**Esercizio: Scansione dei servizi**

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 delle scansioni TCP connect e SYN?
* Version detection

E la seguente sul target Windows 7:

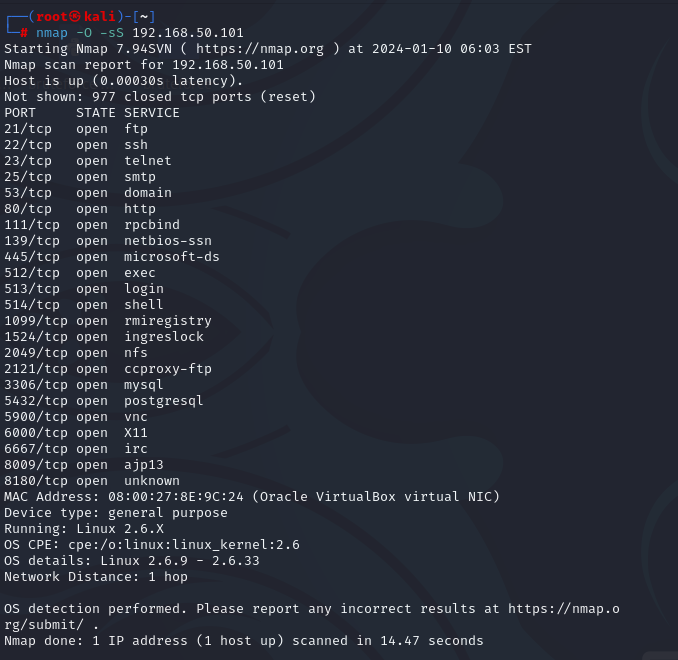
* OS fingerprint

Metasploitable:

**OS fingerprinter + SYN Scan:**

Comando: nmap -0 -sS 192.168.50.101

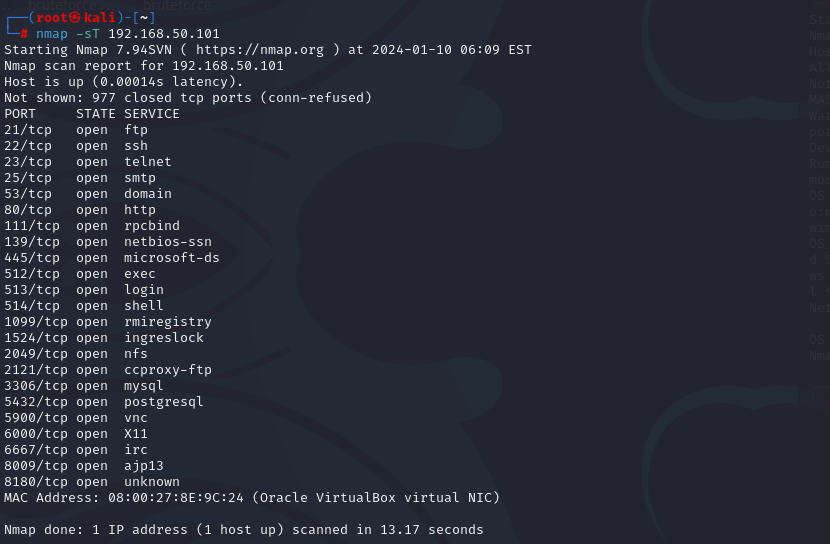
Questa scansione invia pacchetti SYN e attende le risposte, identificando porte aperte senza completare la connessione TCP, e tenta di identificare il sistema operativo del target.



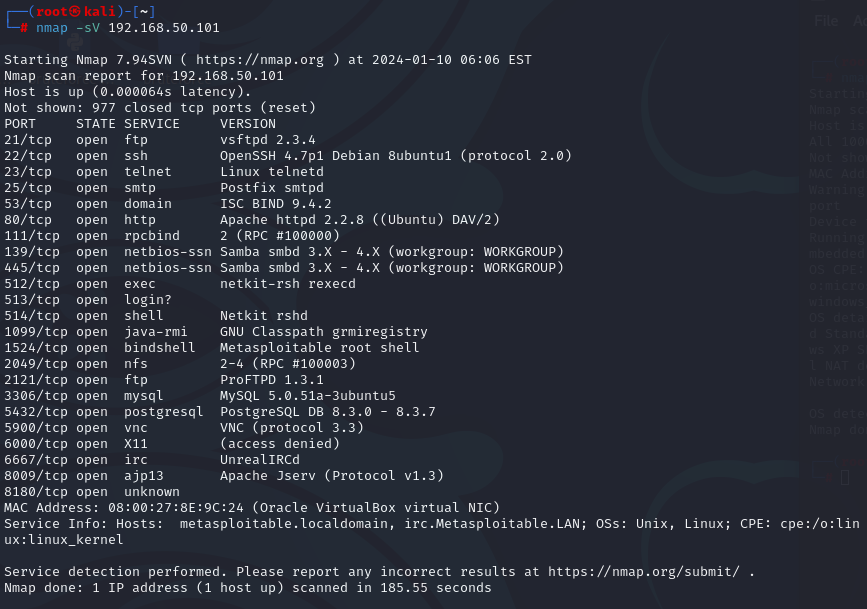
**TCP connect:**

Comando: nmap -sT 192.168.50.101

A differenza dello SYN scan, questa scansione completa la connessione TCP. Puoi confrontare i risultati con quelli dello SYN scan per vedere come alcuni sistemi possono rispondere diversamente a questi due tipi di scansione.



**Version detection:**



**Windows 7:**

Comando: nmap -O 192.168.50.102

Analogamente al primo punto, questo comando cerca di identificare il sistema operativo del target Windows 7.

