

TASK 4

TASK 4:

SUID & Privilege Escalation

Setup:

1. Setting the SUID bit on **/bin/bash** allows it to run with root privileges. The **4755** permission grants the owner full access while allowing others to read and execute.

```
(kali㉿kali)-[~]  
$ sudo chmod u+s /bin/bash  
  
(kali㉿kali)-[~]  
$ chmod 4755 root_script.sh
```

Exploit:

To detect SUID misconfigurations, we search for files with the SUID bit enabled, filtering out errors from restricted directories. If a vulnerable file is found, executing it with preserved privileges allows escalation to root access.

```

(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
/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

```

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.

```

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

```