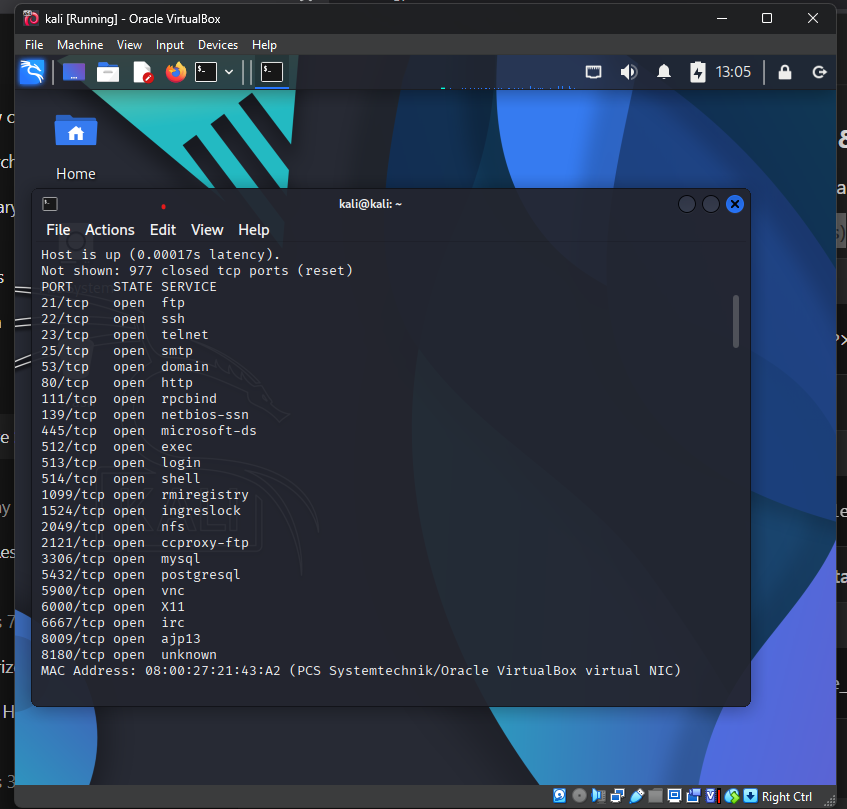
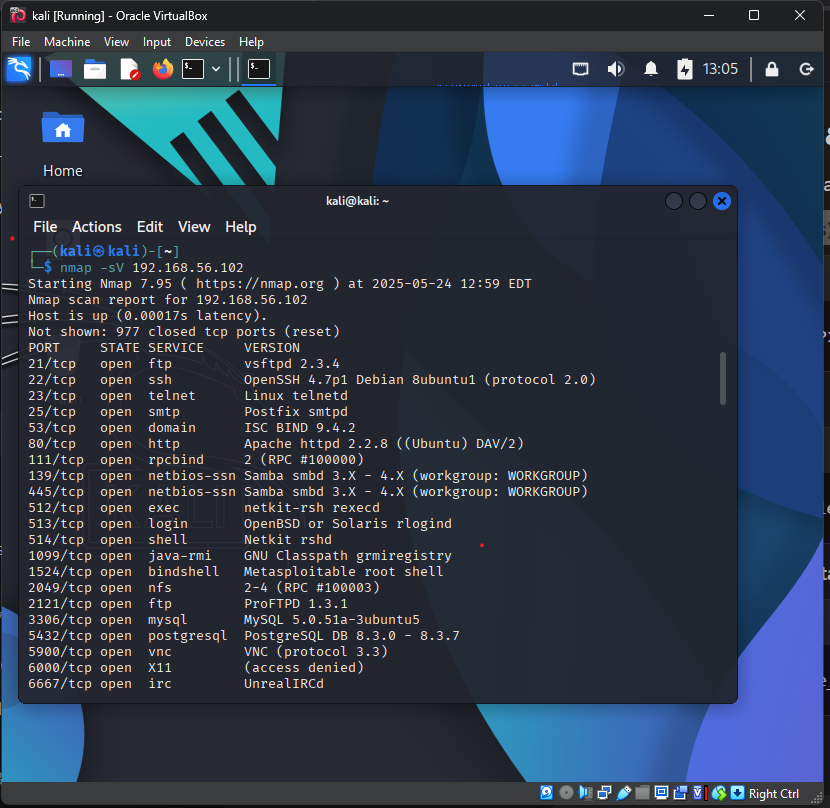
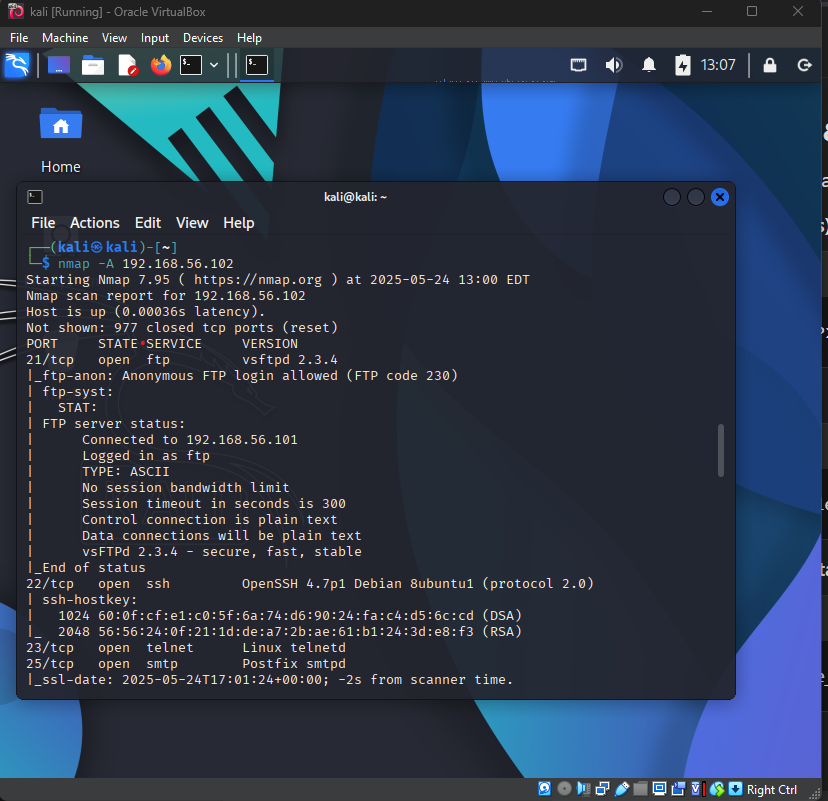
1. Quick Scan



