Traccia Esercizio:

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable**:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

A valle delle scansioni è prevista la produzione di un report contenente le seguenti info (dove disponibili):

- IP.
- Sistema Operativo.
- Porte Aperte.
- Servizi in ascolto con versione.

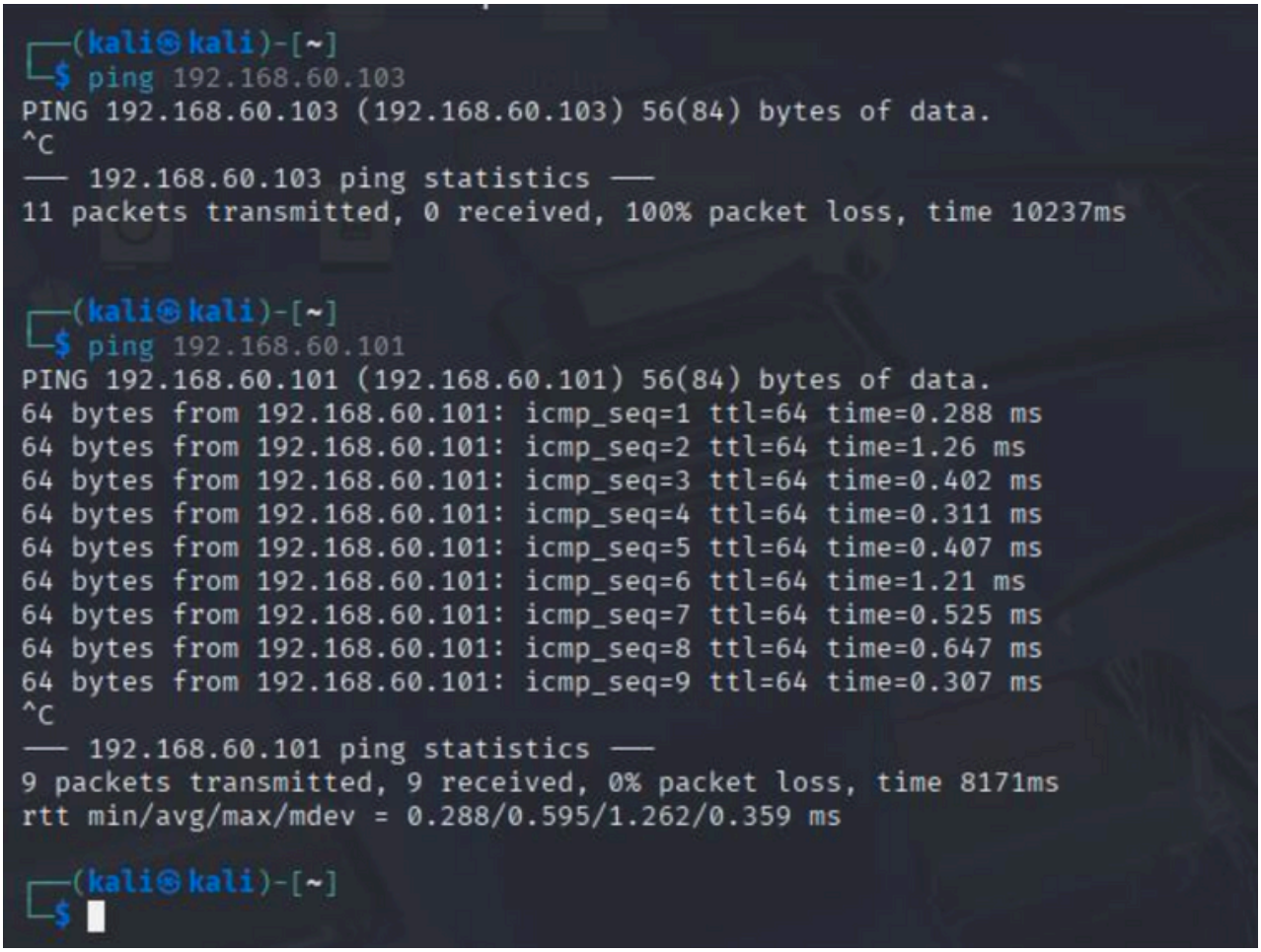
Esecuzione:

Configurazione indirizzi di rete delle macchine virtuali:

