Relazione S5L2 Luca Calvigioni

**SCANSIONI NMAP**

**Traccia: Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:**

**● OS fingerprint**

**● Syn Scan**

**● TCP connect**

**● Version detection**

**E sul target Windows:**

**● OS fingerprint**

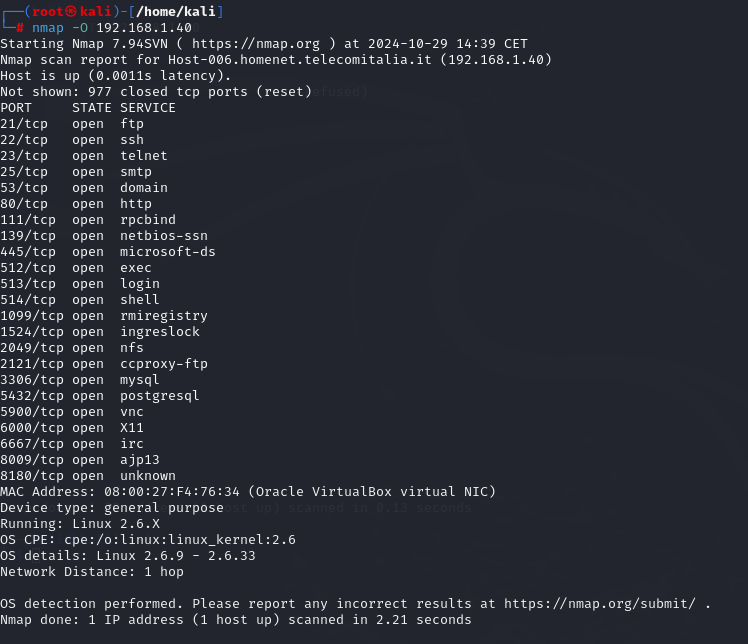
Metasploitable indirizzo ip: 192.168.1.40

**OS fingerprint di Metasploitable:**

Digitiamo sul terminale di Kali Linuxil comando

“nmap –O 192.168.1.40”

una volta terminata la scansione il risultato ci elencherà le porte aperte e i servizi che vengono utilizzati, successivamente il sistema operativo utilizzato.



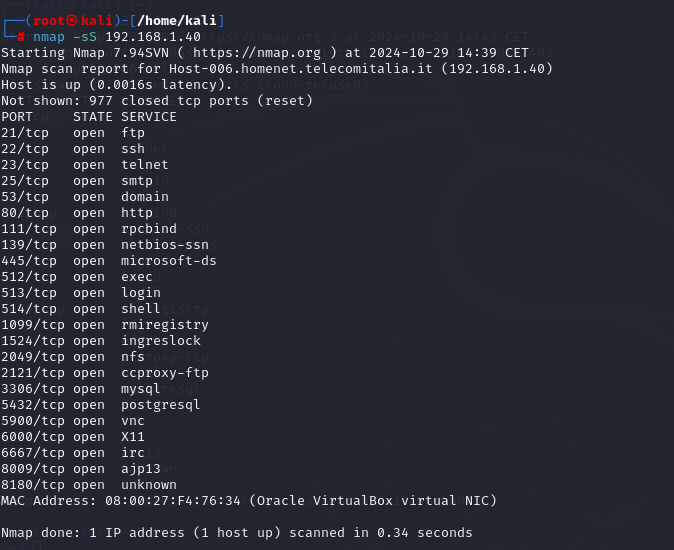
**SYN scan di Metasploitable:**

Digitiamo sul terminale di Kali Linux il comando

“nmap -sS 192.168.1.40”

Con il comando –sS esegue una “TCP SYN scan” per vedere le porte dei servizi aperte, invia pacchetti SYN senza completare però la stretta di mano a 3 vie

Questa è più furtiva perchè non stabilisce una connessione completa ed è generalmente piu veloce, per eseguirla abbiamo però bisogno dei diritti di Root

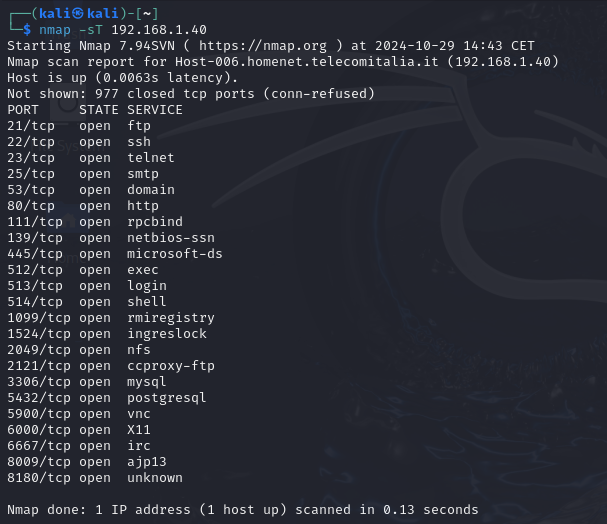


**TCP connect di Metasploitable:**

Digitiamo sul terminale di Kali Linux il comando

“nmap -sT 192.168.1.40”

A differenza di SYN scan, TCP connect fornisce dati più accurati stabilendo connessioni complete (SYN, SYN/ACK, ACK) non servono diritti di Root.

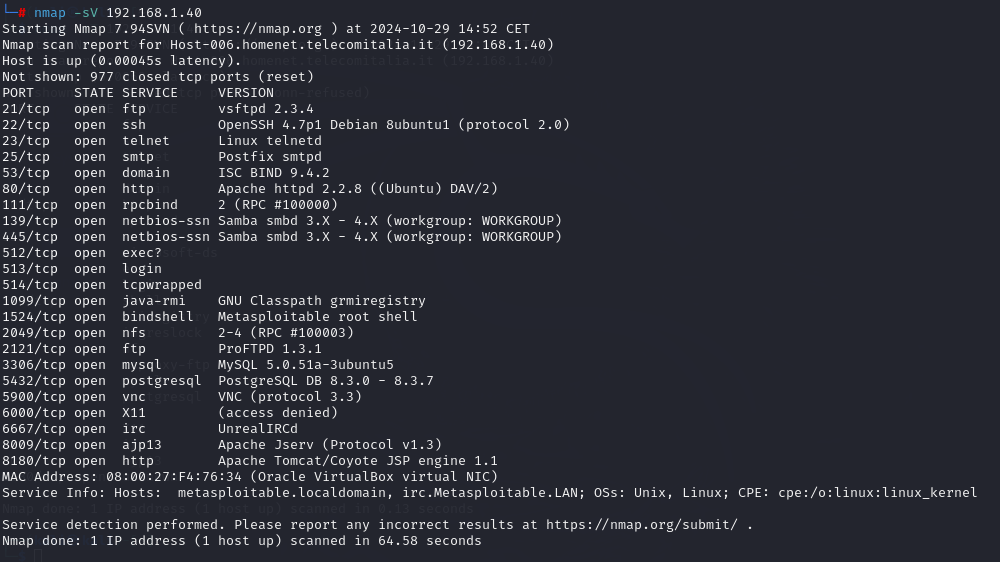


**Version Detection:**

Digitiamo sul terminale di Kali Linux il comando

“nmap -sV 192.168.1.40”

Grazie a questo comando possiamo vedere le versioni dei servizi utilizzati in esecuzione sulle porte aperte.



**OS Fingerprint su Windows:**

IP windows: 192.168.1.41

Digitiamo sul terminale di Kali Linux il comando

“nmap -O 192.168.1.41”

come fatto prima con Metasploitable ma eseguito su un indirizzo IP di un dispositivo Windows.

