NMAP: EVADING THE IDS

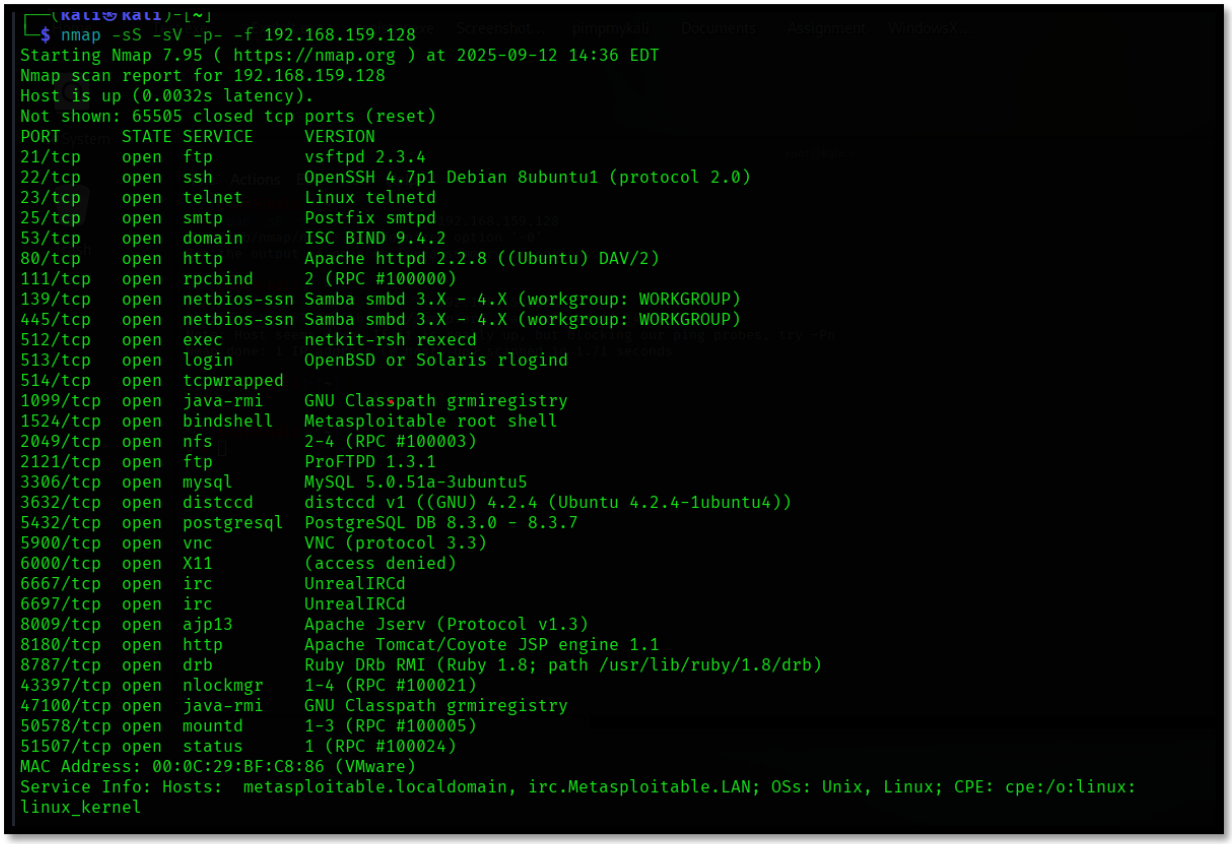
JAWAD ALI

Nmap: Evading the IDS

Introduction:

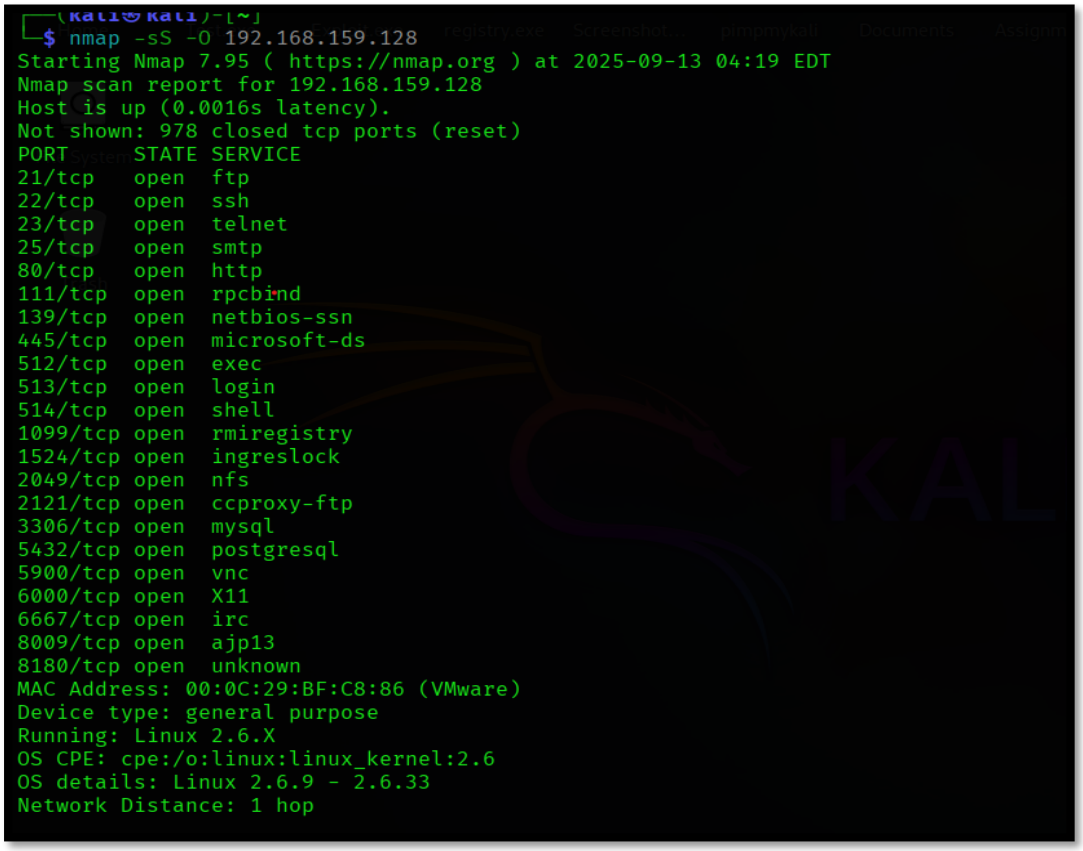
In this report, we will focus on how to perform on a stealth scan and simulate how to evade the IDS alerts. We are using **Metasploitable** as a target machine and using nmap for performing the scans.

Fragmentation of the Packets:



In the above-mentioned figure, we have used **-f** for converting the packets into fragments so that they can bypass the IDS alerts. According to the results we got, we have several ports that are open and can be exploited. Also, we got the MAC address of the virtual machine.

OS Discovery:



Here, we also got the OS running on the target machine and it is **Linux.**