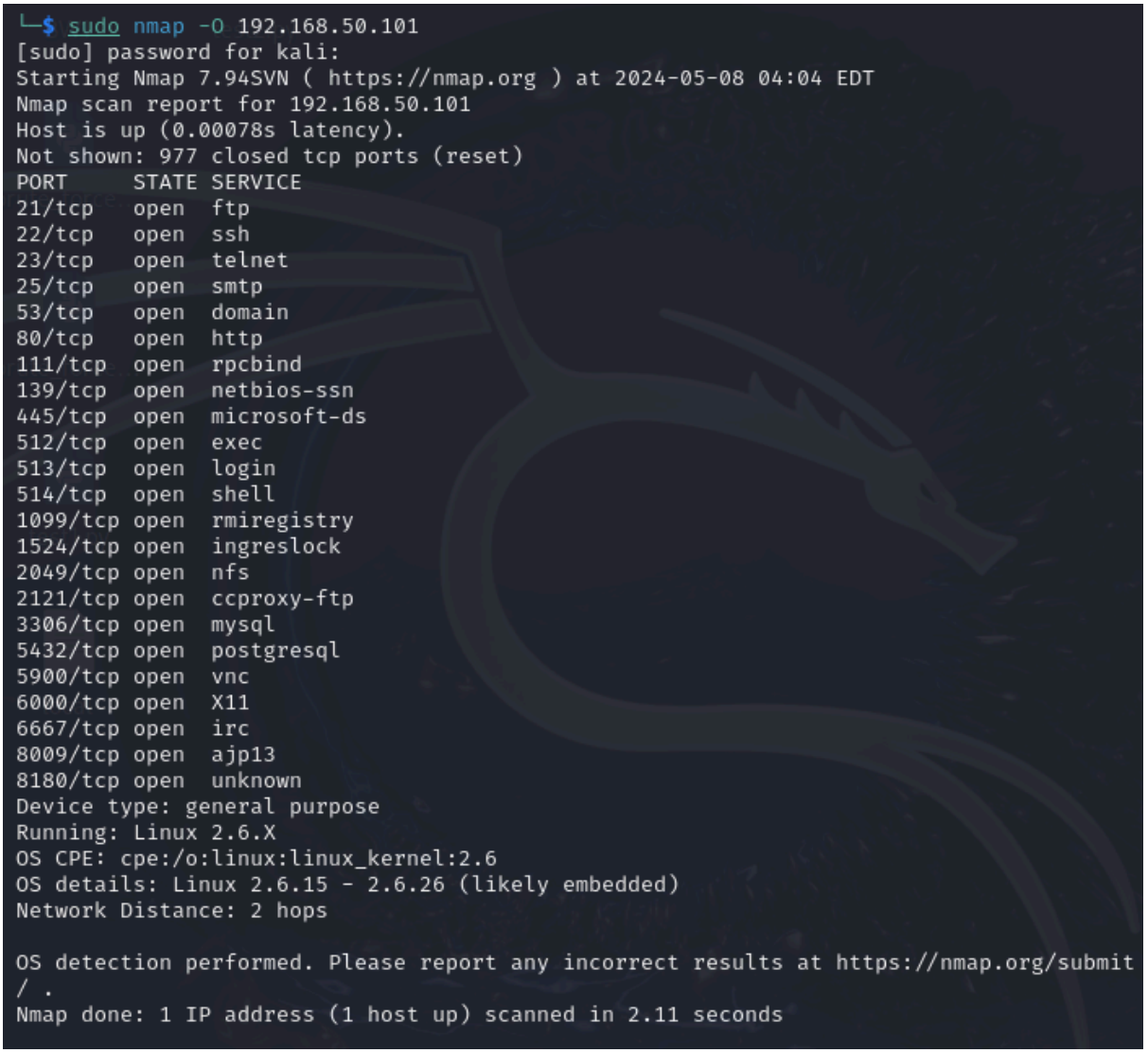
S5L3

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 7:
● OS fingerprint.

