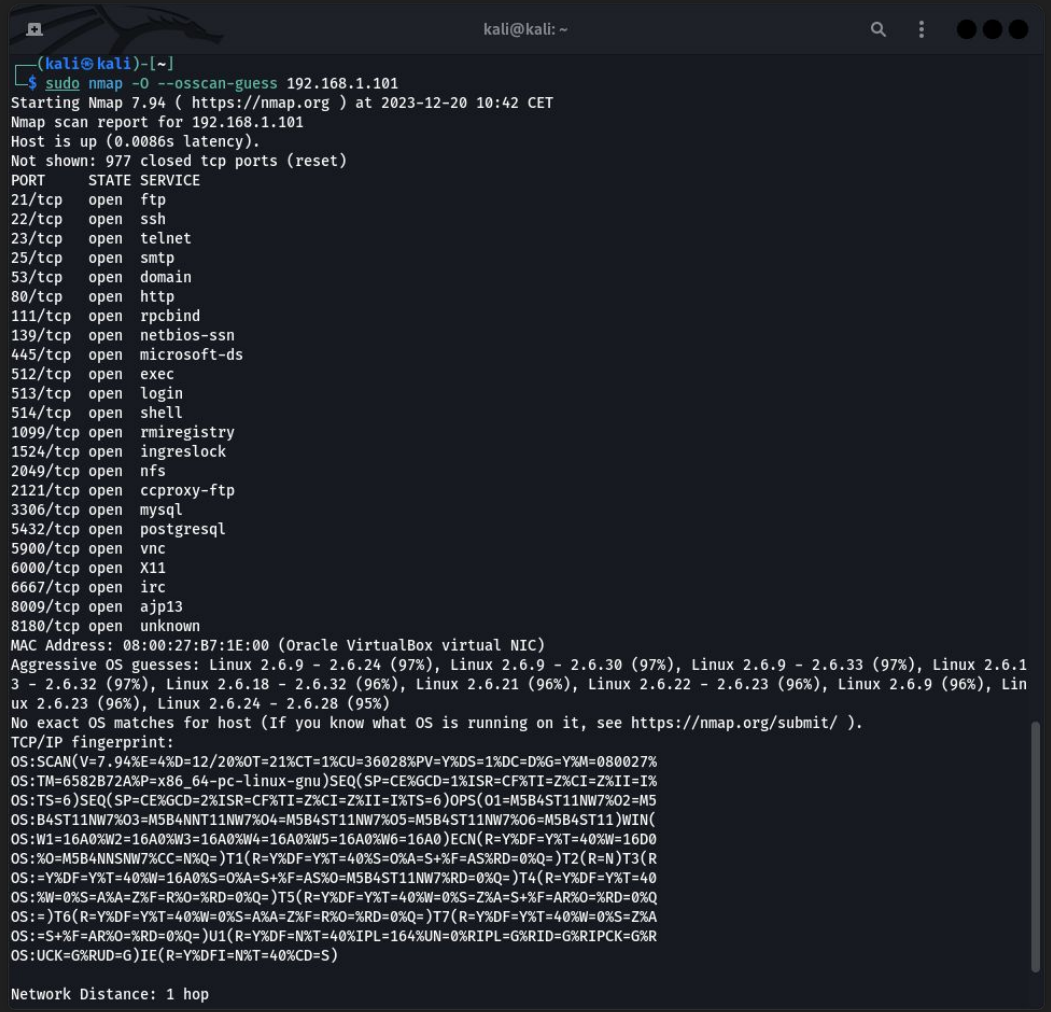
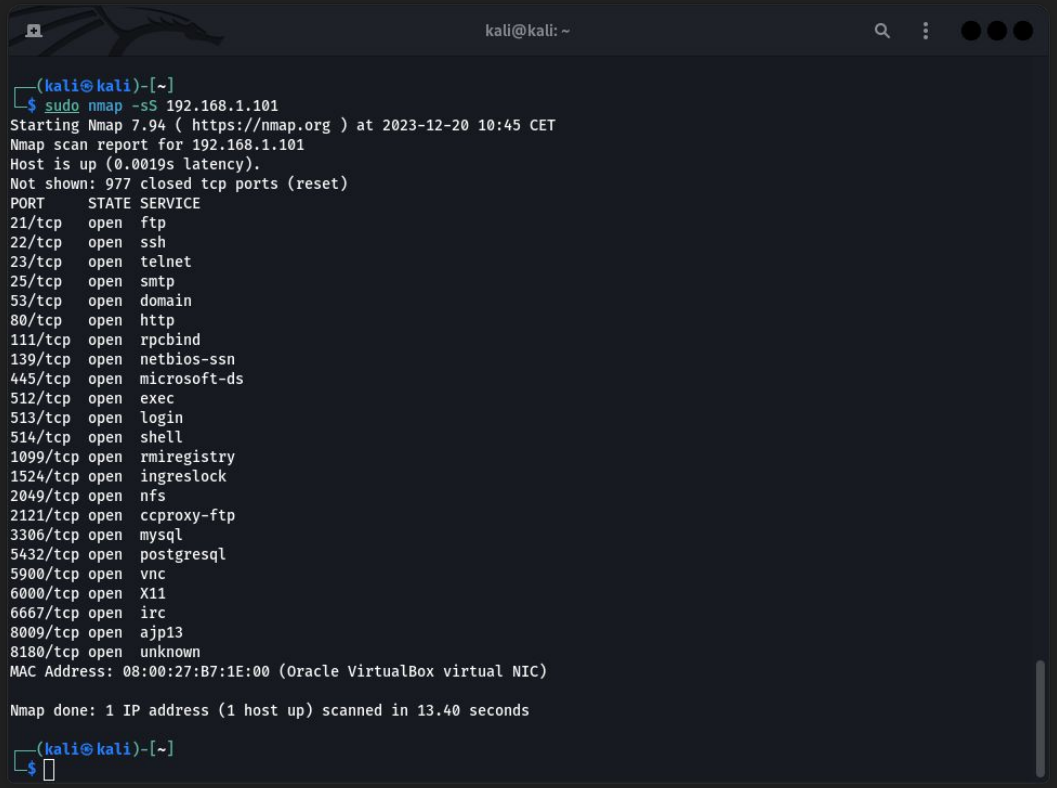
S5L3

