Open your metasploitable linux and login.

Extract the ip address of the server.

We get ip address = 192.168.109.129

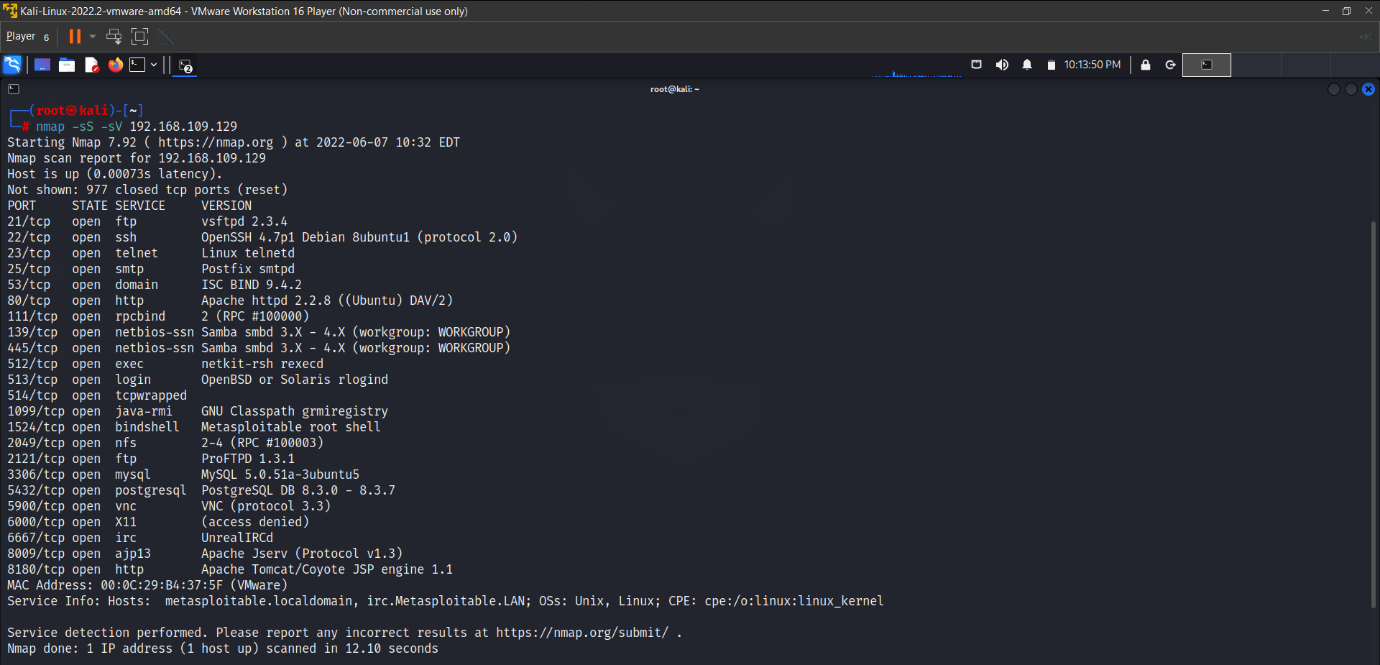


In the kali Linux, login to the root user

Using nmap scan the extracted ip address (192.168.109.129)

Following are the different scans performed on the ip address (192.168.109.129)

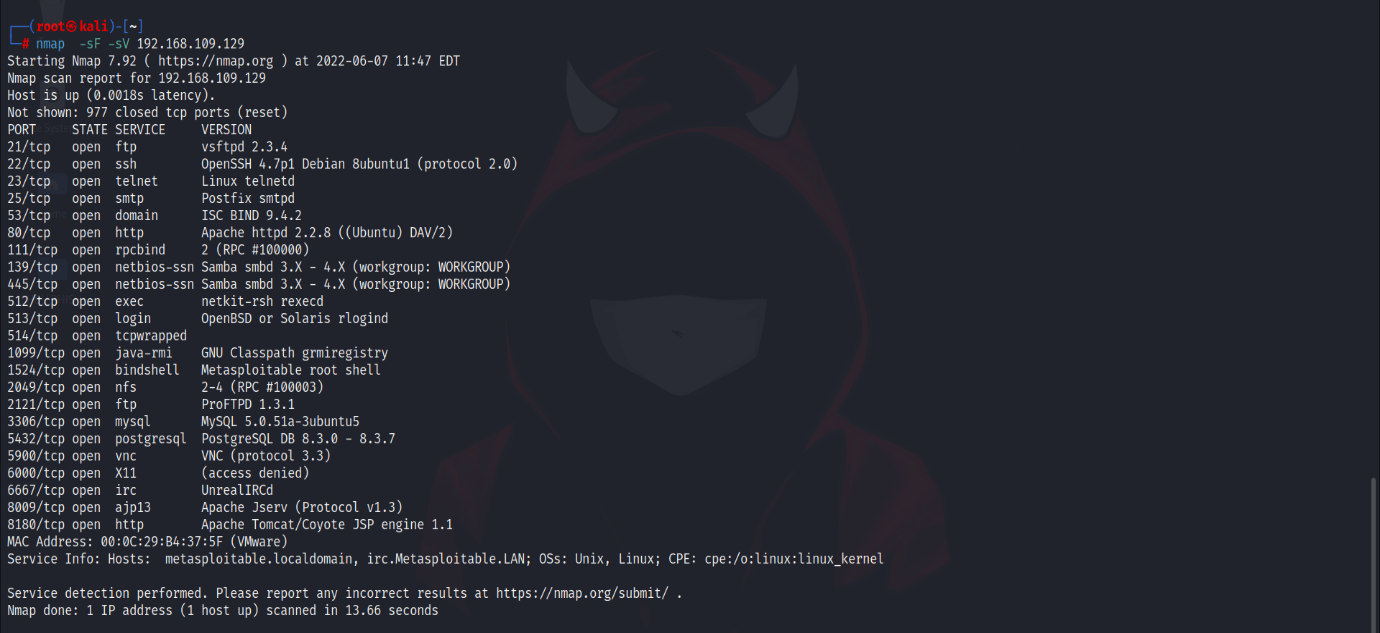
1. Syn Scanning:



1. Acknowledgement Scanning:



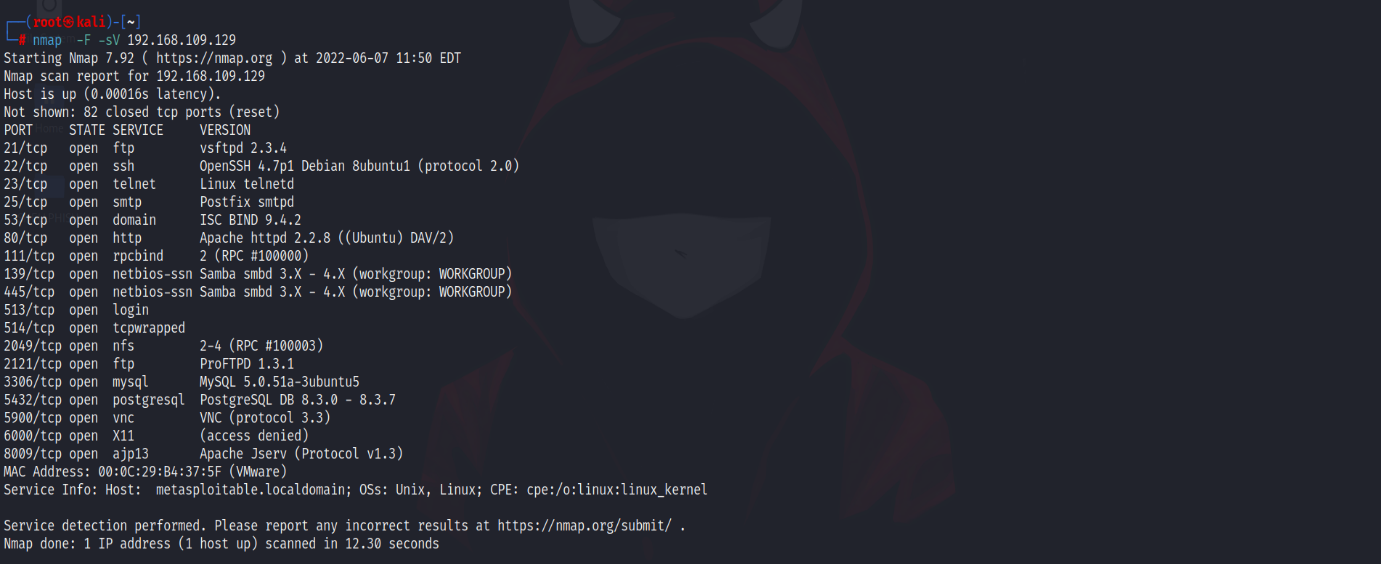
1. Fin Scanning:



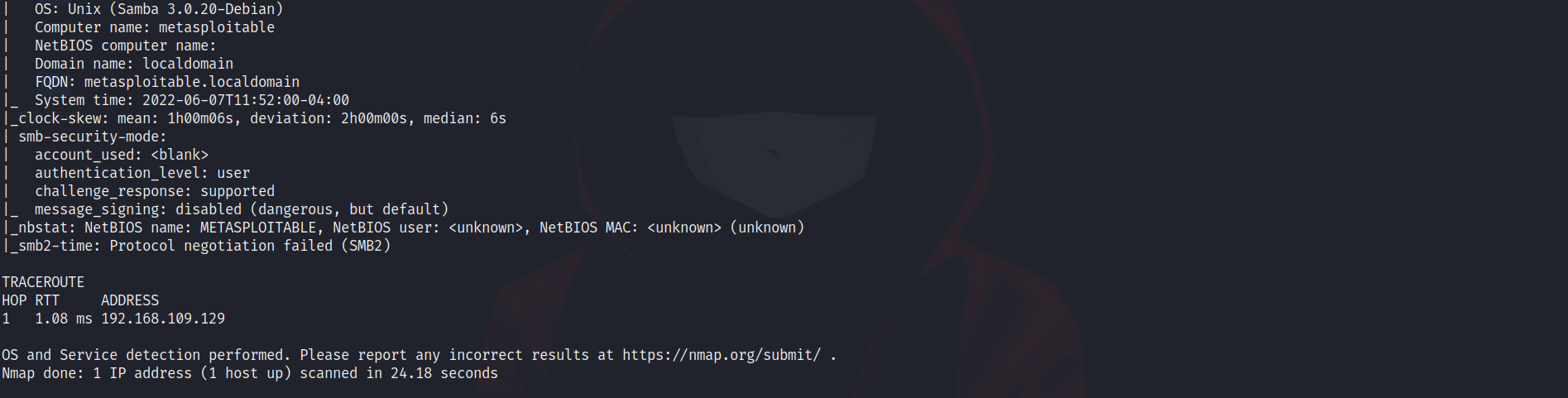
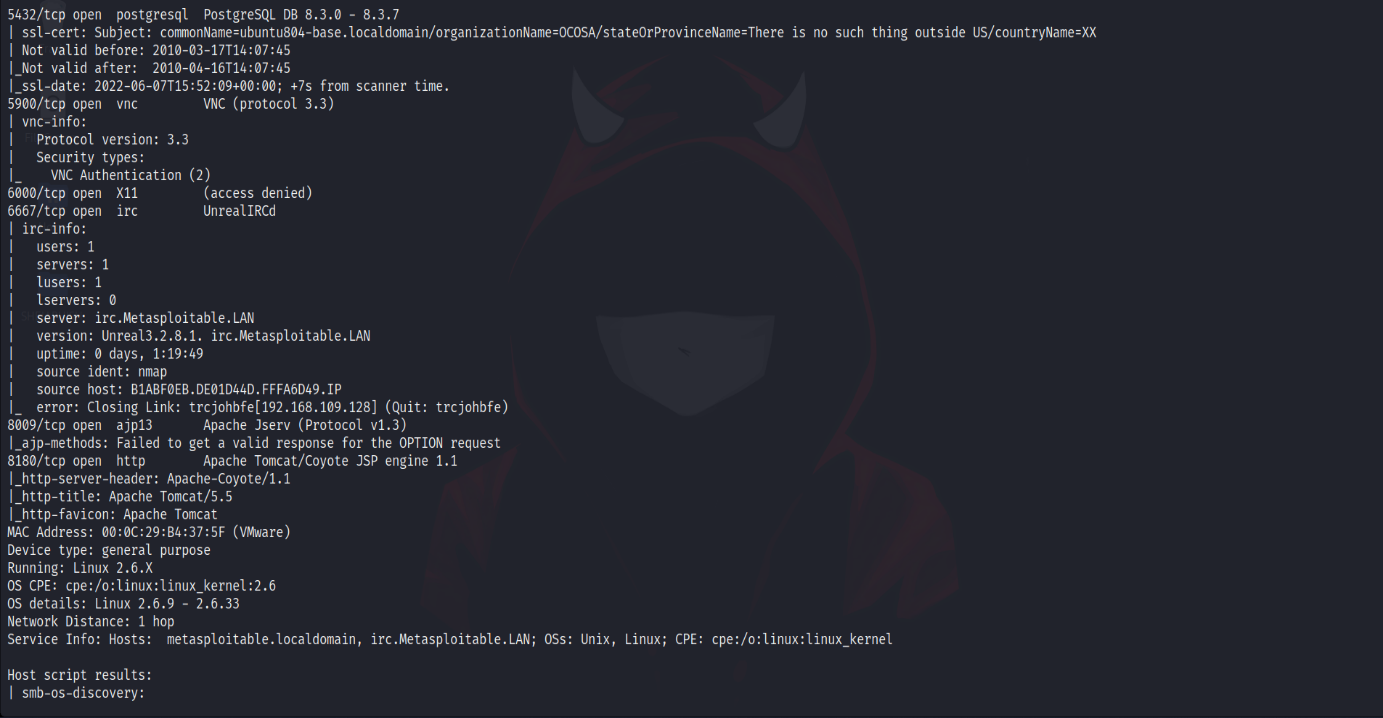
