

## Task 4: SUID & Privilege Escalation

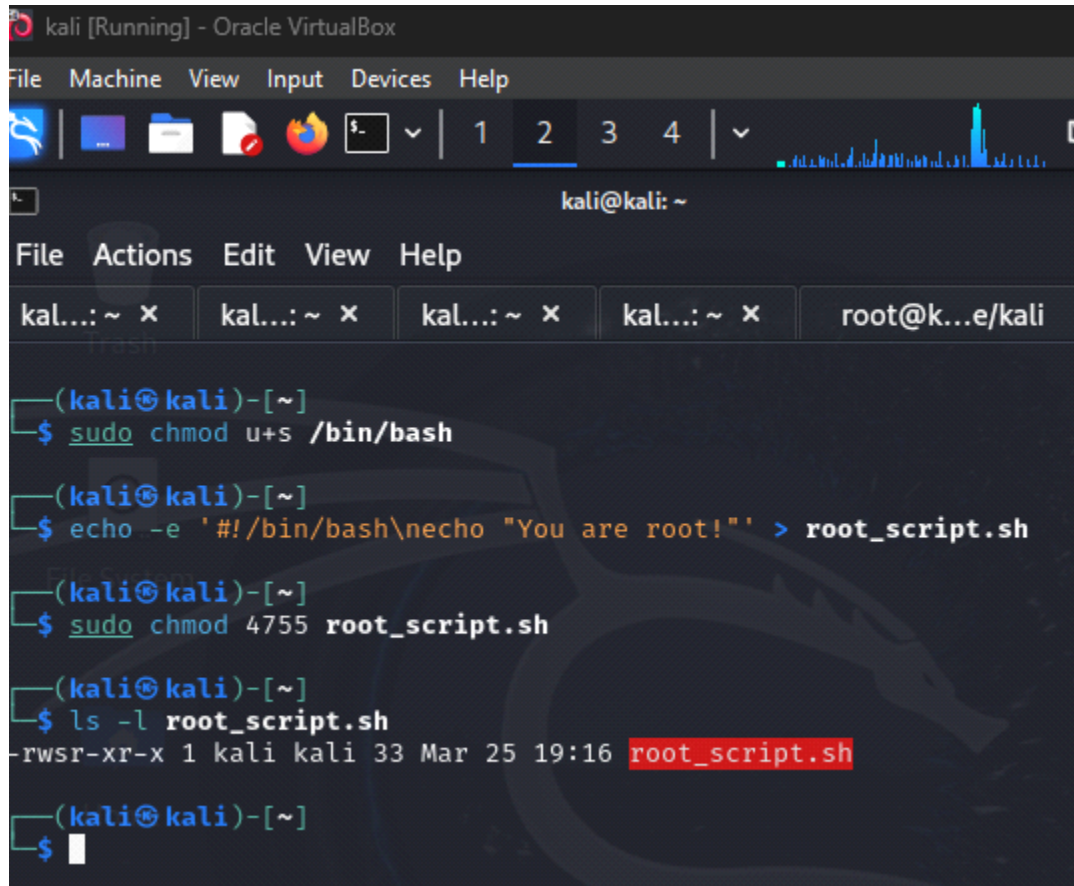
### 1. Setup

sudo chmod u+s /bin/bash ls -l /bin/bash

echo -e "#!/bin/bash\nnecho 'Root Privileges Acquired'\nid" | sudo tee /root\_script.sh # Create a script with root privileges