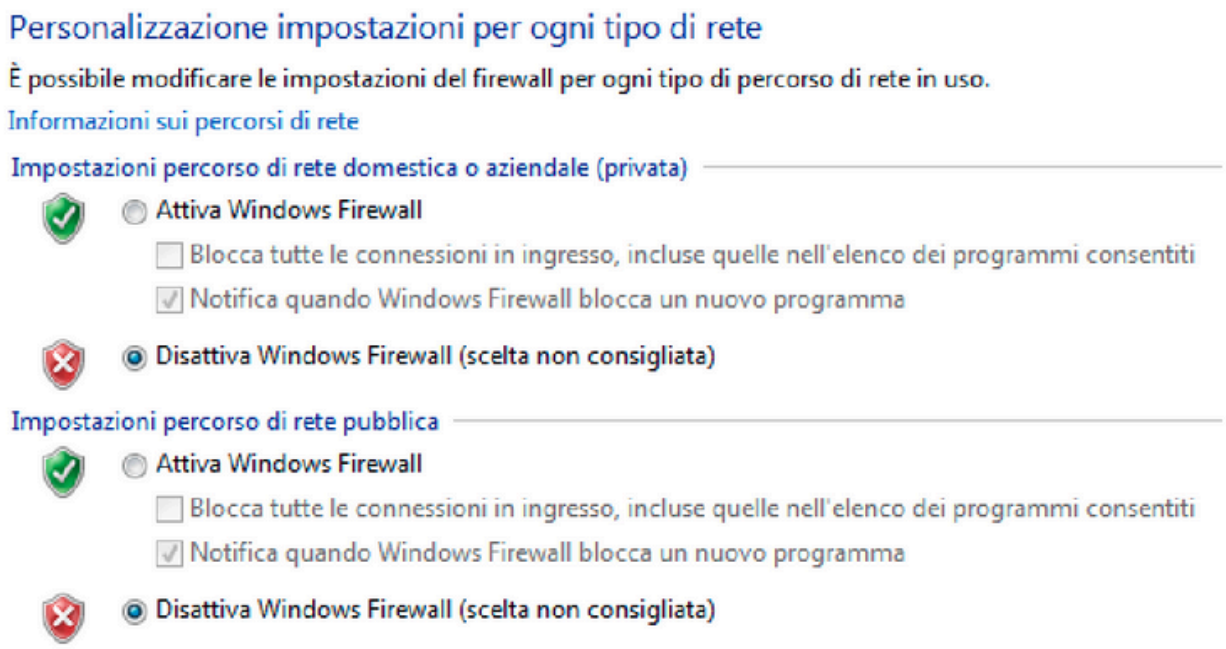
Win 7: 192.168.60.103
Kali: 192.168.60.99
Metasplotable2: 192.168.60.101

Test ping tra le macchine:

Come possiamo notare dallo screenshoot la macchina **kali riesce** a **pingare** la **metasploitalbe2** ma **non win7** per via del **firewall** di windows che interviene sul protocollo **ICMP**



