.50.101**.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 08:46 EST
Nmap scan report for 192.168.50.101
Host is up (0.00064s 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: 08:00:27:1B:C2:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
```

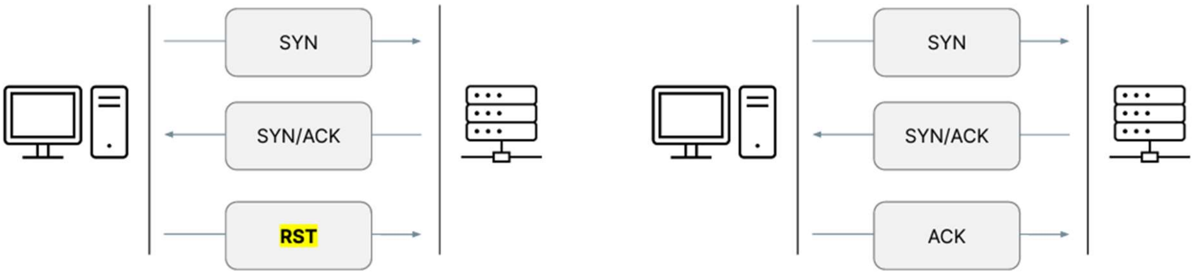


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 08:50 EST
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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: 08:00:27:1B:C2:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

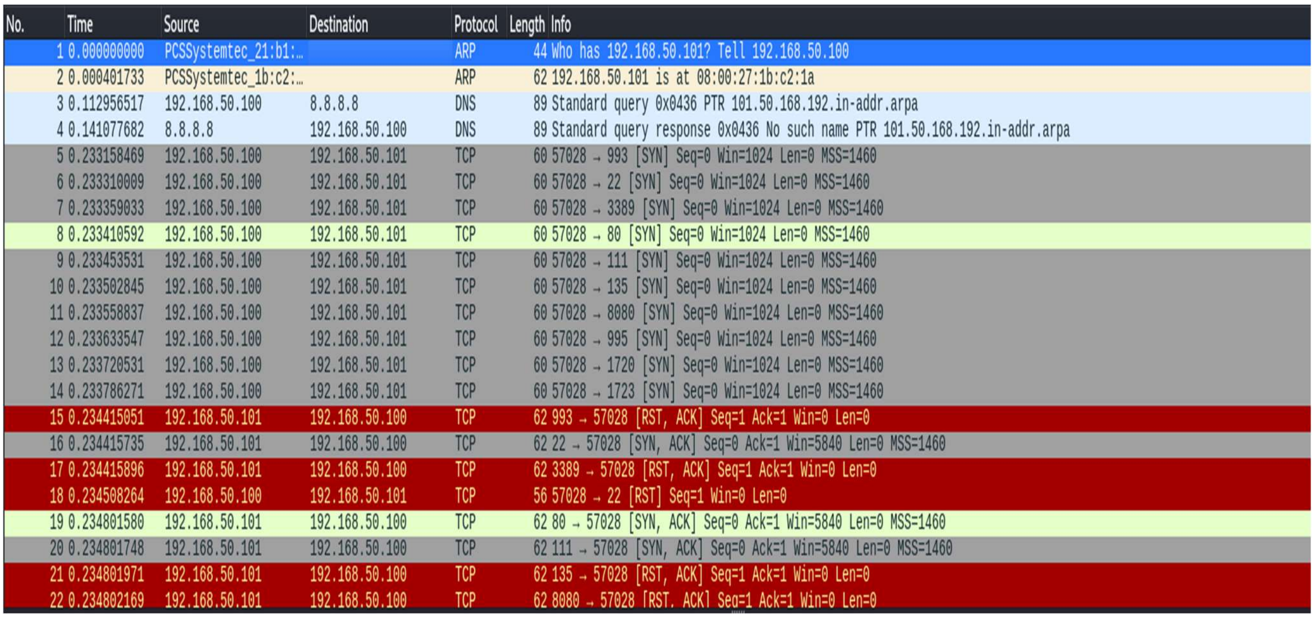
Dal punto di vista del risultato non vi è differenza tra la scansione lanciata con –sS e quella lanciata con -sT.

