**Scansione dei servizi con Nmap**

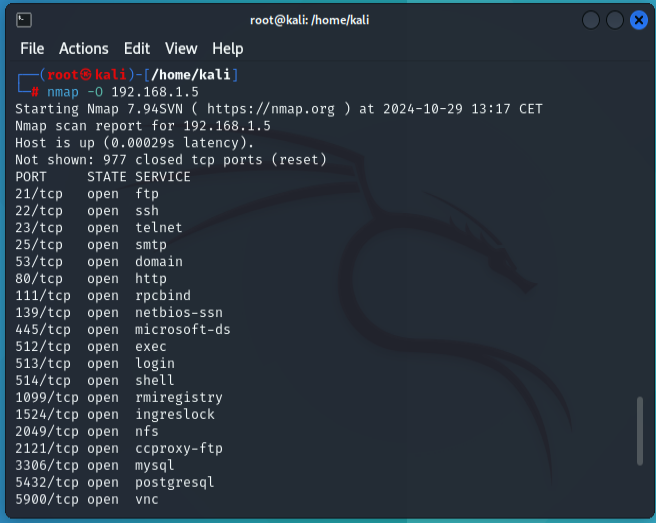
**Cosa è Nmap.**

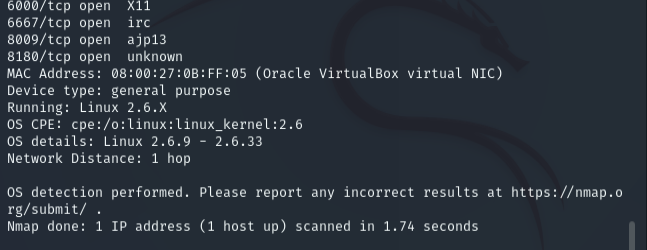
Nmap (Network Mapper) è uno strumento open-source estremamente potente e versatile per la scansione della rete e identificazione dei dispositivi e dei servizi. le funzioni principali sono:

* **Scansione degli Host:** identifica gli host attivi all’interno di una rete
* **Identificazione dei servizi:** rileva i servizi in esecuzione su ciascun host, inclusi i numeri di porta e protocolli.
* **Rilevamento dei Sistemi Operativi:** identifica sistema operativo in esecuzione su un host
* **Scansione delle Vulnerabilità:** può essere utilizzato per identificare le possibili vulnerabilità nei dispositivi (meglio Nessus)

**OS fingerprint (nmap -O 192.168.1.5):**

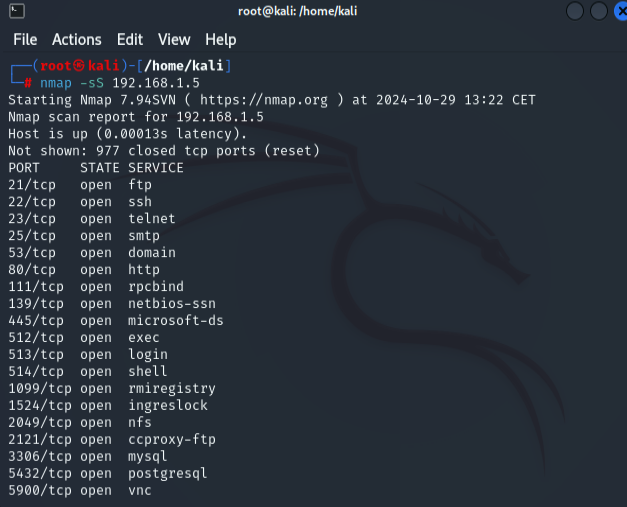
L’opzione -O in Nmap è utilizzata per abilitare il **rilevamento del sistema operativo** (OS detection). Quando utilizzi -O, Nmap cerca di identificare il sistema operativo in uso su un host target analizzando le risposte alle scansioni di rete e altre informazioni.

