

RELAZIONE ES S5 – L2

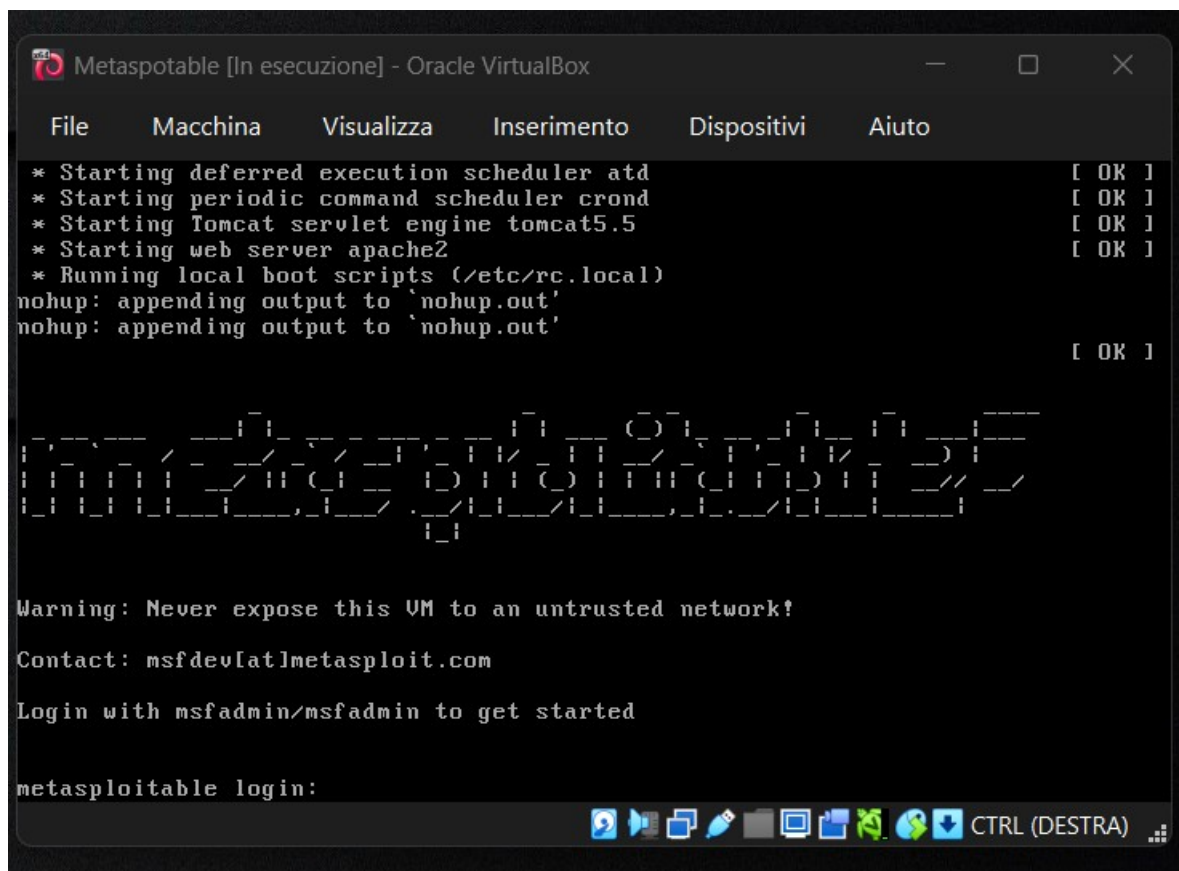
SCANSIONE DEI SERVIZI CON NMAP su target Metasploitable

Introduzione:

L'obiettivo dell'esercizio S5 - L2 è quello di utilizzare lo strumento Nmap per individuare informazioni di base su due sistemi target (Metasploitable e Windows XP), in particolare il sistema operativo, le porte aperte e i servizi in ascolto, quando possibile. L'attaccante utilizzato per l'analisi è Kali Linux, configurato in un ambiente di laboratorio isolato.