Disattiviamo il firewall di WIn 7

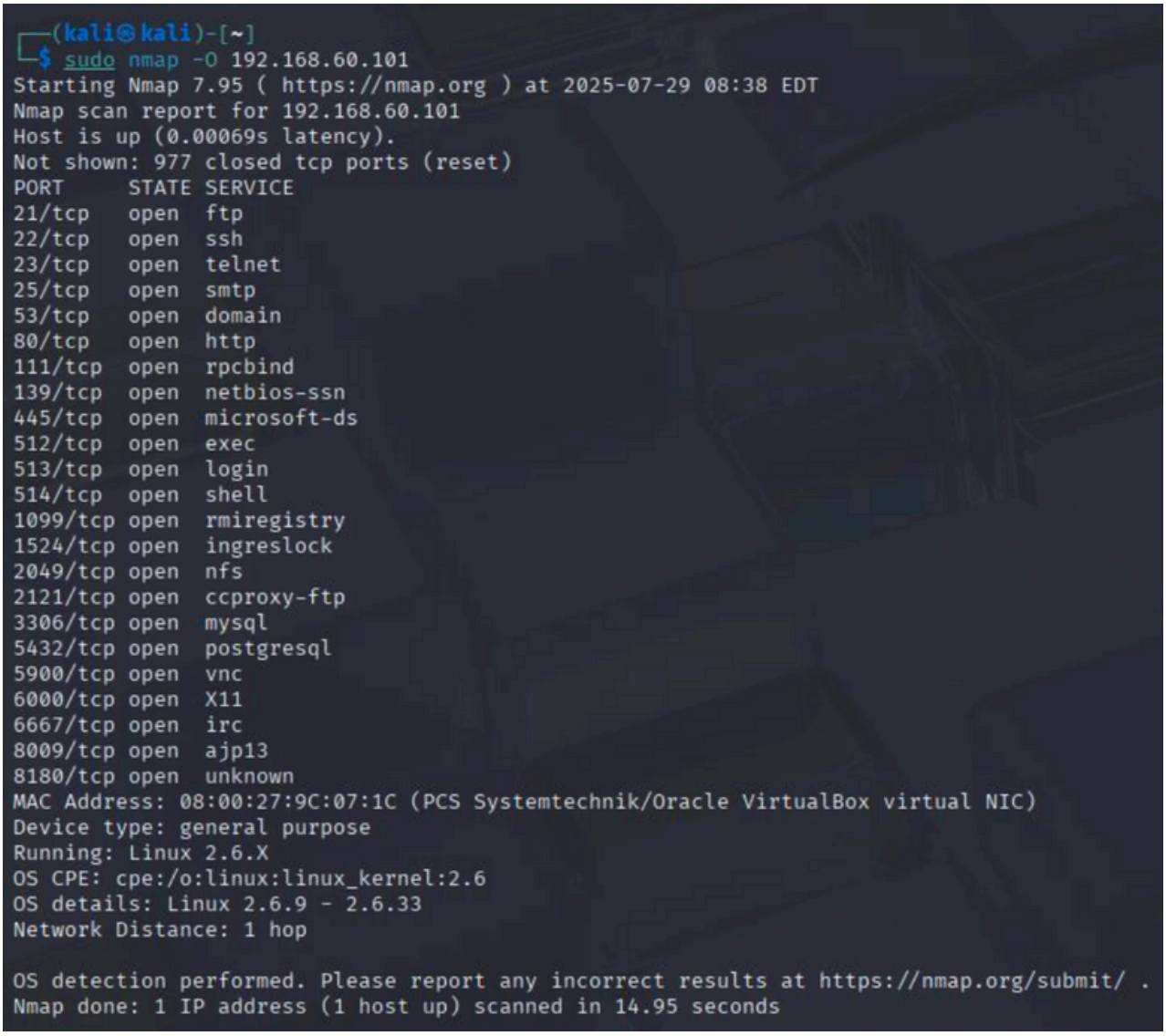


Ora che abbiamo **disattivato** il **firewall** di win7, riproviamo a pingare la macchina

