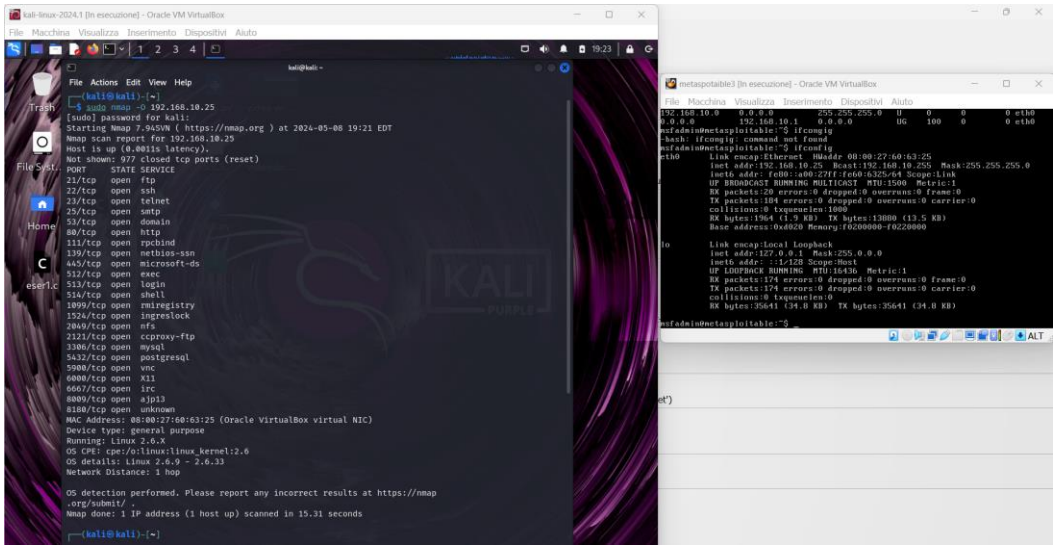
S3L5 - TECNICHE DI SCANSIONE CON NMAP

- Target: Metaspotaible (192.168.10.25) Effettuare scansioni: OS fingerprint, Syn Scan, TCP connect differenze con Syn Scan), Version detection
- Target: Windows 7 (192.168. = Efettuare scansioni: OS fingerprint
- Quesito extra: Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

