Introduzione

È uno scanner di rete. Nello specifico, **scansiona gli host della rete**.

Con nmap raccogliamo tutte le informazioni che riguardano i dispositivi nella rete, come:

- numero dei dispositivi
- tipologia dei dispositivi (web server, nas, eccetera)
- sistema operativo
- servizi attivi, ovvero le porte aperte dei protocolli di rete
- Le vulnerabilità (anche se lo strumento più adatto a questo scopo è Nessus)

Nelle prossime pagine, andiamo a scansionare due macchine virtuali: Metasploitable e Windows 10.

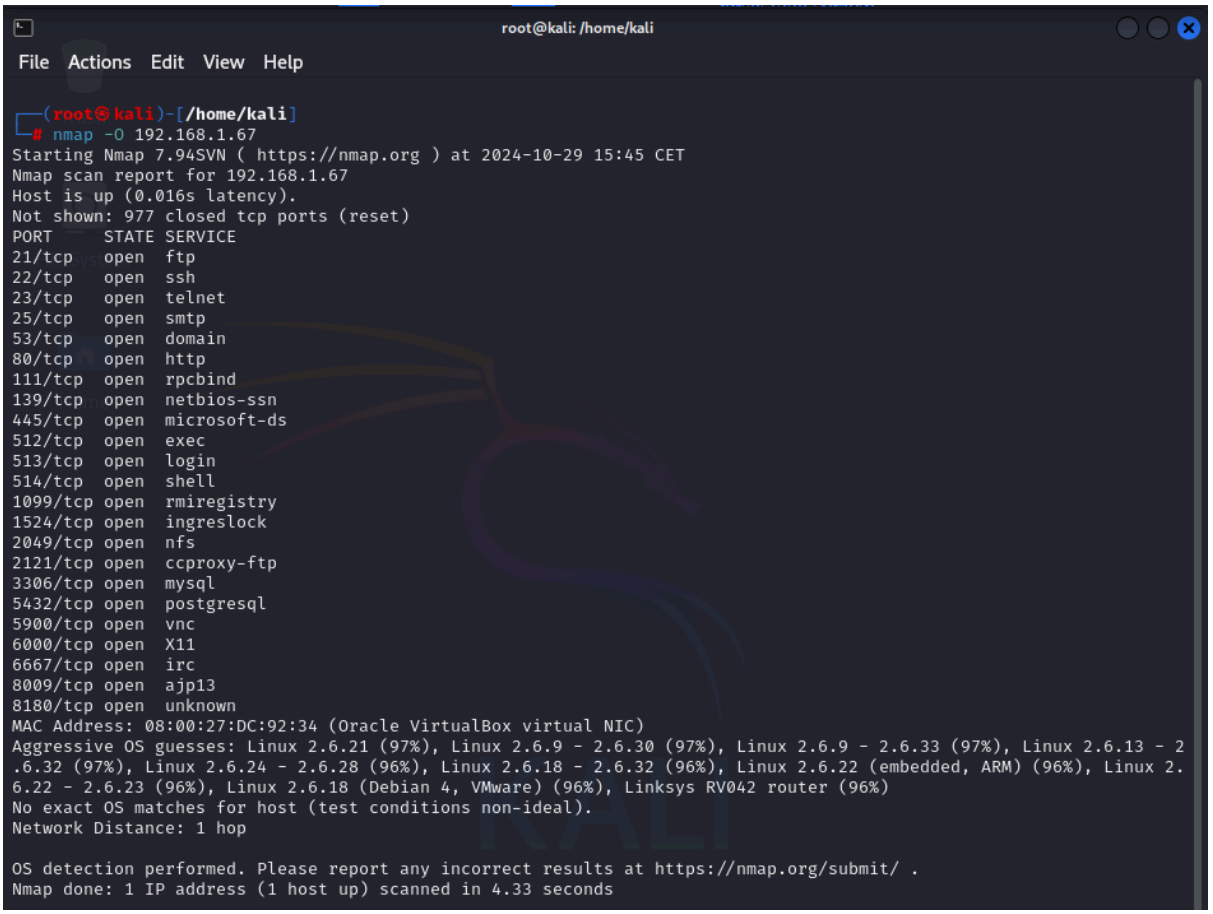
Scansione dei servizi con Nmap

Metasploitable

OS Fingerprint (-O): Tenta di determinare il sistema operativo dell'host di destinazione.