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.60.103
PING 192.168.60.103 (192.168.60.103) 56(84) bytes of data.
64 bytes from 192.168.60.103: icmp_seq=1 ttl=128 time=1.15 ms
64 bytes from 192.168.60.103: icmp_seq=2 ttl=128 time=0.360 ms
64 bytes from 192.168.60.103: icmp_seq=3 ttl=128 time=0.719 ms
64 bytes from 192.168.60.103: icmp_seq=4 ttl=128 time=1.16 ms
64 bytes from 192.168.60.103: icmp_seq=5 ttl=128 time=0.503 ms
64 bytes from 192.168.60.103: icmp_seq=6 ttl=128 time=0.707 ms
64 bytes from 192.168.60.103: icmp_seq=7 ttl=128 time=0.366 ms
64 bytes from 192.168.60.103: icmp_seq=8 ttl=128 time=0.449 ms
64 bytes from 192.168.60.103: icmp_seq=9 ttl=128 time=0.331 ms
64 bytes from 192.168.60.103: icmp_seq=10 ttl=128 time=0.690 ms
64 bytes from 192.168.60.103: icmp_seq=11 ttl=128 time=0.262 ms
64 bytes from 192.168.60.103: icmp_seq=12 ttl=128 time=0.524 ms
^C
── 192.168.60.103 ping statistics ──
12 packets transmitted, 12 received, 0% packet loss, time 11210ms
rtt min/avg/max/mdev = 0.262/0.601/1.156/0.285 ms
```

Ora per fare l'esercizio riattiviamo il firewall di Win7

Per eseguire un **OS FINGERPRINT** utilizziamo il comando "**nmap –O INDIRIZZO**"

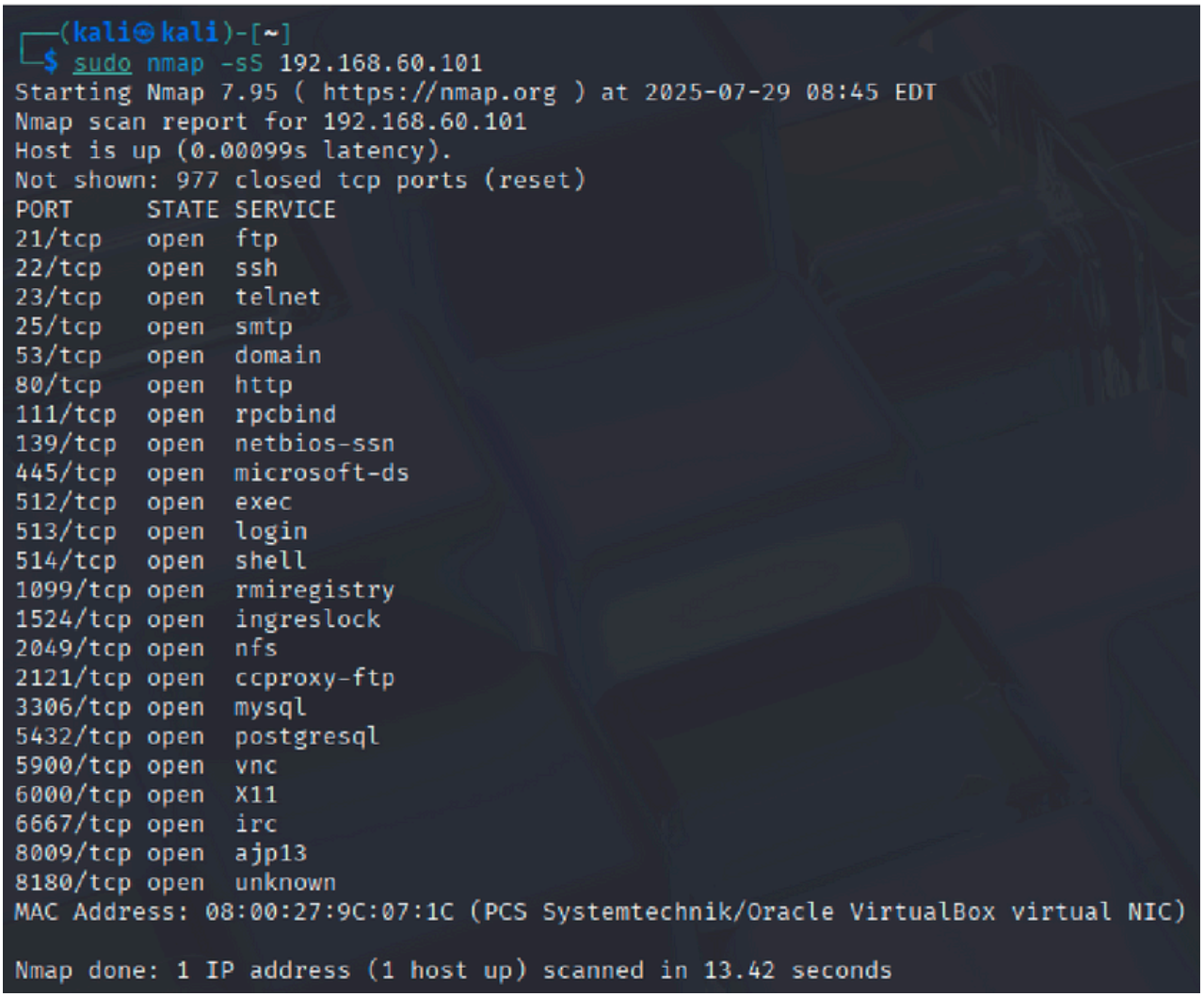


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.60.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:38 EDT
Nmap scan report for 192.168.60.101
Host is up (0.00069s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 08:00:27:9C:07:1C (PCS Systemtechnik/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 14.95 seconds
```

Metasploitable2 risulta essere una macchina **Linux 2.6.X** (2.6.9 alla 2.6.33)

Perche' ci ritorna un range di versioni e non una sola?
*Perche' la scansione ha trovato **corrispondenze presenti** in quel **range** di versioni*

Per eseguire un **SYN SCAN** utilizziamo il comando "**nmap -sS INDIRIZZO**



Per eseguire un **TCP SCAN** usiamo il comando "**nmap -sT INDIRIZZO**"
*Quando eseguiamo un **TCP SCAN** possiamo anche non usare il comando sudo poiche' questo tipo di scansione **non necessita di privilegi del sistema***