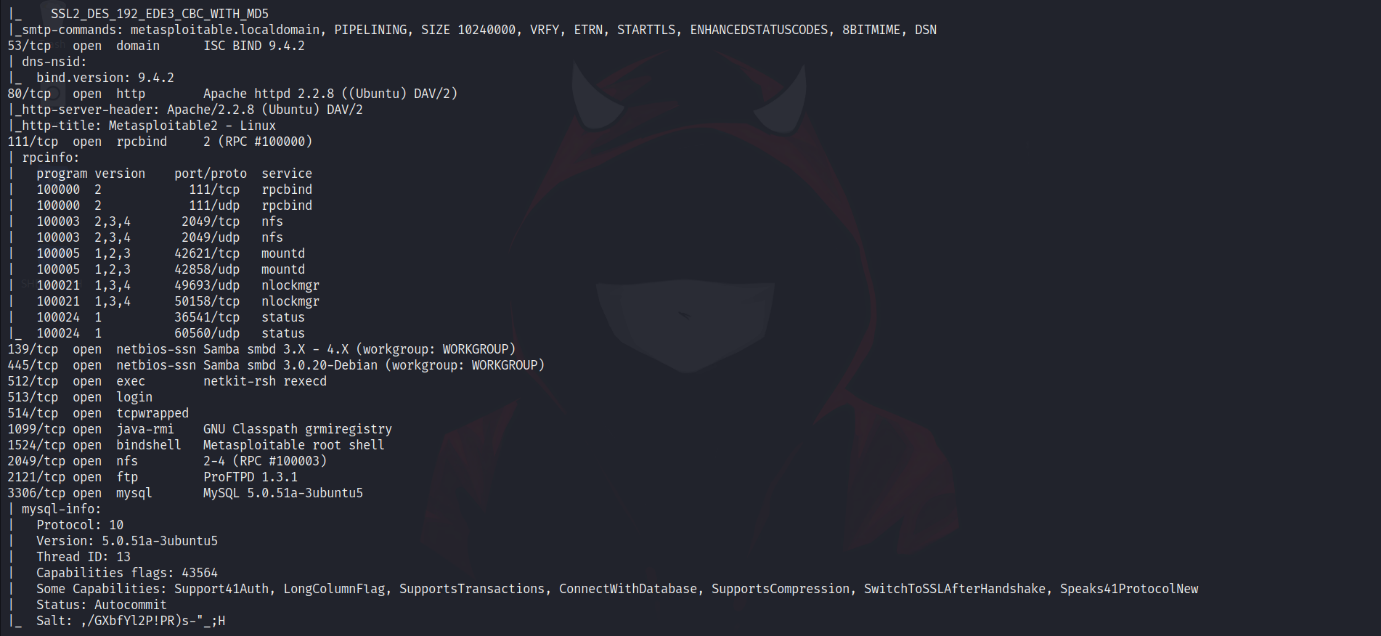
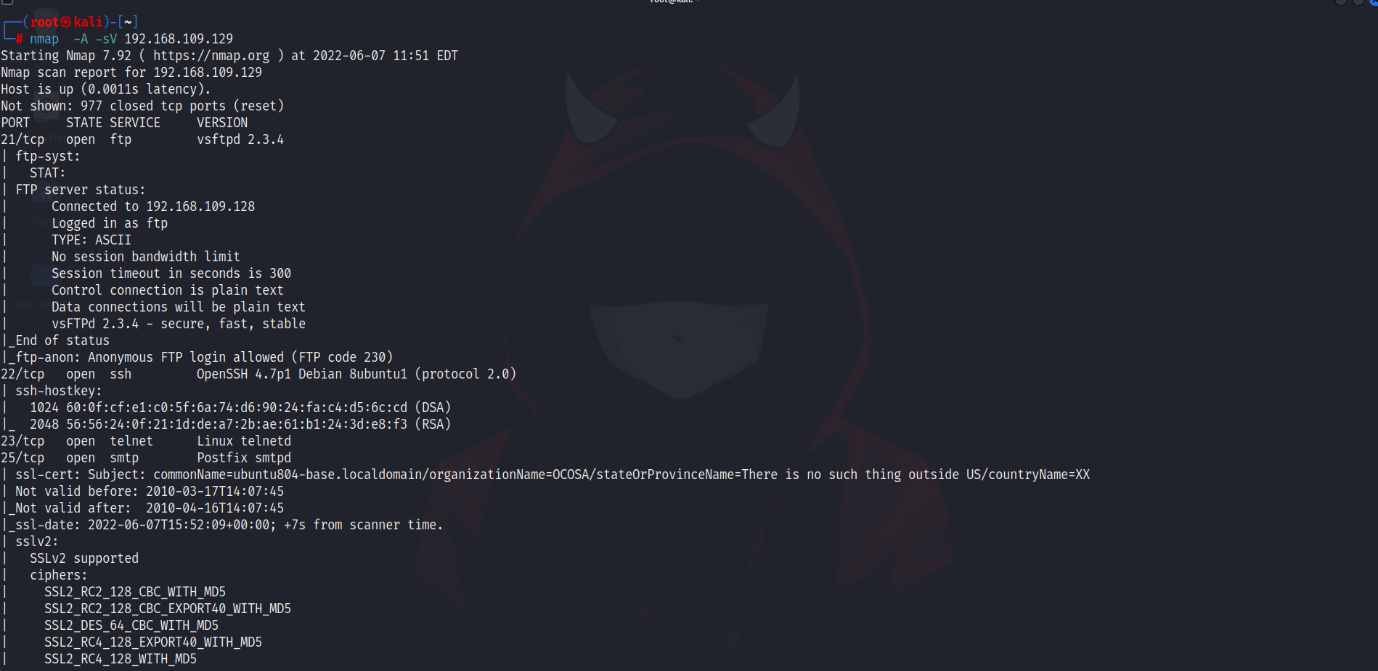
1. Xmas Scanning:



1. Fast Scanning:



1. Aggressive Scanning:



1. TCP Scanning:



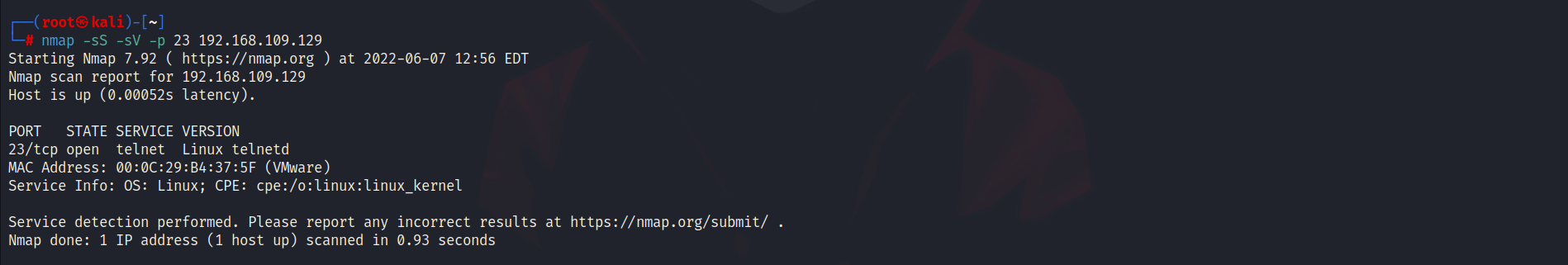
1. UDP Scanning



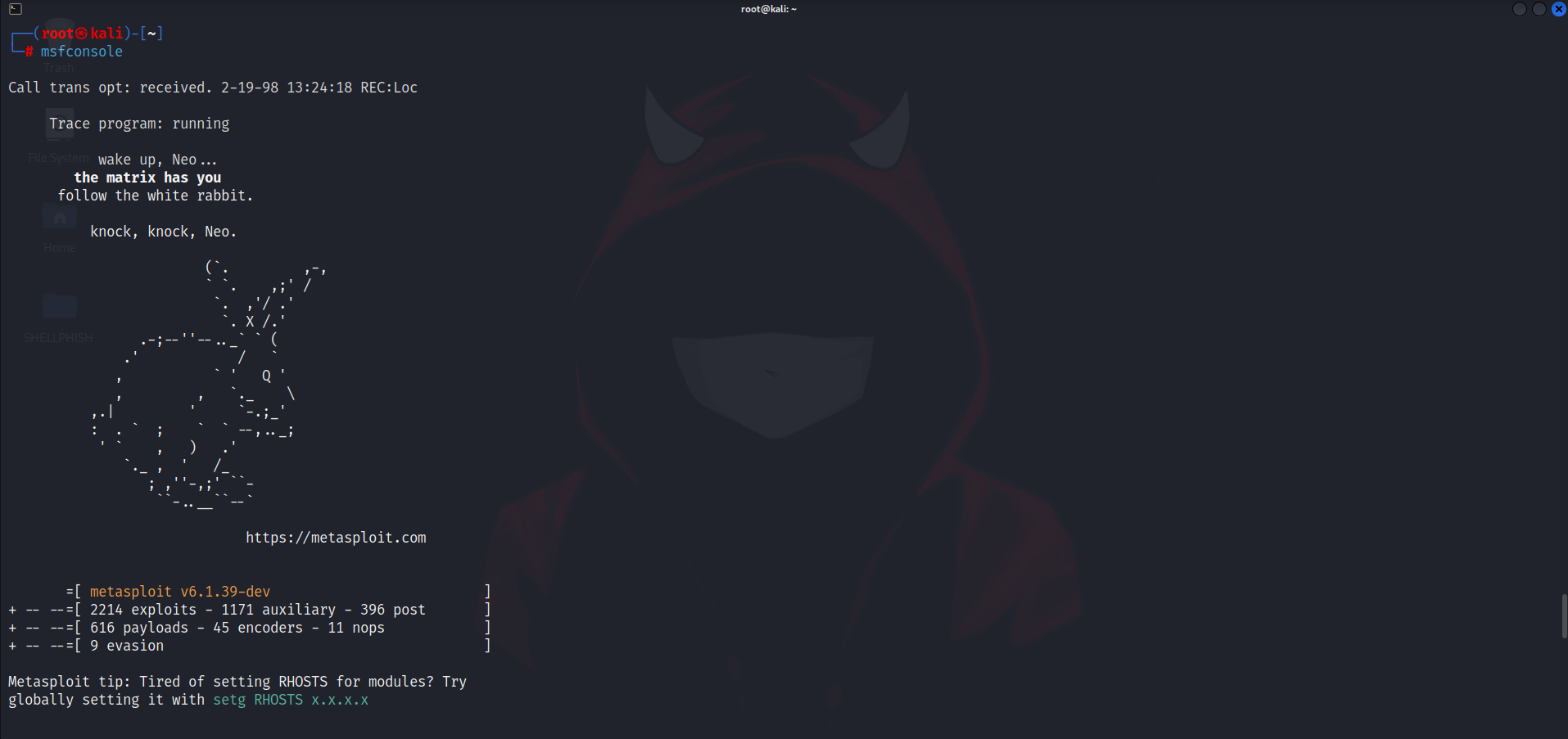
So, from the above scanning methods, we obtained the open port information along with their version details

