TASK 4: SUID & Privilege Escalation

Setup:

1. The command sets the SUID (Set User ID) bit on **/bin/bash** , enabling it to execute with the owner's (root) privileges.

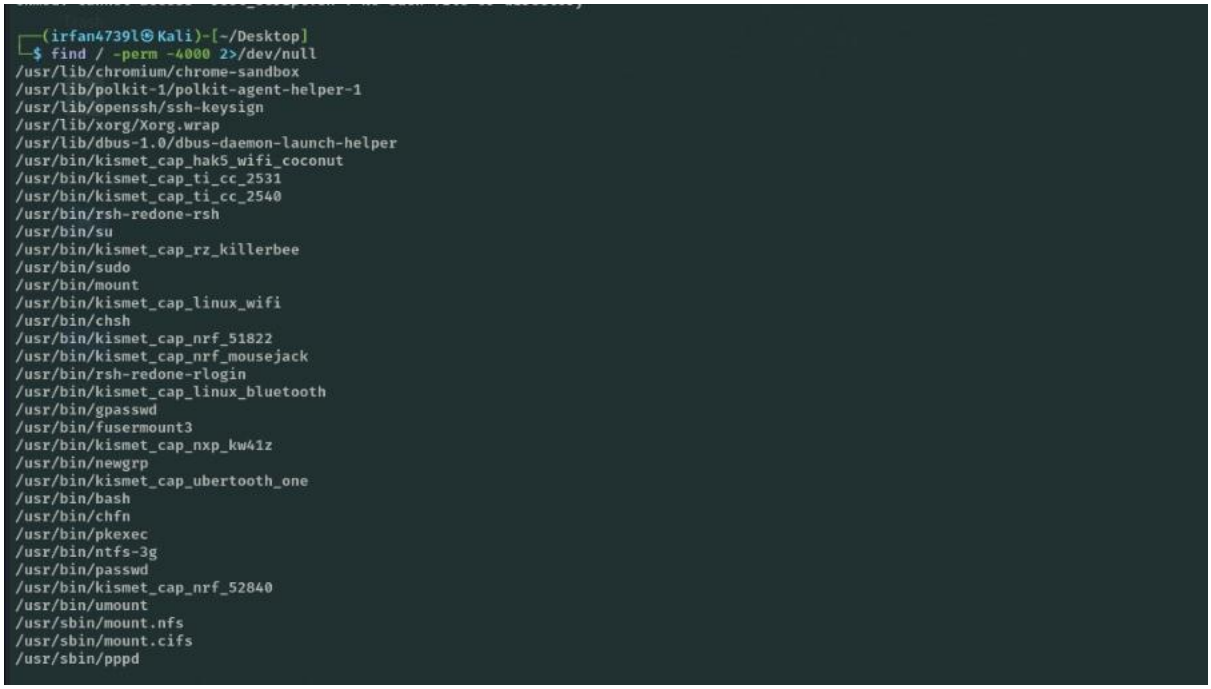
```
┌──(irfan4739l㉿Kali)-[~/Desktop]
└─$ sudo chmod u+s /bin/bash
[sudo] password for irfan4739l:
```

Create 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.

```
┌──(irfan4739l㉿Kali)-[~/Desktop]
└─$ chmod 4755 root_script.sh
```

Exploit:

To identify SUID misconfigurations, use the command **find / -perm -4000 2>/dev/null** , which lists files with the SUID bit set while suppressing error messages from inaccessible directories. To escalate privileges to root, execute **/bin/bash -p** , where the **-p** flag ensures the shell retains elevated privileges, granting 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.