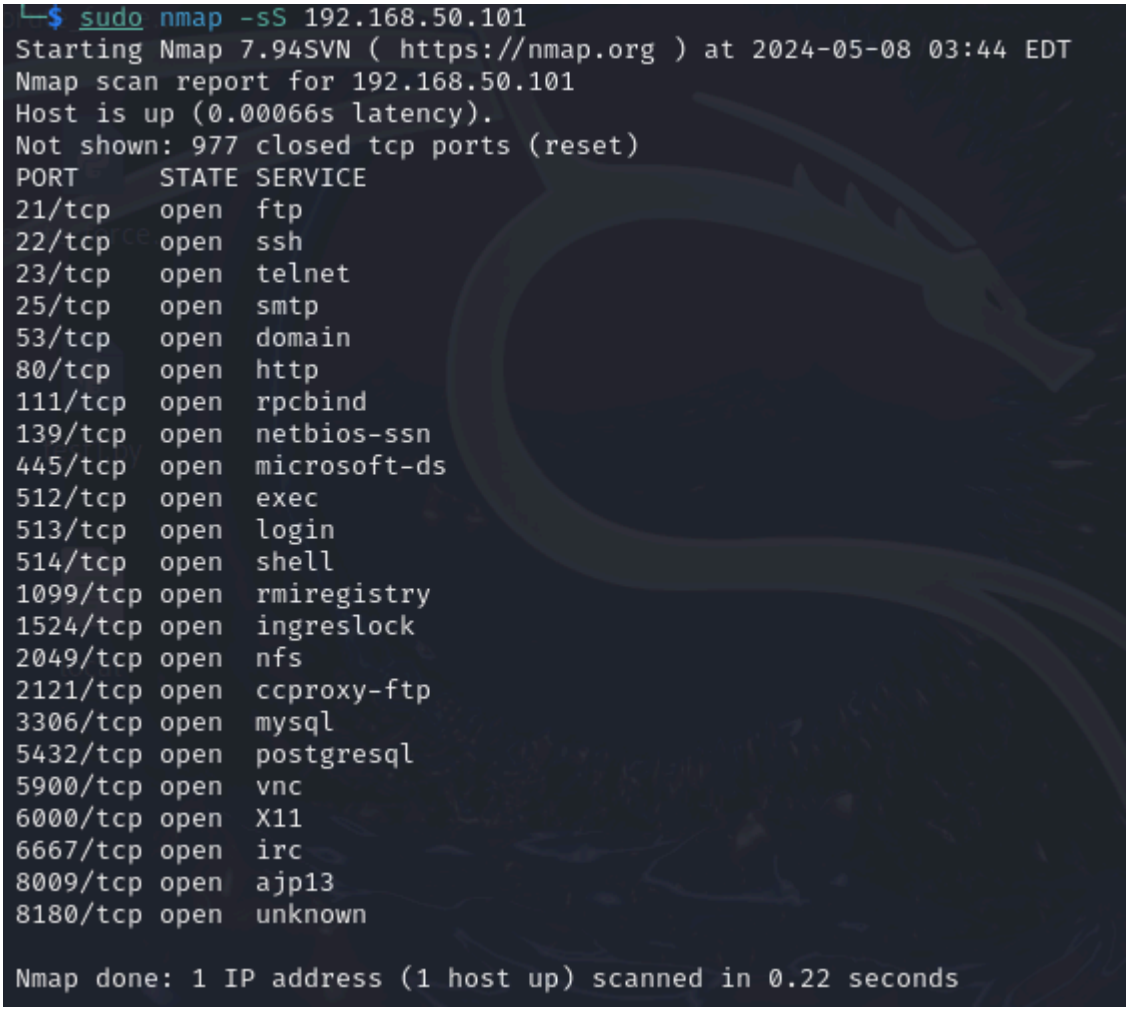
OS fingerprinting: È un processo utilizzato per conoscere il sistema operativo in esecuzione su un host di destinazione sulla base delle caratteristiche delle risposte ricevute durante una scansione di rete.

