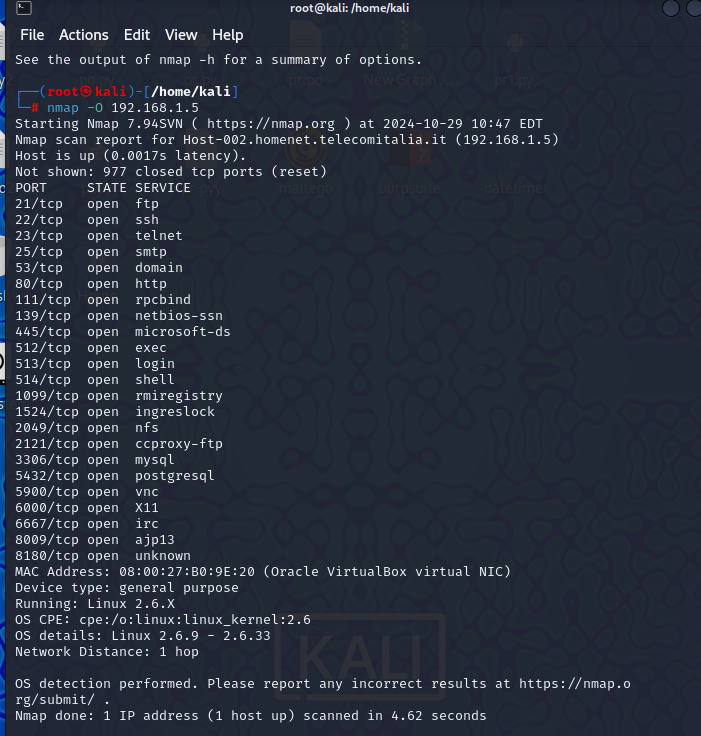
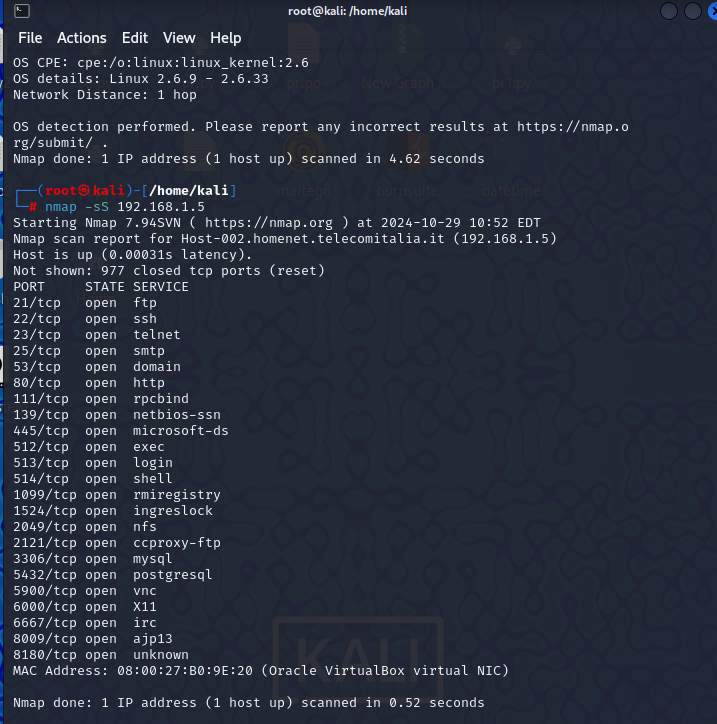
S5 L2

TECNICHE DI SCANSIONE CON NMAP

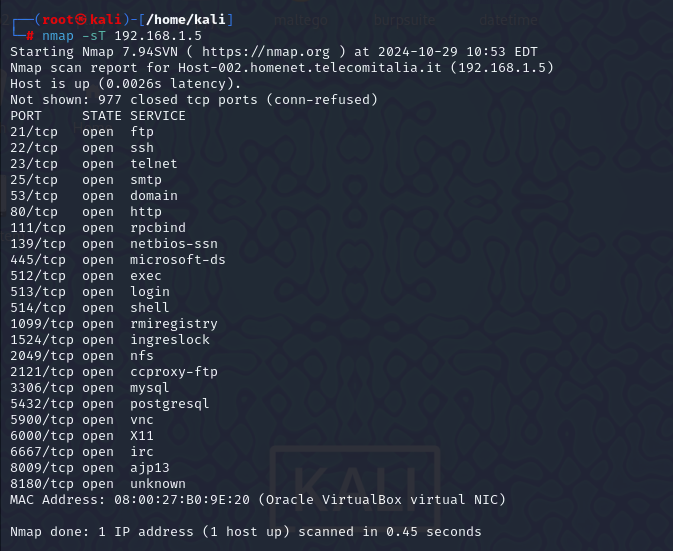
In questa esercitazione abbiamo utilizzato **Nmap** per eseguire una serie di scansioni su due target: **Metasploitable**, e **Windows 10**. Ogni tipo di scansione rivela aspetti diversi delle macchine di destinazione, fornendo così una visione più completa di dati utili.



