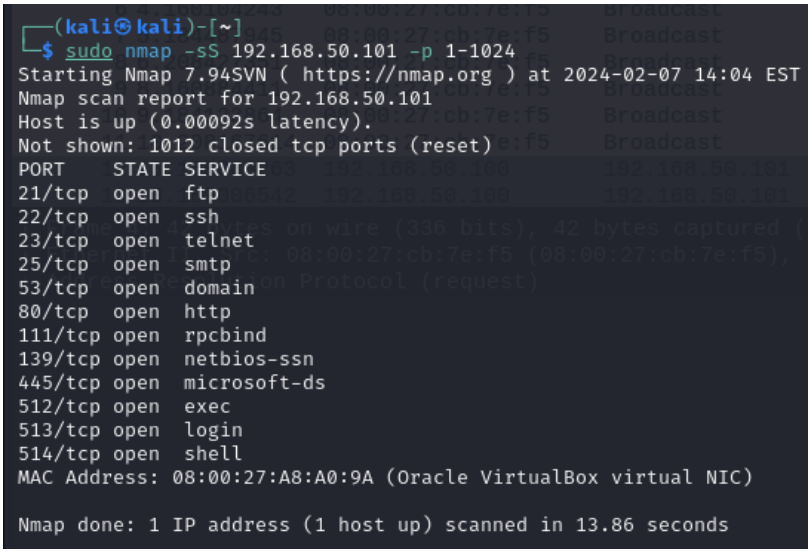
NMAP

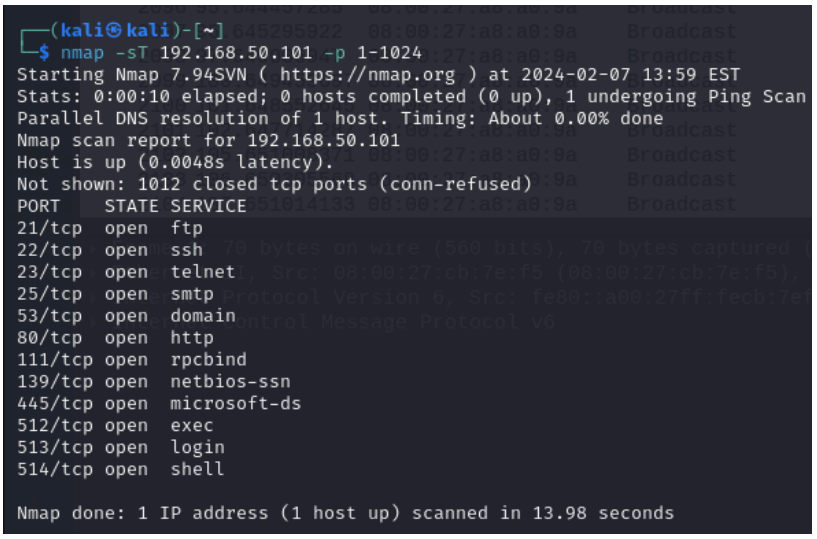
Su questo esercizio vedremo come utilizzare nmap su kali linux.
Per prima cosa, apriamo le macchine virtuali Kali e metasploitable.

Dopo questo, apriamo kali, e sul terminale lanciamo il comando di nmap, la funzione che vogliamo, se sS o sT, sapendo che il comando sS lancia solo una SYN, quindi questo comando risulta meno “aggressivo” quindi in poche parole andrà solo a controllare se la porta è aperta, e non altro. Invece il comando sT lancia uno scan TCP, questo è più aggressivo, risultando nel controllare tutte le porte aperte e tutte le sue vie.

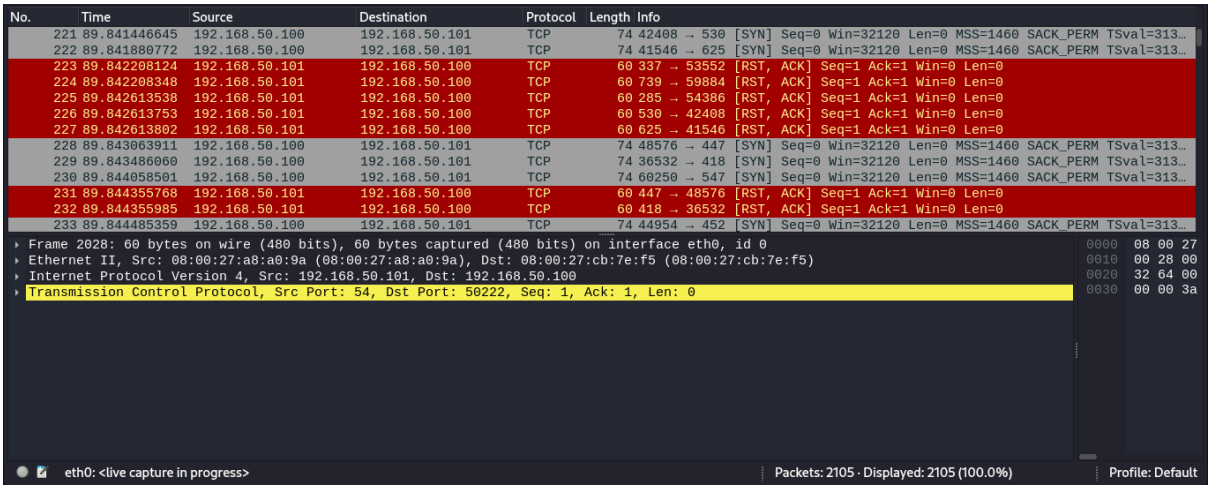
Come in immagine, eseguiamo il comando di nmap -sS:



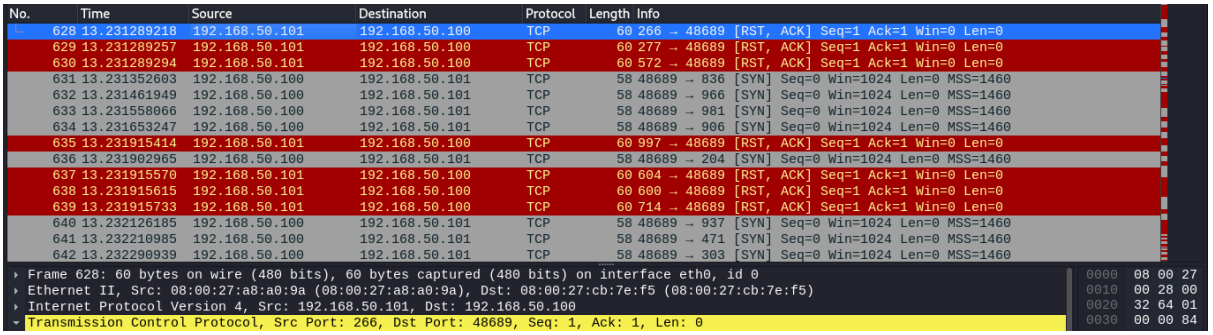
Come in immagine, eseguiamo il comando di nmap -sT:



E su questI, andiamo anche a fare la cattura su Wireshark, confrontando i due scan che abbiamo fatto:



(Scansione comando sT)



(Scansione comando sS)

Con questo vediamo che quando lanciamo il comando sT, la macchina bersaglio risponde con una SYN, ACK ma la nostra macchina risponde con un rst, così non concludendo il 3WH.
Invece con la scansione sS noi inviamo solamente un SYN e la macchina bersaglio ci risponde soltanto con una RST