# RELAZIONE ES S5 – L2

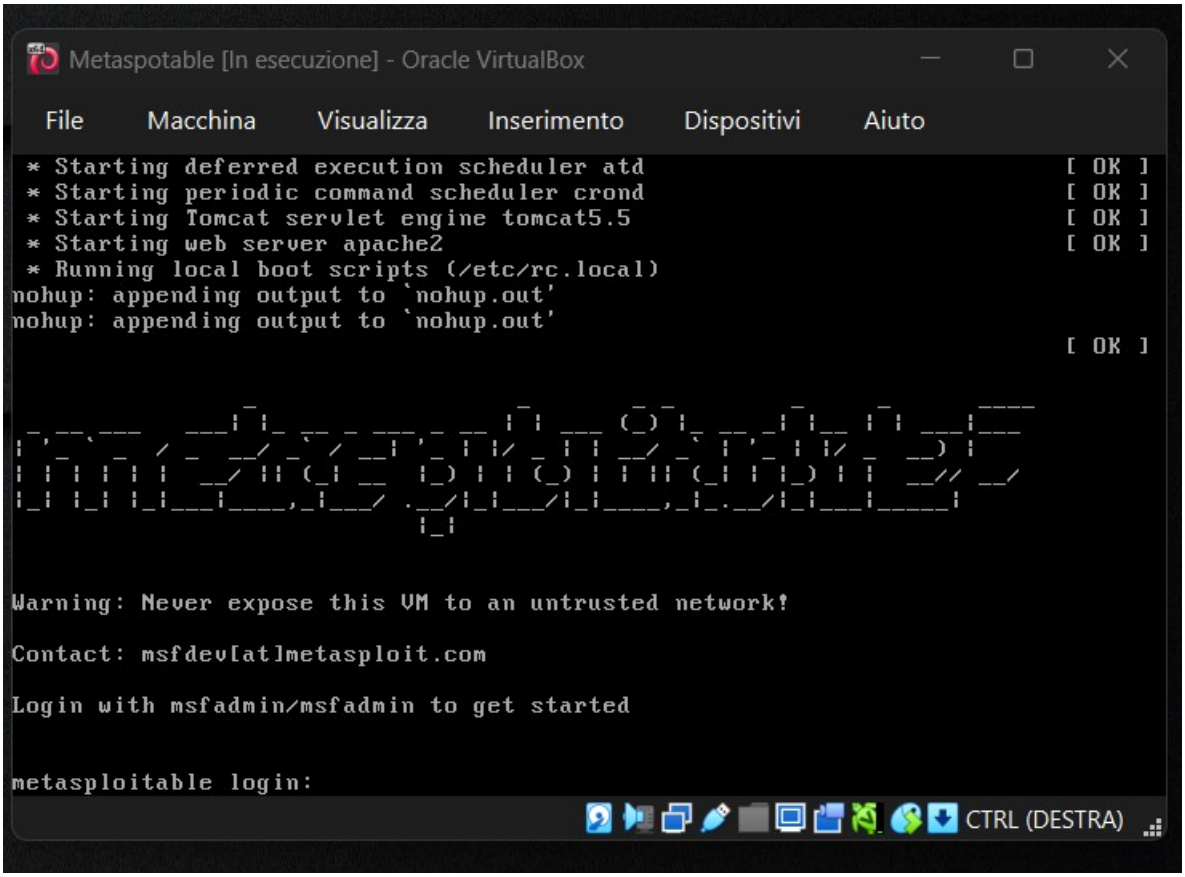
# SCANSIONE DEI SERVIZI CON NMAP su target Metasploitable