Nmaps invia una serie di pacchetti specifici per osservare le risposte del servizio.

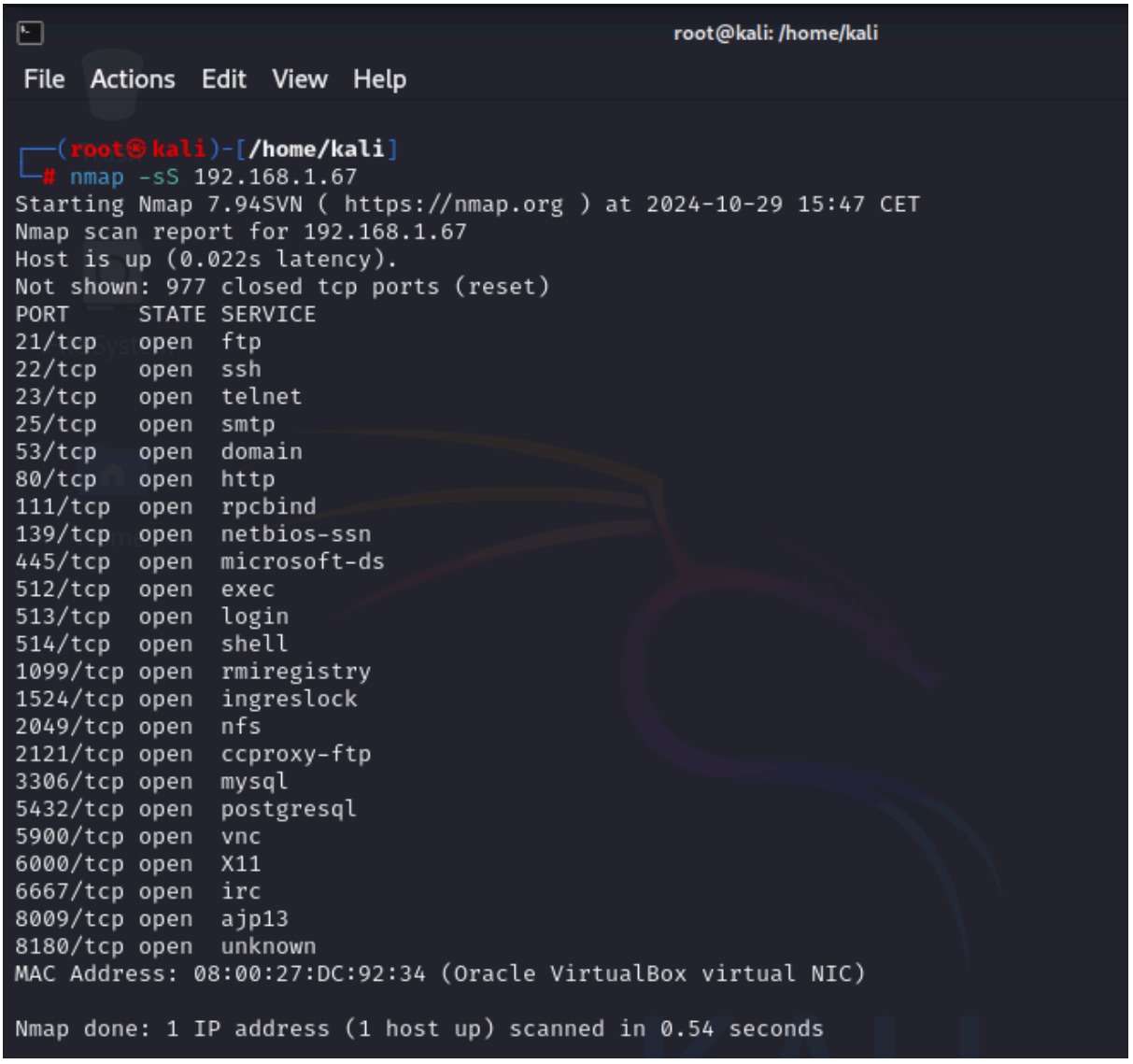
Queste risposte vengono poi confrontate con un database di firme conosciute per identificare il servizio e la sua versione.