NMAP

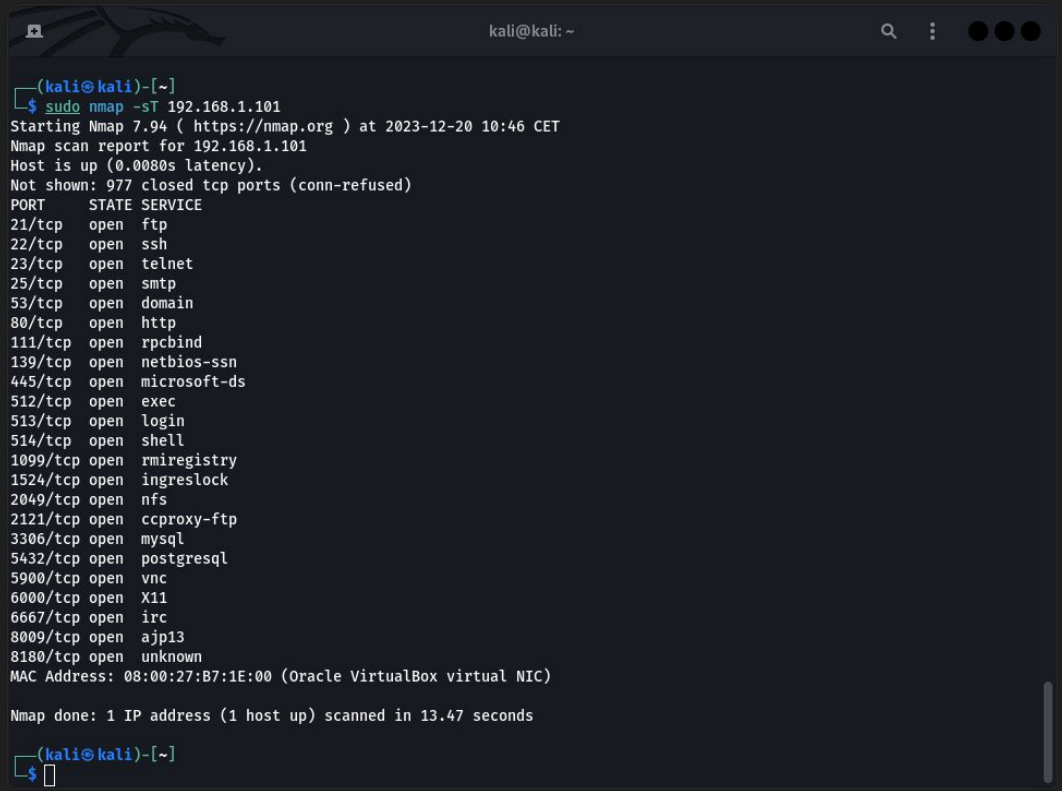
Come da consegna, inizio effettuando uno scan nmap per individuare il sistema operativo della macchina Metasploit.
Per quanto il tool non riesca a trovare risultati precisi, il OS-Guess propone come possibile sistema operativo Linux 2.6.x