- -sS: meno invasivo. Nmap non completa il 3-way-handshake, ma chiude la comunicazione inviando un pacchetto RST (reset). Tuttavia, riesce a recuperare informazioni sullo stato della porta. Utile in quanto genera meno entropia e «rumore» a livello di rete.

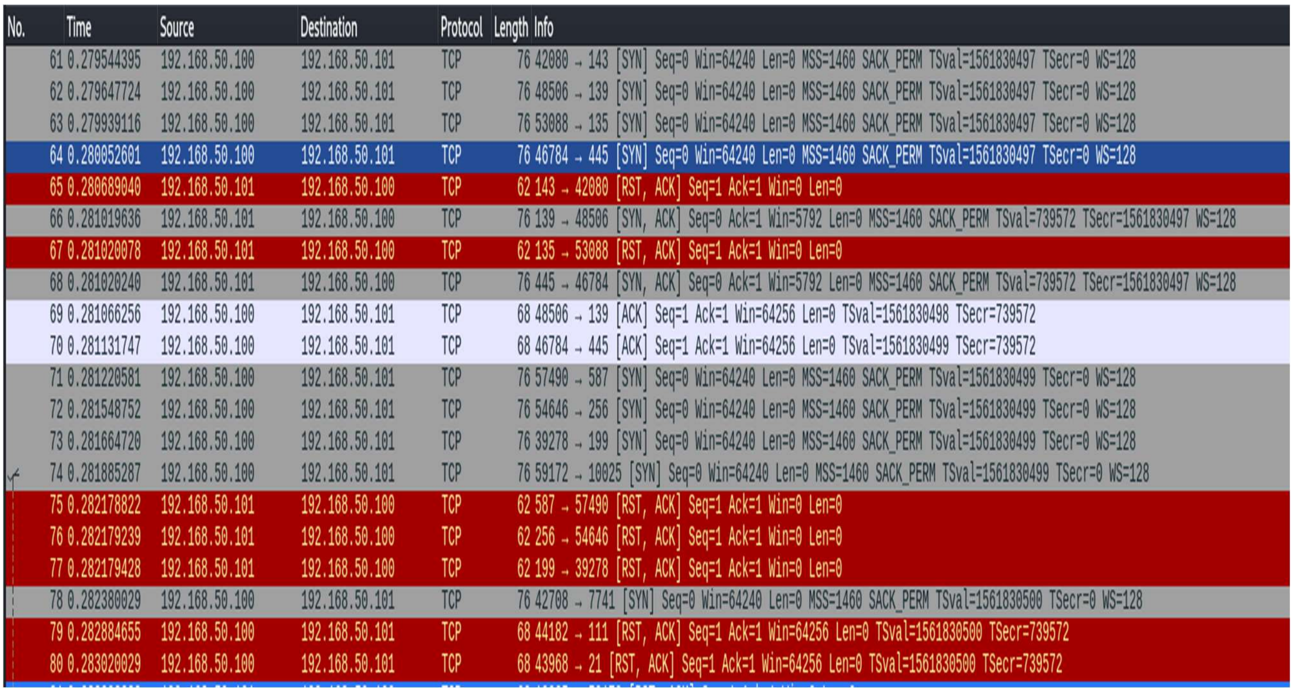
- -sT: scan invasivo. Nmap completa il 3-way-handshake, creando così il canale. Recupera info sullo stato della porta, ma crea più «rumore a livello network» ed è dunque una tecnica di scanning più identificabile e che su grosse reti potrebbe creare congestioni di rete.



Tuttavia conoscendo la differenza tra i due metodi analizzo i pacchetti inviati con **wireshark** ed effettivamente si può notare come nel caso della scansione lanciata con -sT venga effettivamente inviato un pacchetto **ACK** che completa la connessione TCP prima di chiuderla, a differenza del metodo –sS in cui alla ricezione del pacchetto **SYN** viene chiusa la connessione con **RST**.