SYN Scan (-sS): una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3-way-handshake, ma appurato che la porta è aperta chiude la comunicazione, evitando la creazione del canale e generando meno "rumore" a livello di rete.

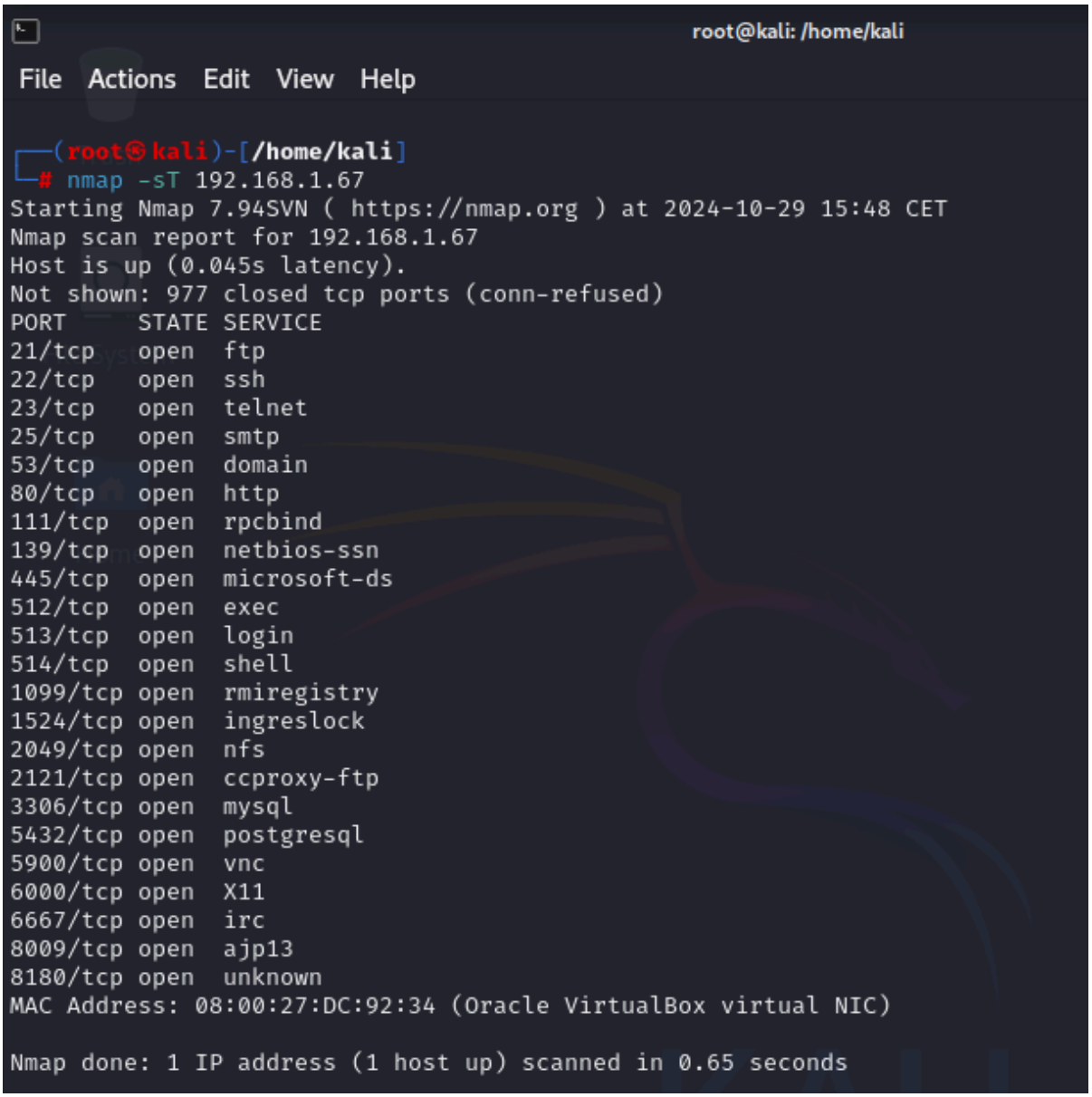
Per chiudere la connessione, anziché inviare nella terza fase il pacchetto ACK, invia il pacchetto **RST (reset).**

