Report di Scansione di Rete e Analisi dei Servizi

Data: 29 Luglio 2025

Autore: Marco Falchi

Obiettivo: Eseguire scansioni di rete sui target forniti per identificare sistemi operativi, porte aperte e servizi attivi, come richiesto dall'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.

Target 1: Metasploitable

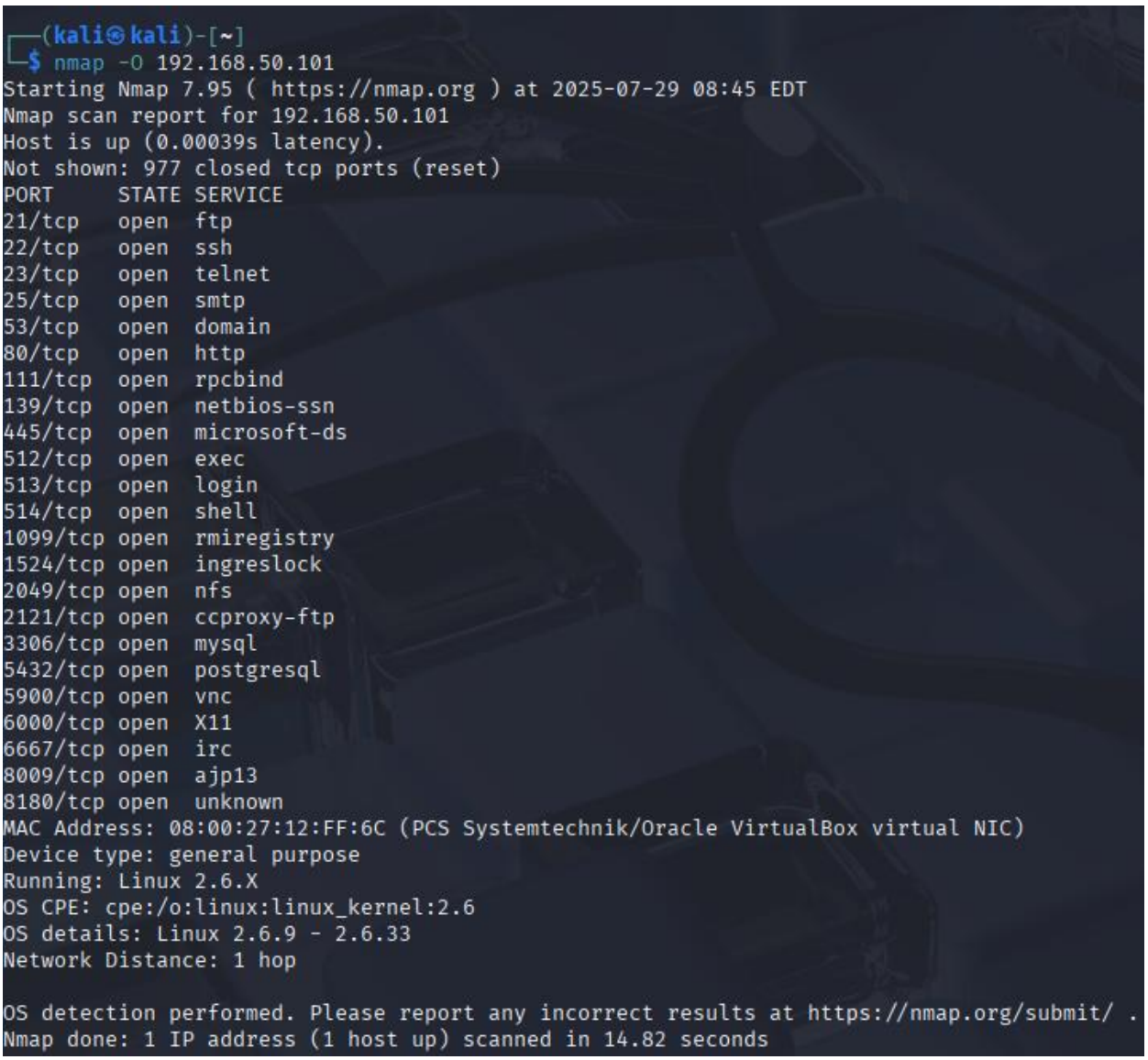
A seguito delle scansioni effettuate sul target Metasploitable, sono state raccolte le seguenti informazioni dall'ip:

- **IP: 192.168.50.101**

1.1 OS Fingerprinting

Questa scansione identifica il sistema operativo del target:

- **Comando:** nmap -O 192.168.50.101

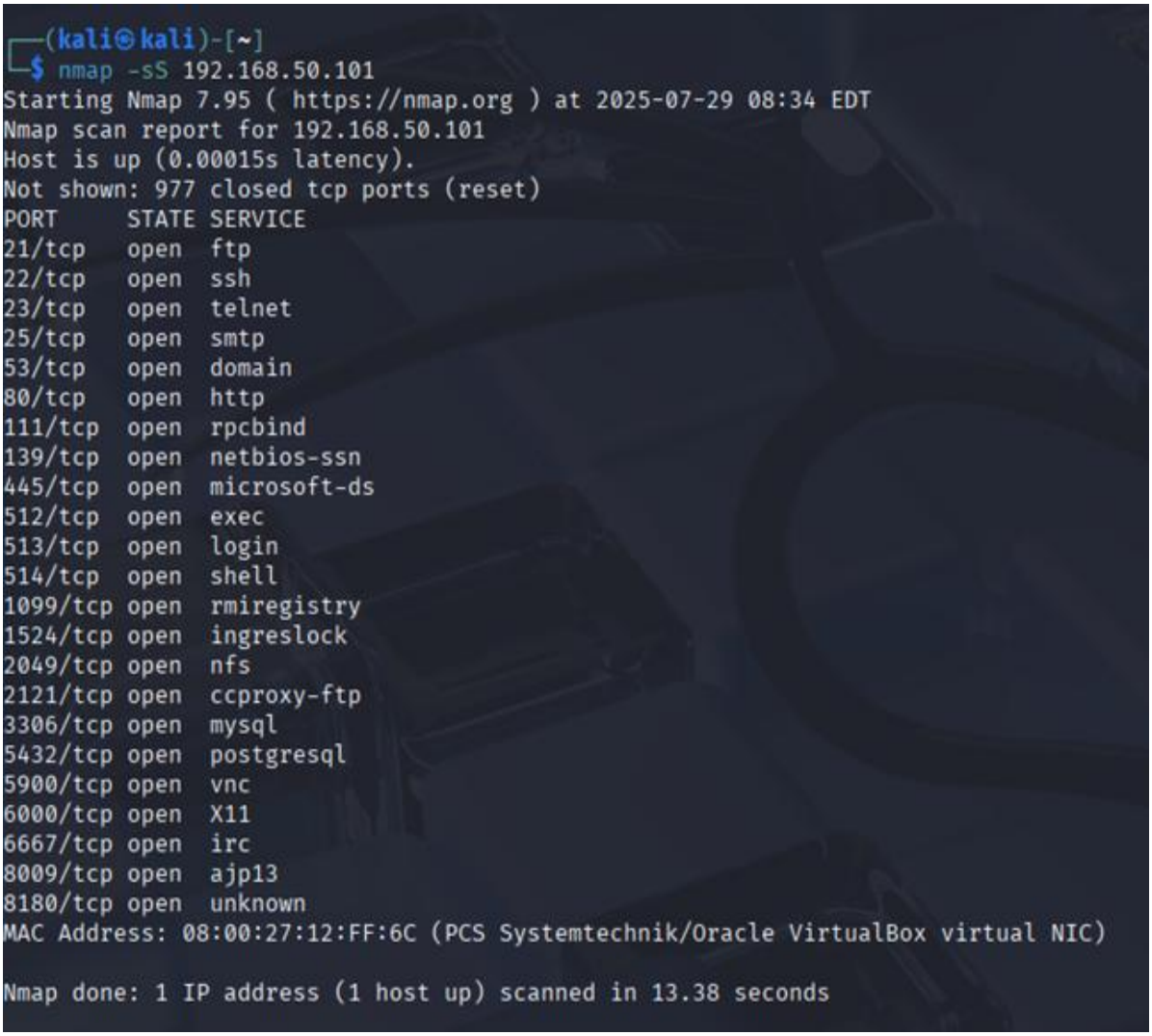


- **Sistema Operativo trovato:** Linux 2.6.9 – 2.6.33

1.2 SYN Scan

Lo SYN scan è un tipo di scansione furtiva che non completa la connessione TCP, rendendola meno facilmente rilevabile