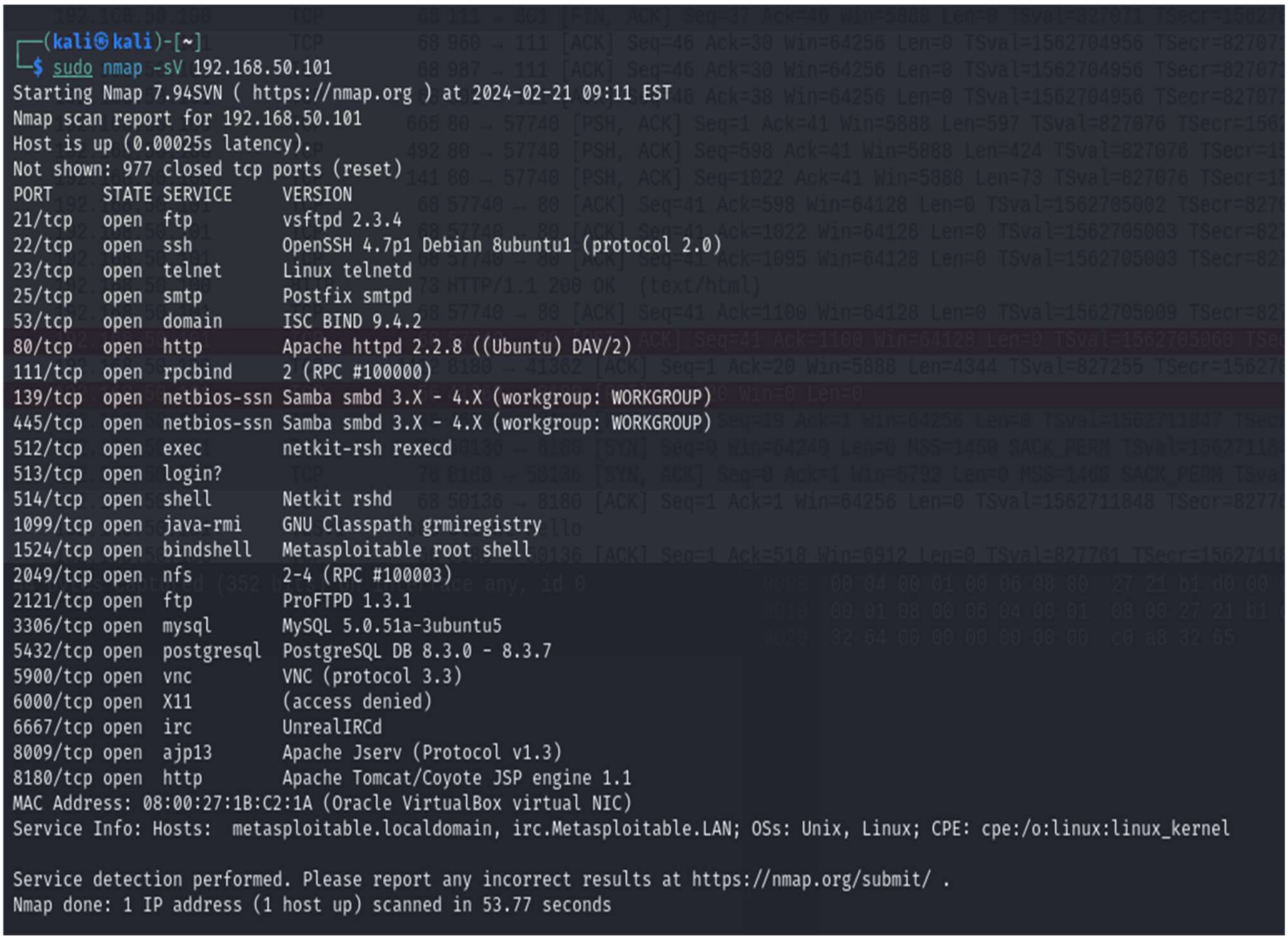


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_21:b1:…		ARP	44	Who has 192.168.50.101? Tell 192.168.50.100
2	0.000401733	PCSSystemtec_1b:c2:…		ARP	62	192.168.50.101 is at 08:00:27:1b:c2:1a
3	0.112956517	192.168.50.100	8.8.8.8	DNS	89	Standard query 0x0436 PTR 101.50.168.192.in-addr.arpa
4	0.141077682	8.8.8.8	192.168.50.100	DNS	89	Standard query response 0x0436 No such name PTR 101.50.168.192.in-addr.arpa
5	0.233158469	192.168.50.100	192.168.50.101	TCP	60	57028 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.233310009	192.168.50.100	192.168.50.101	TCP	60	57028 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.233359033	192.168.50.100	192.168.50.101	TCP	60	57028 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.233410592	192.168.50.100	192.168.50.101	TCP	60	57028 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.233453531	192.168.50.100	192.168.50.101	TCP	60	57028 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	0.233502845	192.168.50.100	192.168.50.101	TCP	60	57028 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.233558837	192.168.50.100	192.168.50.101	TCP	60	57028 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.233633547	192.168.50.100	192.168.50.101	TCP	60	57028 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.233720531	192.168.50.100	192.168.50.101	TCP	60	57028 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.233786271	192.168.50.100	192.168.50.101	TCP	60	57028 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.234415051	192.168.50.101	192.168.50.100	TCP	62	993 → 57028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	0.234415735	192.168.50.101	192.168.50.100	TCP	62	22 → 57028 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
17	0.234415896	192.168.50.101	192.168.50.100	TCP	62	3389 → 57028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	0.234508264	192.168.50.100	192.168.50.101	TCP	56	57028 → 22 [RST] Seq=1 Win=0 Len=0