## 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.

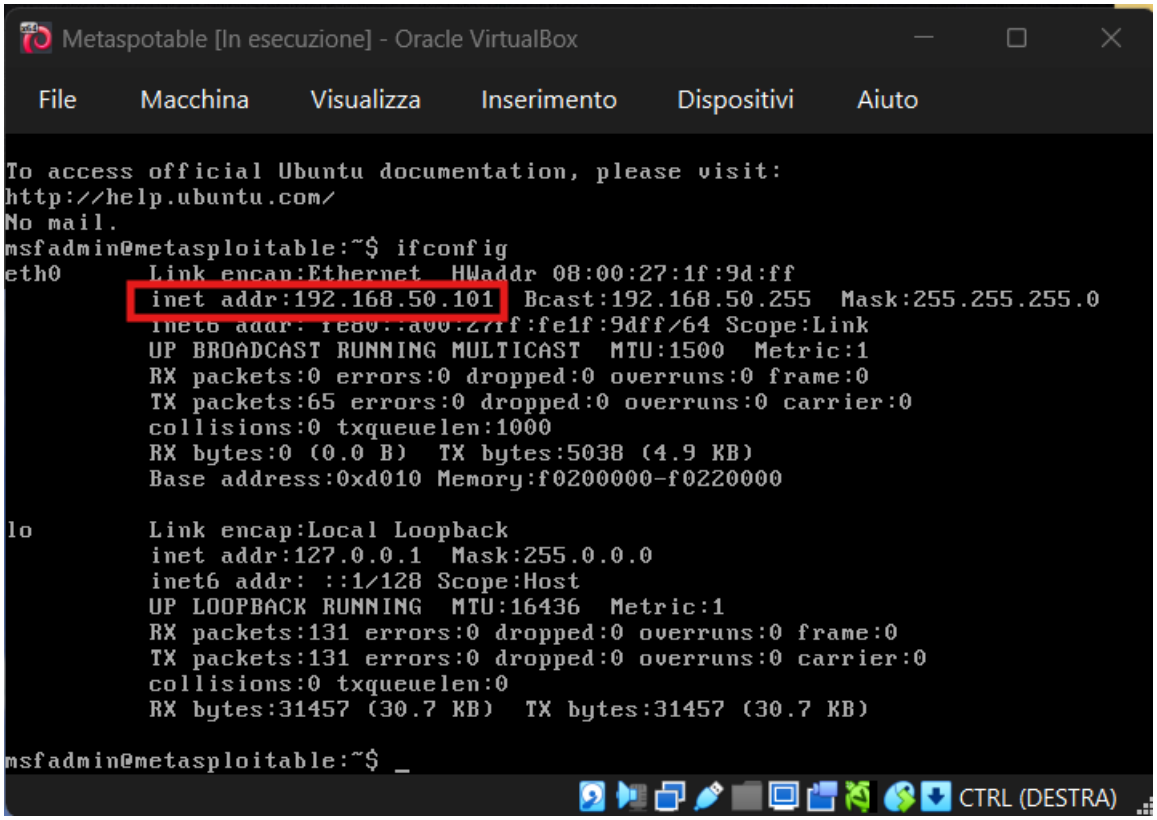
### 1. Avvio di Metasploitable

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.



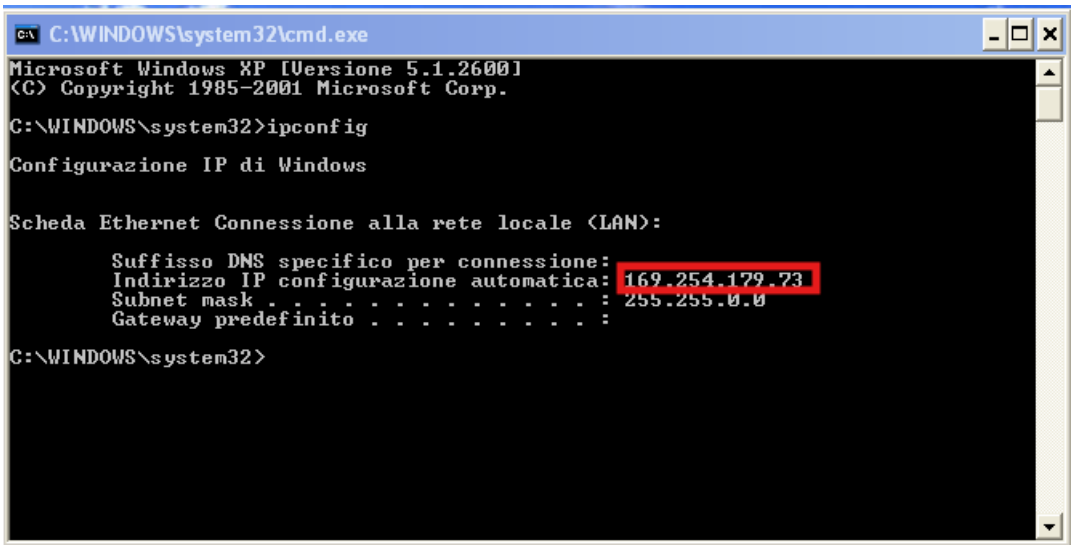
## 2. Identificazione IP di Metasploitable

