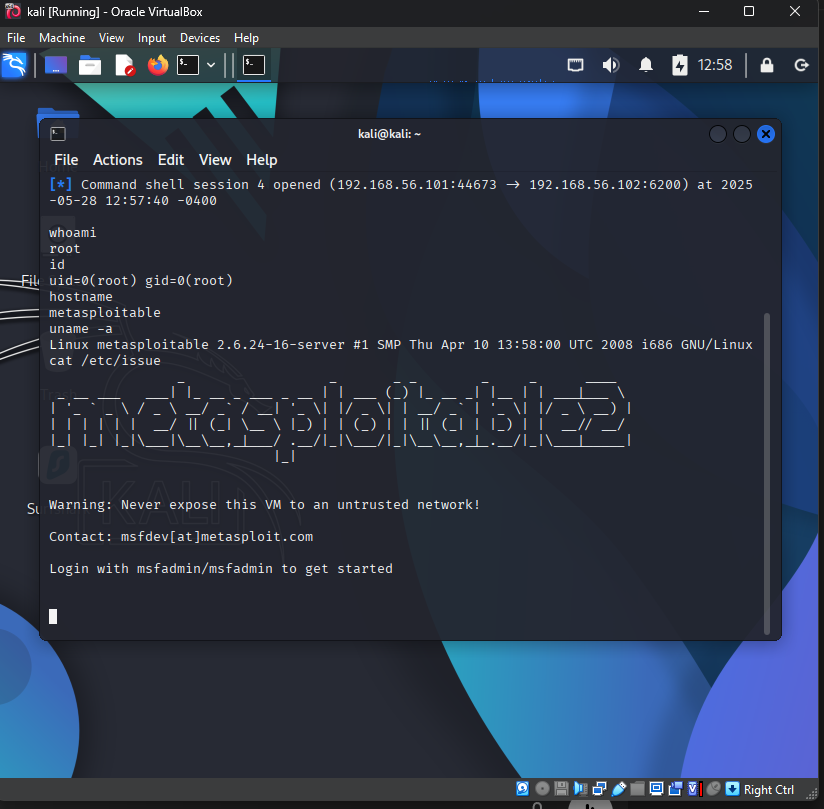
Task 1: **User & System Enumeration**

Once you're inside Metasploitable via the FTP exploit:



1. What OS and kernel version is the target running?

Ans: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux.

1. Who are you logged in as?

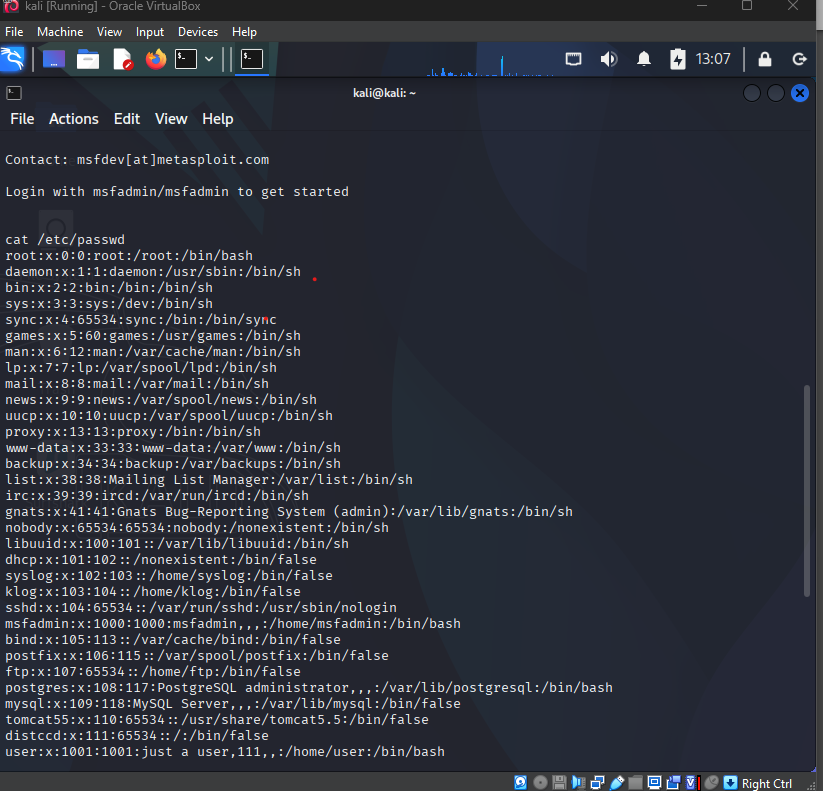
Ans: root user

1. Why is this user privilege level important?

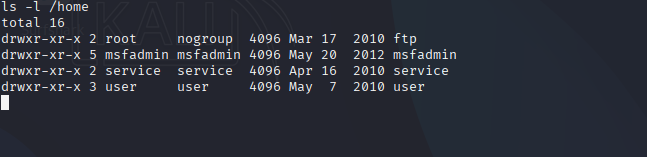
Ans: so that I can get full access of the target system.