19	0.234801580	192.168.50.101	192.168.50.100	TCP	62	80 → 57028 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
20	0.234801748	192.168.50.101	192.168.50.100	TCP	62	111 → 57028 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
21	0.234801971	192.168.50.101	192.168.50.100	TCP	62	135 → 57028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	0.234802169	192.168.50.101	192.168.50.100	TCP	62	8080 → 57028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



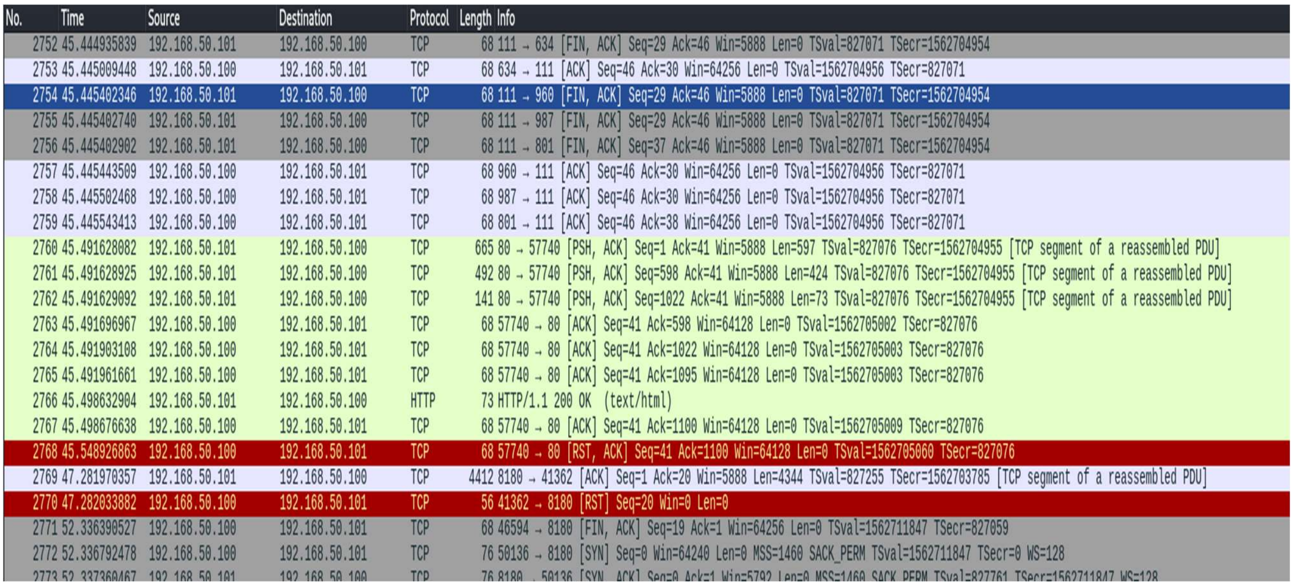
```
No.  Time          Source          Destination     Protocol Length Info
  61 0.279544395   192.168.50.100  192.168.50.101  TCP      76 42080 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1561830497 TSecr=0 WS=128
  62 0.279647724   192.168.50.100  192.168.50.101  TCP      76 48506 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1561830497 TSecr=0 WS=128
  63 0.279939116   192.168.50.100  192.168.50.101  TCP      76 53088 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1561830497 TSecr=0 WS=128
  64 0.280052601   192.168.50.100  192.168.50.101  TCP      76 46784 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1561830497 TSecr=0 WS=128
  65 0.280689040   192.168.50.101  192.168.50.100  TCP      62 143 → 42080 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  66 0.281019636   192.168.50.101  192.168.50.100  TCP      76 139 → 48506 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=739572 TSecr=1561830497 WS=128
  67 0.281020078   192.168.50.101  192.168.50.100  TCP      62 135 → 53088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  68 0.281020240   192.168.50.101  192.168.50.100  TCP      76 445 → 46784 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=739572 TSecr=1561830497 WS=128
  69 0.281066256   192.168.50.100  192.168.50.101  TCP      68 48506 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1561830498 TSecr=739572