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**




## 3. Identificazione IP di Windows XP

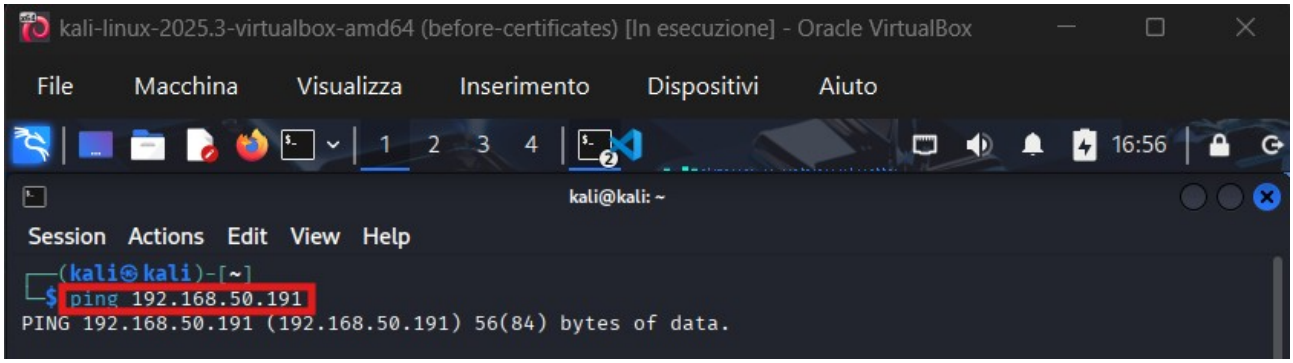
Su Windows XP è stato aperto il prompt dei comandi ed è stato eseguito il comando *ipconfig*. Il sistema ha restituito il seguente indirizzo IP:
IP Windows XP: **169.254.179.73**



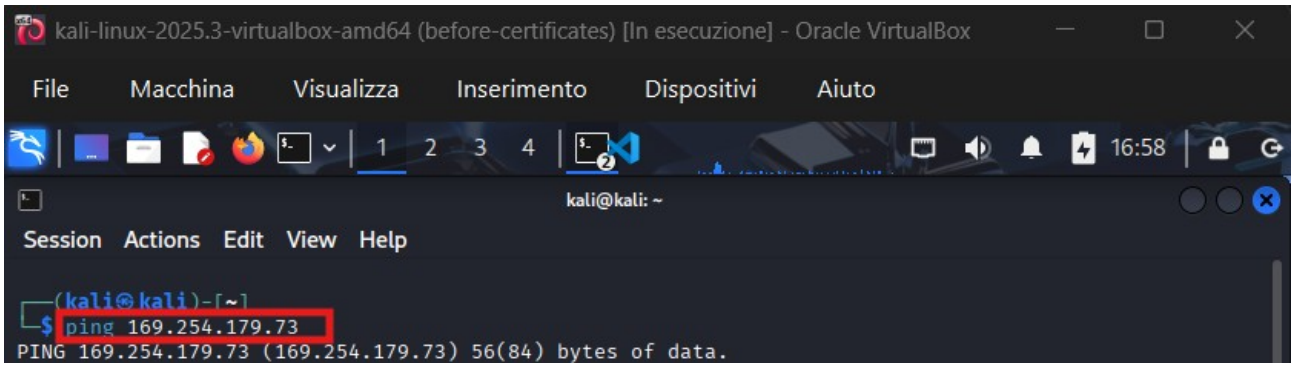
Questo indirizzo è un IP APIPA, assegnato automaticamente in assenza di un server DHCP.