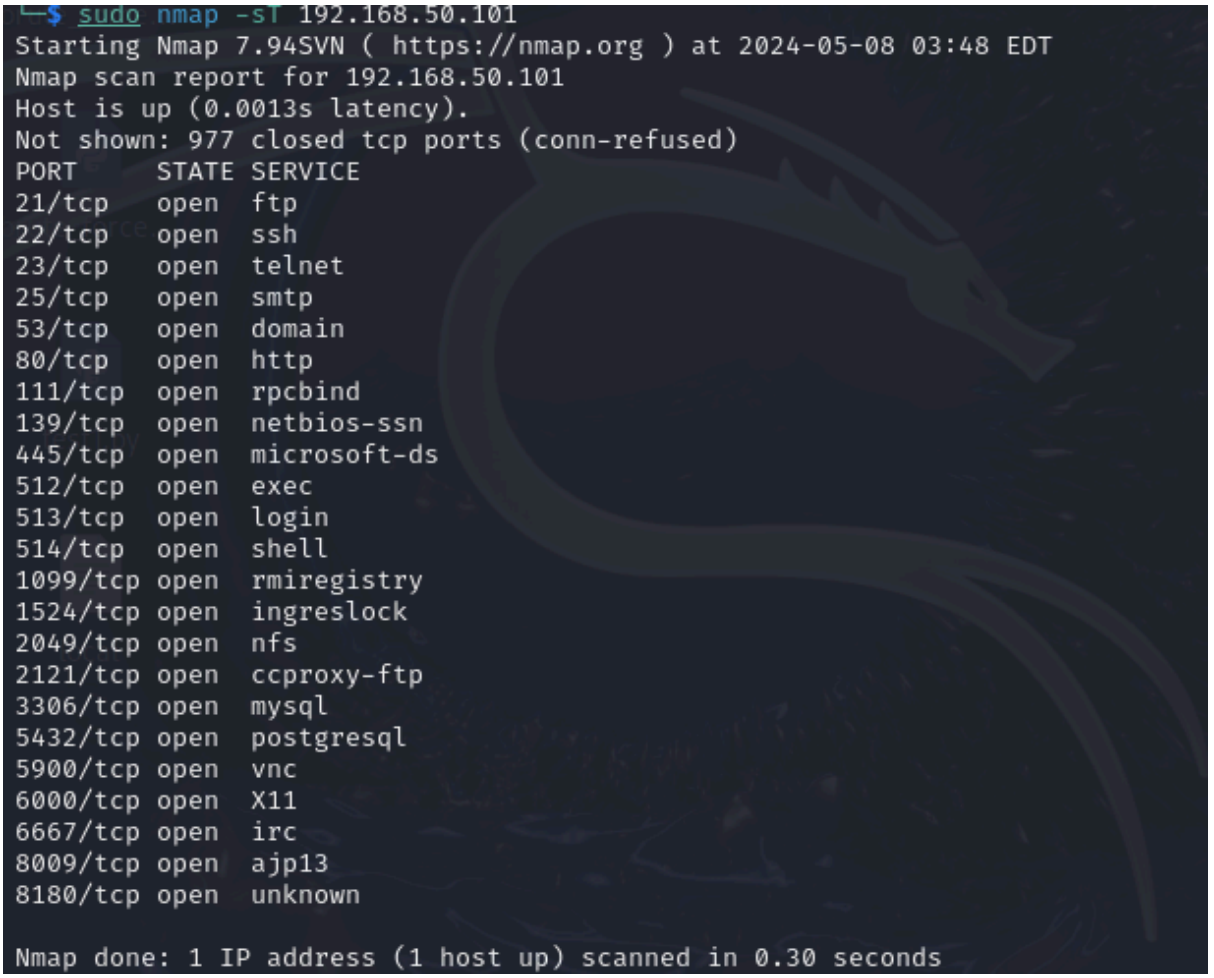


L'OS fingerprinting può essere utile per scopi di sicurezza, ad esempio per individuare dispositivi non autorizzati sulla rete, o per scopi di amministrazione di rete, ad esempio per

tenere traccia dei sistemi operativi utilizzati all'interno di una rete aziendale. Tuttavia, è importante notare che alcuni sistemi possono essere configurati per mascherare la loro identità, rendendo più difficile l'OS fingerprinting.

SYN scan e TCP connect:

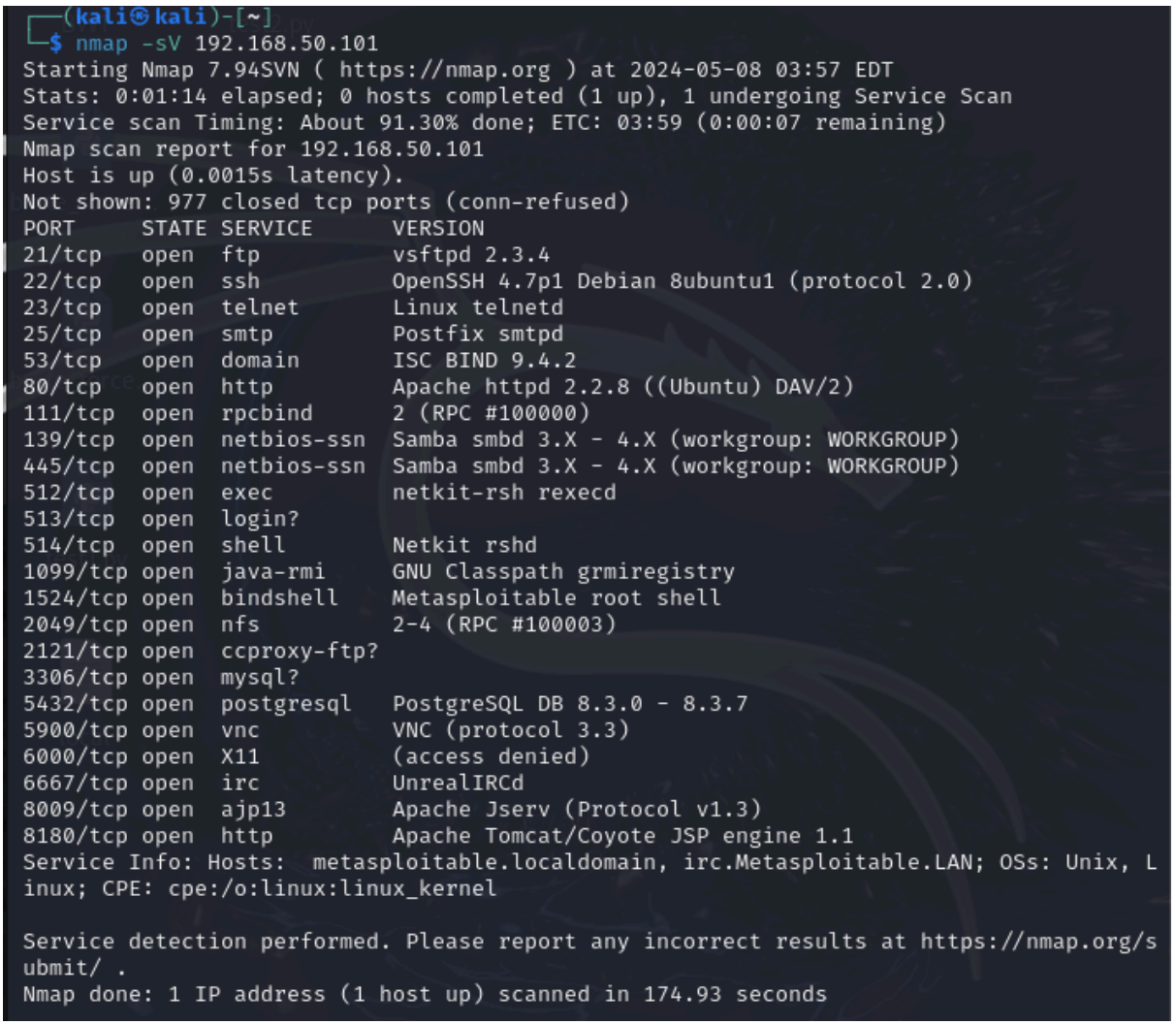




La differenza principale tra una scansione TCP Connect e una scansione SYN (Syn Scan) riguarda il modo in cui viene stabilita la connessione con le porte di destinazione.

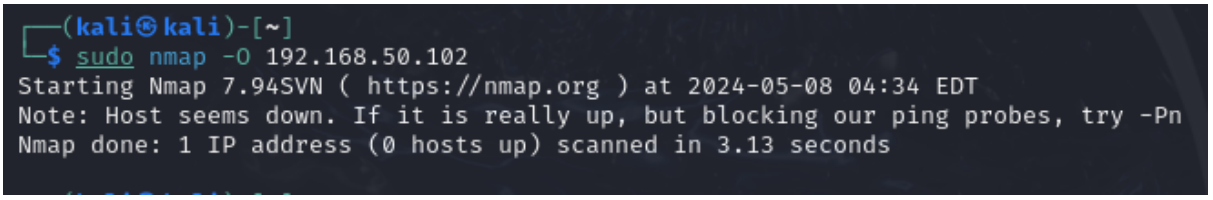
Scansione TCP Connect:
In una scansione TCP Connect, Nmap tenta di stabilire una connessione TCP completa con l'host di destinazione sulla porta specificata.
Questo tipo di scansione richiede l'apertura di una connessione completa per determinare lo stato della porta (aperta, chiusa o filtrata).
È più silenziosa rispetto alla scansione SYN perché completa il handshake TCP.
Scansione SYN (Syn Scan):
In una scansione SYN, Nmap invia pacchetti SYN al host di destinazione senza completare il handshake TCP.
Se il porto è aperto, l'host di destinazione risponderà con un pacchetto SYN-ACK.
Se il porto è chiuso, l'host di destinazione risponderà con un pacchetto RST (reset).
Se il porto è filtrato, non viene ricevuta alcuna risposta.
