

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

```
(irfan4739l@Kali)-[~/Desktop]
$ find / -perm -4000 2>/dev/null
/usr/lib/chromium/chrome-sandbox
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/xorg/Xorg.wrap
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/kismet_cap_hak5_wifi_coconut
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/kismet_cap_ti_cc_2540
/usr/bin/rsh-redone-rsh
/usr/bin/su
/usr/bin/kismet_cap_rz_killerbee
/usr/bin/sudo
/usr/bin/mount
/usr/bin/kismet_cap_linux_wifi
/usr/bin/chsh
/usr/bin/kismet_cap_nrf_51822
/usr/bin/kismet_cap_nrf_mousejack
/usr/bin/rsh-redone-rlogin
/usr/bin/kismet_cap_linux_bluetooth
/usr/bin/gpasswd
/usr/bin/fusermount3
/usr/bin/kismet_cap_nxp_kw41z
/usr/bin/newgrp
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/bash
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/ntfs-3g
/usr/bin/passwd
/usr/bin/kismet_cap_nrf_52840
/usr/bin/umount
/usr/sbin/mount.nfs
/usr/sbin/mount.cifs
/usr/sbin/pppd
```

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.

```
(irfan4739l@Kali)-[~/Desktop]
$ sudo chmod -s /bin/bash
```