1. Avvio di Metasploitable

La macchina virtuale Metasploitable è stata avviata correttamente e utilizzata come target vulnerabile. Dopo il login (**msfadmin user e psw**) il sistema era pronto per essere analizzato tramite Kali Linux.



```
Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

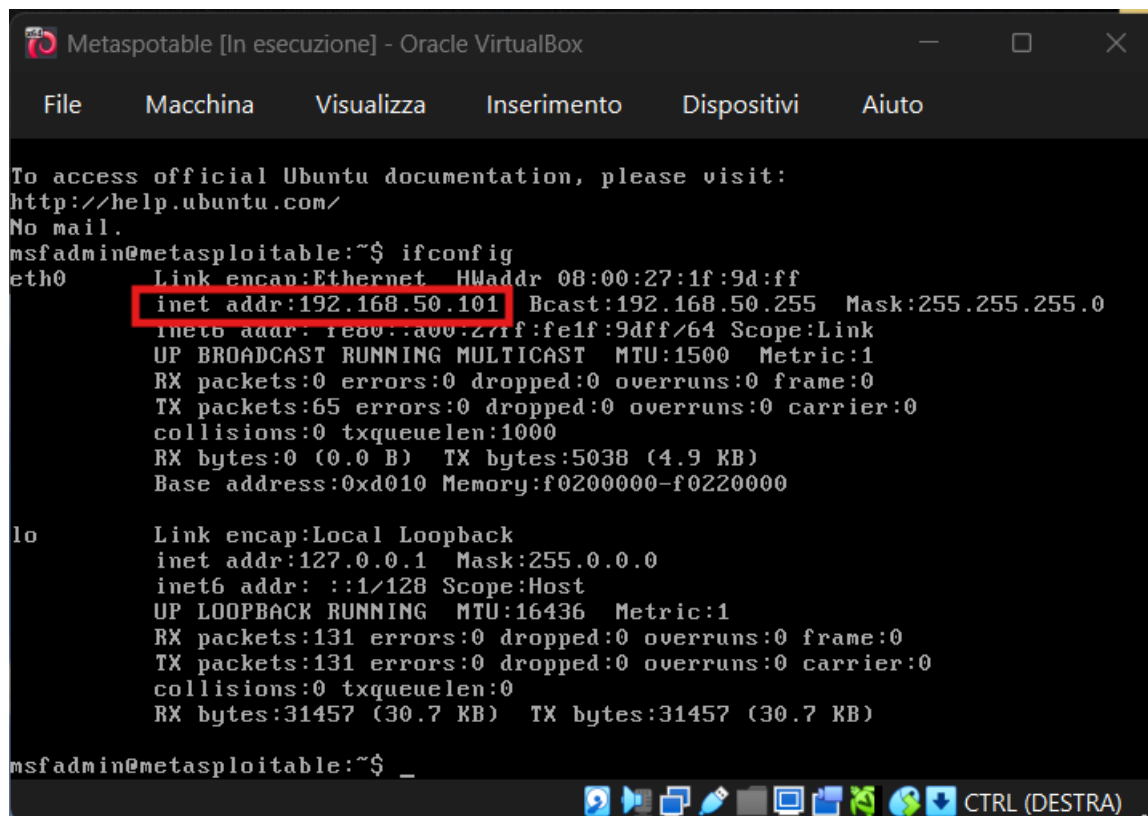
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login:
```

2. Identificazione IP di Metasploitable

Su Metasploitable è stato eseguito il comando *ifconfig* per visualizzare la configurazione di rete. È stato individuato l'indirizzo IP assegnato all'interfaccia eth0:

IP Metasploitable: **192.168.50.101**



```
Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1f:9d:ff
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1f:9dff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:5038 (4.9 KB)
          Base address:0xd010 Memory:f0200000-f0220000

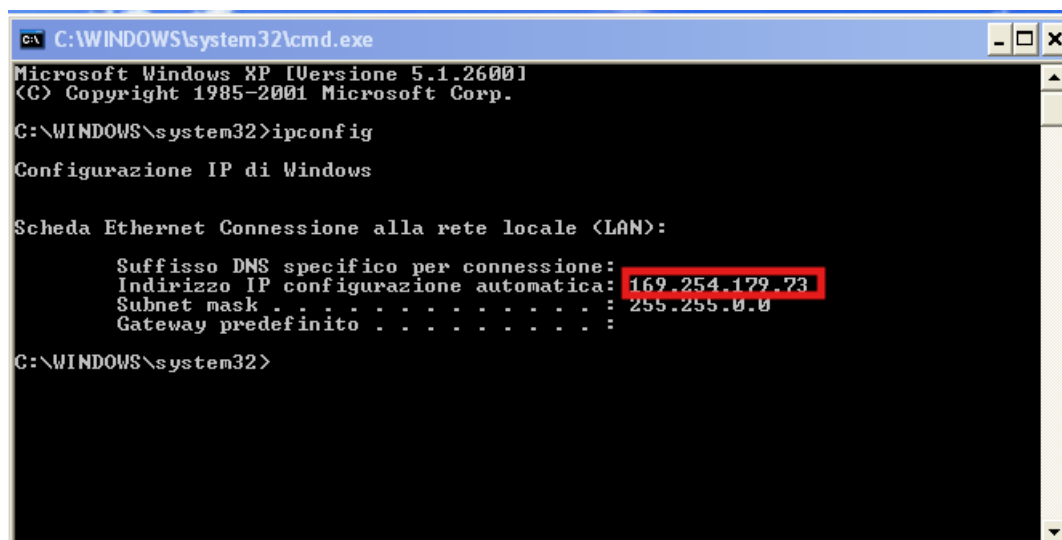
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:131 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31457 (30.7 KB)  TX bytes:31457 (30.7 KB)

msfadmin@metasploitable:~$
```

3. Identificazione IP di Windows XP

Su Windows XP è stato aperto il prompt dei comandi ed è stato eseguito il comando *ipconfig*. Il sistema ha restituito il seguente indirizzo IP:

IP Windows XP: **169.254.179.73**



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IP configurazione automatica: 169.254.179.73
    Subnet mask . . . . . : 255.255.0.0
    Gateway predefinito . . . . . :

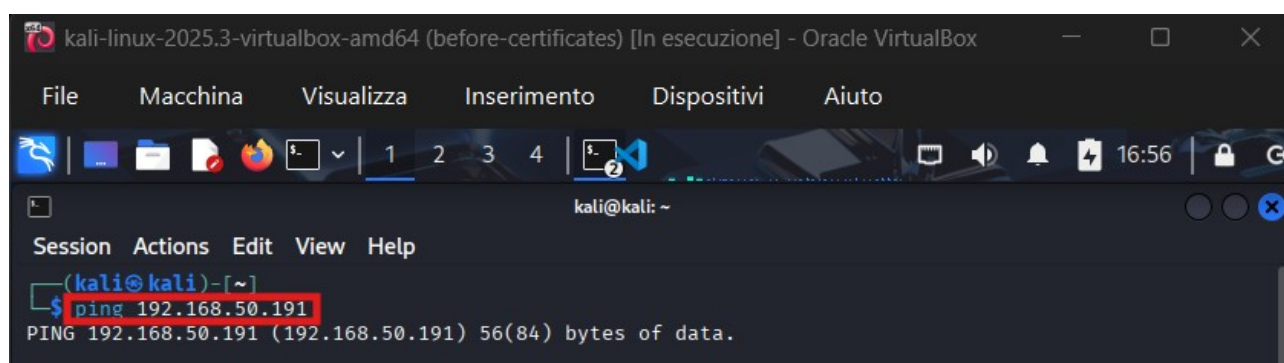
C:\WINDOWS\system32>
```

Questo indirizzo è un IP APIPA, assegnato automaticamente in assenza di un server DHCP.

4. Verifica della connettività (Ping)

Da Kali Linux è stato utilizzato il comando *ping* per verificare la raggiungibilità dei target. Il ping verso Metasploitable e verso Windows XP ha permesso di confermare che i sistemi erano visibili in rete e pronti per le scansioni Nmap.

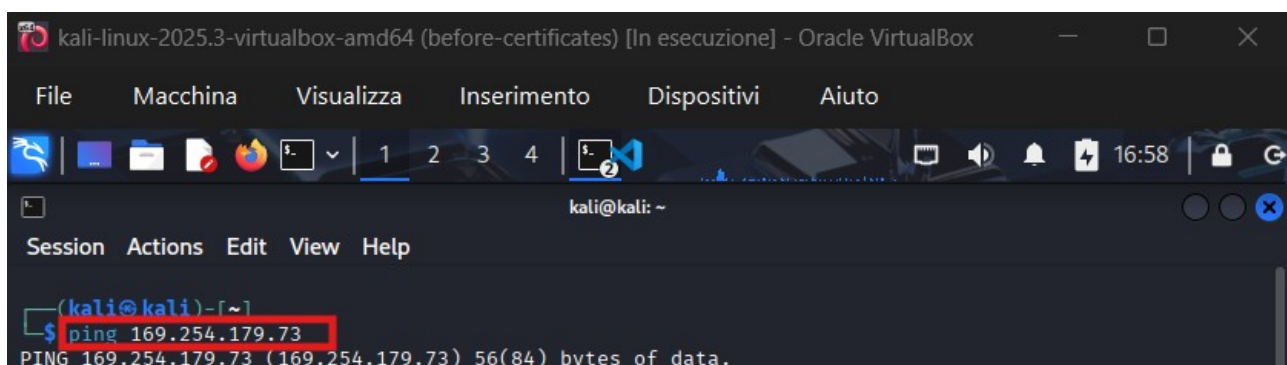
PING METASPOITABLE:



The screenshot shows a terminal window titled "kali-linux-2025.3-virtualbox-amd64 (before-certificates) [In esecuzione] - Oracle VirtualBox". The terminal prompt is "kali@kali: ~". The command "ping 192.168.50.191" has been entered and executed. The output shows "PING 192.168.50.191 (192.168.50.191) 56(84) bytes of data." with a successful response.

