# S5/L2

08/01/2025

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

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

E la seguente sul target Windows:

- OS fingerprint.

Ho impostato lo stesso indirizzo ip di metasploitable e kali per farli comunicare

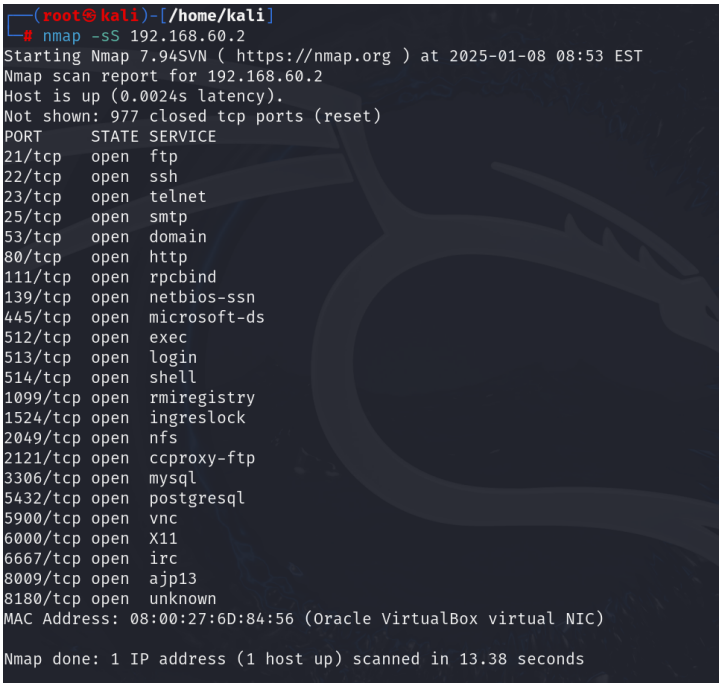
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.60.2
PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
64 bytes from 192.168.60.2: icmp_seq=1 ttl=64 time=12.0 ms
64 bytes from 192.168.60.2: icmp_seq=2 ttl=64 time=0.856 ms
64 bytes from 192.168.60.2: icmp_seq=3 ttl=64 time=1.70 ms
64 bytes from 192.168.60.2: icmp_seq=4 ttl=64 time=0.685 ms
64 bytes from 192.168.60.2: icmp_seq=5 ttl=64 time=1.09 ms
64 bytes from 192.168.60.2: icmp_seq=6 ttl=64 time=1.06 ms
^C
── 192.168.60.2 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 0.685/2.899/12.009/4.086 ms
```

Fatto ciò ho cominciato con i comandi nmap per trovare il sistema operativo

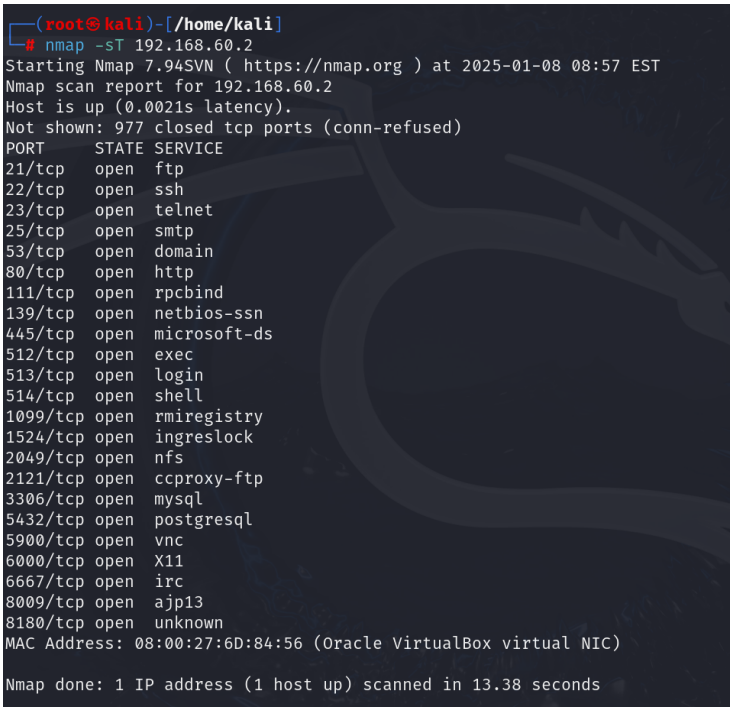
```
File  Actions  Edit  View  Help
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.60.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 08:48 EST
Nmap scan report for 192.168.60.2
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     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: 08:00:27:6D:84:56 (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 14.67 seconds
```

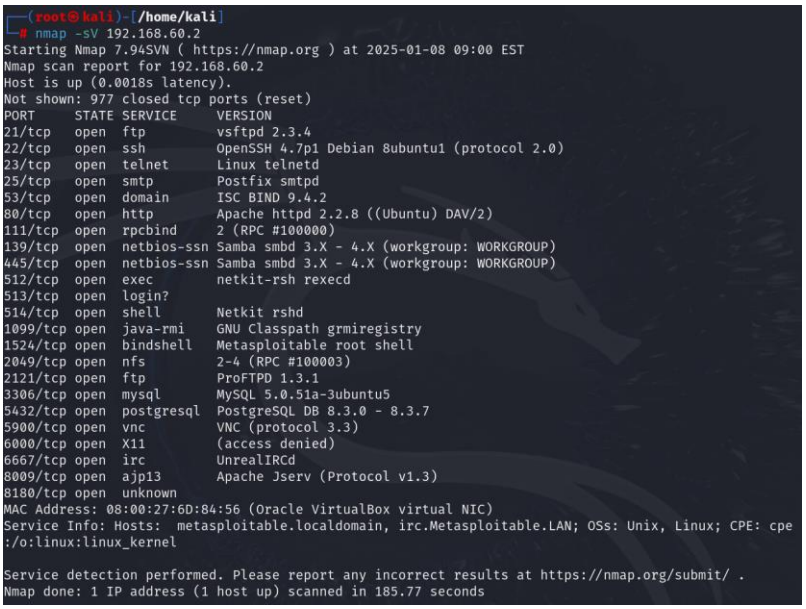
Poi il comando per il syn scan



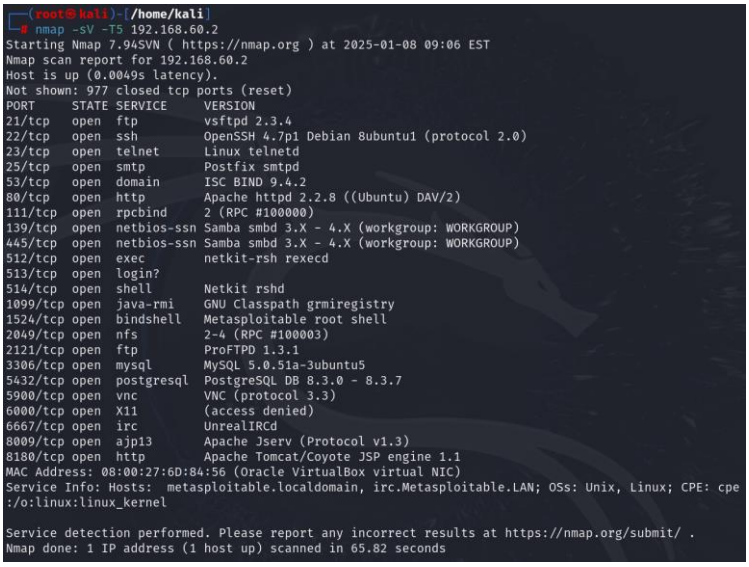

Successivamente il comando per il tcp connect scan



Ed infine il version detection




Ha impiegato un po di tempo quindi ho fatto un'altra prova usando il timing –T5 per rendere la ricerca più aggressiva e veloce




Si può vedere come il tempo sia minore

La consegna chiedeva di fare gli stessi passaggi con un altro target, in questo caso windows, ho usato windows 10 in macchina virtuale, ho modificato il suo indirizzo ip rendendolo come quello di kali per avviare la comunicazione tra le due MV.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.60.10
PING 192.168.60.10 (192.168.60.10) 56(84) bytes of data.
64 bytes from 192.168.60.10: icmp_seq=1 ttl=128 time=42.7 ms