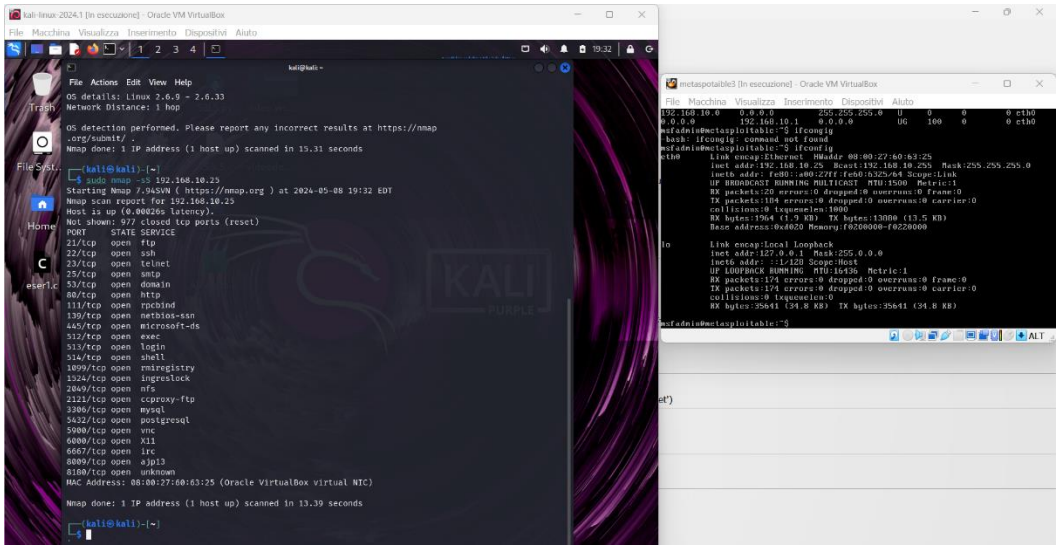
Metaspotaible - Uso OS Fingerprinting



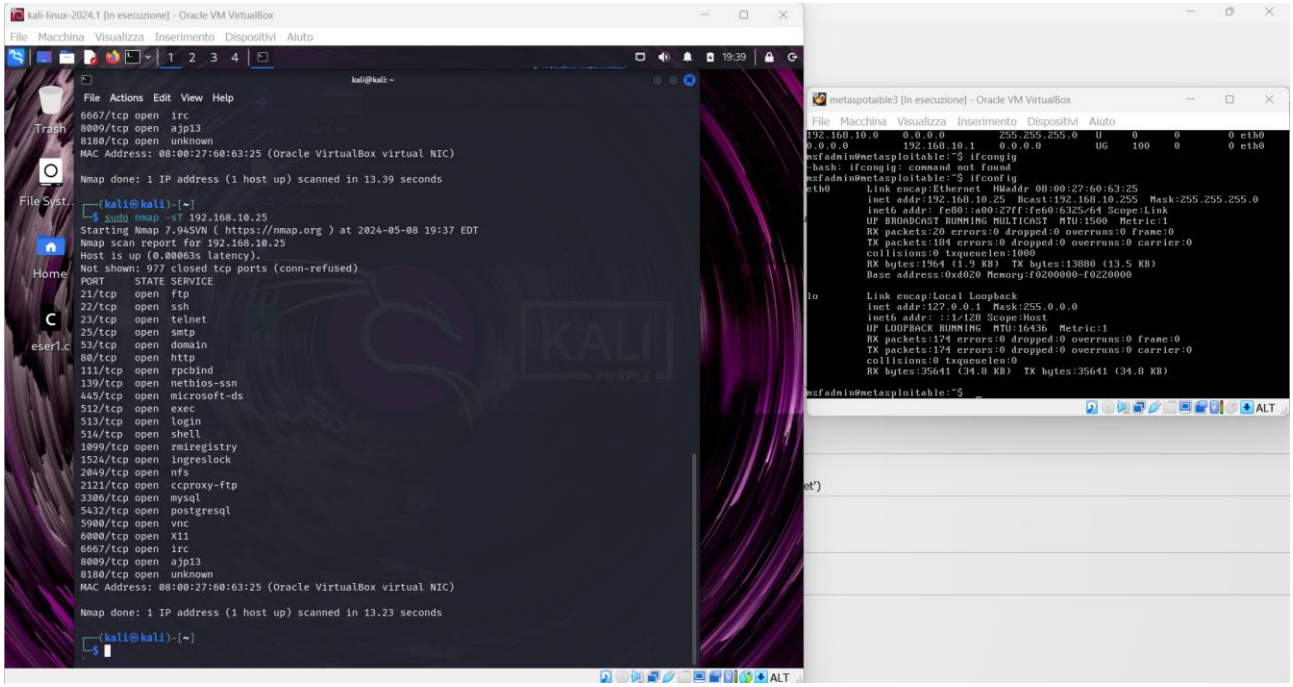
In questa scansione con l'uso de comando "nmap -O" questa funzionalitá stima lo stato della porta e anche il servizio es cerca di fare una scansione per capire il sistema operativo.

Metaspotaible - Uso Syn Scan

Questo comando "nmap -sS" questa funzionalitá riesce a recuperare informazioni sullo stato della porta ma non fa una scansione completa quindi manda solo la richiesta syn e aspetta una risposta



