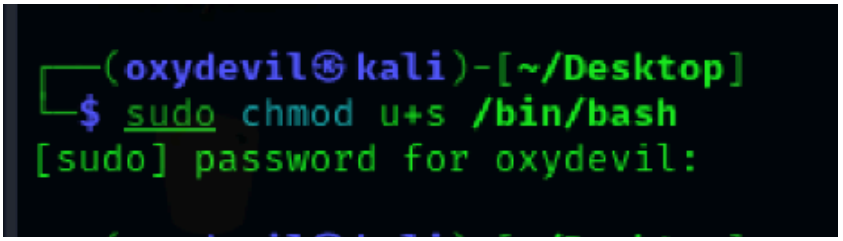
Task 4

SUID & Privilege Escalation

1. The command enables the SUID (Set User ID) bit on /bin/bash, allowing it to run with the owner's (root) privileges.



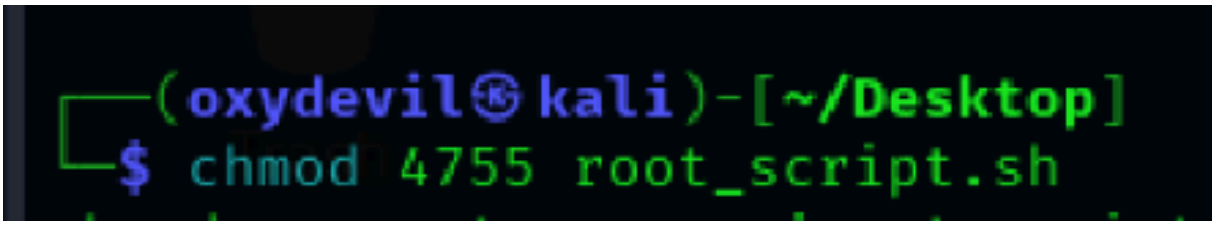
2. Creating a script with root privileges ➤ The 4755 permission setting ensures the following:

   4 → Sets the SUID (Set User ID) bit.

   7 → Grants the owner read (**r**), write (**w**), and execute (**x**) permissions.

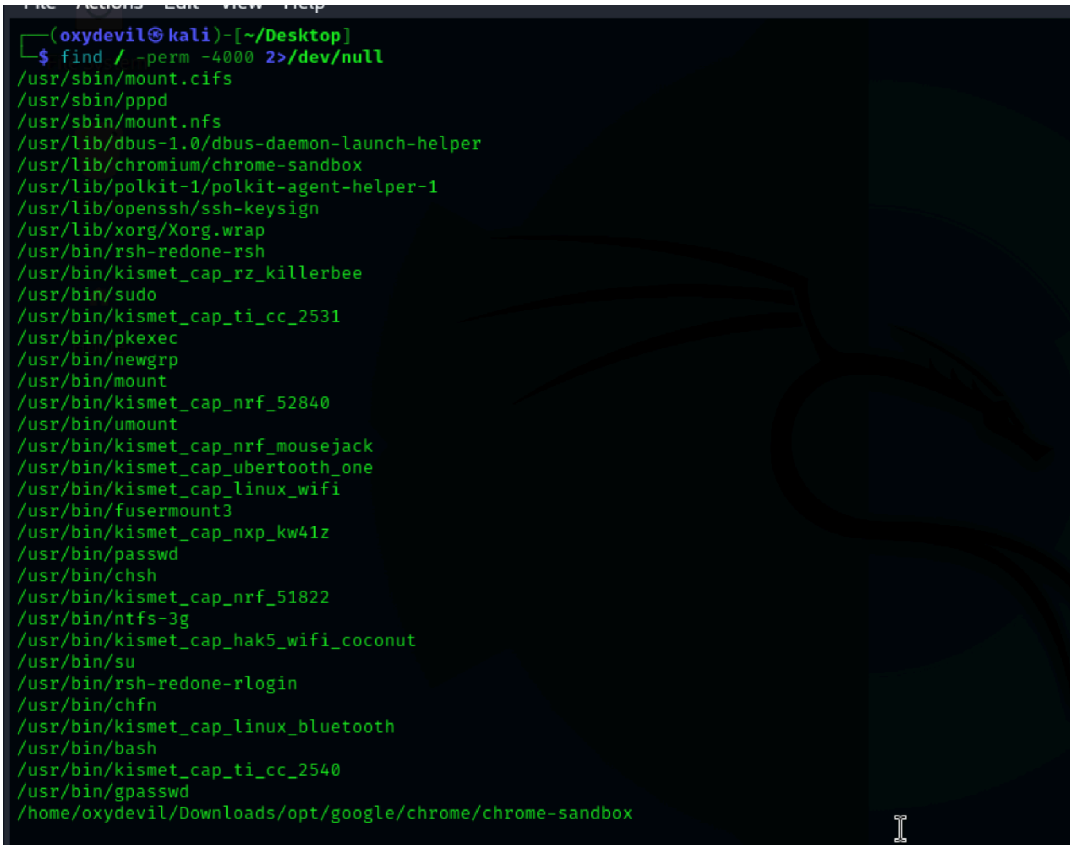
   5 → Grants the group read (**r**) and execute (**x**) permissions.

   5 → Grants others read (**r**) and execute (**x**) permissions.



Exploit

1. To detect SUID misconfigurations, run the command find / -perm -4000 2>/dev/null, which lists files with the SUID bit set while suppressing errors from inaccessible directories. To escalate privileges to root, execute /bin/bash -p, where the -pflag ensures the shell retains elevated privileges, granting root access.



Mitigation

1.To improve security, remove unnecessary SUID permissions with chmod -s /bin/bash, and limit script execution to specific users by adjusting file ownership using chown root:trusted_user root_script.sh. Additionally, configure the sudoers file for stricter access control.