**OS Fingerprint** La prima scansione effettuata su Metasploitable è stata l’**OS Fingerprint** con il comando nmap -O 192.168.1.5. Questo tipo di scansione ci serve per identificare il sistema operativo. Questo è uno dei modi fondamentali per avere un quadro generale della macchina target.

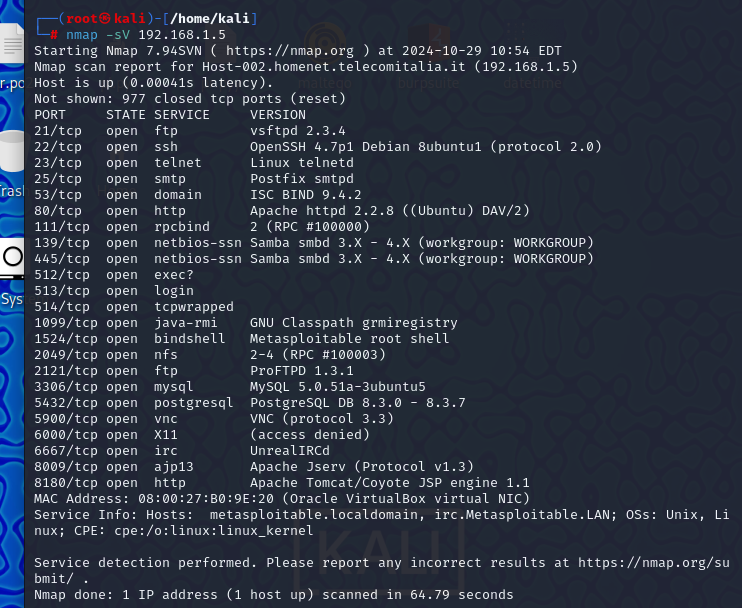


**Syn Scan** Successivamente, abbiamo eseguito una **Syn Scan** (nmap -sS 192.168.1.5). Questo tipo di scansione invia pacchetti SYN al target senza completare la connessione. Questa tecnica è particolarmente utile in quanto è più veloce e meno rilevabile da eventuali sistemi di difesa, poiché lascia meno tracce nel registro di sistema.

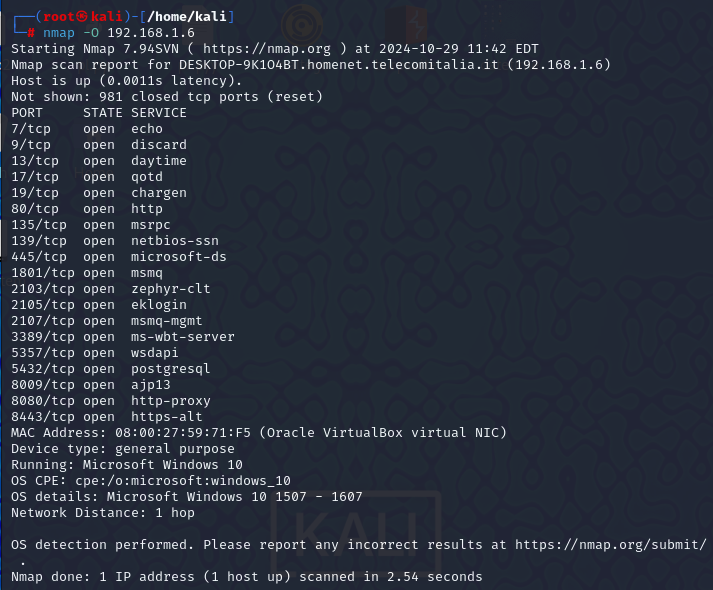


**TCP Connect Scan** Per confrontare i risultati ottenuti con la Syn Scan, abbiamo eseguito una **TCP Connect Scan** (nmap -sT 192.168.1.5). Questa scansione stabilisce una connessione completa (completando il "three-way handshake") con ogni porta rilevata. A differenza della Syn Scan, è meno discreta e più visibile al target.

**Differenze tra Syn Scan e TCP Connect**: In termini di porte e servizi rilevati, i risultati delle due scansioni sono simili, come mostrato negli screenshot allegati. Tuttavia, la Syn Scan è generalmente preferita per scansioni iniziali di scoperta grazie alla sua maggiore velocità e furtività, mentre la TCP Connect può essere usata quando non si hanno privilegi elevati.



**Version Detection** Abbiamo poi utilizzato la funzione di **Version Detection** (nmap -sV 192.168.1.5) per identificare le versioni specifiche dei servizi in esecuzione sulle porte aperte. Questo tipo di scansione è utile per ottenere dettagli più approfonditi su possibili vulnerabilità dei servizi stessi, dal momento che versioni datate o specifiche possono avere vulnerabilità note.



**OS Fingerprint** Per il sistema Windows, abbiamo eseguito nuovamente la scansione **OS Fingerprint** (nmap -O 192.168.1.6). Anche in questo caso, l’obiettivo era identificare il sistema operativo.