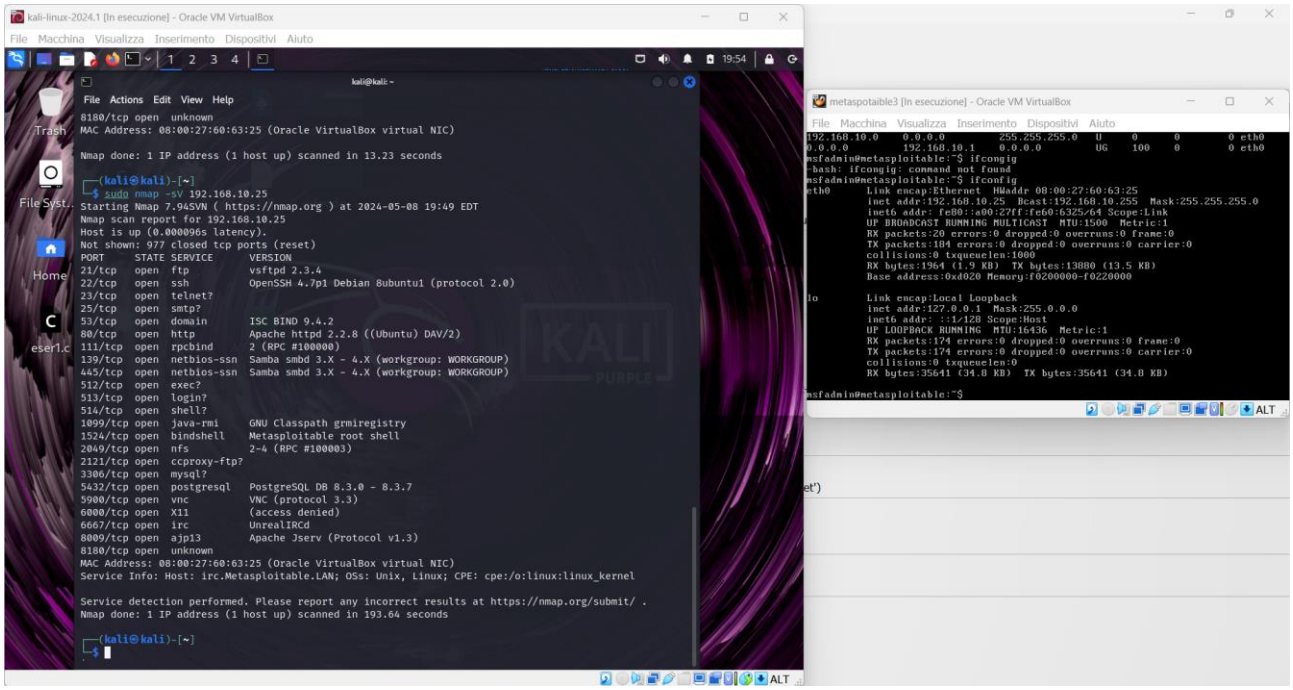
Metaspotaible - Uso TCP connect



Questo comando “nmap -sT” questa funzionalitá riesce a fare la scansione completa rispetto al -sS quindi usa il protocollo TCP

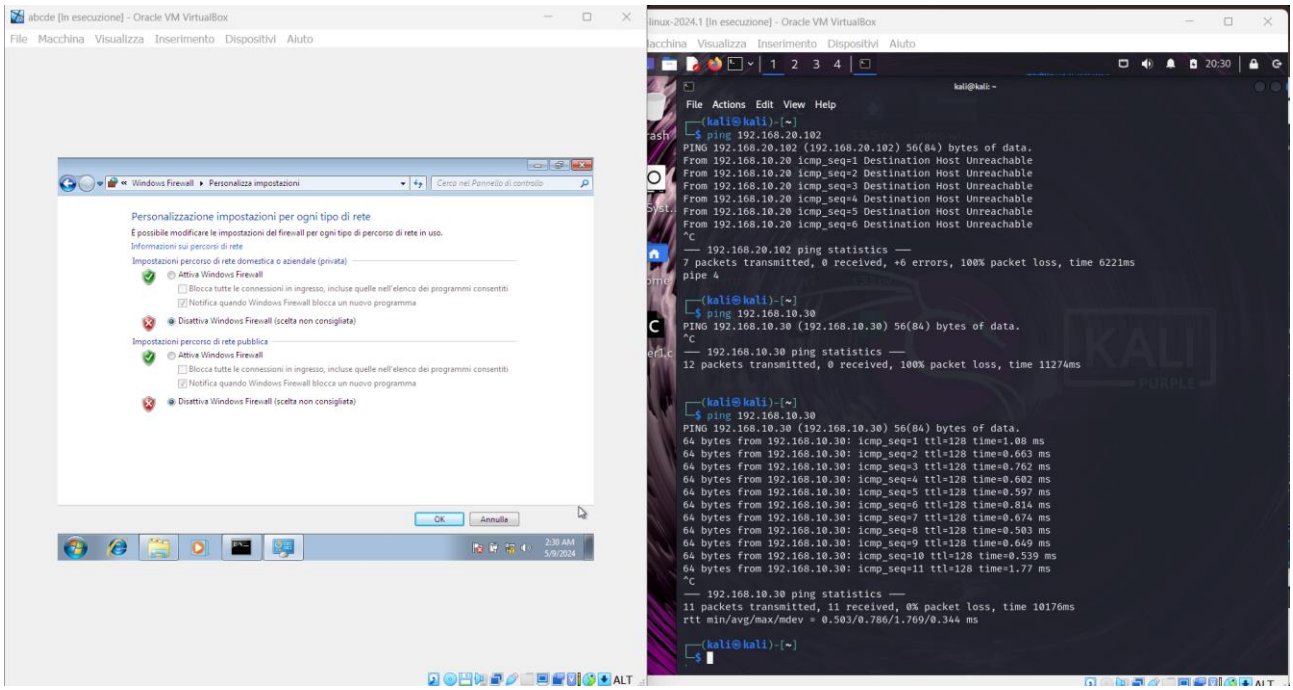
- **Domanda**: Trovate differenze tra i risultati delle scansioni TCP connect e SYN?
  No, può essere perché il host e la rete rispondono allo stesso modo o magari perché Metasploitable è un ambiente di prova/formazione e la macchina è configurata così.