  70 0.281131747   192.168.50.100  192.168.50.101  TCP      68 46784 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1561830499 TSecr=739572
  71 0.281220581   192.168.50.100  192.168.50.101  TCP      76 57490 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1561830499 TSecr=0 WS=128
  72 0.281548752   192.168.50.100  192.168.50.101  TCP      76 54646 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1561830499 TSecr=0 WS=128
  73 0.281664720   192.168.50.100  192.168.50.101  TCP      76 39278 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1561830499 TSecr=0 WS=128
  74 0.281885287   192.168.50.100  192.168.50.101  TCP      76 59172 → 10025 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1561830499 TSecr=0 WS=128
  75 0.282178822   192.168.50.101  192.168.50.100  TCP      62 587 → 57490 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  76 0.282179239   192.168.50.101  192.168.50.100  TCP      62 256 → 54646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  77 0.282179428   192.168.50.101  192.168.50.100  TCP      62 199 → 39278 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  78 0.282380029   192.168.50.100  192.168.50.101  TCP      76 42708 → 7741 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1561830500 TSecr=0 WS=128
  79 0.282884655   192.168.50.100  192.168.50.101  TCP      68 44182 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1561830500 TSecr=739572
  80 0.283020029   192.168.50.100  192.168.50.101  TCP      68 43968 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1561830500 TSecr=739572
```

Il version detection dei servizi in ascolto lo otteniamo con **sudo nmap -sV 192.168.50.101**; -sV è a tutti gli effetti una scansione TCP connect con l'aggiunta di specifici test grazie ai quali oltre al servizio recuperiamo anche la versione e i relativi dettagli.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:11 EST
