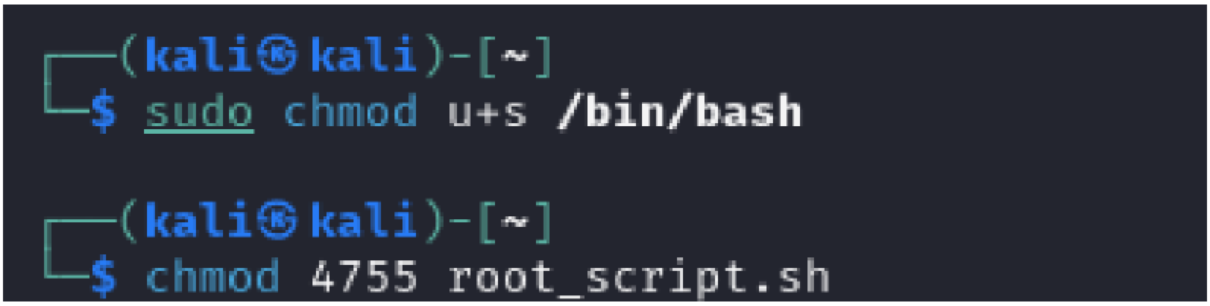
POC TASK 4

1)

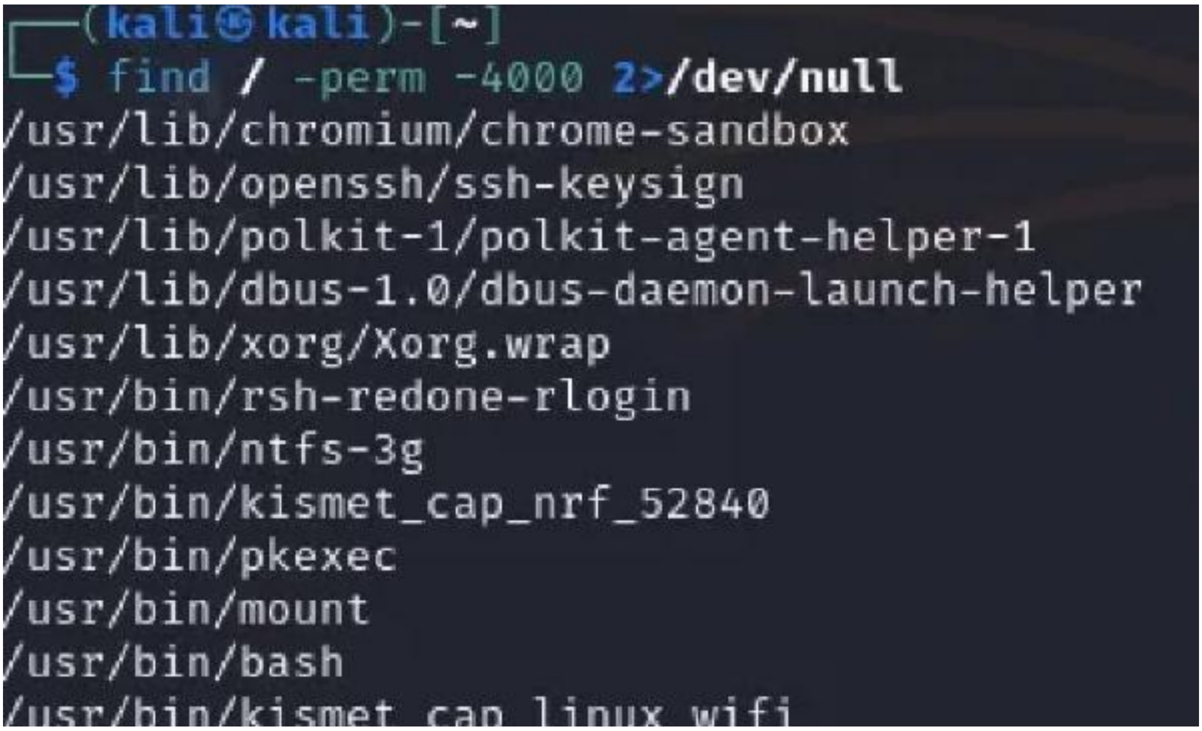


```
┌──(kali㉿kali)-[~]
└─$ sudo chmod u+s /bin/bash

┌──(kali㉿kali)-[~]
└─$ chmod 4755 root_script.sh
```

- The “chmod u+s /bin/bash” used to run root privileges
- The 4755 grants the owner full access

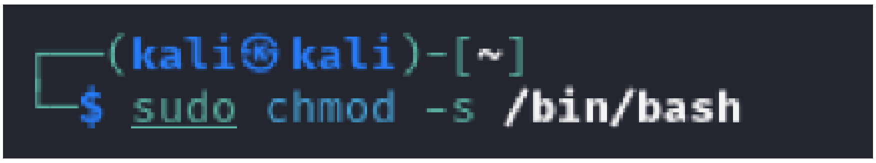
2)



```
┌──(kali㉿kali)-[~]
└─$ find / -perm -4000 2>/dev/null
/usr/lib/chromium/chrome-sandbox
/usr/lib/openssh/ssh-keysign
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/bin/rsh-redone-rlogin
/usr/bin/ntfs-3g
/usr/bin/kismet_cap_nrf_52840
/usr/bin/pkexec
/usr/bin/mount
/usr/bin/bash
/usr/bin/kismet_cap_linux_wifi
```

- We search for files with SUID to detect misconfiguration
- If any vulnerable file is found it privileges it

3)



```
┌──(kali㉿kali)-[~]
└─$ sudo chmod -s /bin/bash
```

We use “chmod -s /bin/bash” to enhance security.