ESERCIZIO: Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

● OS fingerprint.

● Syn Scan.

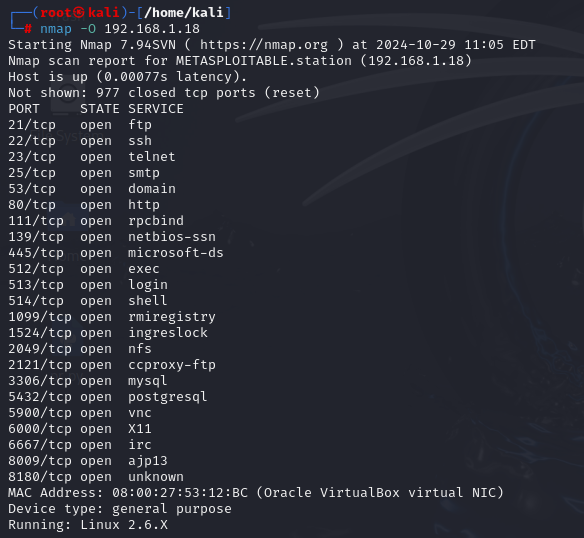
● TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?

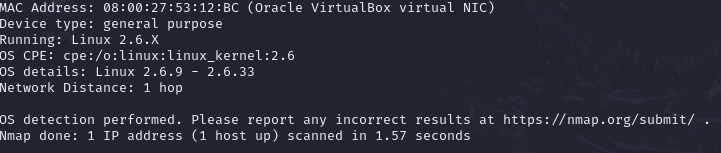
● Version detection.

L’esercizio l’ho eseguito interamente usando nmap, dal terminale di Kali Linux.

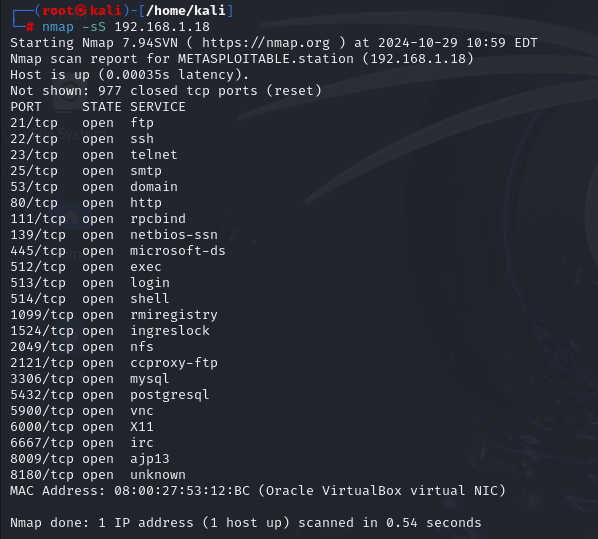
OS FINGERPRINT

Per trovare il sistema operativo ho usato il comando: *nmap -O*

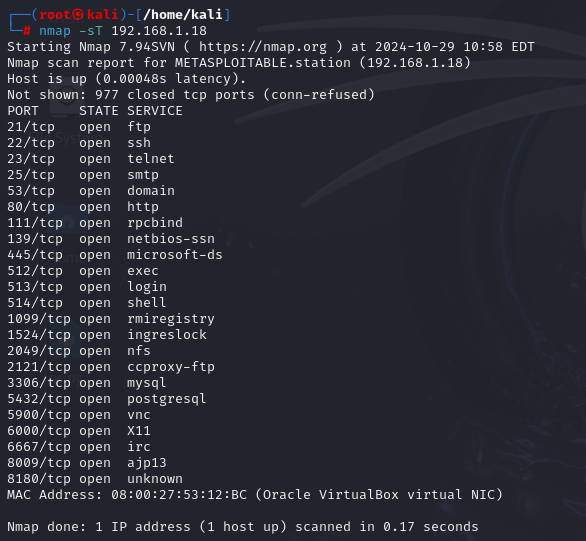




SYN SCAN

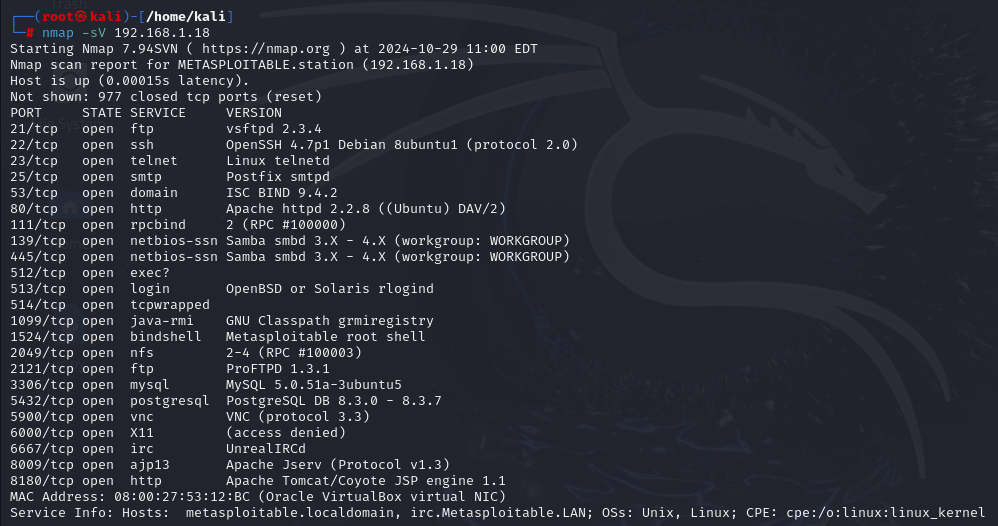


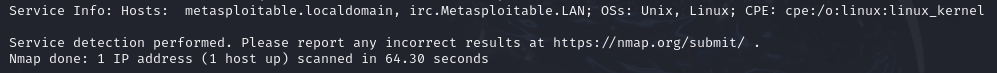
TCP CONNECT



Il risultato di *SYN SCAN* e *TCP CONNECT* non ci sono differenze sostanziali. Cambia solamente il tempo di scan

VERSION DETECTION





Ho fatto anche uno scree alle porte aperte dell’indirizzo ip di metasploitable (lo stesso usato anche negli screen precedenti) usando il comando: *nmap -p- 192.168.1.18*