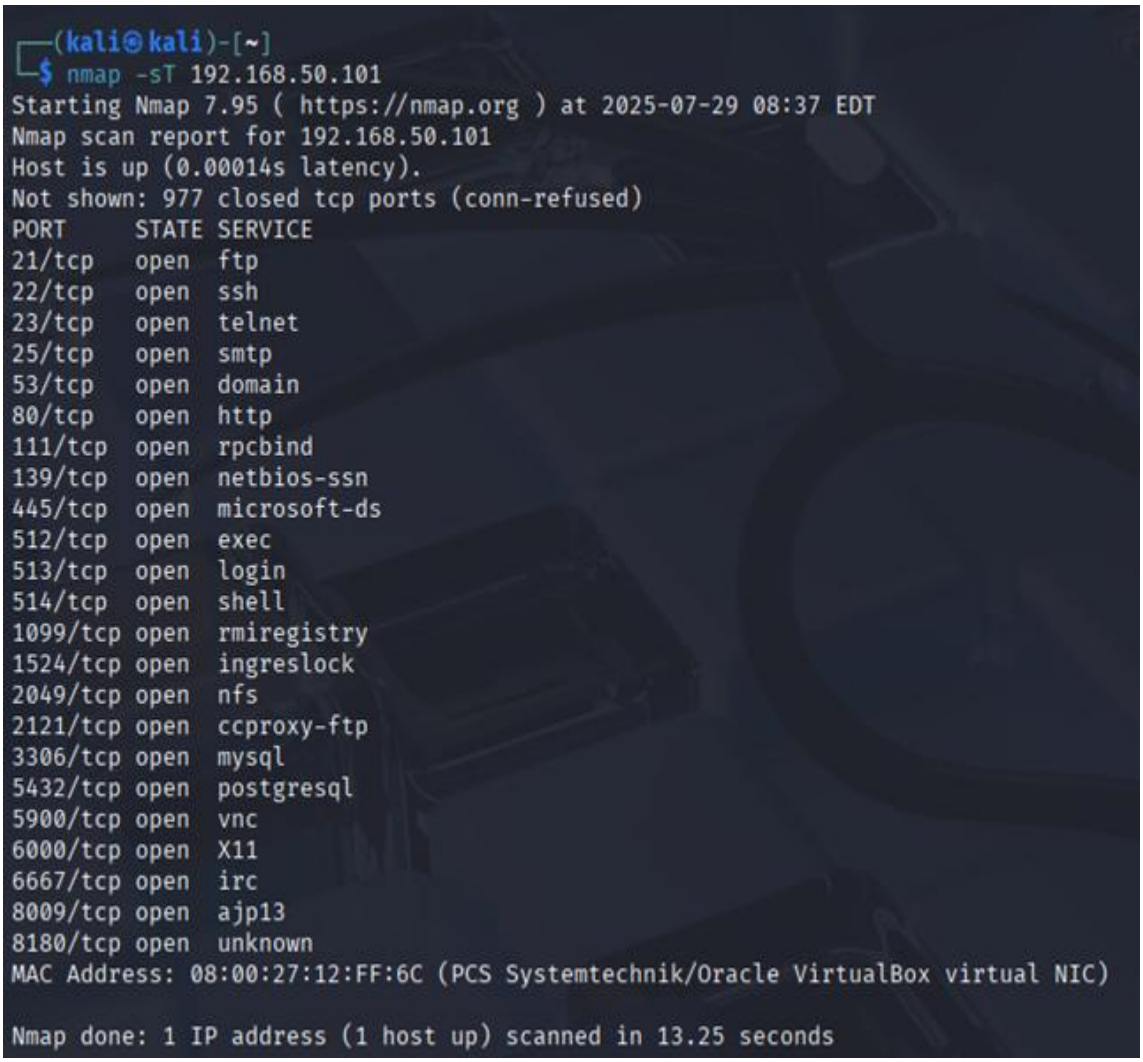
- **Comando:** nmap -sS 192.168.50.101



1.3. TCP Connect Scan

A differenza dello SYN scan, questa tecnica completa la connessione TCP a tre vie. È più rumorosa ma può essere più affidabile in certi contesti.

- **Comando:** nmap -sT 192.168.50.101



Differenze tra i risultati di TCP Connect e SYN Scan:

Le differenze tra queste due scansioni sono generalmente:

-Velocità: Lo SYN scan è spesso più veloce perché non completa la connessione.