Nmap scan report for 192.168.50.101
Host is up (0.00025s 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: 08:00:27:1B:C2:1A (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 53.77 seconds
```

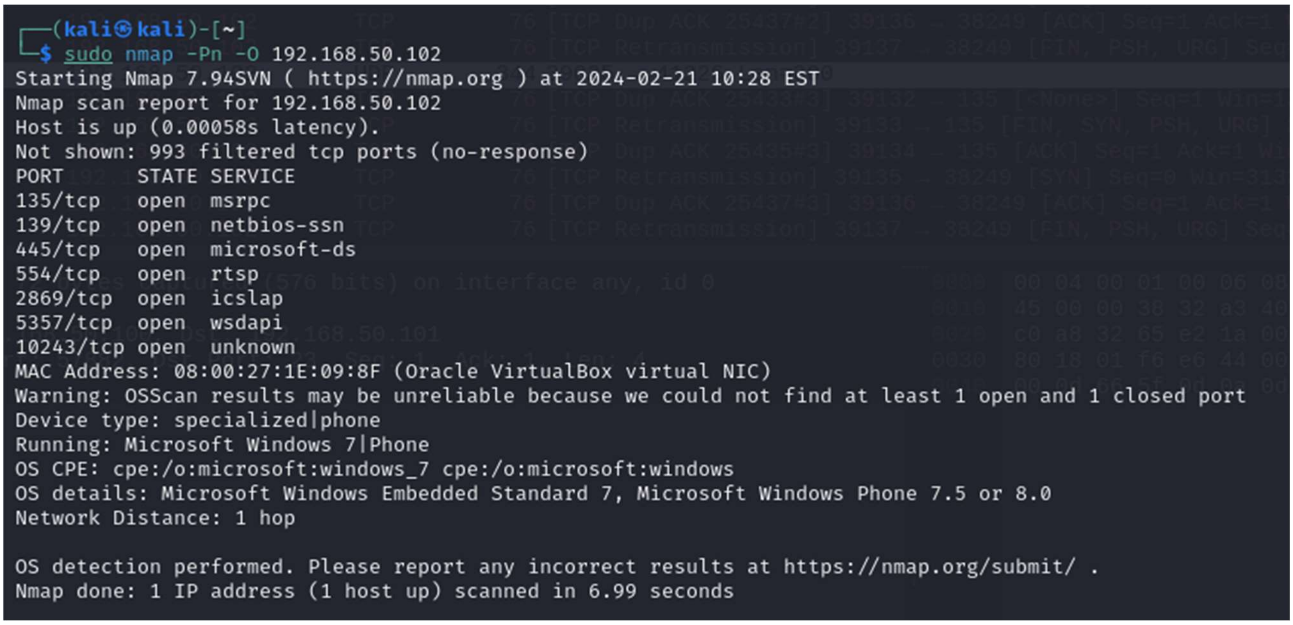
In particolare possiamo notare utilizzando wireshark che vengono scambiati dei messaggi contenenti **dati** una volta stabilita la connessione TCP per determinare la versione dei servizi che rispondono.



No.	Time	Source	Destination	Protocol	Length	Info
2752	45.444935839	192.168.50.101	192.168.50.100	TCP	68	111 → 634 [FIN, ACK] Seq=29 Ack=46 Win=5888 Len=0 TSval=827071 TSecr=1562704954
2753	45.445009448	192.168.50.100	192.168.50.101	TCP	68	634 → 111 [ACK] Seq=46 Ack=30 Win=64256 Len=0 TSval=1562704956 TSecr=827071
2754	45.445402346	192.168.50.101	192.168.50.100	TCP	68	111 → 960 [FIN, ACK] Seq=29 Ack=46 Win=5888 Len=0 TSval=827071 TSecr=1562704954
2755	45.445402740	192.168.50.101	192.168.50.100	TCP	68	111 → 987 [FIN, ACK] Seq=29 Ack=46 Win=5888 Len=0 TSval=827071 TSecr=1562704954
2756	45.445402902	192.168.50.101	192.168.50.100	TCP	68	111 → 801 [FIN, ACK] Seq=37 Ack=46 Win=5888 Len=0 TSval=827071 TSecr=1562704954
2757	45.445443509	192.168.50.100	192.168.50.101	TCP	68	960 → 111 [ACK] Seq=46 Ack=30 Win=64256 Len=0 TSval=1562704956 TSecr=827071
2758	45.445502468	192.168.50.100	192.168.50.101	TCP	68	987 → 111 [ACK] Seq=46 Ack=30 Win=64256 Len=0 TSval=1562704956 TSecr=827071
2759	45.445543413	192.168.50.100	192.168.50.101	TCP	68	801 → 111 [ACK] Seq=46 Ack=38 Win=64256 Len=0 TSval=1562704956 TSecr=827071
2760	45.491628082	192.168.50.101	192.168.50.100	TCP	665	80 → 57740 [PSH, ACK] Seq=1 Ack=41 Win=5888 Len=597 TSval=827076 TSecr=1562704955 [TCP segment of a reassembled PDU]
2761	45.491628925	192.168.50.101	192.168.50.100	TCP	492	80 → 57740 [PSH, ACK] Seq=598 Ack=41 Win=5888 Len=424 TSval=827076 TSecr=1562704955 [TCP segment of a reassembled PDU]