Non effettuerà il ping, bypassa il firewall, a discapito di un **risultato meno attendile.**

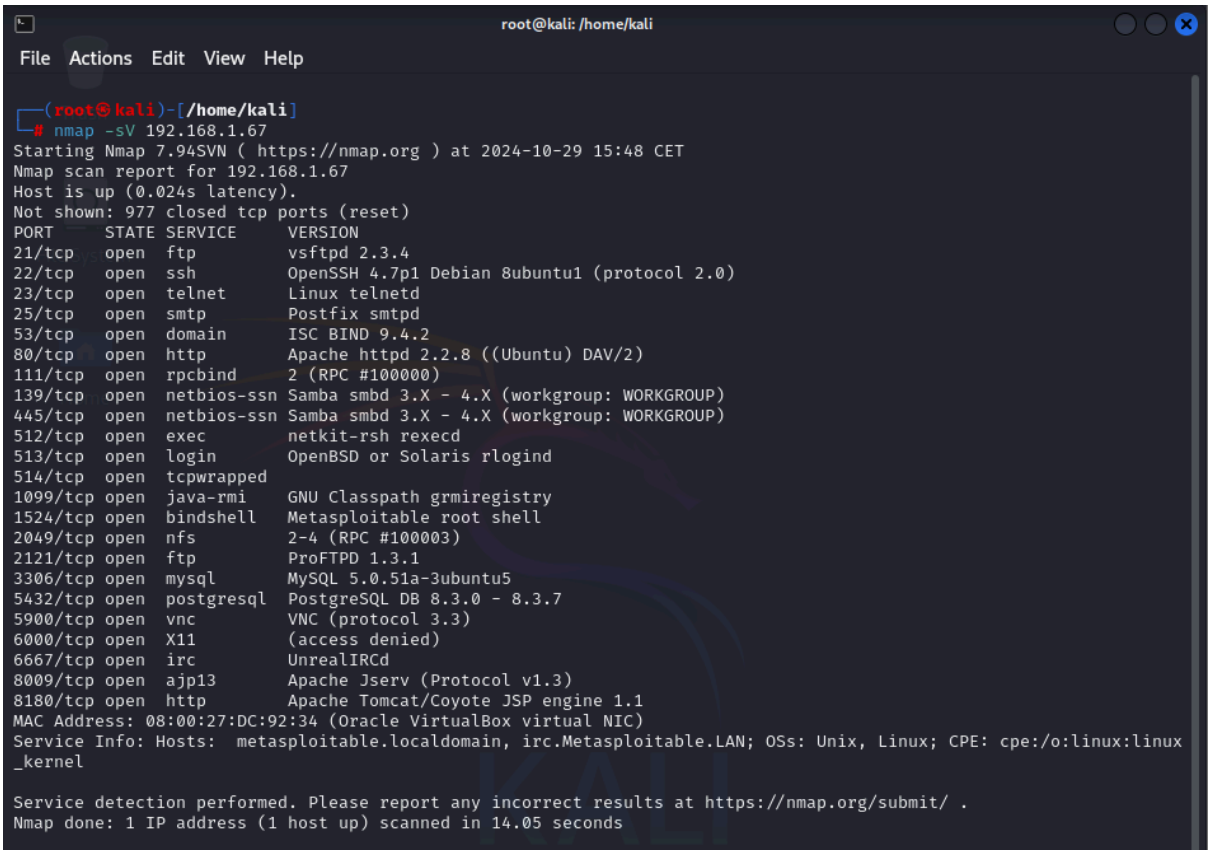


TCP Scan (-sT): è il metodo di scansione più invasivo, in quanto per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.

Nmap effettuerà un **ping** e di conseguenza il risultato sarà più accurato



Version Detection (-sV): Identifica i servizi in esecuzione e le loro versioni.



Windows

OS Fingerprint (-O):