PoC Task 4: SUID & Privilege Escalation

1) Setup

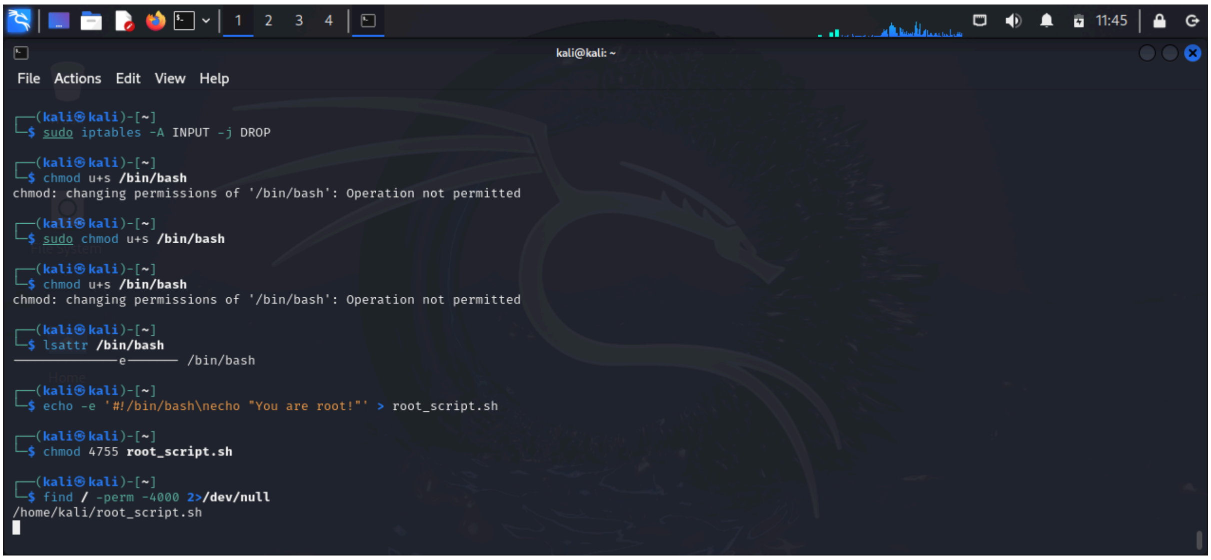
1.1) Set the SUID bit on /bin/bash:

chmod u+s /bin/bash

1.2) Create a script running as root:

echo -e '#!/bin/bash\necho "You are root!"' > root_script.sh

chmod 4755 root_script.sh

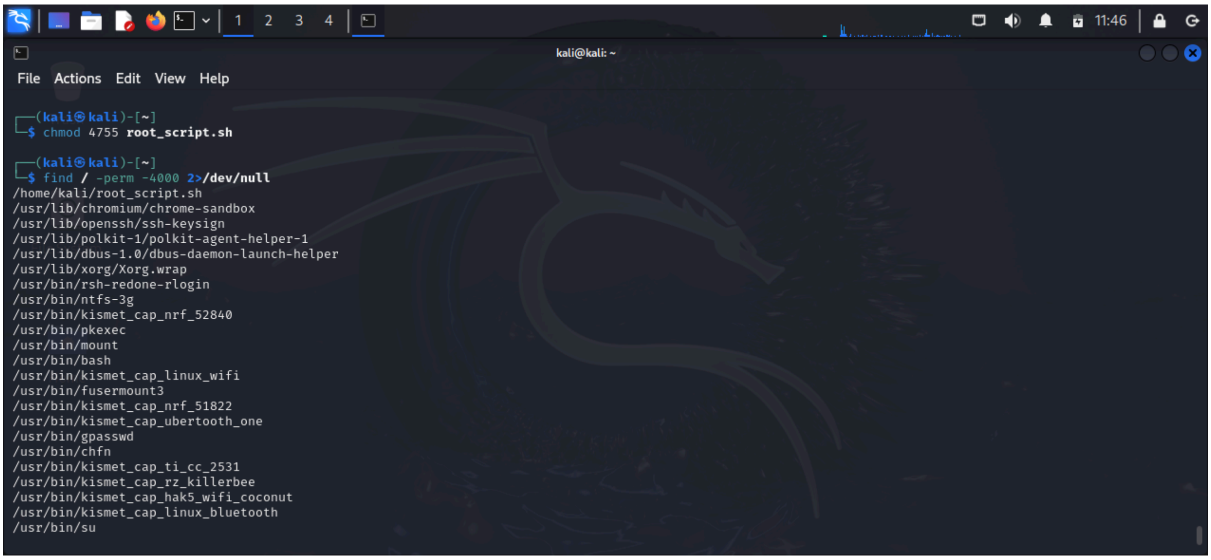


```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -j DROP

┌──(kali㉿kali)-[~]
└─$ chmod u+s /bin/bash
chmod: changing permissions of '/bin/bash': Operation not permitted

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

┌──(kali㉿kali)-[~]
└─$ chmod u+s /bin/bash
chmod: changing permissions of '/bin/bash': Operation not permitted

┌──(kali㉿kali)-[~]
└─$ lsattr /bin/bash
──────────────e──────── /bin/bash

┌──(kali㉿kali)-[~]
└─$ echo -e '#!/bin/bash\necho "You are root!"' > root_script.sh

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

┌──(kali㉿kali)-[~]
└─$ find / -perm -4000 2>/dev/null
/home/kali/root_script.sh
█
```