-Rilevabilità: Lo SYN scan è considerato "stealth" o furtivo perché non stabilisce una sessione TCP completa, generando meno log sui sistemi target. Il TCP Connect scan, invece, è facilmente registrabile dai firewall e dai sistemi di rilevamento delle intrusioni.

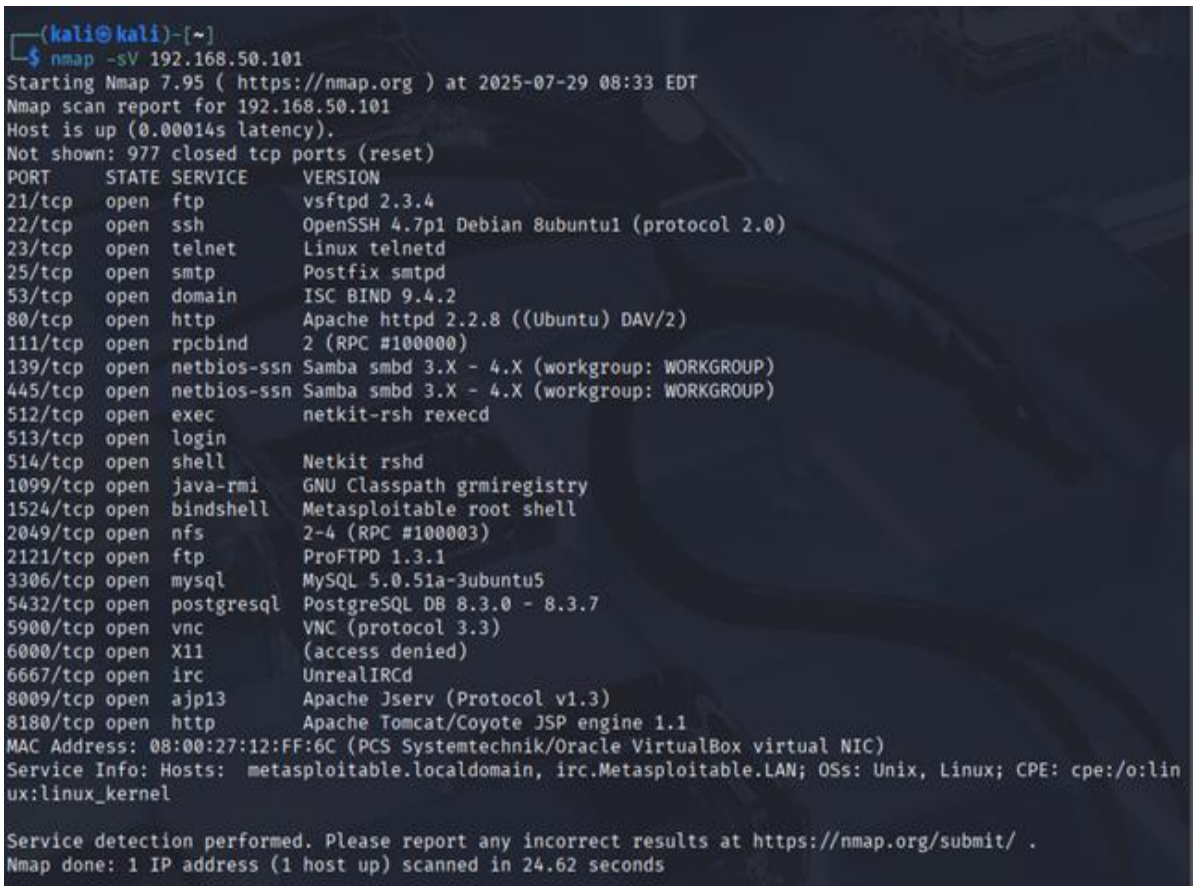
-Privilegi: Per eseguire uno SYN scan (-sS) sono necessari i privilegi di root (o amministratore), mentre un TCP Connect scan (-sT) può essere eseguito da un utente standard.

I risultati in termini di porte aperte dovrebbero essere identici. Qualsiasi differenza potrebbe indicare la presenza di un firewall o di un IDS/IPS che blocca specificamente i pacchetti SYN.