64 bytes from 192.168.60.10: icmp_seq=2 ttl=128 time=10.8 ms
64 bytes from 192.168.60.10: icmp_seq=3 ttl=128 time=0.428 ms
64 bytes from 192.168.60.10: icmp_seq=4 ttl=128 time=43.4 ms
64 bytes from 192.168.60.10: icmp_seq=5 ttl=128 time=42.8 ms
64 bytes from 192.168.60.10: icmp_seq=6 ttl=128 time=51.3 ms
^C
── 192.168.60.10 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5038ms
rtt min/avg/max/mdev = 0.428/31.898/51.309/19.050 ms
```

## OS FINGERPRINT

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -T5 192.168.60.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:19 EST
Nmap scan report for 192.168.60.10
Host is up (0.031s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:17:45:2C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
t
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|XP (91%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows Server 2019 (91%), Microsoft Windows 10 1909 (90%), Microso
ft Windows XP SP3 (85%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
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 23.42 seconds
```

## SYN SCAN

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -T5 192.168.60.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:23 EST
Nmap scan report for 192.168.60.10
Host is up (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:17:45:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.12 seconds
```

## TCP CONNECT

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT -T5 192.168.60.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:26 EST
Nmap scan report for 192.168.60.10
Host is up (0.053s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:17:45:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 20.51 seconds
```

## VERSION DETECTION

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -T5 192.168.60.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:30 EST
Nmap scan report for 192.168.60.10
Host is up (0.026s latency).
Not shown: 997 filtered tcp ports (no-response)
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?
MAC Address: 08:00:27:17:45:2C (Oracle VirtualBox virtual NIC)
Service Info: 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 28.60 seconds
```