Metaspotaible - Uso Version Detection

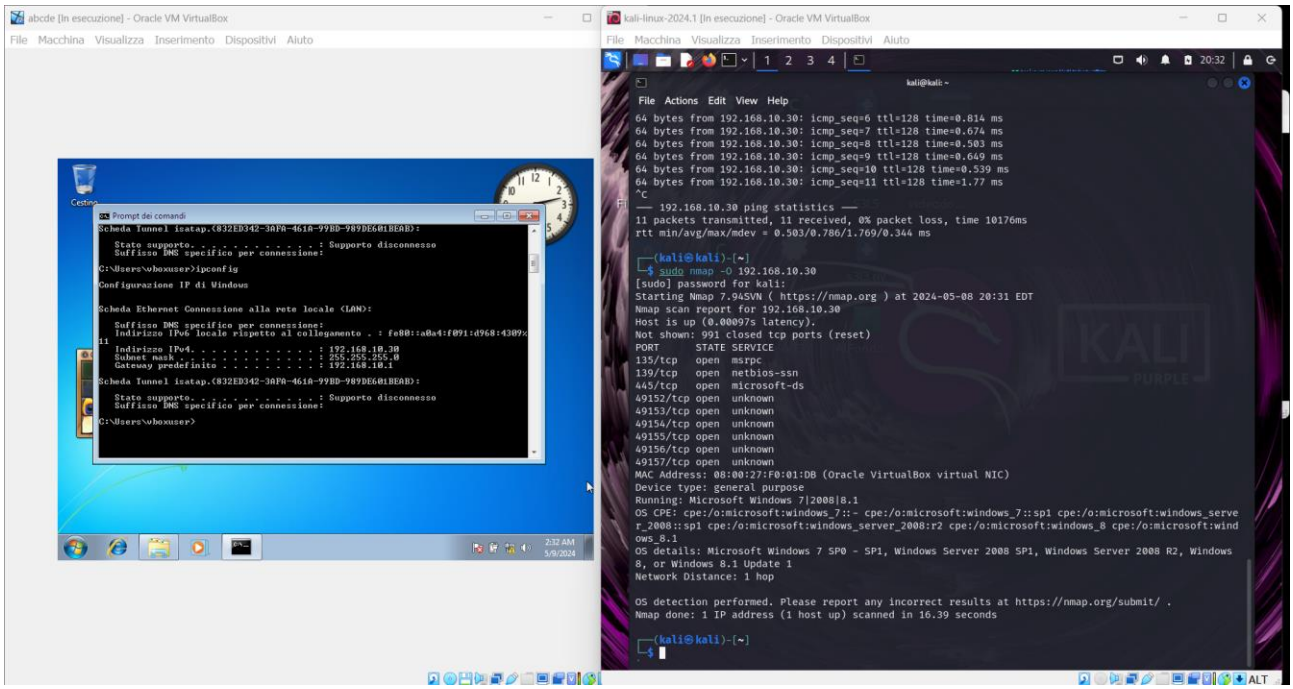


Col comando “nmap -sV” non solo recuperiamo i servizi ma anche le versioni e altri dettagli.

Windows – Uso OS Fingerprinting



Disattivando il firewall di windows sono riuscita pingarla con kali



Col comando “nmap -O” possiamo vedere il sistema operativo, lo stato delle porte e il servizio. Ci sono alcune porte che sono aperte ma il servizio è sconosciuto.

Quesito extra: Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Il risultato ottenuto ci ha riportato parecchie porte aperte i cui servizi si listano come "unknown" questo può significare che ci sono firewall o regole che bloccano questa informazione o magari il servizio non è incluso nel database. Per capire meglio e dare una soluzione a questo problema possiamo proporre le seguenti idee:

- Usare altri comandi per capire il servizio come, per esempio, il comando -sV che determina la versione e ci fornisci indizi.
- Usare comandi con nmap più dettagliati.
- Fare uso di altri tool come Netcat, Wireshark, ecc.