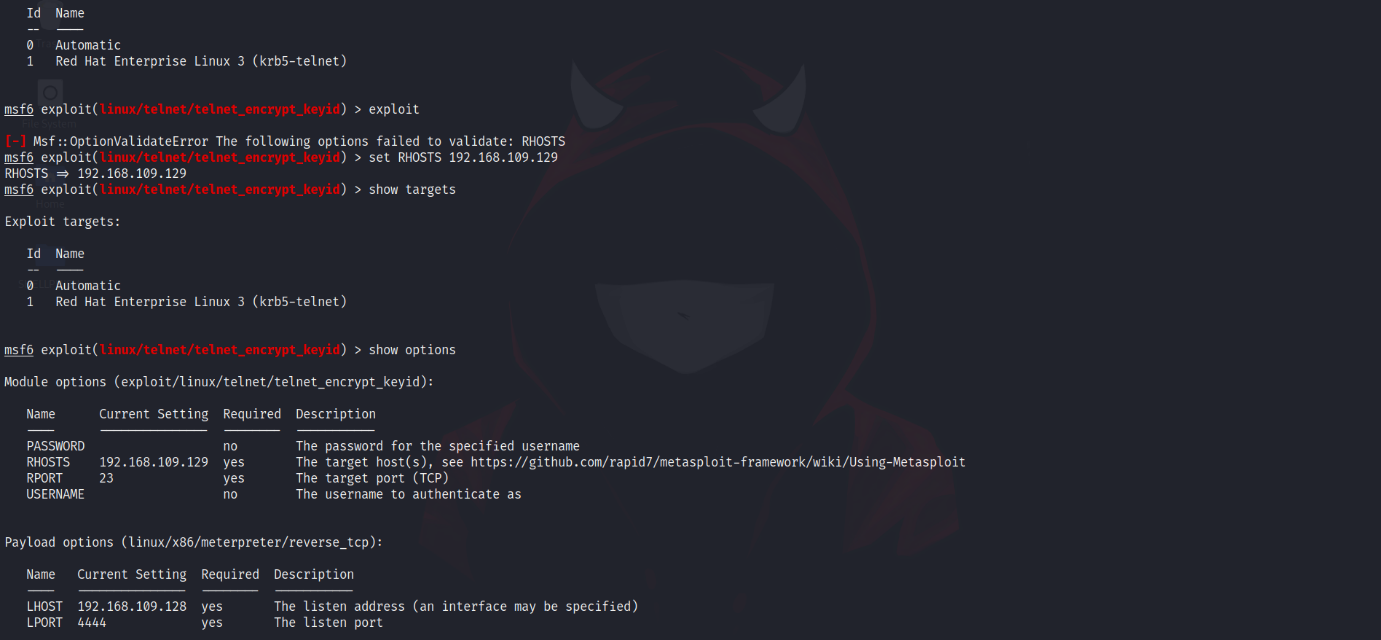
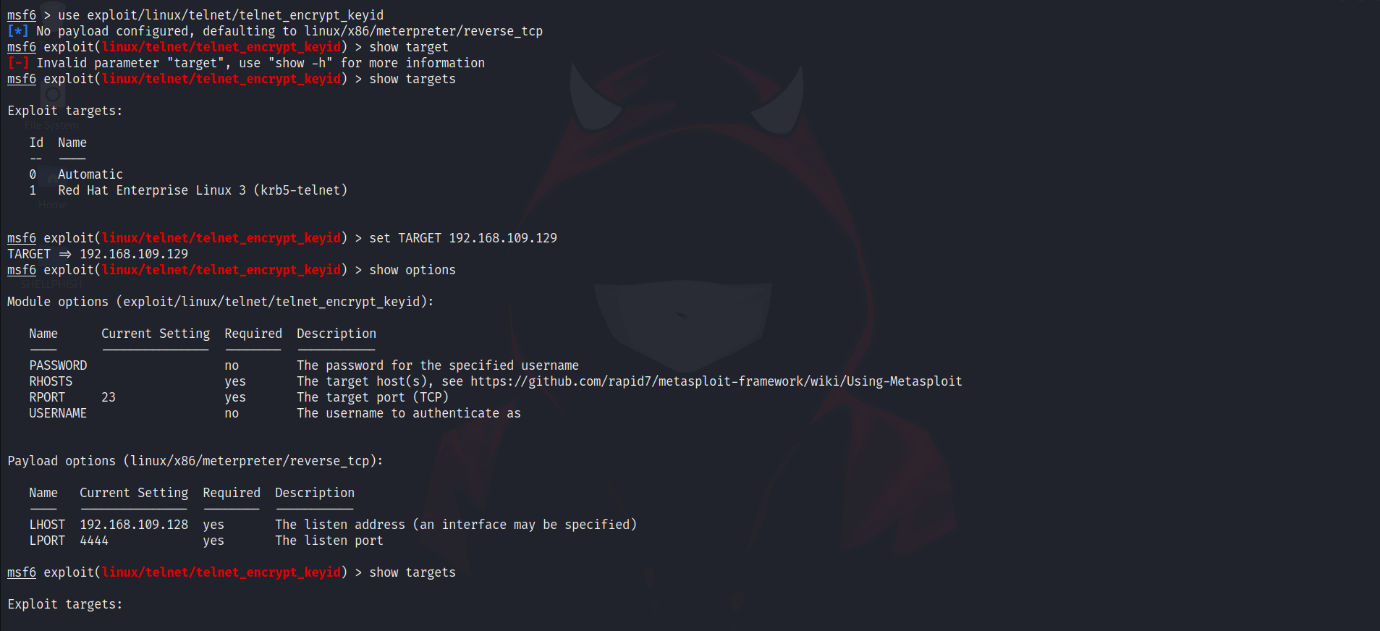
Let us Exploit the following ports using their version details