2762	45.491629092	192.168.50.101	192.168.50.100	TCP	141	80 → 57740 [PSH, ACK] Seq=1022 Ack=41 Win=5888 Len=73 TSval=827076 TSecr=1562704955 [TCP segment of a reassembled PDU]
2763	45.491696967	192.168.50.100	192.168.50.101	TCP	68	57740 → 80 [ACK] Seq=41 Ack=598 Win=64128 Len=0 TSval=1562705002 TSecr=827076
2764	45.491903108	192.168.50.100	192.168.50.101	TCP	68	57740 → 80 [ACK] Seq=41 Ack=1022 Win=64128 Len=0 TSval=1562705003 TSecr=827076
2765	45.491961661	192.168.50.100	192.168.50.101	TCP	68	57740 → 80 [ACK] Seq=41 Ack=1095 Win=64128 Len=0 TSval=1562705003 TSecr=827076
2766	45.498632904	192.168.50.101	192.168.50.100	HTTP	73	HTTP/1.1 200 OK (text/html)
2767	45.498676638	192.168.50.100	192.168.50.101	TCP	68	57740 → 80 [ACK] Seq=41 Ack=1100 Win=64128 Len=0 TSval=1562705009 TSecr=827076
2768	45.548926863	192.168.50.100	192.168.50.101	TCP	68	57740 → 80 [RST, ACK] Seq=41 Ack=1100 Win=64128 Len=0 TSval=1562705060 TSecr=827076
2769	47.281970357	192.168.50.101	192.168.50.100	TCP	4412	8180 → 41362 [ACK] Seq=1 Ack=20 Win=5888 Len=4344 TSval=827255 TSecr=1562703785 [TCP segment of a reassembled PDU]
2770	47.282033882	192.168.50.100	192.168.50.101	TCP	56	41362 → 8180 [RST] Seq=20 Win=0 Len=0
2771	52.336390527	192.168.50.100	192.168.50.101	TCP	68	46594 → 8180 [FIN, ACK] Seq=19 Ack=1 Win=64256 Len=0 TSval=1562711847 TSecr=827059
2772	52.336792478	192.168.50.100	192.168.50.101	TCP	76	50136 → 8180 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1562711847 TSecr=0 WS=128
2773	52.337360467	192.168.50.101	192.168.50.100	TCP	76	8180 → 50136 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=827761 TSecr=1562711847 WS=128

Per **Windows 7**:

Dobbiamo lanciare i comandi nmap con target windows 7 con il flag **-Pn** sempre presente; infatti il **firewall** di windows di default blocca i ping da altre macchine e con il flag evitiamo che essi vengano mandati.