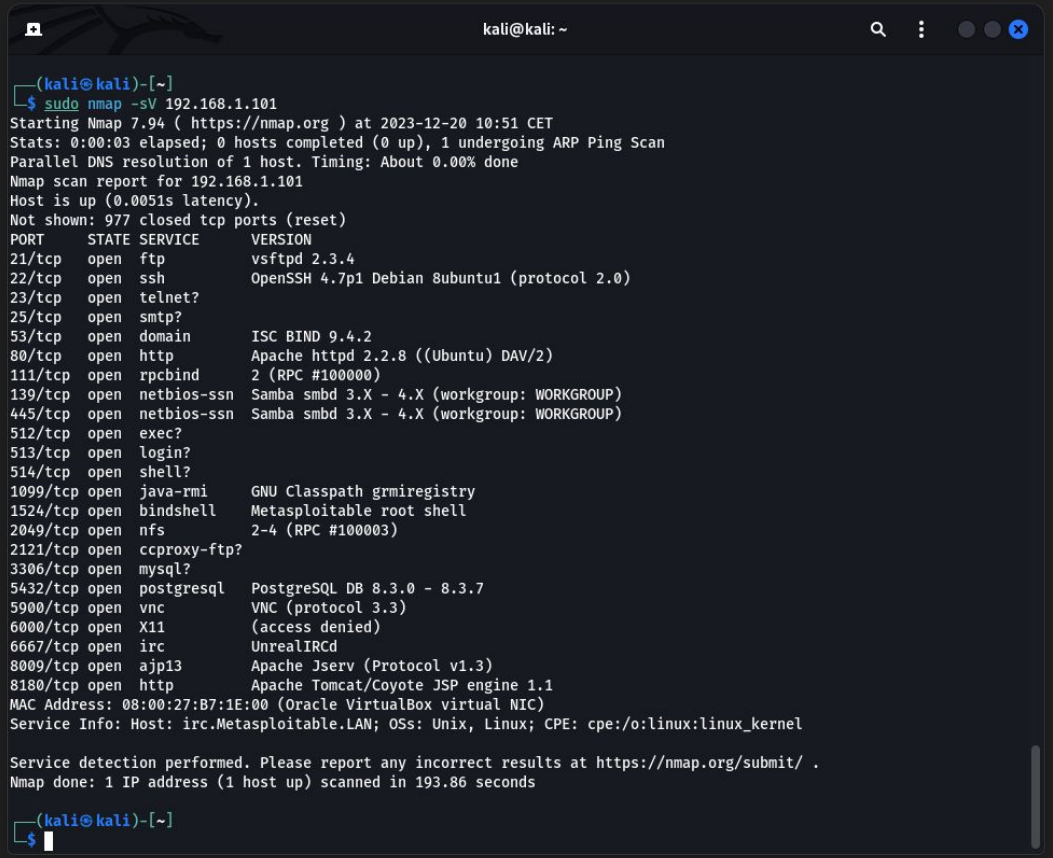




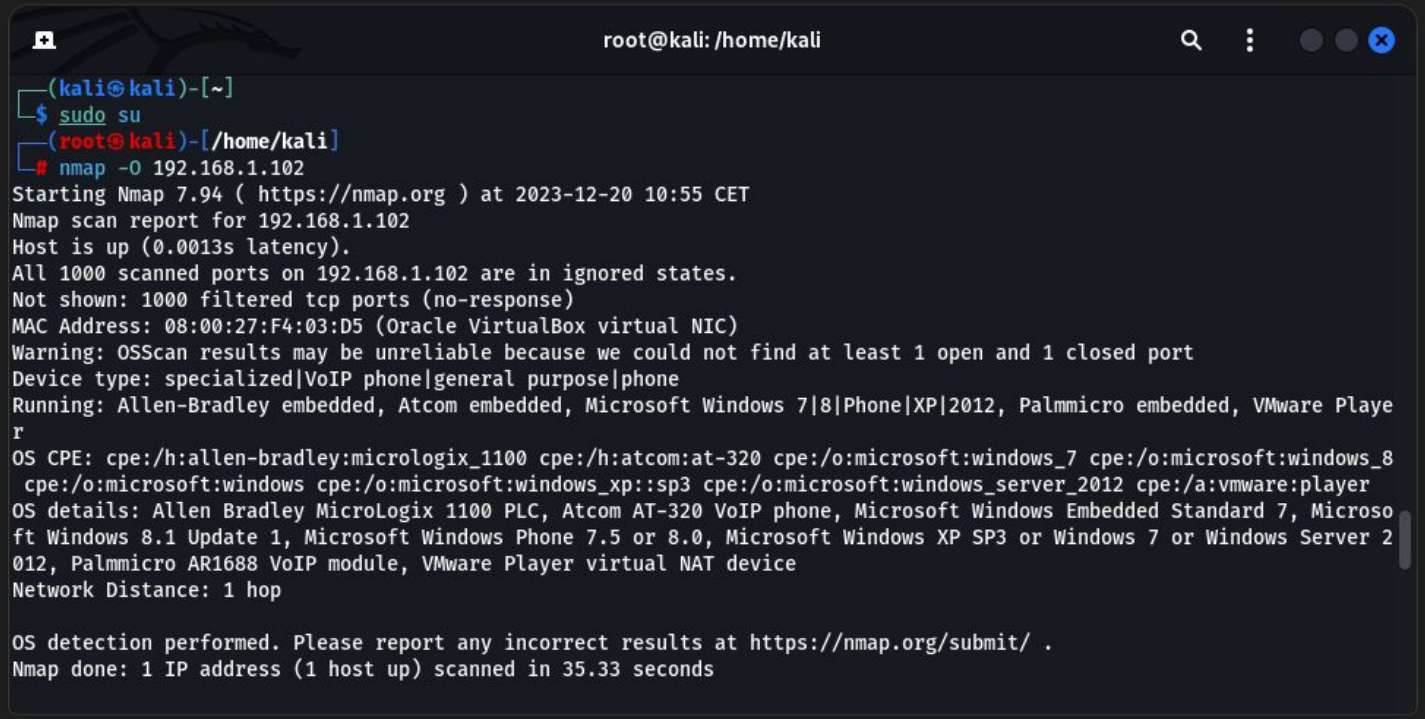
Procedo con una scansione SYN, che da come risultati queste porte e questi servizi. Notare la voce “(reset)” nella riga “Not shown: 977 closed ports”

Il prossimo scan della consegna è quello TCP. La differenza tra i due è nella voce evidenziata precedentemente: in questa scansione il risultato è “(conn-refused)”





L'ultima scansione della macchina Meta è quella della versione dei servizi attivi, i risultati sono quelli nell'immagine qui riportata



Passiamo adesso alla macchina Windows 7, per la quale è stato richiesto di fare una scansione del sistema operativo.
Come ci mostrano i risultati non è possibile trovare con certezza il sistema operativo della macchina, poiché tutte le porte sono filtrate.
Nonostante tutto rileva il fatto che sia una macchina Windows di qualche tipo.

Come scansionare Windows?

Probabilmente il metodo migliore per riuscire ad effettuare la scansione su windows sia modificare il suo firewall per aprire delle porte alla macchina Kali