1. Telnet port:

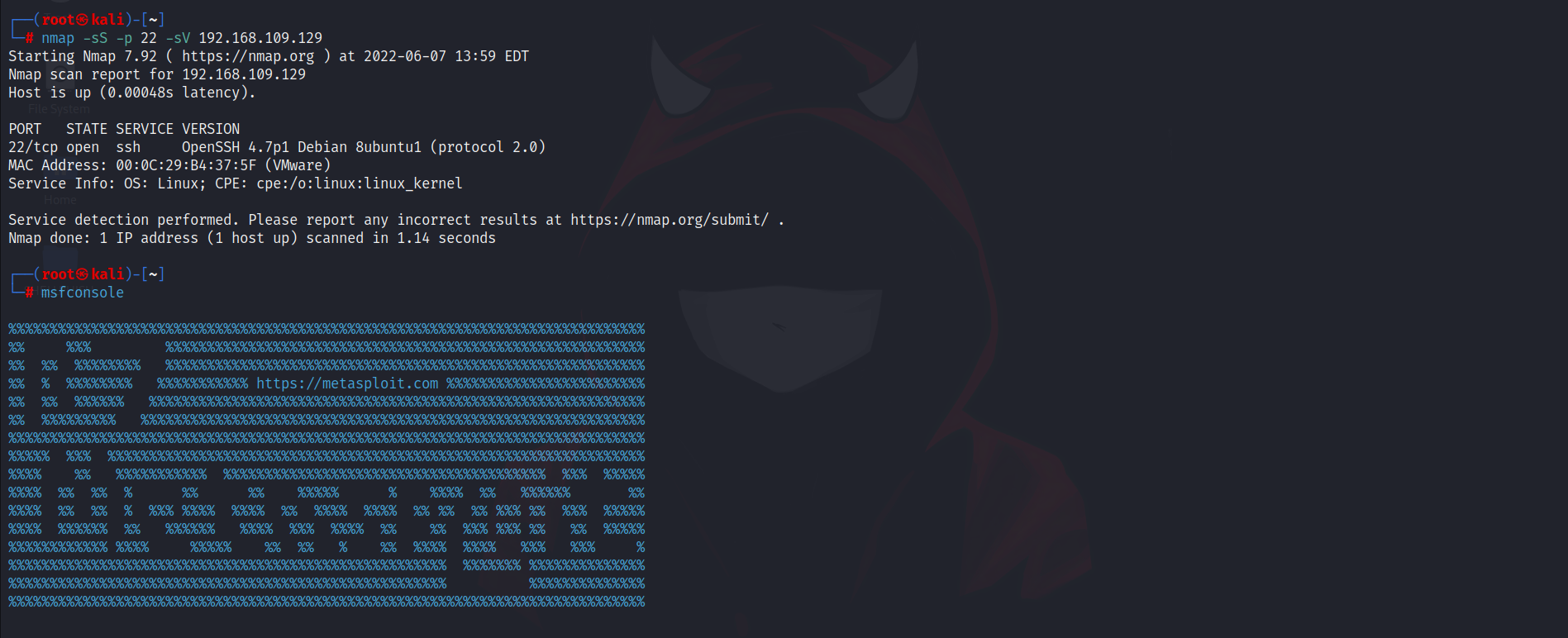


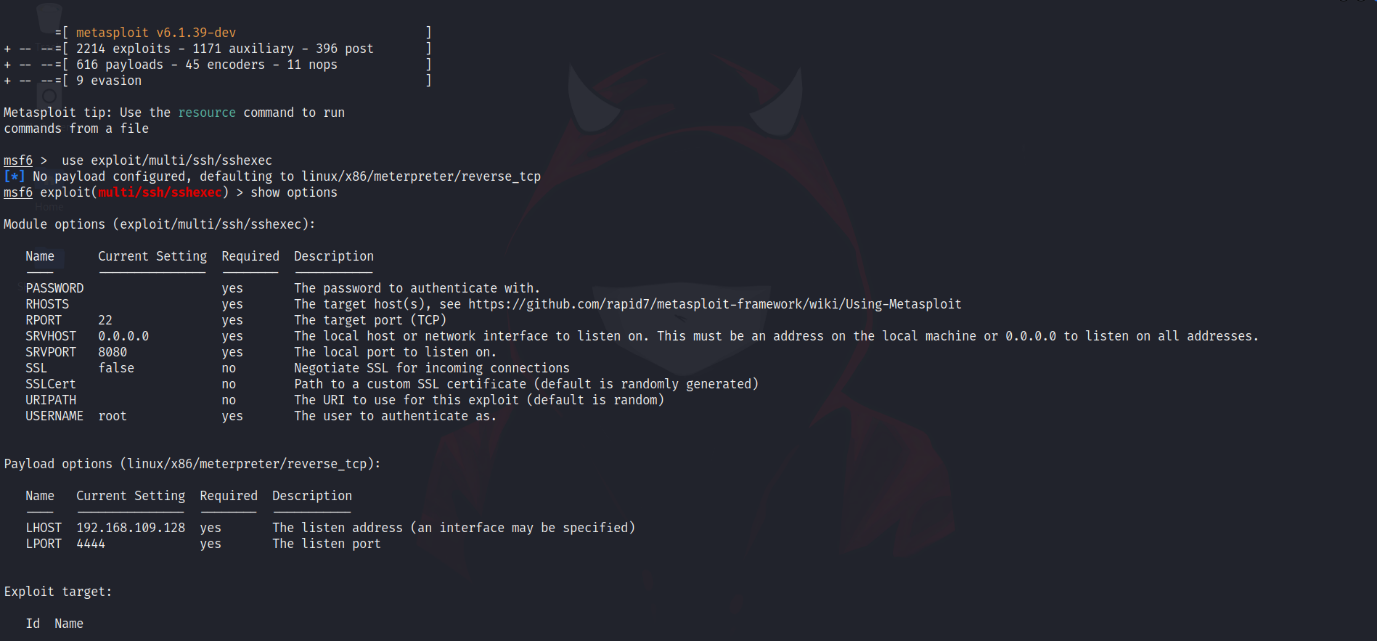