**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:**

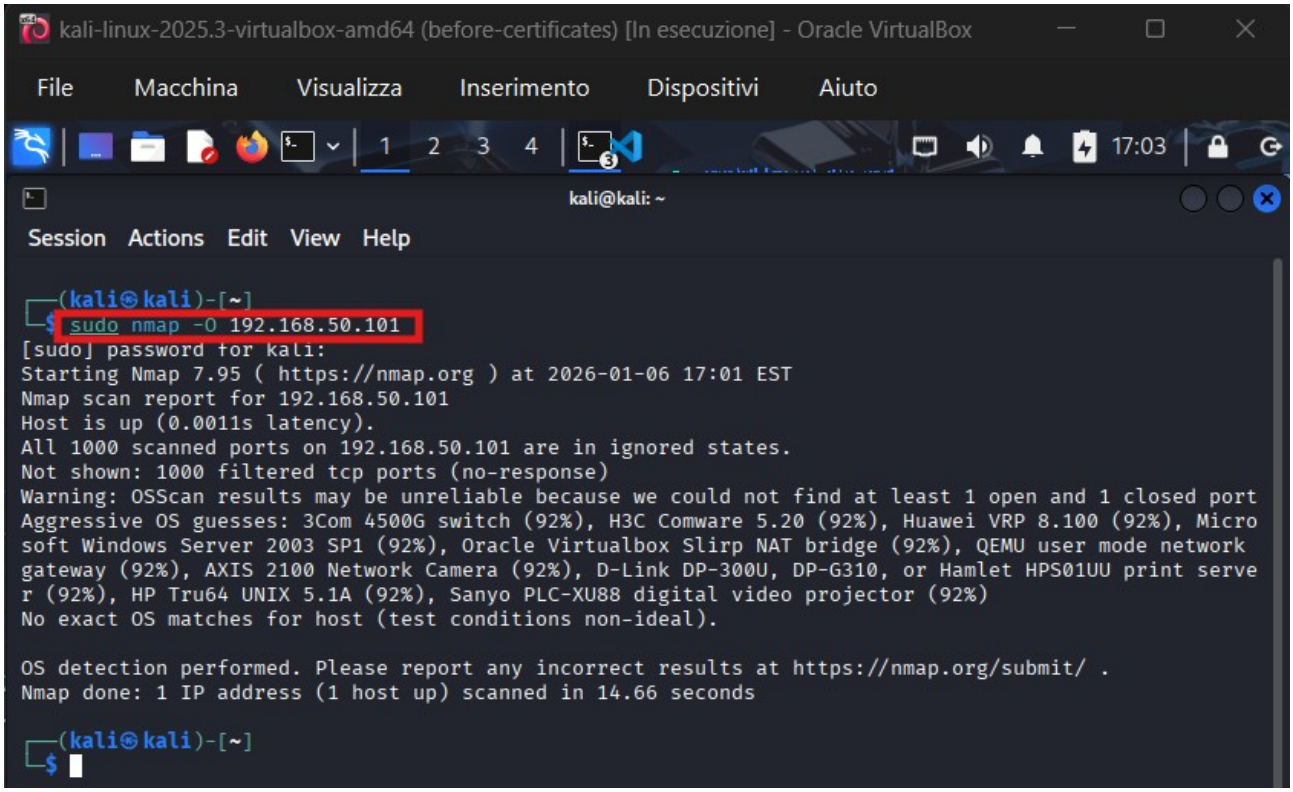



**PING WIN XP:**

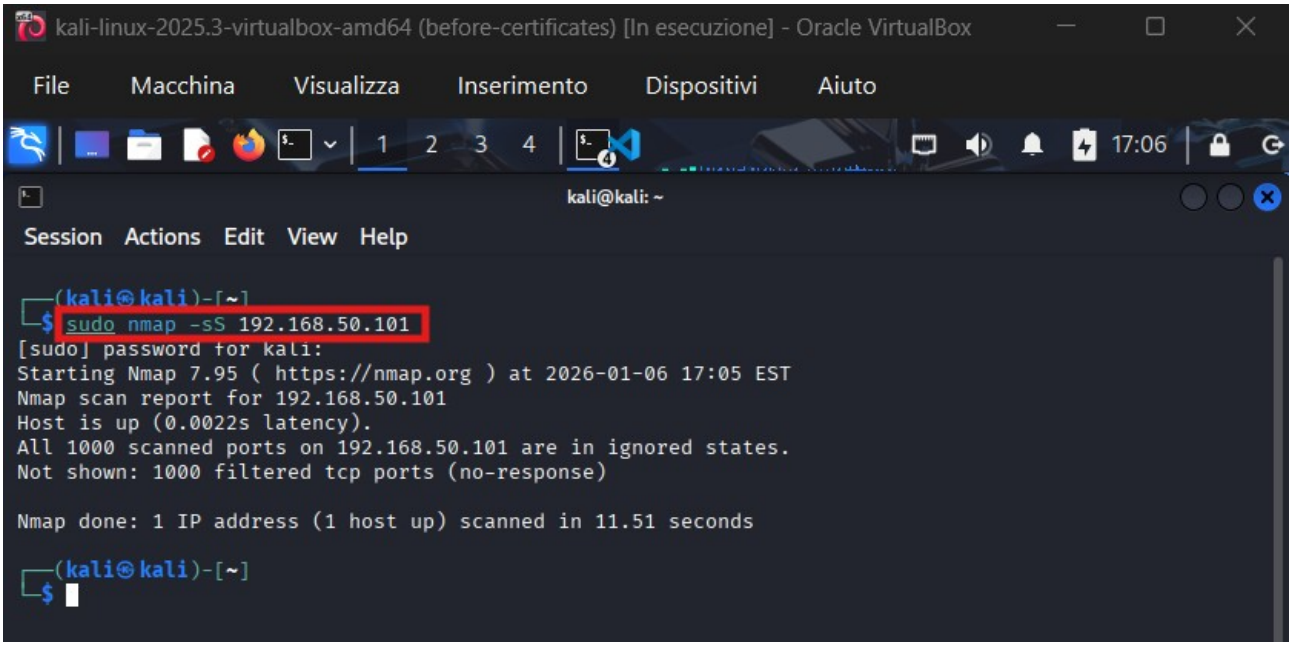


## 5. OS Fingerprint su Metasploitable

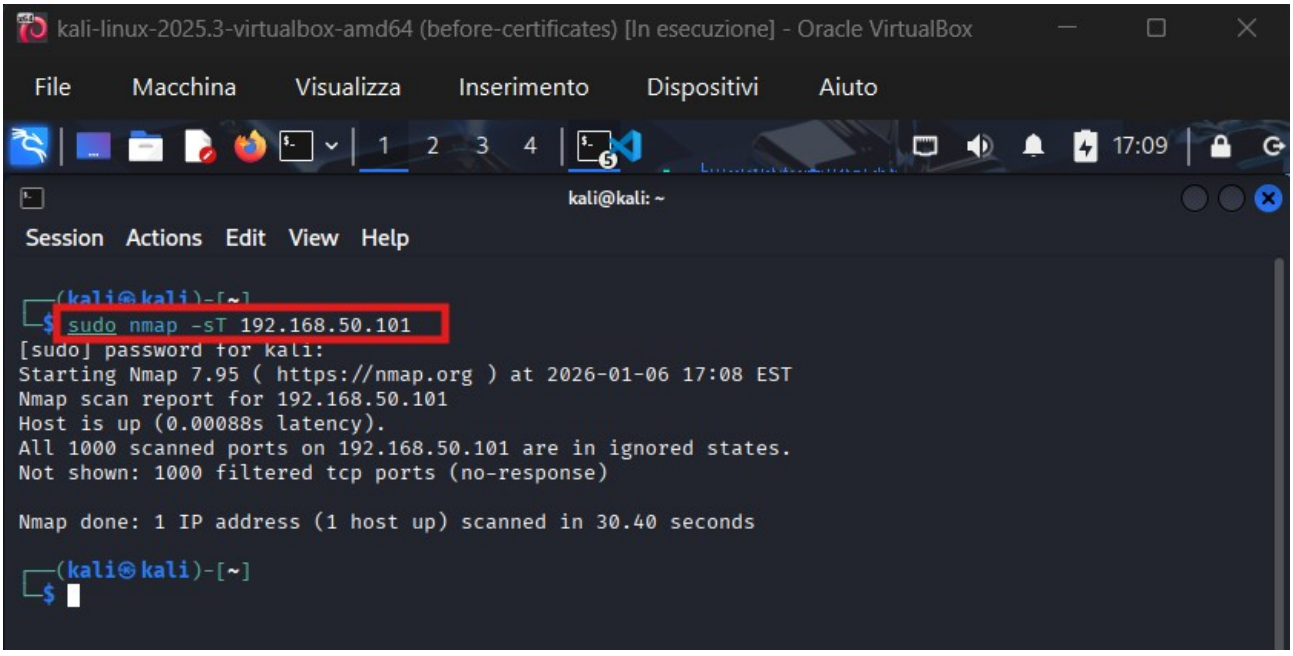
Da Kali Linux è stato eseguito il comando:
***sudo nmap -O 192.168.50.101***
Questa scansione ha avuto lo scopo di identificare il sistema operativo del target. Nmap ha segnalato che i risultati dell'OS detection non sono completamente affidabili a causa della mancanza di porte aperte e chiuse sufficienti.