Task 2: **List Users & Home Directories**

cat /etc/passwd



ls -l /home



1. What usernames exist on this system?

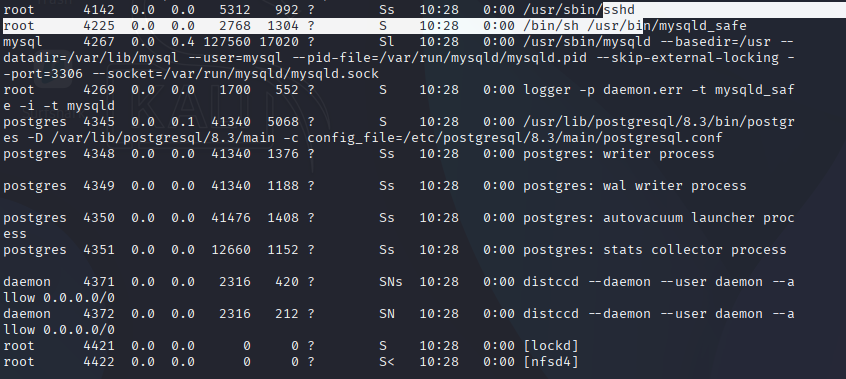
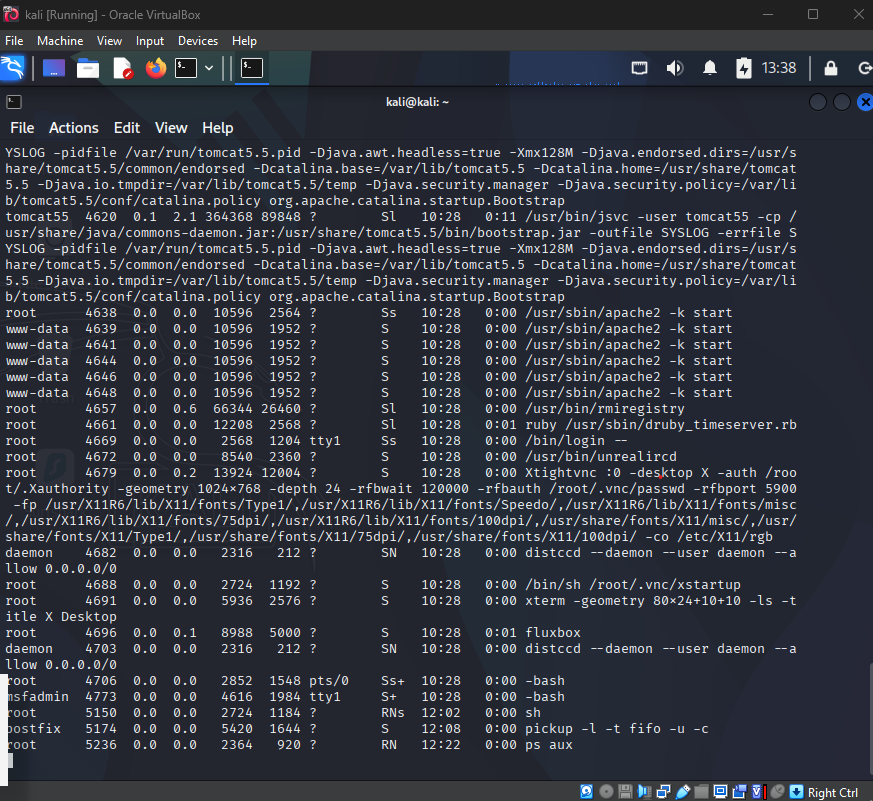
Ans: root, daemon, bin, sys and more.

1. Which home directories look interesting to explore?

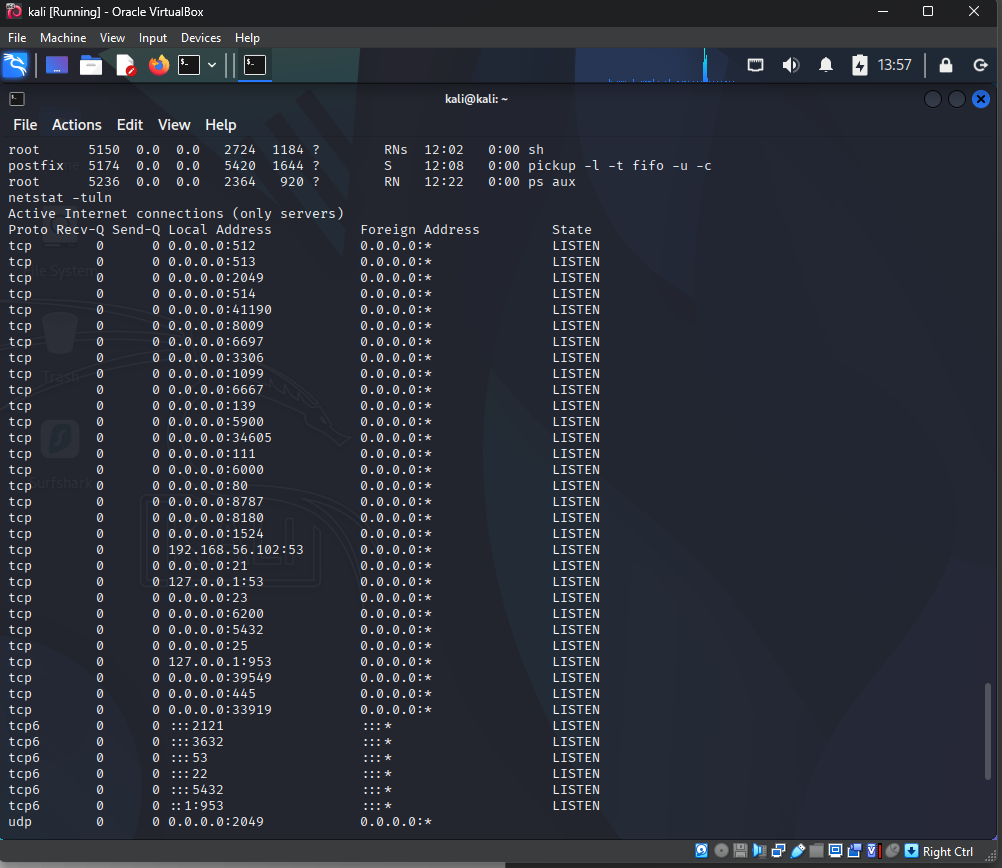
Ans: daemon and msfadmin looks interesting.