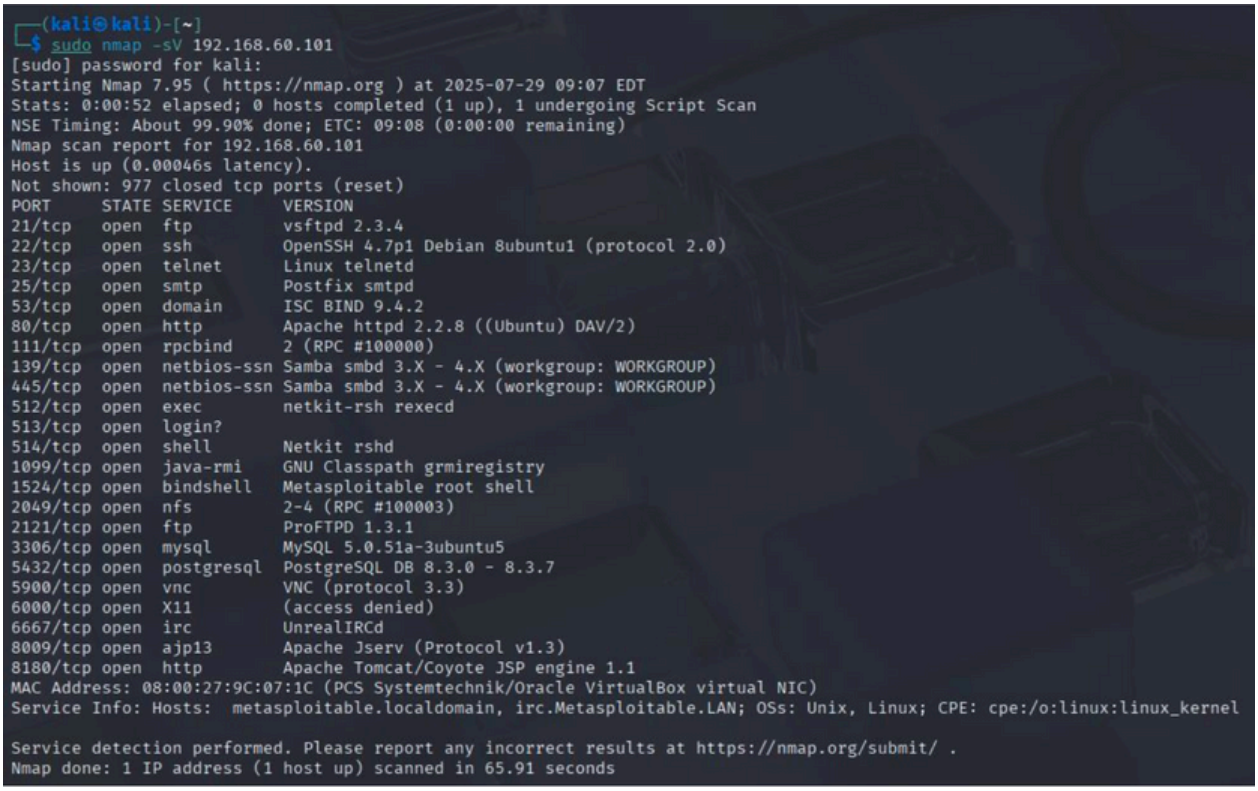
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.60.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:50 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 08:00:27:9C:07:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
```

La differenza principale e' come funzionano.

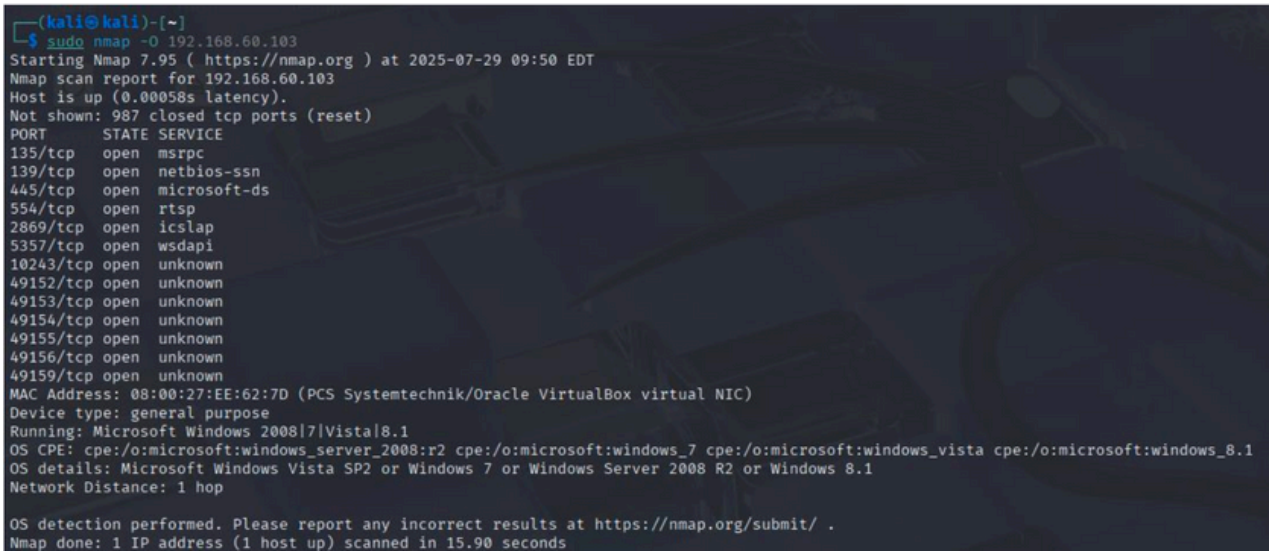
-sS e' un tipo di scansione meno invasiva, dove **handshake a tre vie** per completare la connessione TCP **non viene portato a termine**.
*Questo permette di non far scattare alcune misure di sicurezza come un firewall e dare un risultato piu' **accurato** su alcune porte.*

-sT e' un tipo di scansione che **completa handshake 3 ways** del protocllo TCP. Il firewall, o altre **misure di sicurezza** come **sensori IPS**, potrebbero intervenire e darci un risultato **alterato**.