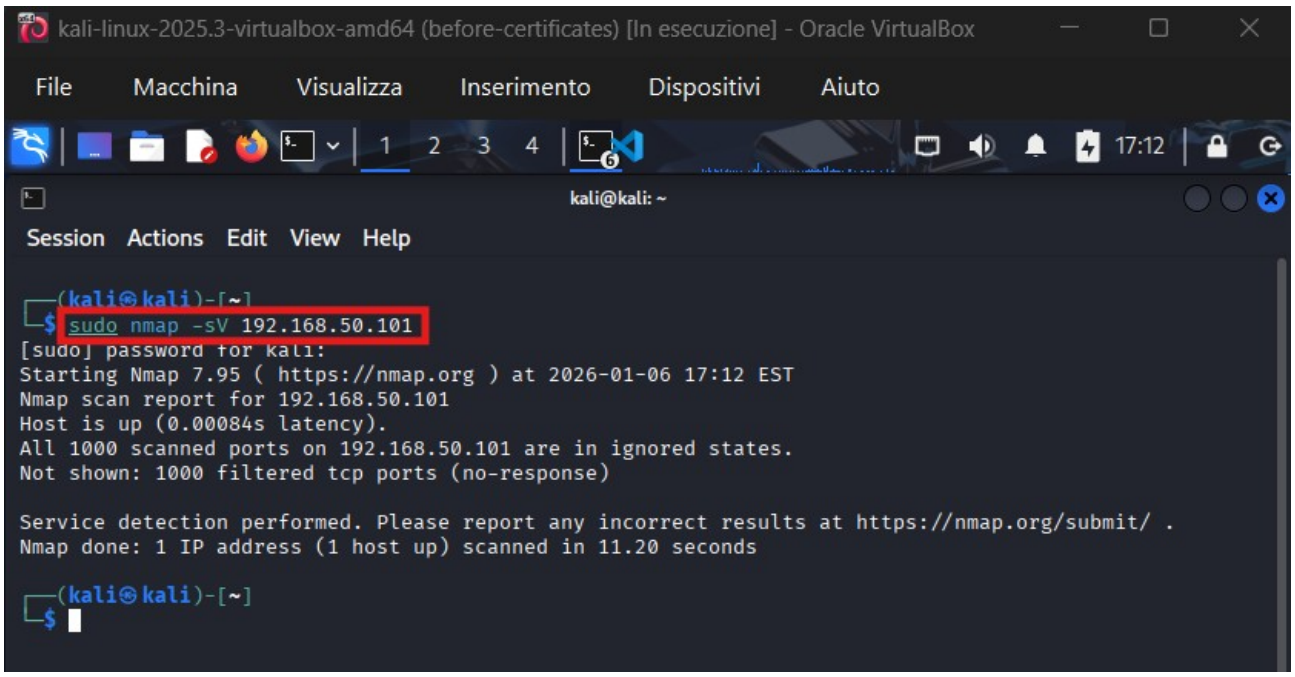
**6. SYN Scan su Metasploitable**
È stata eseguita una scansione SYN tramite il comando:
***sudo nmap -sS 192.168.50.101***
Questa scansione serve a individuare le porte TCP aperte con una tecnica half-open. Il risultato ha
mostrato porte filtrate o senza risposta.