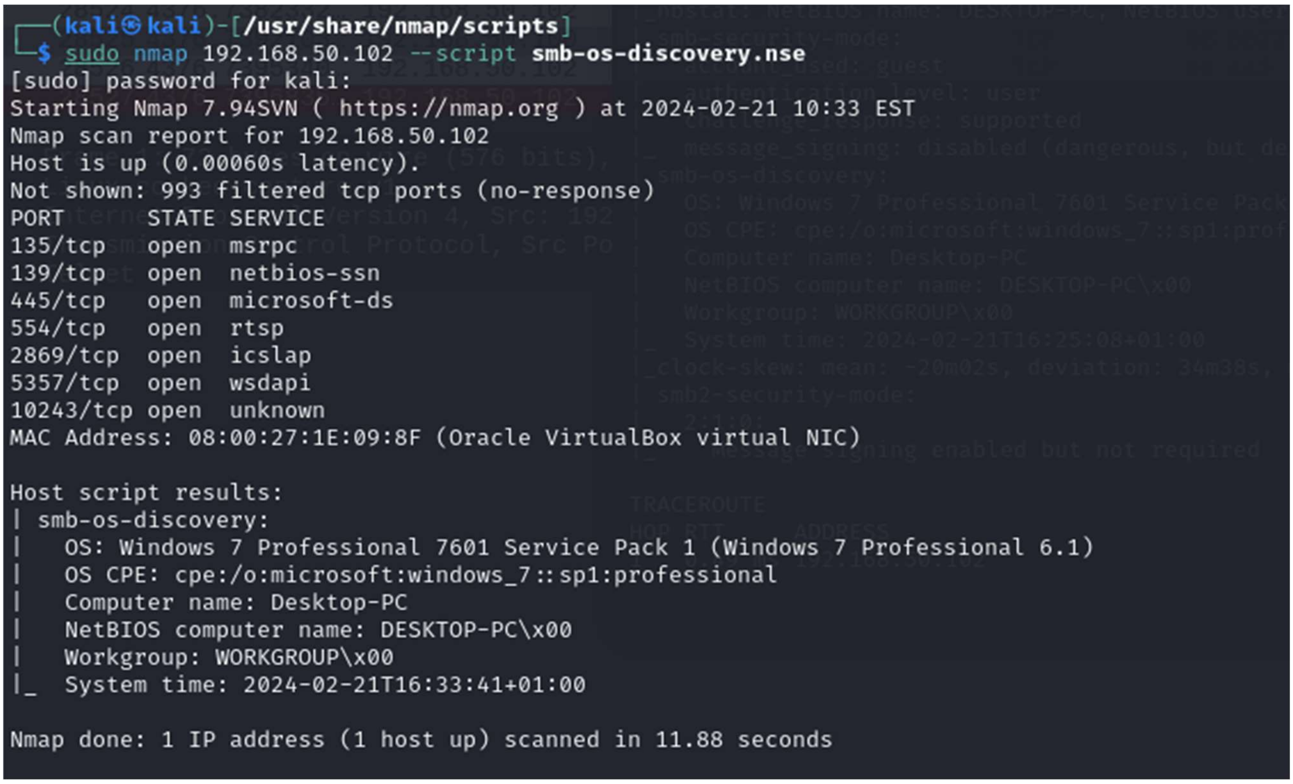


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:28 EST
Nmap scan report for 192.168.50.102
Host is up (0.00058s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:1E:09:8F (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
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 6.99 seconds
```

Notiamo che nmap ci indica che i risultati della scansione sono inaffidabili, probabilmente proprio a causa del sopracitato firewall che ostacola il recupero di informazioni da parte del programma.

Una possibile soluzione al problema è quella di provare ad effettuare l'OS fingerprint su windows 7 utilizzando un protocollo diverso, non ostacolato dal firewall. Utilizziamo quindi lo script nmap smb-os-discovery.nse già installato su Kali Linux presente nella cartella /usr/share/nmap/scripts che è basato sul protocollo **SMB (Server Message Block)**, usato soprattutto dai sistemi microsoft windows, principalmente per condividere file, stampanti, porte seriali e comunicazioni di varia natura tra diversi nodi di una rete; esso include anche un meccanismo di comunicazione tra processi autenticata.

Osserviamo che tale script fornisce dettagli decisamente più accurati e veritieri sul sistema operativo target in questo caso.



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap 192.168.50.102 --script smb-os-discovery.nse
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:33 EST
Nmap scan report for 192.168.50.102
Host is up (0.00060s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:1E:09:8F (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Desktop-PC
|   NetBIOS computer name: DESKTOP-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-02-21T16:33:41+01:00

Nmap done: 1 IP address (1 host up) scanned in 11.88 seconds
```