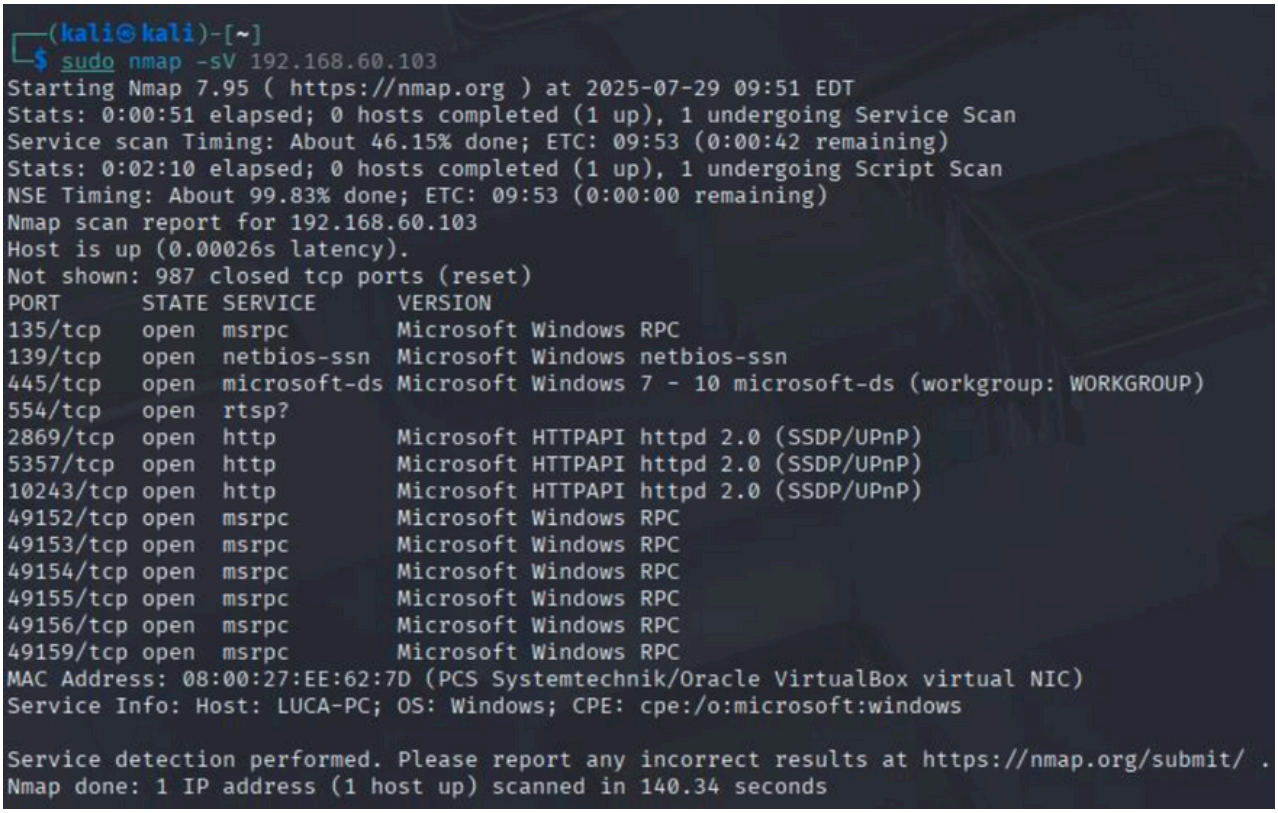
Per lo scan con **detenzione di versione** usiamo il comando "**nmap -sV INDIRIZZO**"
Possiamo notare nello screenshoot diversi dettagli interessanti sotto la colonna VERSION



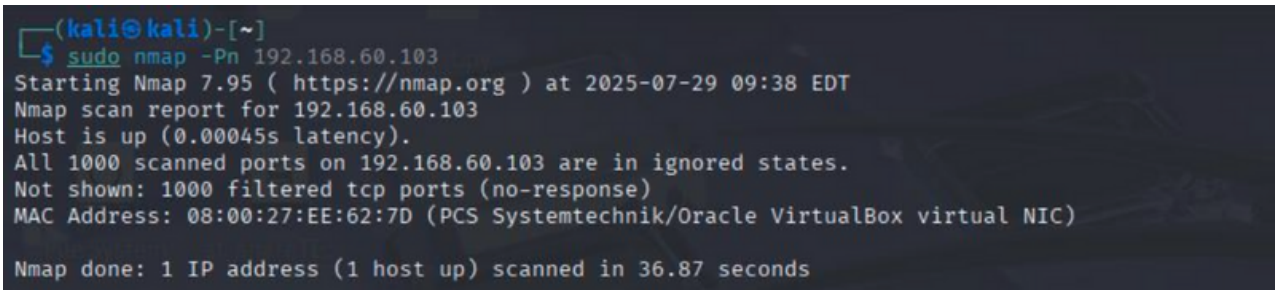
OS FOOTPRINTING Win7:

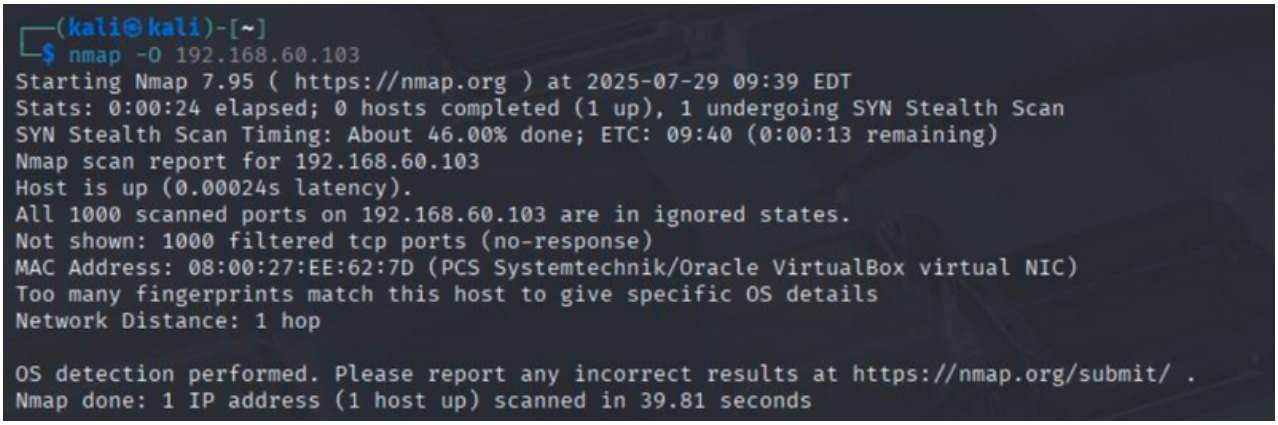


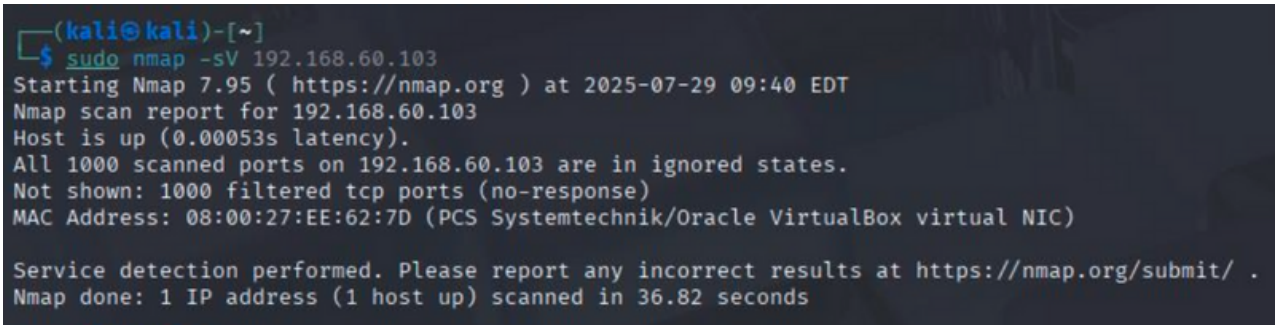
Scan con **detenzione di versione** su **win 7** con il comando "**nmap -sV INDIRIZZO**



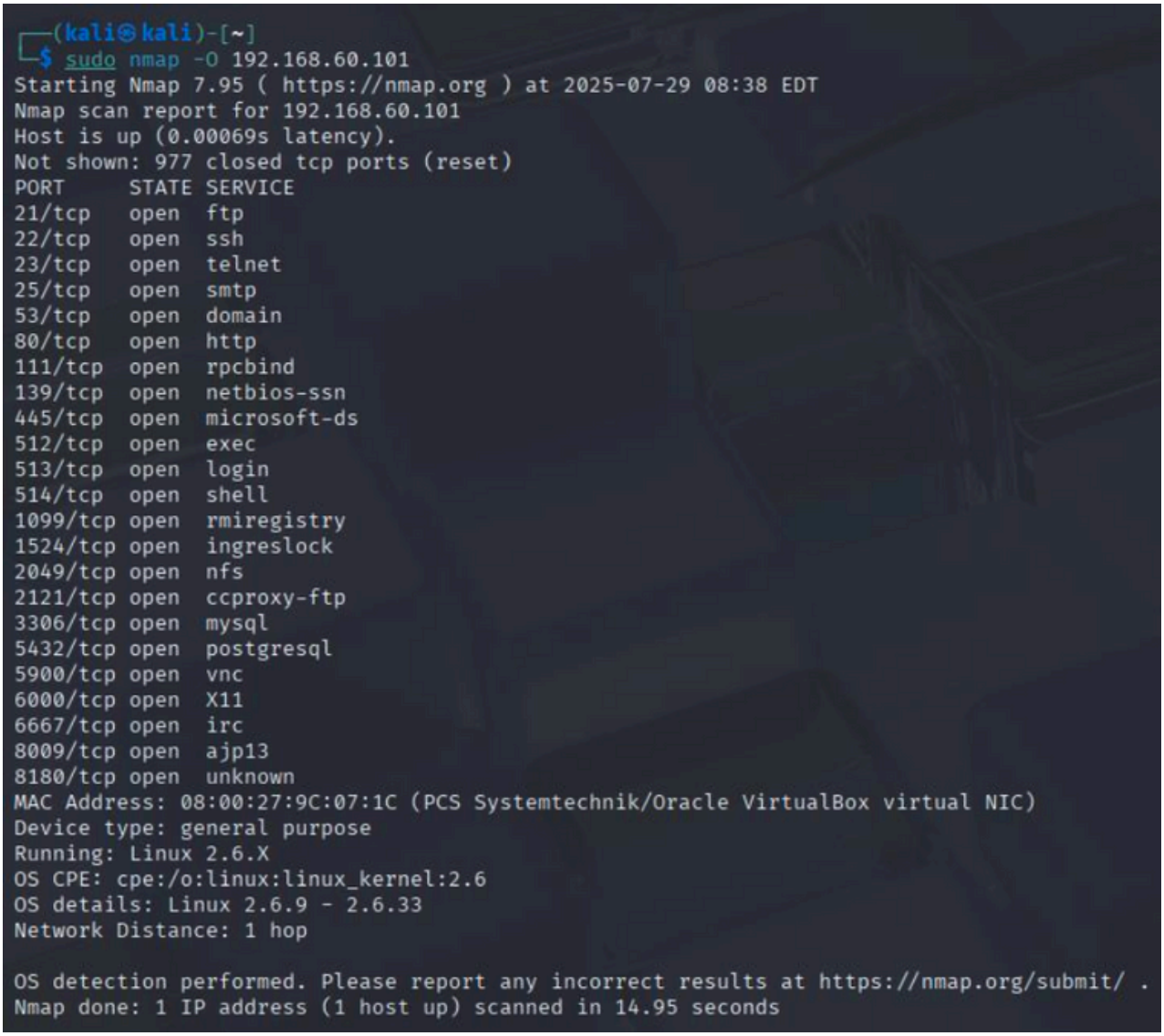
Risultatiu su **Win 7 con** il **Firewall Attivo**i







Scan su Metasploitable2:
IP: 192.168.60.101
SO: Linux 2.6.X



PORTE APERTE & SERVIZI:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.60.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:45 EDT
Nmap scan report for 192.168.60.101
Host is up (0.00099s 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: 08:00:27:9C:07:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

Servizi e Versioni:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.60.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 10:10 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.60.101
Host is up (0.00073s 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: 08:00:27:9C:07:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lir

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.76 seconds
```

Scan su Windows 7
IP: 192.168.60.103
OS: Win 7

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.60.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 10:16 EDT
Nmap scan report for 192.168.60.103
Host is up (0.00070s latency).
Not shown: 987 closed tcp ports (reset)
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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:EE:62:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 R2 SP1 or Windows 7 SP1, Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
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 16.09 seconds
```

Porte, servizi e Versioni:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.60.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:51 EDT
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 46.15% done; ETC: 09:53 (0:00:42 remaining)
Stats: 0:02:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.83% done; ETC: 09:53 (0:00:00 remaining)
Nmap scan report for 192.168.60.103
Host is up (0.00026s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:EE:62:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: LUCA-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.34 seconds
```