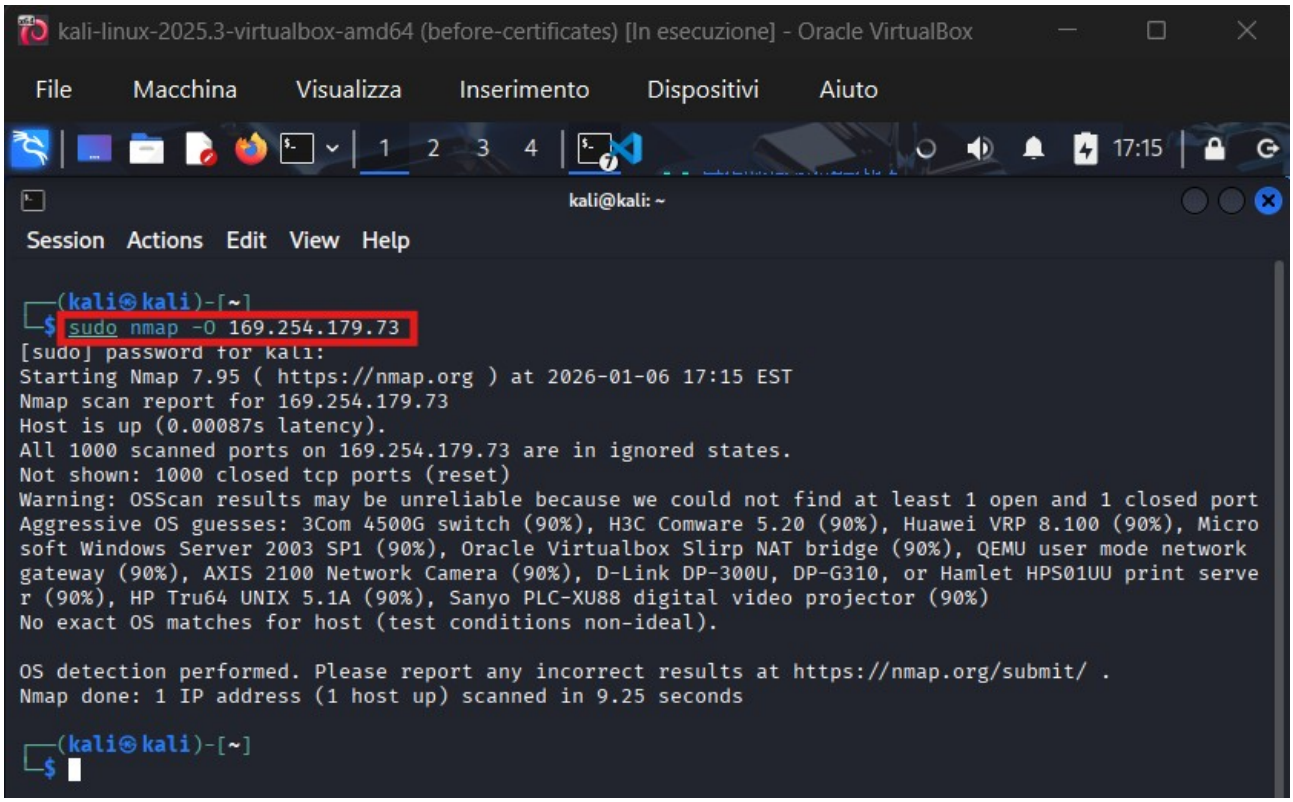

**7. TCP Connect Scan su Metasploitable**
Successivamente è stata eseguita una TCP Connect Scan con il comando:
***sudo nmap -sT 192.168.50.101***
Il risultato è stato simile alla SYN scan: non sono emerse differenze nelle porte individuate, ma cambia il metodo utilizzato per la scansione.



**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.




**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.



## 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.