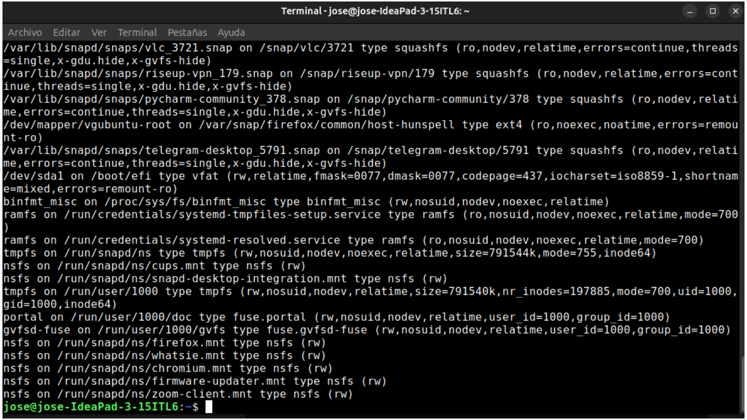
№5

12.03.2024

, ,

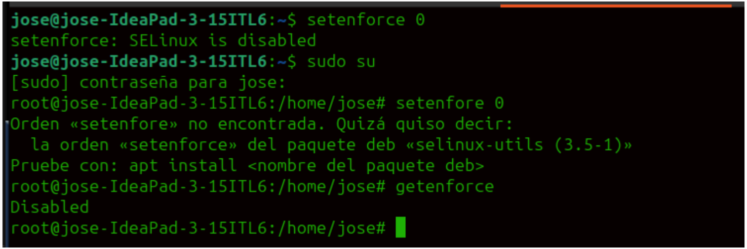
-
- , -03-22
-
- 1032225355@pfur.ru

, SetUID- Sticky- .



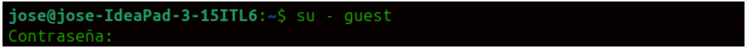
```
/var/lib/snapd/snaps/vlc_3721.snap on /snap/vlc/3721 type squashfs (ro,nodev,relatime,errors=continue,threads
=single,x-gdu.hide,x-gvfs-hide)
/var/lib/snapd/snaps/riseup-vpn_179.snap on /snap/riseup-vpn/179 type squashfs (ro,nodev,relatime,errors=cont
inue,threads=single,x-gdu.hide,x-gvfs-hide)
/var/lib/snapd/snaps/pycharm-community_378.snap on /snap/pycharm-community/378 type squashfs (ro,nodev,relati
me,errors=continue,threads=single,x-gdu.hide,x-gvfs-hide)
/dev/mapper/vgubuntu-root on /var/snap/firefox/common/host-hunspell type ext4 (ro,noexec,noatime,errors=remou
nt-ro)
/var/lib/snapd/snaps/telegram-desktop_5791.snap on /snap/telegram-desktop/5791 type squashfs (ro,nodev,relati
me,errors=continue,threads=single,x-gdu.hide,x-gvfs-hide)
/dev/sda1 on /boot/efi type vfat (rw,relatime,fmask=0077,dmask=0077,codepage=437,iocharset=iso8859-1,shortnam
e=mixed,errors=remount-ro)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-tmpfiles-setup.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700
)
ramfs on /run/credentials/systemd-resolved.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
tmpfs on /run/snapd/ns type tmpfs (rw,nosuid,nodev,noexec,relatime,size=791544k,mode=755,inode64)
nsfs on /run/snapd/ns/cups.mnt type nsfs (rw)
nsfs on /run/snapd/ns/snapd-desktop-integration.mnt type nsfs (rw)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=791540k,nr_inodes=197885,mode=700,uid=1000,
gid=1000,inode64)
portal on /run/user/1000/doc type fuse.portal (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)
nsfs on /run/snapd/ns/firefox.mnt type nsfs (rw)
nsfs on /run/snapd/ns/whatsie.mnt type nsfs (rw)
nsfs on /run/snapd/ns/chromium.mnt type nsfs (rw)
nsfs on /run/snapd/ns/firmware-updater.mnt type nsfs (rw)
nsfs on /run/snapd/ns/zoom-client.mnt type nsfs (rw)
jose@jose-IdeaPad-3-15ITL6:~$ 
```