```
kali@kali: ~  
$ ping 192.168.50.191  
PING 192.168.50.191 (192.168.50.191) 56(84) bytes of data.
```

PING WIN XP:



The screenshot shows a terminal window titled "kali-linux-2025.3-virtualbox-amd64 (before-certificates) [In esecuzione] - Oracle VirtualBox". The terminal prompt is "kali@kali: ~". The command "ping 169.254.179.73" has been entered and executed. The output shows "PING 169.254.179.73 (169.254.179.73) 56(84) bytes of data." with a successful response.

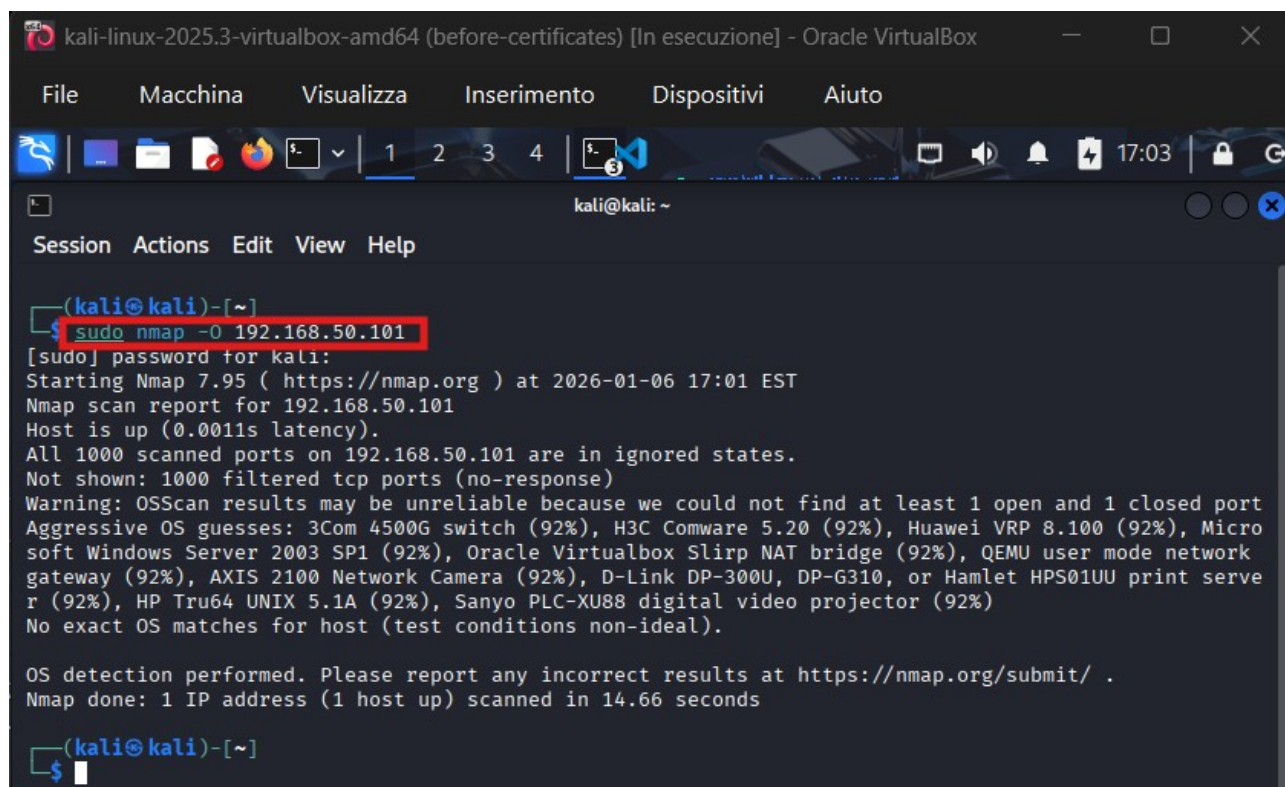
```
kali@kali: ~  
$ ping 169.254.179.73  
PING 169.254.179.73 (169.254.179.73) 56(84) bytes of data.
```

5. OS Fingerprint su Metasploitable

Da Kali Linux è stato eseguito il comando:

`sudo nmap -O 192.168.50.101`

Questa scansione ha avuto lo scopo di identificare il sistema operativo del target. Nmap ha segnalato che i risultati dell'OS detection non sono completamente affidabili a causa della mancanza di porte aperte e chiuse sufficienti.