sudo chmod 4755 /root\_script.sh

ls -l /root\_script.sh

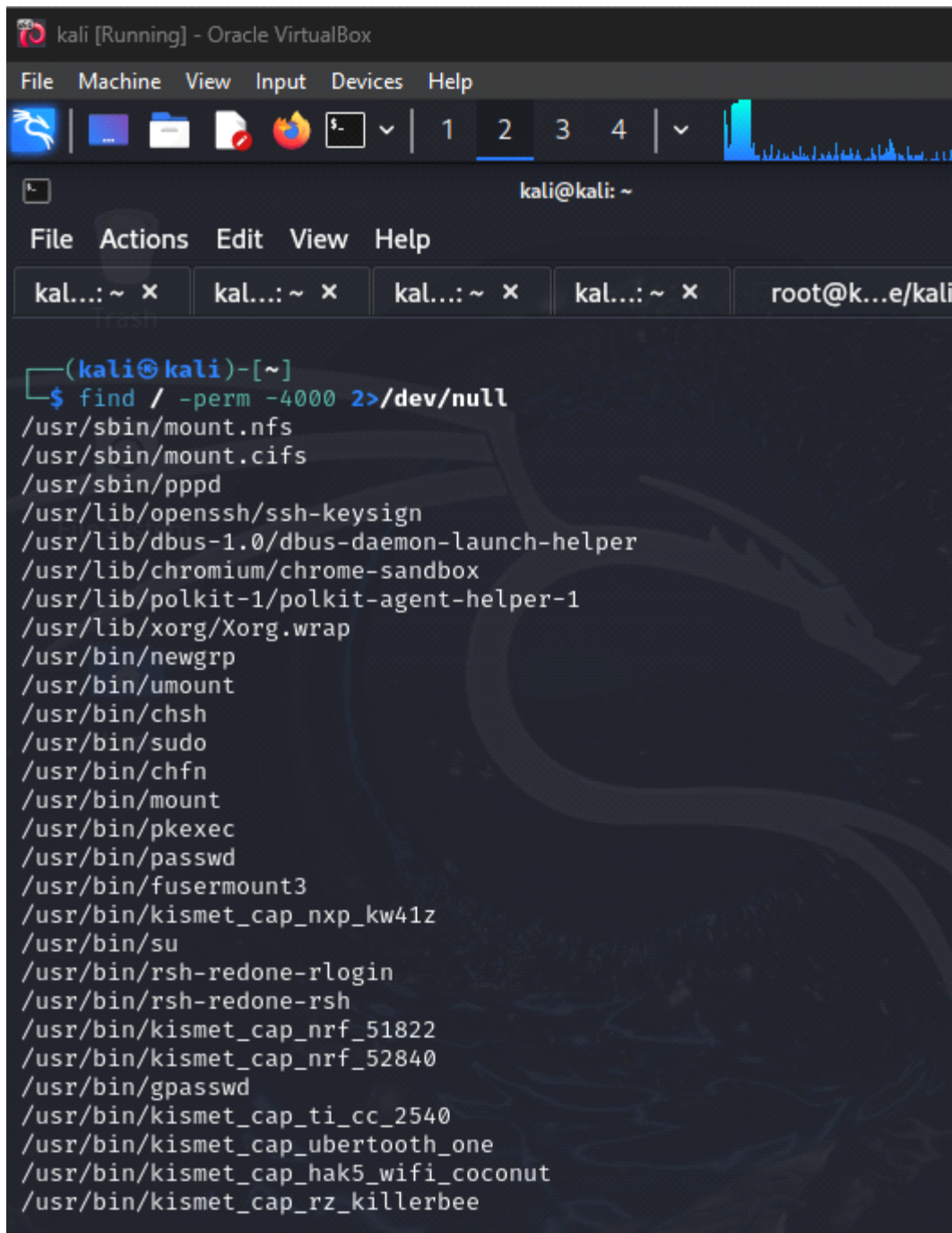
A screenshot of a Kali Linux terminal window titled 'kali [Running] - Oracle VirtualBox'. The terminal shows the execution of several commands to set up a SUID script. The commands and their outputs are as follows:  
1. `sudo chmod u+s /bin/bash`  
2. `echo -e "#!/bin/bash\nnecho 'You are root!'\nid" > root_script.sh`  
3. `sudo chmod 4755 root_script.sh`  
4. `ls -l root_script.sh`  
The output of the last command is `-rwsr-xr-x 1 kali kali 33 Mar 25 19:16 root_script.sh`, where the file name is highlighted in red. The terminal also shows the prompt `(kali@kali)-[~]` and the user `kali`.

```
(kali@kali)-[~]  
$ sudo chmod u+s /bin/bash  
  
(kali@kali)-[~]  
$ echo -e "#!/bin/bash\nnecho 'You are root!'\nid" > root_script.sh  
  
(kali@kali)-[~]  
$ sudo chmod 4755 root_script.sh  
  
(kali@kali)-[~]  
$ ls -l root_script.sh  
-rwsr-xr-x 1 kali kali 33 Mar 25 19:16 root_script.sh  
  
(kali@kali)-[~]  
$
```

### 2) Exploit

2.1) Find SUID misconfigurations:

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



The screenshot shows a Kali Linux virtual machine window titled "kali [Running] - Oracle VirtualBox". The terminal window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu bar is a toolbar with icons for file operations and a tab bar showing four tabs labeled "kal...: ~ x". The terminal prompt is "kali@kali: ~". The command being executed is `find / -perm -4000 2>/dev/null`. The output lists various files and directories with SUID bits set, including `/usr/sbin/mount.nfs`, `/usr/sbin/mount.cifs`, `/usr/sbin/pppd`, `/usr/lib/openssh/ssh-keysign`, `/usr/lib/dbus-1.0/dbus-daemon-launch-helper`, `/usr/lib/chromium/chrome-sandbox`, `/usr/lib/polkit-1/polkit-agent-helper-1`, `/usr/lib/xorg/Xorg.wrap`, `/usr/bin/newgrp`, `/usr/bin/umount`, `/usr/bin/chsh`, `/usr/bin/sudo`, `/usr/bin/chfn`, `/usr/bin/mount`, `/usr/bin/pkexec`, `/usr/bin/passwd`, `/usr/bin/fusermount3`, `/usr/bin/kismet_cap_nxp_kw41z`, `/usr/bin/su`, `/usr/bin/rsh-redone-rlogin`, `/usr/bin/rsh-redone-rsh`, `/usr/bin/kismet_cap_nrf_51822`, `/usr/bin/kismet_cap_nrf_52840`, `/usr/bin/gpasswd`, `/usr/bin/kismet_cap_ti_cc_2540`, `/usr/bin/kismet_cap_ubertooth_one`, `/usr/bin/kismet_cap_hak5_wifi_coconut`, and `/usr/bin/kismet_cap_rz_killerbee`.

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

### 3) Mitigation

#### 3.1) Remove SUID:

`sudo chmod -s /bin/bash`

#### 3.2) Restrict script execution:

`chmod 700 root_script.sh`

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

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

```
(kali㉿kali)-[~]  
$ chmod 700 root_script.sh
```