. 1:



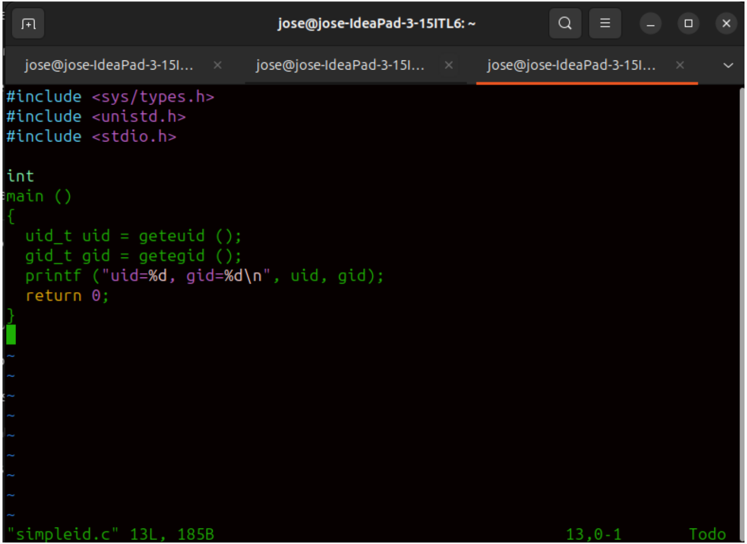
```
jose@jose-IdeaPad-3-15ITL6:~$ setenforce 0
setenforce: SELinux is disabled
jose@jose-IdeaPad-3-15ITL6:~$ sudo su
[sudo] contraseña para jose:
root@jose-IdeaPad-3-15ITL6:/home/jose# setenfore 0
Orden «setenfore» no encontrada. Quizá quiso decir:
  la orden «setenforce» del paquete deb «selinux-utils (3.5-1)»
Pruebe con: apt install <nombre del paquete deb>
root@jose-IdeaPad-3-15ITL6:/home/jose# getenforce
Disabled
root@jose-IdeaPad-3-15ITL6:/home/jose# 
```

. **2:** setenforce 0



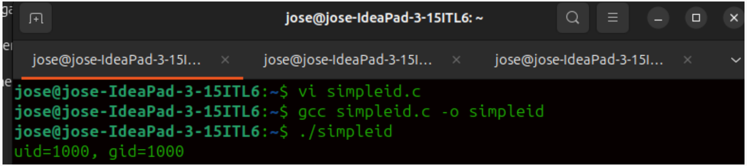
```
jose@jose-IdeaPad-3-15ITL6:~$ su - guest
Contraseña:
```

. 3:


jose@jose-IdeaPad-3-15ITL6: ~
jose@jose-IdeaPad-3-15I...
jose@jose-IdeaPad-3-15I...
jose@jose-IdeaPad-3-15I...

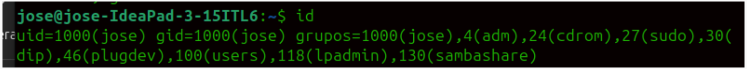
```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main ()
{
  uid_t uid = geteuid ();
  gid_t gid = getegid ();
  printf ("uid=%d, gid=%d\n", uid, gid);
  return 0;
}

~
~
~
~
~
~
~
~
~
"simpleid.c" 13L, 185B                                  13,0-1        Todo
```

4:


jose@jose-IdeaPad-3-15ITL6: ~
jose@jose-IdeaPad-3-15I...
jose@jose-IdeaPad-3-15I...
jose@jose-IdeaPad-3-15I...

