

Deliverable 1. Using the code above, create a file called `effective_user.c` and compile and execute the file as a normal user and using `sudo`. Provide a screenshot similar to the one below.

```
(champuser@kali)-[~/SEC335/SEC-335/week10]
$ ls
effective_user.c

(champuser@kali)-[~/SEC335/SEC-335/week10]
$ sudo vim effective_user.c

(champuser@kali)-[~/SEC335/SEC-335/week10]
$ gcc effective_user.c -o effective_user

(champuser@kali)-[~/SEC335/SEC-335/week10]
$ ./effective_user
champuser

(champuser@kali)-[~/SEC335/SEC-335/week10]
$ sudo ./effective_user
root
```

Deliverable 2. What are the octal (numeric) permissions of the `effective_user` program? Using `ls -l` you should be able to calculate these permissions, you can also use the "stat" program as a shortcut. Remember `r=4`, `w=2`, `x=1`, and `"-"` is a 0

```
(champuser@kali)-[~/SEC335/SEC-335/week10]
$ ls -l effective_user
-rwxr-xr-x 1 champuser champuser 16112 Apr  6 15:01 effective_user
```

□ The numerical code is 755

Owner:  $7 = 4(r) + 2(w) + 1(x)$

Group:  $5 = 4(r) + 1(x)$

Others:  $: 5 = 4(r) + 1(x)$

□

Deliverable 3. Figure out how to change the ownership of your c program executable such that the file is owned by user: root and group: root. Once you've done that, add the suid bit to the program (this is shown in the screenshot) and execute the program as a normal user. Provide a screenshot similar to the one below:

```
(champuser@kali)-[~/SEC335/SEC-335/week10]
$ ls -l
total 20
-rwxr-xr-x 1 root      root      16112 Apr  6 15:01 effective_user
-rw-r--r-- 1 champuser champuser  563 Apr  6 15:01 effective_user.c

(champuser@kali)-[~/SEC335/SEC-335/week10]
$ sudo chmod u+s effective_user

(champuser@kali)-[~/SEC335/SEC-335/week10]
$ ./effective_user
root
```

Deliverable 4. Hit the internet and find a means to search for suid programs across your kali system. Do so as a normal user as this is a privilege escalation technique you might use. Make sure to document this. You will need to deal with permissions errors by piping those to /dev/null. Provide a screenshot showing your command and listing similar to that below. Your own sudo program should be in the list.

```
(champususer@kali)-[~/SEC335/SEC-335/week10]
$ find / -perm -4000 -type f -print 2>/dev/null
/home/champususer/SEC335/SEC-335/week10/effective_user

/usr/sbin/mount.nfs
/usr/sbin/pppd
/usr/sbin/mount.cifs
/usr/bin/mount
/usr/bin/kismet_cap_nrf_mousejack
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/kismet_cap_rz_killerbee
/usr/bin/kismet_cap_linux_wifi
/usr/bin/umount
/usr/bin/passwd
/usr/bin/kismet_cap_nrf_52840
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/chfn
/usr/bin/kismet_cap_nxp_kw41z
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/kismet_cap_ti_cc_2540
/usr/bin/kismet_cap_linux_bluetooth
/usr/bin/ntfs-3g
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/kismet_cap_nrf_51822
/usr/bin/vmware-user-suid-wrapper
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/opt/google/chrome/chrome-sandbox
```

Deliverable 5. A suid program has been hidden on rocky (10.0.17.200). Please hunt it down. Provide a screenshot that shows the command and file found. It will be obvious and the name will start with a 'b'.

```
(champuser@kali)-[~/SEC335/SEC-335/week10]
$ ssh david.thomsen@10.0.17.200
david.thomsen@10.0.17.200's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Mar 26 16:04:22 2023 from 10.0.17.26
[david.thomsen@sec335-rocky ~]$ find / -perm -4000 -type f -print 2>/dev/null
/usr/bin/su
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/umount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/at
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/crontab
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/booger
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
/usr/libexec/sss/krb5_child
/usr/libexec/sss/ldap_child
/usr/libexec/sss/selinux_child
/usr/libexec/sss/proxy_child
/usr/libexec/cockpit-session
[david.thomsen@sec335-rocky ~]$
```

Deliverable 6. Consider the following screenshot. This user created a file under /etc/ that is world writable. Were this file to be of any security relevance, this could be a problem. Create such a file, and figure out how to find it. Show your command.

```
(champuser@kali)-[~/SEC335/SEC-335/week10]
$ find /etc -perm -646 -type f
find: '/etc/ssl/private': Permission denied
find: '/etc/ipsec.d/private': Permission denied
find: '/etc/redis': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
find: '/etc/vnc': Permission denied
/etc/test.txt
(champuser@kali)-[~/SEC335/SEC-335/week10]
$
```

Deliverable 7. A world writable file has been hidden on rocky. Please hunt it down. Provide a screenshot that shows the command and file found. It will start with an 's'. (note, the sys and proc directories will give you a lot of false positives)

```
File Actions Edit View Help
[david.thomsen@sec335-rocky ~]$ find / -perm -o+w -type f -print 2>/dev/null | grep -
v sys | grep -v proc
/usr/share/games/solitaire
[david.thomsen@sec335-rocky ~]$ cat /usr/share/games/solitaire
yes,this is the file you are looking for. Add your Name
Saaaaam

Adam - Happy Thanksgiving
Hasan Hashim - "No pain No gain"
Jahseem - "Honey, WHERE'S MY SUPERSUIT"
McHugh
Alex - no pain no gain. more like just pain and a lot of it.
DavyStayWavey aka MilkTruck aka David Thomsen aka Davey Crockett was here
[david.thomsen@sec335-rocky ~]$
```