1. Service Version Detection



1. Aggressive Scan



1. How many ports are open on Metasploitable?

Ans: 23

1. List 3 services that are running (with port numbers).

Ans: 21/tcp ftp, 22/tcp ssh, 23/tcp telnet, are up.

1. What does -sV do in Nmap?

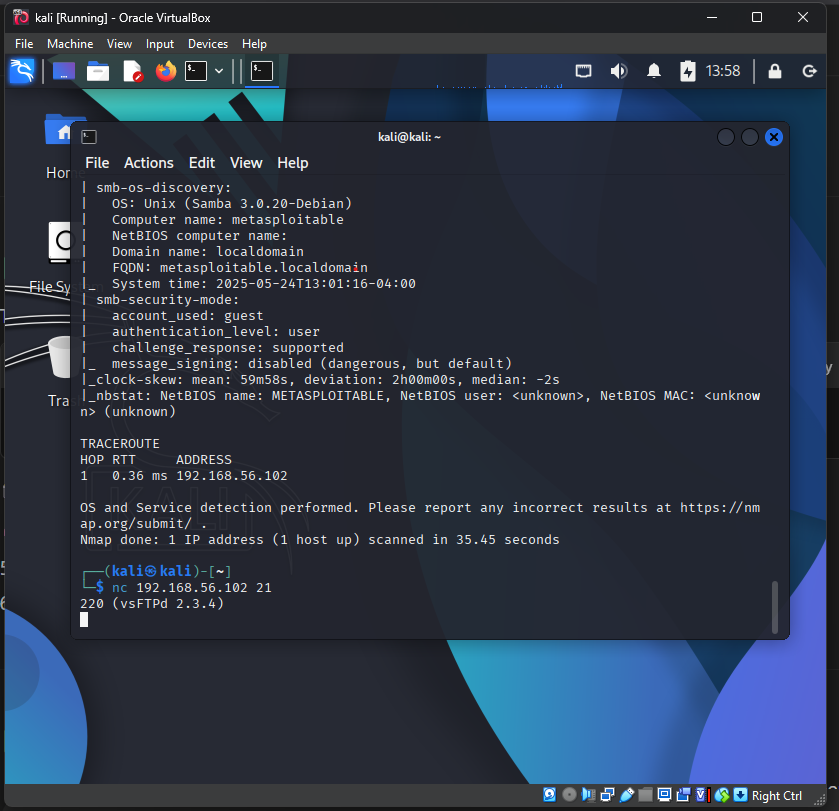
Ans: it scans all the port, state, services and version that are running.

1. What information did the -A scan give that wasn’t in the basic scan?

Ans: it gave me the version detection, OS detection, script scanning and traceroute.

Task 2

Netcat – Manual Banner Grabbing



1. What did the banner tell you about the service?

Ans: what’s the version the pot is running.

1. Why is banner grabbing useful for hackers?

Ans: it reveals exact version and software info. Which help hacker to find venerability and exploit it.