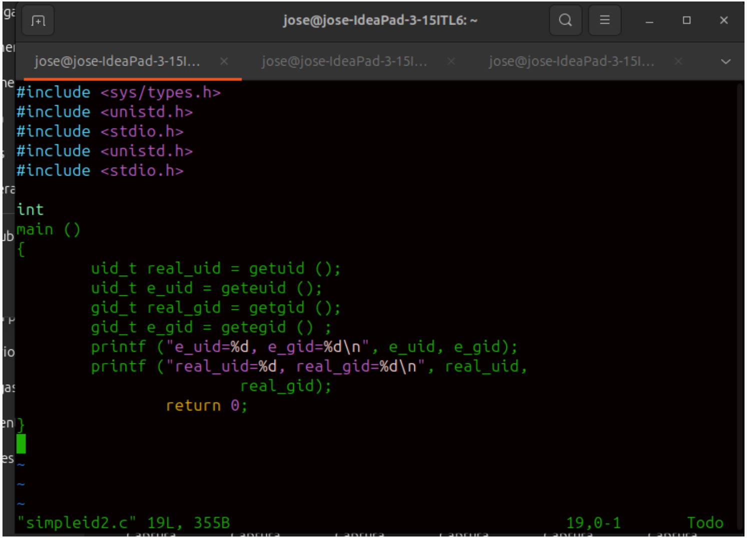
```
jose@jose-IdeaPad-3-15ITL6:~$ vi simpleid.c
jose@jose-IdeaPad-3-15ITL6:~$ gcc simpleid.c -o simpleid
jose@jose-IdeaPad-3-15ITL6:~$ ./simpleid
uid=1000, gid=1000
```

. 5:



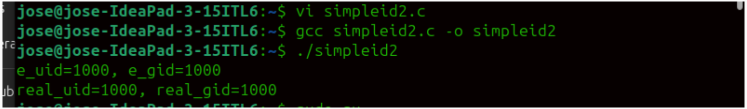
```
jose@jose-IdeaPad-3-15ITL6:~$ id
uid=1000(jose) gid=1000(jose) grupos=1000(jose),4(adm),24(cdrom),27(sudo),30(
dip),46(plugdev),100(users),118(lpadmin),130(sambashare)
```

. **6:** id


jose@jose-IdeaPad-3-15ITL6: ~
jose@jose-IdeaPad-3-15I...
jose@jose-IdeaPad-3-15I...
jose@jose-IdeaPad-3-15I...

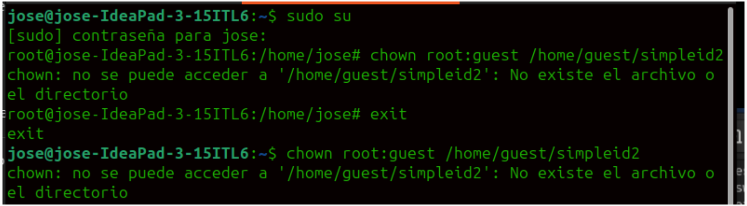
```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
#include <unistd.h>
#include <stdio.h>

int
main ()
{
        uid_t real_uid = getuid ();
        uid_t e_uid = geteuid ();
        gid_t real_gid = getgid ();
        gid_t e_gid = getegid () ;
        printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
        printf ("real_uid=%d, real_gid=%d\n", real_uid,
                        real_gid);
                return 0;
}

~
~
~
"simpleid2.c" 19L, 355B                                      19,0-1        Todo
```

7:



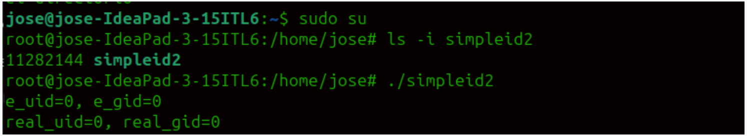
```
jose@jose-IdeaPad-3-15ITL6:~$ vi simpleid2.c
jose@jose-IdeaPad-3-15ITL6:~$ gcc simpleid2.c -o simpleid2
jose@jose-IdeaPad-3-15ITL6:~$ ./simpleid2
e_uid=1000, e_gid=1000
real_uid=1000, real_gid=1000
```

. 8:



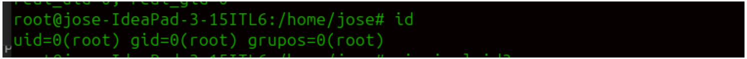
```
jose@jose-IdeaPad-3-15ITL6:~$ sudo su
[sudo] contraseña para jose:
root@jose-IdeaPad-3-15ITL6:/home/jose# chown root:guest /home/guest/simpleid2
chown: no se puede acceder a '/home/guest/simpleid2': No existe el archivo o
el directorio
root@jose-IdeaPad-3-15ITL6:/home/jose# exit
exit
jose@jose-IdeaPad-3-15ITL6:~$ chown root:guest /home/guest/simpleid2
chown: no se puede acceder a '/home/guest/simpleid2': No existe el archivo o
el directorio
```

. **9:**



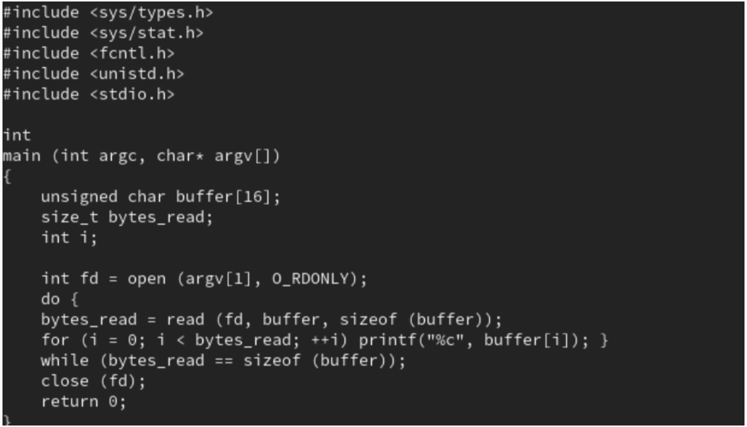
```
jose@jose-IdeaPad-3-15ITL6:~$ sudo su
root@jose-IdeaPad-3-15ITL6:/home/jose# ls -i simpleid2
11282144 simpleid2
root@jose-IdeaPad-3-15ITL6:/home/jose# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
```

. **10:** ls -l



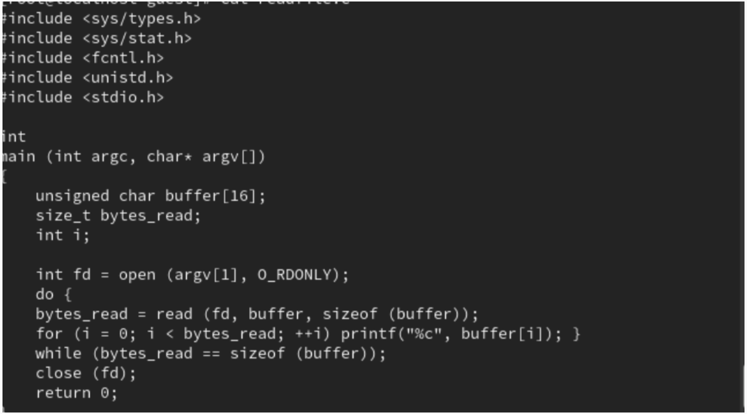
```
real_uid=0, real_gid=0
root@jose-IdeaPad-3-15ITL6:/home/jose# id
uid=0(root) gid=0(root) grupos=0(root)
```

. 11:



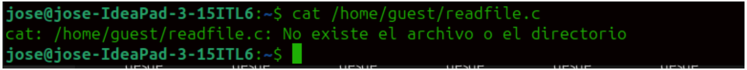
```
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <unistd.h>
#include <stdio.h>

int
main (int argc, char* argv[])
{
    unsigned char buffer[16];
    size_t bytes_read;
    int i;

    int fd = open (argv[1], O_RDONLY);
    do {
    bytes_read = read (fd, buffer, sizeof (buffer));
    for (i = 0; i < bytes_read; ++i) printf("%c", buffer[i]); }
    while (bytes_read == sizeof (buffer));
    close (fd);
    return 0;
}
```