```
kali-linux-2025.3-virtualbox-amd64 (before-certificates) [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 17:01 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Micro
soft Windows Server 2003 SP1 (92%), Oracle Virtualbox Slirp NAT bridge (92%), QEMU user mode network
gateway (92%), AXIS 2100 Network Camera (92%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print serve
r (92%), HP Tru64 UNIX 5.1A (92%), Sanyo PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).

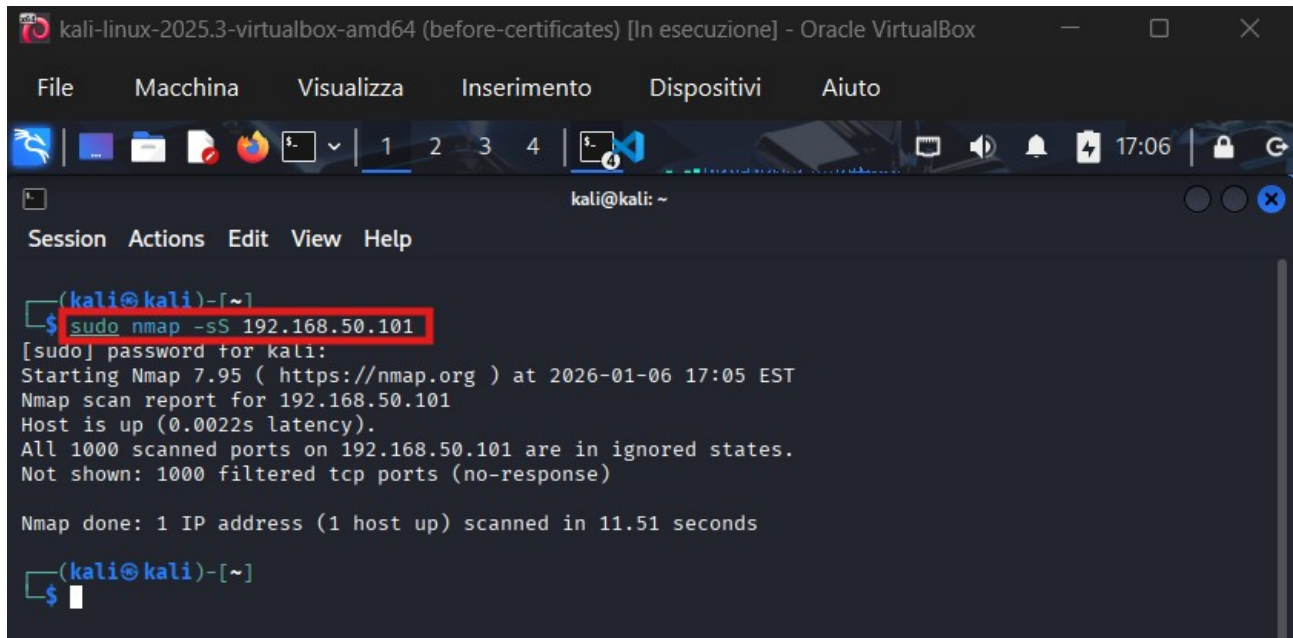
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.66 seconds
(kali@kali)-[~]
$
```

6. SYN Scan su Metasploitable

È stata eseguita una scansione SYN tramite il comando:

`sudo nmap -sS 192.168.50.101`

Questa scansione serve a individuare le porte TCP aperte con una tecnica half-open. Il risultato ha mostrato porte filtrate o senza risposta.



```
kali-linux-2025.3-virtualbox-amd64 (before-certificates) [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
1  2  3  4
kali@kali: ~
Session  Actions  Edit  View  Help
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 17:05 EST
Nmap scan report for 192.168.50.101
Host is up (0.0022s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

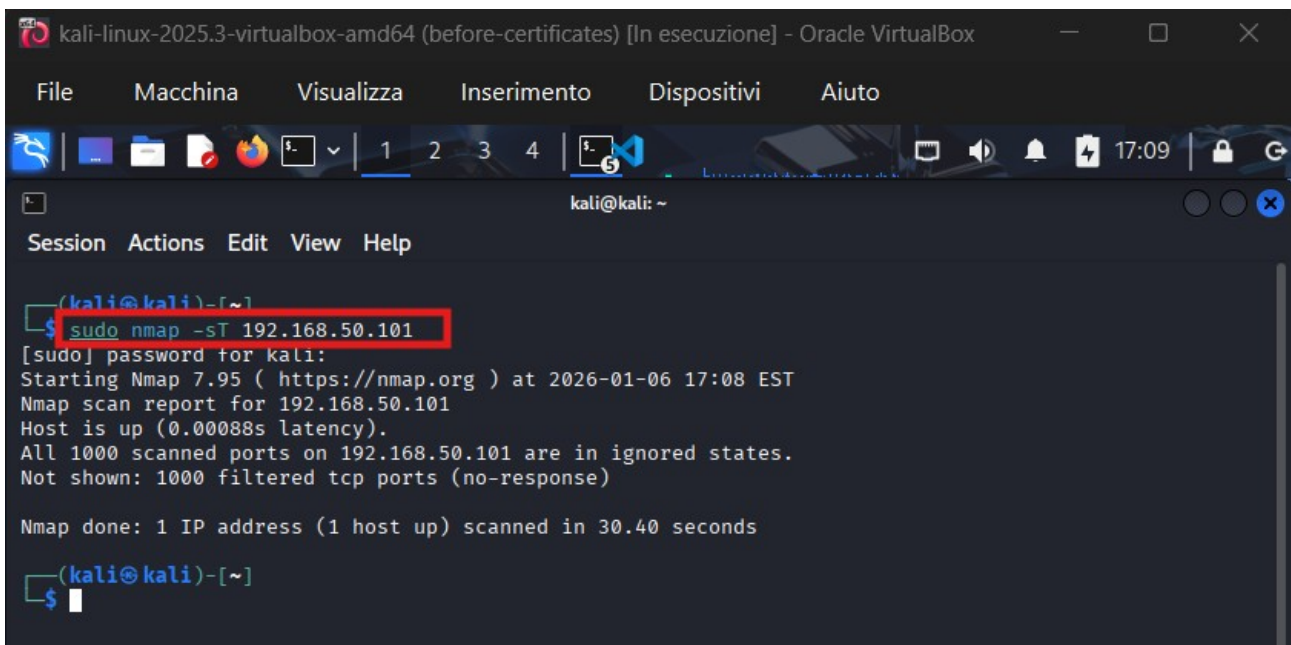
Nmap done: 1 IP address (1 host up) scanned in 11.51 seconds
(kali@kali)-[~]
$
```

7. TCP Connect Scan su Metasploitable

Successivamente è stata eseguita una TCP Connect Scan con il comando:

`sudo nmap -sT 192.168.50.101`

Il risultato è stato simile alla SYN scan: non sono emerse differenze nelle porte individuate, ma cambia il metodo utilizzato per la scansione.



```
kali-linux-2025.3-virtualbox-amd64 (before-certificates) [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
1  2  3  4
kali@kali: ~
Session  Actions  Edit  View  Help
(kali@kali)-[~]
$ sudo nmap -sT 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 17:08 EST
Nmap scan report for 192.168.50.101
Host is up (0.00088s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

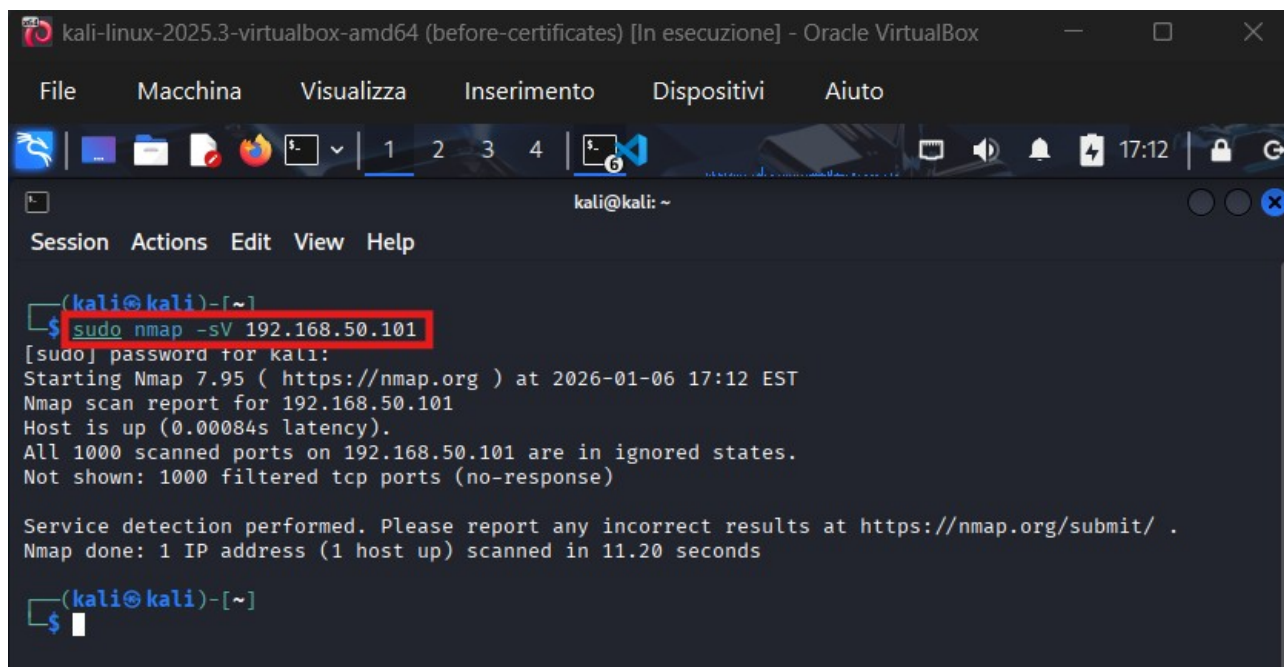
Nmap done: 1 IP address (1 host up) scanned in 30.40 seconds
(kali@kali)-[~]
$
```


8. Version Detection su Metasploitable

È stata effettuata la rilevazione dei servizi e delle versioni tramite:

`sudo nmap -sV 192.168.50.101`

La scansione è stata completata, ma non sono state rilevate versioni specifiche dei servizi, poiché non sono state trovate porte open con banner utili.

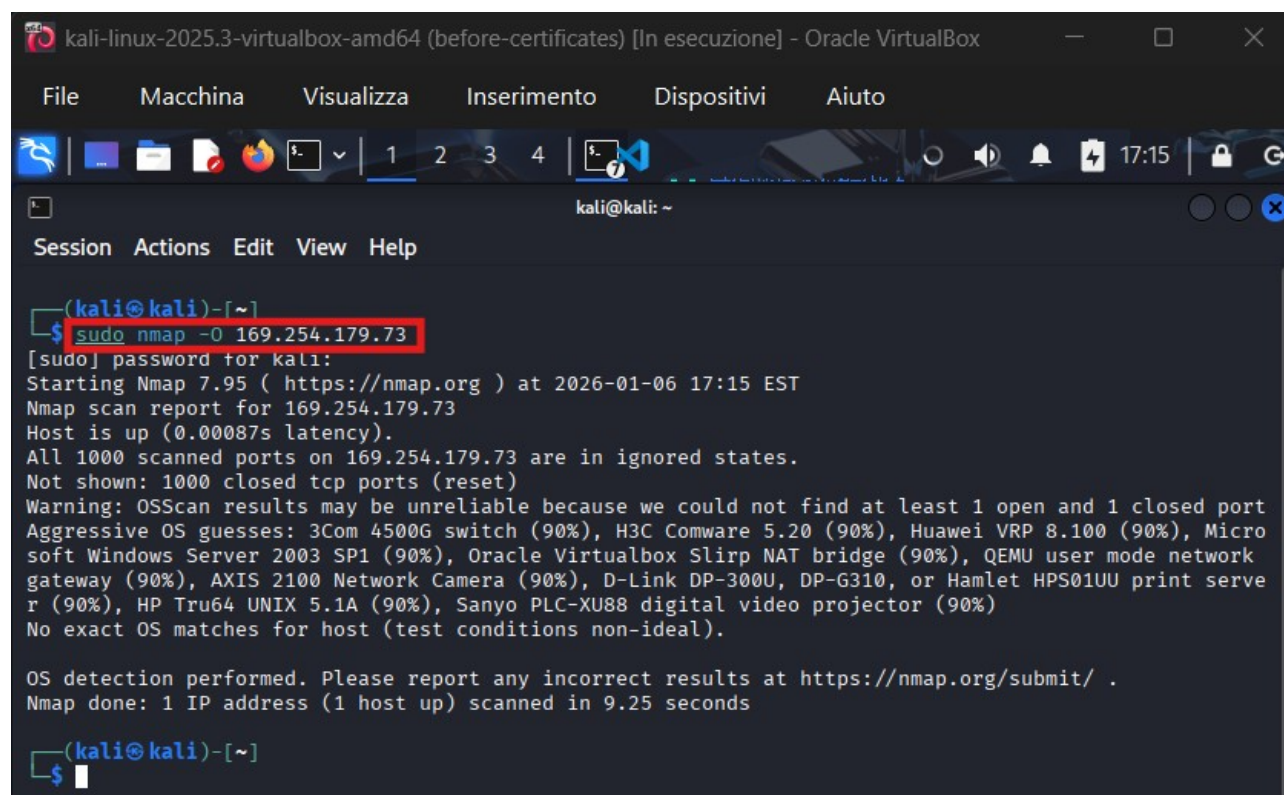


```
kali-linux-2025.3-virtualbox-amd64 (before-certificates) [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
1  2  3  4  5  6
kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sV 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 17:12 EST
Nmap scan report for 192.168.50.101
Host is up (0.00084s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.20 seconds
(kali@kali)-[~]
$
```

9. OS Fingerprint su Windows XP

Infine è stato eseguito l'OS fingerprinting su Windows XP con il comando: Anche in questo caso Nmap ha indicato che il risultato non è completamente affidabile, ma l'host è risultato attivo e raggiungibile.



```
kali-linux-2025.3-virtualbox-amd64 (before-certificates) [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
1  2  3  4  5  6
kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -O 169.254.179.73
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 17:15 EST
Nmap scan report for 169.254.179.73
Host is up (0.00087s latency).
All 1000 scanned ports on 169.254.179.73 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (90%), H3C Comware 5.20 (90%), Huawei VRP 8.100 (90%), Micro
soft Windows Server 2003 SP1 (90%), Oracle Virtualbox Slirp NAT bridge (90%), QEMU user mode network
gateway (90%), AXIS 2100 Network Camera (90%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print serve
r (90%), HP Tru64 UNIX 5.1A (90%), Sanyo PLC-XU88 digital video projector (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
(kali@kali)-[~]
$
```

Conclusione:

In conclusione, l'esercizio ha permesso di applicare le principali tecniche di scansione con Nmap. Sono stati identificati gli indirizzi IP dei target, verificata la connettività e svolte le scansioni richieste.

N.B: L'assenza di porte open e di informazioni dettagliate sui servizi non è dovuta a un errore di scansione, ma alle condizioni dell'ambiente.

In mancanza di risposte sulle porte TCP, Nmap non è in grado di eseguire correttamente la service detection e l'OS fingerprinting risulta parzialmente affidabile. Nonostante ciò, tutte le scansioni richieste dalla traccia sono state eseguite correttamente.