La scansione SYN è più veloce e discreta poiché non completa la connessione TCP.
In breve, la scansione TCP Connect è più accurata ma meno discreta e più lenta rispetto alla scansione SYN, che è più veloce e discreta ma può essere meno accurata in determinate situazioni di filtraggio del firewall.

Version detection: È utile per comprendere meglio il panorama dei servizi in esecuzione su un host di destinazione e per individuare potenziali vulnerabilità legate a versioni obsolete o note di software.



OS fingerprint su Windows:

Protezione contro la scansione: Alcuni sistemi possono essere configurati per rilevare e bloccare attivamente le scansioni di rete, rendendo difficile per Nmap ottenere una risposta.



Se facciamo una fingerprint su Windows con il firewall attivo ci bloccherà senza poter fare la scansione.

Ma come nell'esempio avendo fatta una scansione è possibile visionare in questi casi con il block disattivato. Ulteriormente si può fare anche un fingerprint parallelo, implementando così anche il comando -T, che varierà dalla potenza minima, ovvero, 0 alla massima, cioè, 5. Oppure un'altra tecnica di evasione del blocco IPS/IDS può essere quella di puntare alla porta sorgente, e attaccheremo la porta 80/443 dato che generalmente non bloccano i pacchetti provenienti da porte http/https.