1.4 Version Detection

Questa scansione non solo rileva le porte aperte, ma interroga anche i servizi in esecuzione per determinarne la versione software

- **Comando:** nmap -sV 192.168.50.101



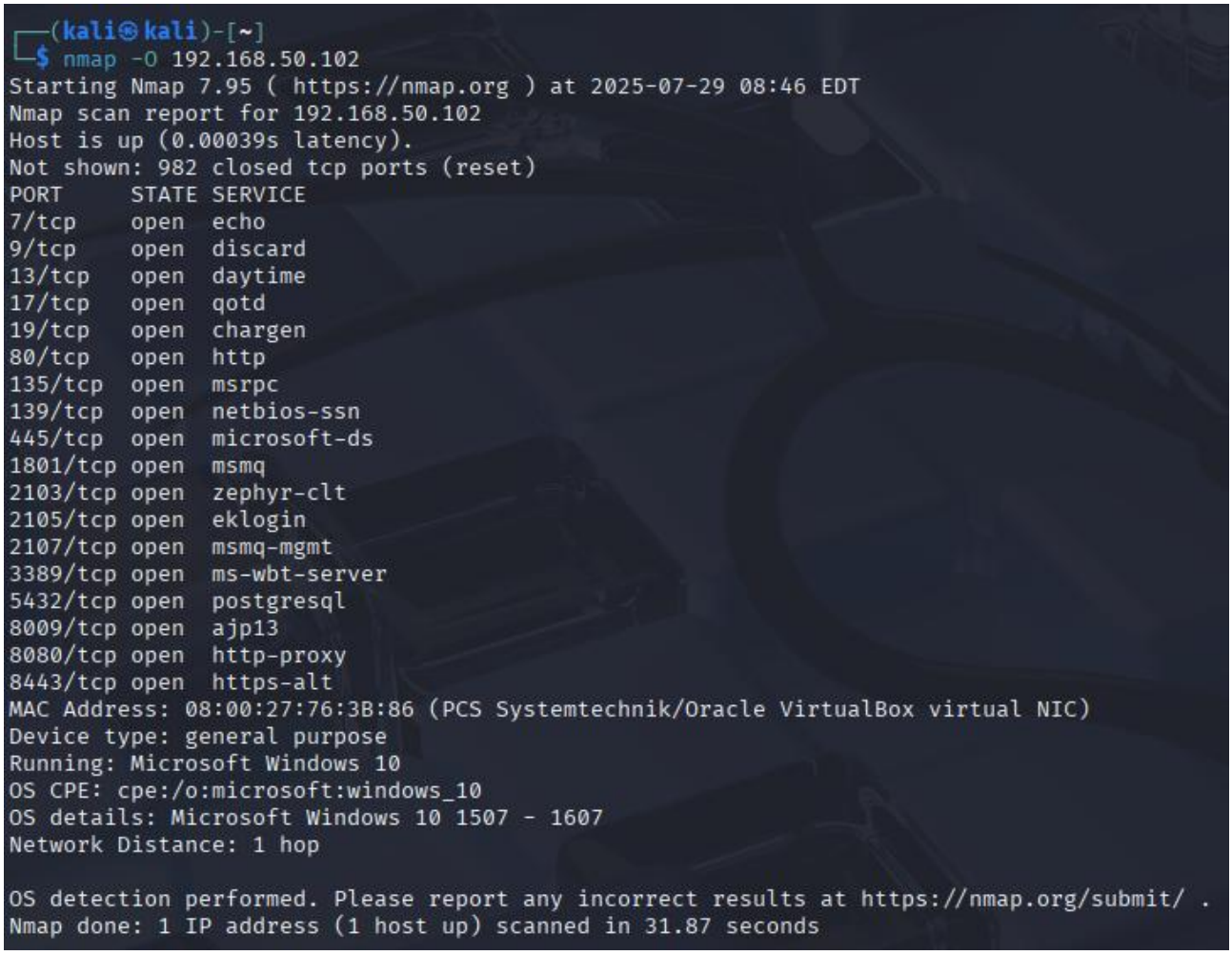
Target 2: Windows

A seguito delle scansioni effettuate sul target Metasploitable, sono state raccolte le seguenti informazioni dall'ip:

- **IP:** 192.168.50.102

2.1 OS Fingerprinting

Comando: nmap -O 192.168.50.102



- **Sistema Operativo trovato:** Windows 10 1507-1607