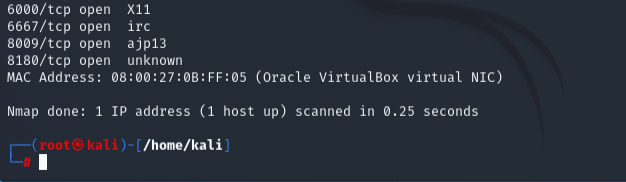




**SYN Scan (nmap -sS 192.168.1.5):**

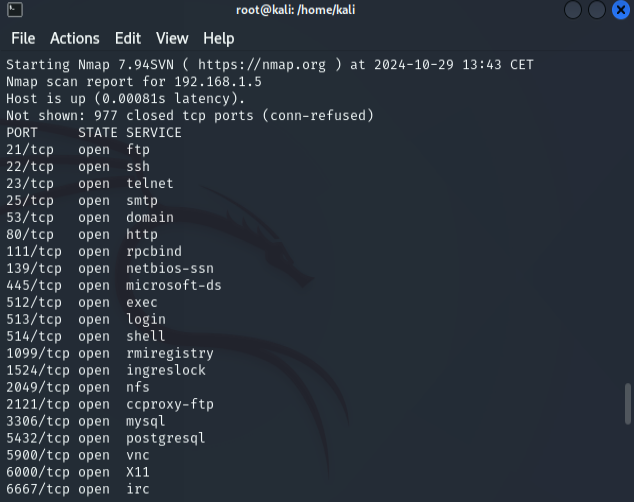
L’opzione -sS in Nmap è utilizzata per eseguire una scansione SYN, conosciuta anche come scansione stealth o scansione half-open. Questo tipo di scansione è progettato per essere più furtivo rispetto alla scansione TCP connect (-sT), poiché non stabilisce una connessione completa.

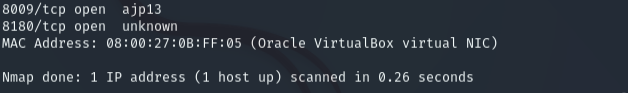




**TCP connect (nmap -sT 192.168.1.5):**

L’opzione -sT in Nmap è utilizzata per eseguire una **scansione TCP connect**. Questo tipo di scansione stabilisce una connessione completa (TCP handshake) con le porte del target, il che la rende una delle modalità di scansione più semplici e dirette.





**Differenza tra -SYN scan (-sS) e TCP connect (-sT):**

La differenza principale tra -sS (SYN scan) e -sT (TCP connect scan) in nmap sta nel modo in cui le connessioni alle porte vengono gestite e nel livello di intrusività delle scansioni.

**1. SYN Scan (-sS)**

• **Come funziona**: Durante una SYN scan, nmap invia un pacchetto **SYN** alla porta di destinazione e attende una risposta.

• Se la porta è **aperta**, il sistema target risponderà con un pacchetto **SYN-ACK**.

• nmap interrompe quindi la connessione inviando un pacchetto **RST** (Reset) per evitare di stabilire una connessione completa.

• Se la porta è **chiusa**, il sistema risponderà con un pacchetto **RST**.

• **Vantaggi**:

• È più **discreta** rispetto alla TCP connect scan perché non stabilisce una connessione completa, rendendola meno rilevabile dai sistemi di rilevamento intrusioni (IDS).

• È **più veloce** e consuma meno risorse.

• **Limiti**: Richiede privilegi di **root** o **amministratore** per essere eseguita, poiché utilizza pacchetti raw (pacchetti a livello IP).

**2. TCP Connect Scan (-sT)**

• **Come funziona**: In una TCP connect scan, nmap tenta di stabilire una **connessione completa** utilizzando il **Three-Way Handshake** (SYN, SYN-ACK, ACK) per ogni porta.

• Se la porta è **aperta**, si completa la connessione (SYN-ACK seguito da ACK).

• Se la porta è **chiusa**, il sistema risponde con un pacchetto **RST**.

• **Vantaggi**:

• Può essere eseguita senza privilegi di root, quindi è utile per utenti non amministratori.