Task 3: **Check Running Services & Open Ports**

**Ps aux**



**netstat -tuln**



1. What services are running?

Ans: MySQL, apache2, ssh

1. Which ports are open and listening?

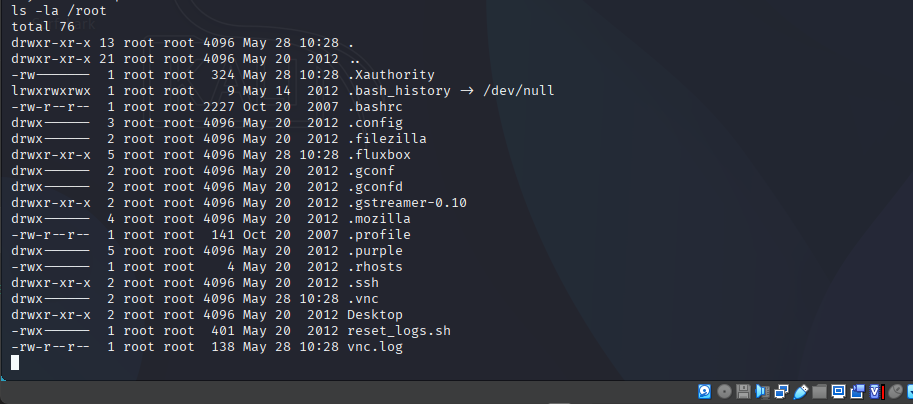
Ans: tcp and tcp6

1. Do you see any services that may be exploitable or worth digging into?

Ans: apache2 looks exploitable.

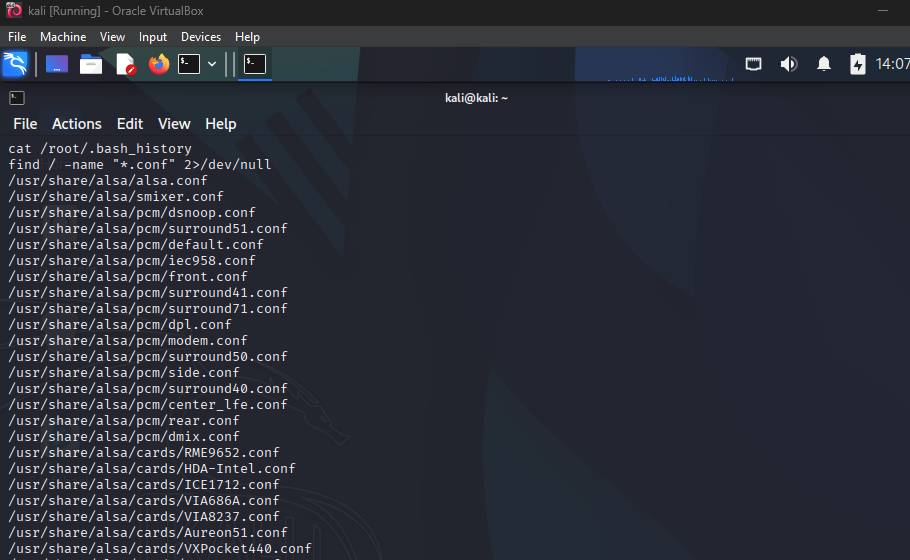
Task 4: **Explore for Sensitive Files**

ls -la /root



cat /root/.bash\_history

find / -name "\*.conf" 2>/dev/null



1. Did you find anything sensitive or useful?

Ans: no.

10. Why are .conf files often a gold mine for attackers?

Ans: Configuration files often store sensitive information in plain text, including database login credentials, API tokens, email passwords, or hardcoded system secrets. Attackers can use these to gain further access or pivot to other services.