. 12:



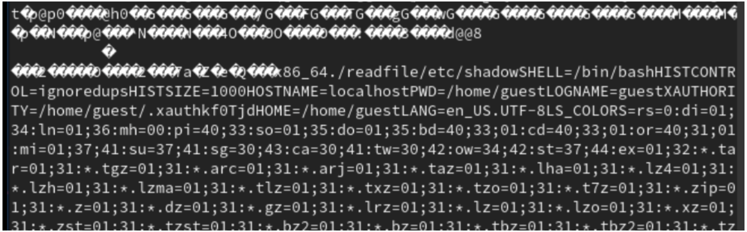
```
[root@localhost guest]# cat readfile.c
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <unistd.h>
#include <stdio.h>

int
main (int argc, char* argv[])
{
   unsigned char buffer[16];
   size_t bytes_read;
   int i;

   int fd = open (argv[1], O_RDONLY);
   do {
   bytes_read = read (fd, buffer, sizeof (buffer));
   for (i = 0; i < bytes_read; ++i) printf("%c", buffer[i]); }
   while (bytes_read == sizeof (buffer));
   close (fd);
   return 0;
```

. 13:



```
jose@jose-IdeaPad-3-15ITL6:~$ cat /home/guest/readfile.c
cat: /home/guest/readfile.c: No existe el archivo o el directorio
jose@jose-IdeaPad-3-15ITL6:~$ 
```

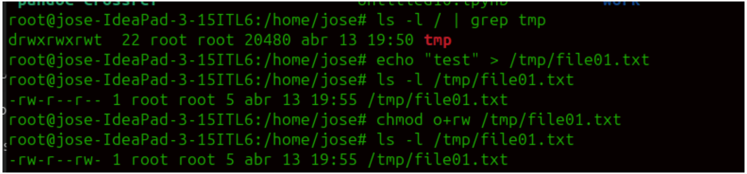
. 14:



```
t�p@p0����@h0���6���6���6���/G���FG���TG���gG���wG����6����6����6����6����M����M�
�p��N���p@���N����N���40����O����O���.����8����d@@8
          �
���2�����0����2���7a�Z�e�Q���x86_64./readfile/etc/shadowSHELL=/bin/bashHISTCONTR
OL=ignoredupsHISTSIZE=1000HOSTNAME=localhostPWD=/home/guestLOGNAME=guestXAUTHORI
TY=/home/guest/.xauthkf0TjdHOME=/home/guestLANG=en_US.UTF-8LS_COLORS=rs=0:di=01;
34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01
:mi=01;37;41:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.ta
r=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:
*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=0
1;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;
31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz
```

. 15:

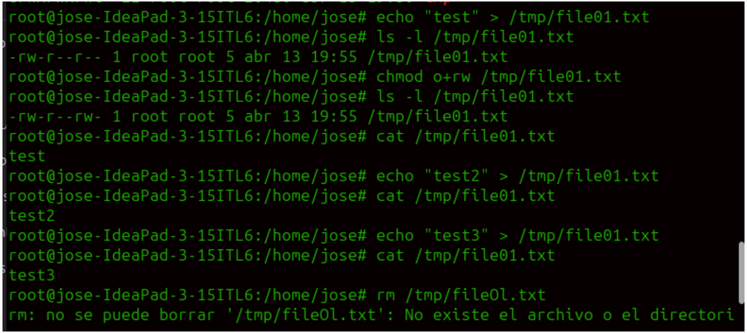
Sticky-



```
root@jose-IdeaPad-3-15ITL6:/home/jose# ls -l / | grep tmp
drwxrwxrwt  22 root root 20480 abr 13 19:50 tmp
root@jose-IdeaPad-3-15ITL6:/home/jose# echo "test" > /tmp/file01.txt
root@jose-IdeaPad-3-15ITL6:/home/jose# ls -l /tmp/file01.txt
-rw-r--r-- 1 root root 5 abr 13 19:55 /tmp/file01.txt
root@jose-IdeaPad-3-15ITL6:/home/jose# chmod o+rw /tmp/file01.txt
root@jose-IdeaPad-3-15ITL6:/home/jose# ls -l /tmp/file01.txt
-rw-r--rw- 1 root root 5 abr 13 19:55 /tmp/file01.txt
```