2) Exploit

2.1) Find SUID misconfigurations:

find / -perm -4000 2>/dev/null



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

┌──(kali㉿kali)-[~]
└─$ find / -perm -4000 2>/dev/null
/home/kali/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
```

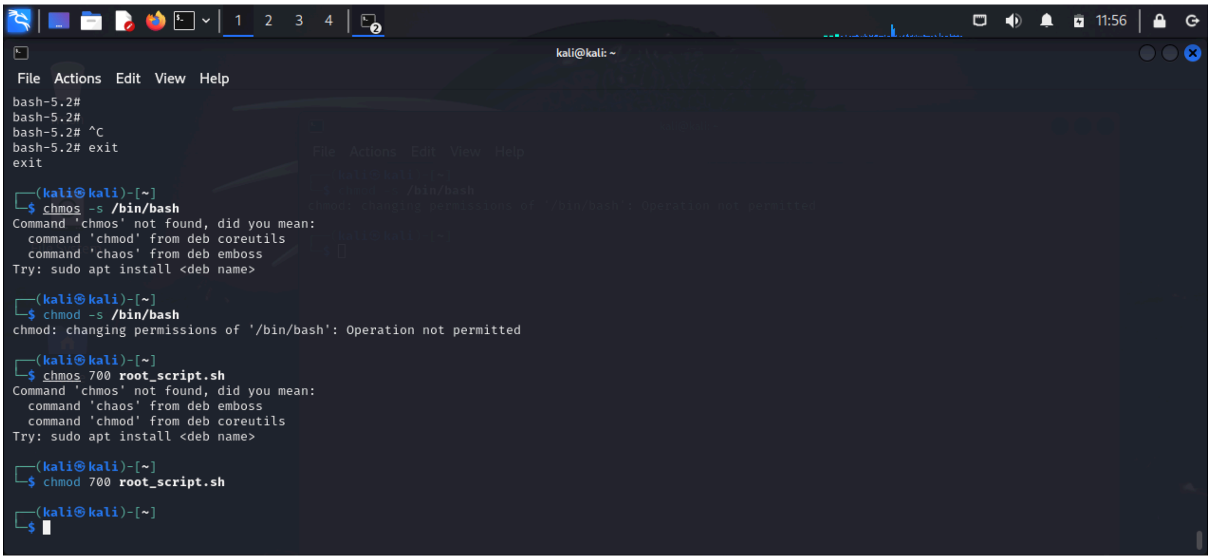
3) Mitigation

3.1) Remove SUID:

chmod -s /bin/bash

3.2) Restrict script execution:

chmod 700 root_script.sh



```
bash-5.2#
bash-5.2#
bash-5.2# ^C
bash-5.2# exit
exit

┌──(kali㉿kali)-[~]
└─$ chmos -s /bin/bash
Command 'chmos' not found, did you mean:
  command 'chmod' from deb coreutils
  command 'chaos' from deb emboss
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$ chmod -s /bin/bash
chmod: changing permissions of '/bin/bash': Operation not permitted

┌──(kali㉿kali)-[~]
└─$ chmos 700 root_script.sh
Command 'chmos' not found, did you mean:
  command 'chaos' from deb emboss
  command 'chmod' from deb coreutils
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$ chmod 700 root_script.sh

┌──(kali㉿kali)-[~]
└─$ █
```