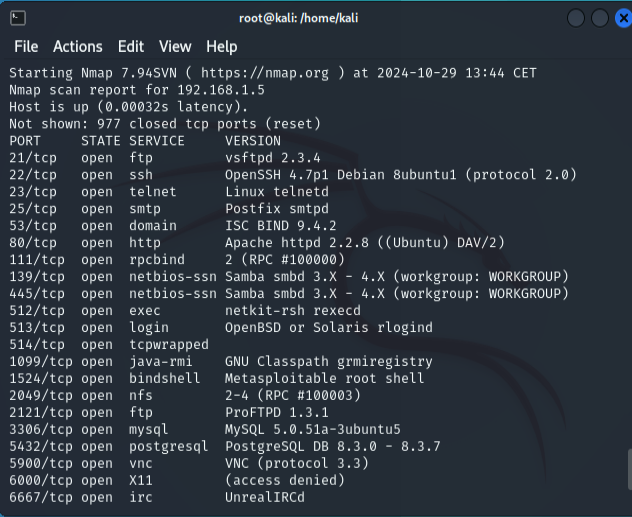
• **Limiti**:

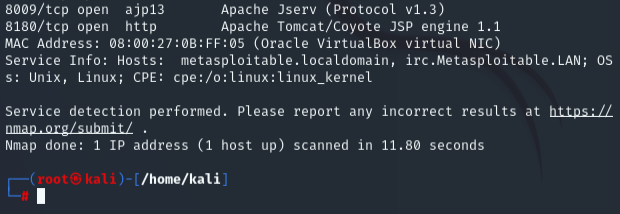
• È più **rilevabile** dai sistemi di sicurezza perché crea connessioni complete.

• È generalmente più **lenta** e può consumare più risorse rispetto alla SYN scan.

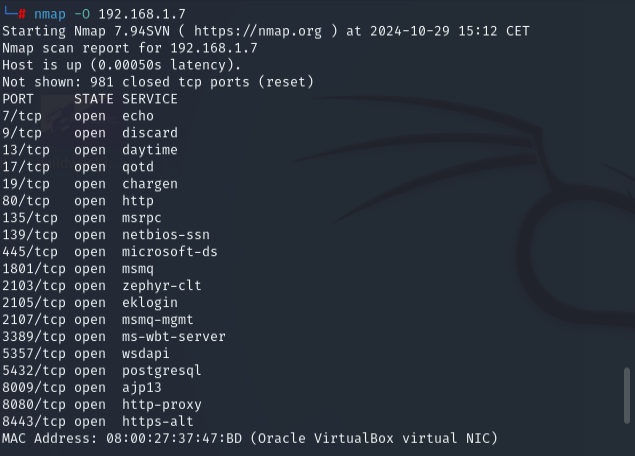
**Version Detection (nmap -sV 192.168.1.5):**

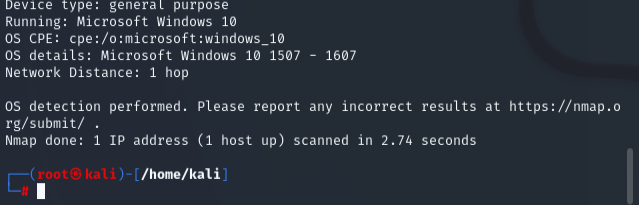
L’opzione -sV in Nmap è utilizzata per il rilevamento della versione dei servizi in esecuzione sulle porte aperte di un host target. Quando utilizzi -sV, Nmap non solo identifica le porte aperte, ma cerca anche di determinare quale servizio è in esecuzione su ciascuna porta e la sua versione specifica.





**OS fingerprint (nmap -O 192.168.1.7)**





**Conclusione:**

Dopo aver utilizzato le principali opzioni di nmap come -O (rilevamento del sistema operativo), -sS (SYN scan), -sT (TCP connect) e -sV (rilevamento versione dei servizi), abbiamo esplorato vari aspetti della rete e degli host target, ottenendo un quadro completo della loro configurazione e delle loro potenziali vulnerabilità.