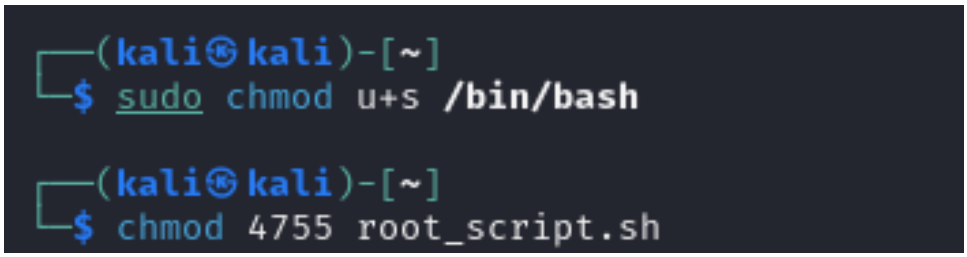
TASK 4

TASK 4:

SUID & Privilege Escalation

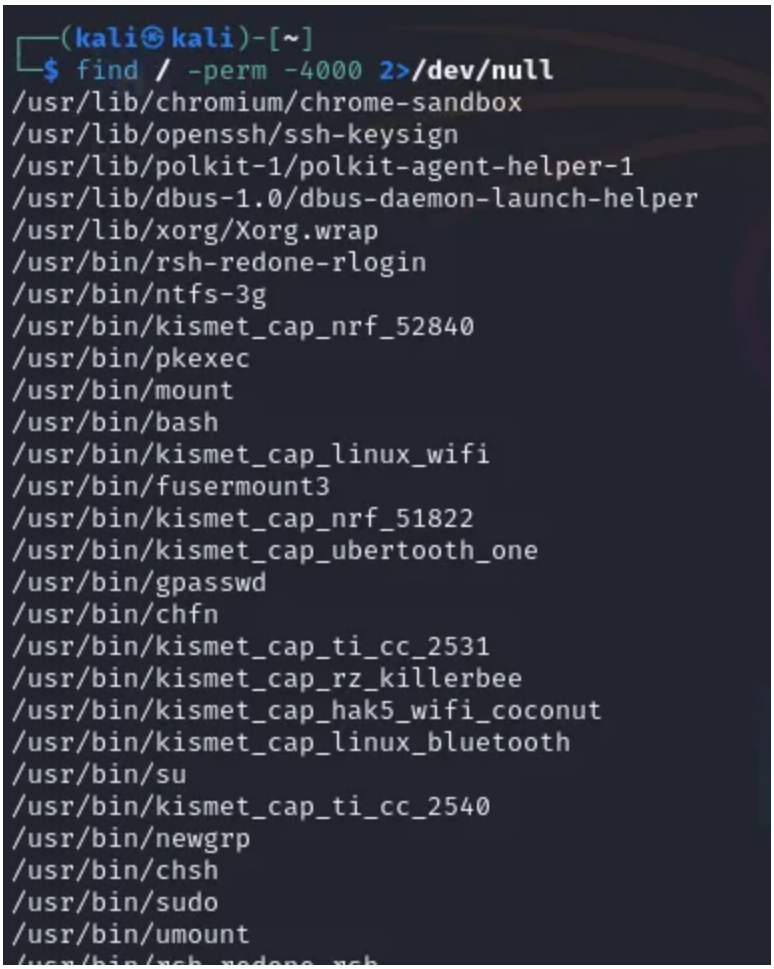
Setup:

1.Setting the SUID bit on **/bin/bash** allows it to run with root privileges. The **4755** permission grants the owner full access while allowing others to read and execute.



Exploit:

To detect SUID misconfigurations, we search for files with the SUID bit enabled, filtering out errors from restricted directories. If a vulnerable file is found, executing it with preserved privileges allows escalation to root access.



Mitigation

To enhance security, remove unnecessary SUID permissions using **chmod -s /bin/bash**, and restrict script execution to specific users by adjusting file ownership with **chown root:trusted_user root_script.sh**and configuring the sudoers file for stricter control.