. 16:

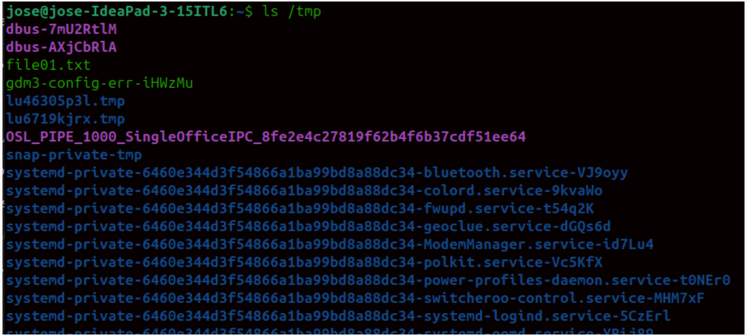
Sticky-



```
root@jose-IdeaPad-3-15ITL6:/home/jose# echo "test" > /tmp/file01.txt
root@jose-IdeaPad-3-15ITL6:/home/jose# ls -l /tmp/file01.txt
-rw-r--r-- 1 root root 5 abr 13 19:55 /tmp/file01.txt
root@jose-IdeaPad-3-15ITL6:/home/jose# chmod o+rw /tmp/file01.txt
root@jose-IdeaPad-3-15ITL6:/home/jose# ls -l /tmp/file01.txt
-rw-r--rw- 1 root root 5 abr 13 19:55 /tmp/file01.txt
root@jose-IdeaPad-3-15ITL6:/home/jose# cat /tmp/file01.txt
test
root@jose-IdeaPad-3-15ITL6:/home/jose# echo "test2" > /tmp/file01.txt
root@jose-IdeaPad-3-15ITL6:/home/jose# cat /tmp/file01.txt
test2
root@jose-IdeaPad-3-15ITL6:/home/jose# echo "test3" > /tmp/file01.txt
root@jose-IdeaPad-3-15ITL6:/home/jose# cat /tmp/file01.txt
test3
root@jose-IdeaPad-3-15ITL6:/home/jose# rm /tmp/fileOl.txt
rm: no se puede borrar '/tmp/fileOl.txt': No existe el archivo o el directori
```

. 17:

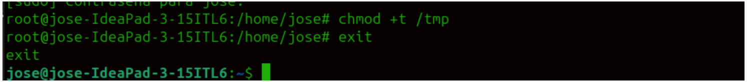
Sticky-



```
jose@jose-IdeaPad-3-15ITL6:~$ ls /tmp
dbus-7mU2RtlM
dbus-AXjCbRlA
file01.txt
gdm3-config-err-iHWzMu
lu46305p3l.tmp
lu6719kjrx.tmp
OSL_PIPE_1000_SingleOfficeIPC_8fe2e4c27819f62b4f6b37cdf51ee64
snap-private-tmp
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-bluetooth.service-VJ9oyy
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-colord.service-9kvaWo
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-fwupd.service-t54q2K
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-geoclue.service-dGQs6d
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-ModemManager.service-id7Lu4
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-polkit.service-Vc5KfX
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-power-profiles-daemon.service-t0NEr0
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-switcheroo-control.service-MHM7xF
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-systemd-logind.service-5CzErl
systemd-private-6460e344d3f54866a1ba99bd8a88dc34-systemd-oomd.service-YBij89
```

. **18:** t

Sticky-



```
[sudo] contraseña para jose:
root@jose-IdeaPad-3-15ITL6:/home/jose# chmod +t /tmp
root@jose-IdeaPad-3-15ITL6:/home/jose# exit
exit
jose@jose-IdeaPad-3-15ITL6:~$ 
```

. 19: Sticky

, SetUID- Sticky- .

.