Using Metasploit framework set the target and exploit.

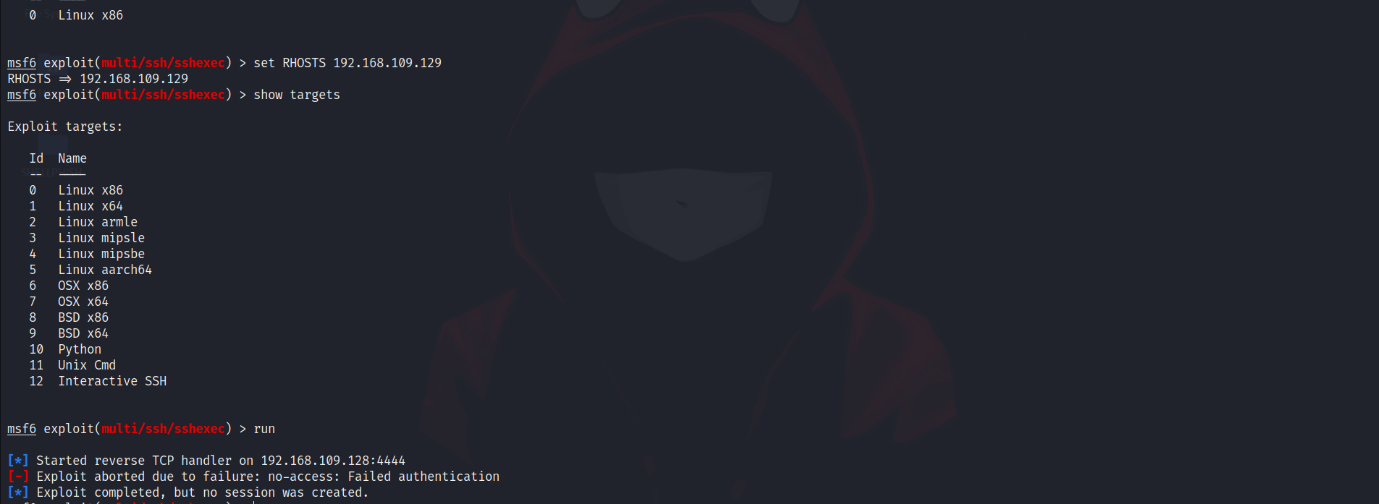




1. SSH:







1. FTP:

