

Лабораторная работа 5

Генералов Даниил, 1032212280

2024 г.

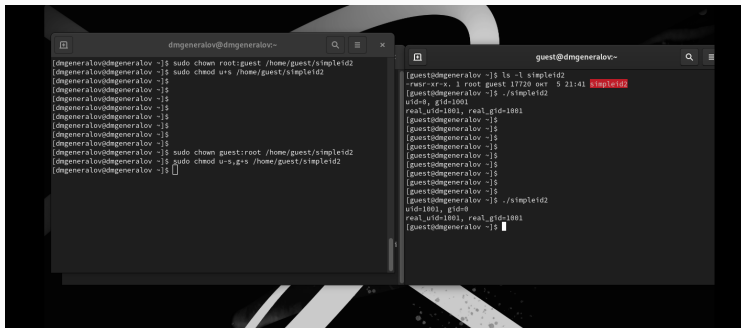
Российский университет дружбы народов, Москва, Россия

Задание

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов.
Получение практических навыков работы в консоли с дополнительными атрибутами.
Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Выполнение

Рис. 1: id



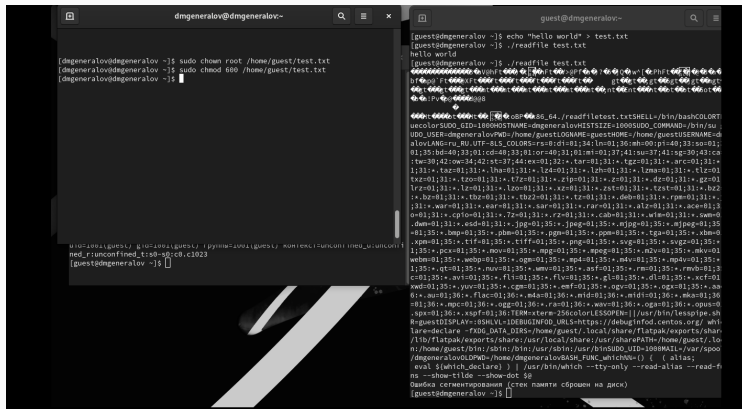
The image shows two terminal windows. The left window is titled 'dmgeneralov@dmgeneralov-' and shows the following commands and output:

```
[dmgeneralov@dmgeneralov ~]$ sudo chown root:guest /home/guest/simpleid2
[dmgeneralov@dmgeneralov ~]$ sudo chmod u-rs /home/guest/simpleid2
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$ sudo chown guest:root /home/guest/simpleid2
[dmgeneralov@dmgeneralov ~]$ sudo chmod u-s,g+s /home/guest/simpleid2
[dmgeneralov@dmgeneralov ~]$
```

The right window is titled 'guest@dmgeneralov-' and shows the following commands and output:

```
[guest@dmgeneralov ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 17720 окт 5 21:41 simpleid2
[guest@dmgeneralov ~]$ ./simpleid2
uid=0, gid=1001
real_uid=1001, real_gid=1001
[guest@dmgeneralov ~]$
[guest@dmgeneralov ~]$
[guest@dmgeneralov ~]$
[guest@dmgeneralov ~]$
[guest@dmgeneralov ~]$
[guest@dmgeneralov ~]$
[guest@dmgeneralov ~]$
[guest@dmgeneralov ~]$ ./simpleid2
uid=1001, gid=0
real_uid=1001, real_gid=1001
[guest@dmgeneralov ~]$
```

Рис. 2: simpleid2



```

dmgeneralov@dmgeneralov-
[dmgeneralov@dmgeneralov ~]$ sudo chown root /home/guest/test.txt
[dmgeneralov@dmgeneralov ~]$ sudo chmod 600 /home/guest/test.txt
[dmgeneralov@dmgeneralov ~]$

guest@dmgeneralov-
[guest@dmgeneralov ~]$ echo "hello world" > test.txt
[guest@dmgeneralov ~]$ ./readfile test.txt
hello world
[guest@dmgeneralov ~]$ ./readfile test.txt
*****vuhf*****Pht400apR*****PHET*****
br000Ft*****gt*****
bt*****
Pv*****
*****cSP*****_ss_64_./readfiletest.txt$SHELL=/bin/bashCOLOR
ucolor$UDO_GID=1000HOSTNAME=dmgeneralovHISTSIZE=1000$UDO_COMMAND=/bin/su
UDO_USER=dmgeneralovPWD=/home/guestLOGNAME=guestHOME=/home/guestUSERNAME=d
alovLANG=ru_RU.UTF-8LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;
01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=01;37;41:su=37;41:sg=30;43:cn
:tw=30;42:ow=34;42:st=37;44:ex=01;32:.*.tar=01;31:.*.tgz=01;31:.*.arc=01;31:
1;31:.*.taz=01;31:.*.lha=01;31:.*.lzd=01;31:.*.lzm=01;31:.*.lcz=01
xz=01;31:.*.tzo=01;31:.*.tzz=01;31:.*.zip=01;31:.*.z=01;31:.*.dz=01;31:.*.gz=01
lrz=01;31:.*.lzo=01;31:.*.lzo=01;31:.*.xz=01;31:.*.zst=01;31:.*.tzt=01;31:.*.bz2
.*.bz=01;31:.*.tbz=01;31:.*.tbz2=01;31:.*.tz=01;31:.*.deb=01;31:.*.rpm=01;31:.*
;31:.*.war=01;31:.*.ear=01;31:.*.sar=01;31:.*.rar=01;31:.*.alz=01;31:.*.ace=01;3
0=01;31:.*.cpt=01;31:.*.7z=01;31:.*.rz=01;31:.*.cab=01;31:.*.wim=01;31:.*.swm=0
.dwn=01;31:.*.xnd=01;31:.*.jpg=01;35:.*.jpeg=01;35:.*.mjpg=01;35:.*.mjpeg=01;35
=01;35:.*.bmp=01;35:.*.pbm=01;35:.*.pgm=01;35:.*.ppm=01;35:.*.tga=01;35:.*.xnm=0
.xpm=01;35:.*.tif=01;35:.*.tiff=01;35:.*.png=01;35:.*.svg=01;35:.*.svgz=01;35:.*
1;35:.*.pcx=01;35:.*.mov=01;35:.*.mpeg=01;35:.*.mjpeg=01;35:.*.n2v=01;35:.*.mkv=01
webm=01;35:.*.webp=01;35:.*.ogm=01;35:.*.mp4=01;35:.*.m4v=01;35:.*.mp4v=01;35:.*
1;35:.*.qt=01;35:.*.nuv=01;35:.*.wmv=01;35:.*.asf=01;35:.*.rm=01;35:.*.rmvb=01;3
c01;35:.*.avi=01;35:.*.flv=01;35:.*.flv=01;35:.*.gl=01;35:.*.dl=01;35:.*.xcf=01
xwd=01;35:.*.puv=01;35:.*.cgm=01;35:.*.emf=01;35:.*.eps=01;35:.*.ps=01;35:.*.se
6:.*.au=01;36:.*.flac=01;36:.*.m4a=01;36:.*.mid=01;36:.*.midi=01;36:.*.mka=01;36
=01;36:.*.mpc=01;36:.*.ogg=01;36:.*.ra=01;36:.*.wav=01;36:.*.oga=01;36:.*.opus=0
.spx=01;36:.*.xspf=01;36:TERM=xterm-256colorLESSOPEN=||/usr/bin/lesspipe.sh
R=guestDISPLAY=:0$HVL=1DEBUGINFOD_URLS=https://debuginfod.centos.org/whi
lare=declare -FXDG_DATA_DIRS=/home/guest/.local/share/Flatpak/exports/share
/1/b/flatpak/exports/share:/usr/local/share:/usr/sharePATH=/home/guest/.lo
n:/home/guest/bin:/sbin:/bin:/usr/sbin:/usr/bin$UDO_UID=1000$MAIL=/var/spoo
/dmgeneralov$LD$PWD=/home/dmgeneralov$BASH_FUNC_which%%=() { ( alias;
eval $(which declare) ) } /usr/bin/which --tty-only --read-alias --read-f
ns --show-tilde --show-dot $@
Ошибка сегментирования (стек памяти сброшен на диск)
[guest@dmgeneralov ~]$

```

Рис. 3: readfile

```

Обзор Терминал Сб, 5 октября 22:05 en
dmgeneralov@dmgeneralov-
[dmgeneralov@dmgeneralov ~]$ sudo chown root /home/guest/readfile
[dmgeneralov@dmgeneralov ~]$ sudo chmod u+s /home/guest/readfile
[dmgeneralov@dmgeneralov ~]$

guest@dmgeneralov-
Ошибка сегментирования (стек памяти сброшен на диск)
[guest@dmgeneralov ~]$
[guest@dmgeneralov ~]$ ./readfile test.txt
hello world
[guest@dmgeneralov ~]$ cat test.txt
cat: test.txt: Отказано в доступе
[guest@dmgeneralov ~]$ cat /etc/shadow
cat: /etc/shadow: Отказано в доступе
[guest@dmgeneralov ~]$ ./readfile /etc/shadow
root:$6$1tw6LPhT1P36wdM5$ICJ.nTKHv1w2KFZsk.2/P1x$ADAKmL7AeQTucTH6EegNAly0h
2w3MDKZy/HBhkHToJz46VH9g3V3e7u1::0:99999:7:::
bin:*:19828:0:99999:7:::
daemon:*:19820:0:99999:7:::
adm:*:19820:0:99999:7:::
lp:*:19820:0:99999:7:::
sync:*:19820:0:99999:7:::
shutdown:*:19820:0:99999:7:::
halt:*:19820:0:99999:7:::
mail:*:19820:0:99999:7:::
operator:*:19820:0:99999:7:::
games:*:19820:0:99999:7:::
ftp:*:19820:0:99999:7:::
nobody:*:19820:0:99999:7:::
tss:!:19973:!:!:
systemd-coredump:!:19973:!:!:
dbus:!:19973:!:!:
polkitd:!:19973:!:!:
sssd:!:19973:!:!:
avahi:!:19973:!:!:
geoclue:!:19973:!:!:
cockpit-ws:!:19973:!:!:
cockpit-ws:instances:!:19973:!:!:
rtkit:!:19973:!:!:
pipewire:!:19973:!:!:
libstorageengine:!:19973:!:!:
flatpak:!:19973:!:!:
colord:!:19973:!:!:
clovefs:!:19973:!:!:
setroubleshot:!:19973:!:!:
gdm:!:19973:!:!:
gnome-initial-setup:!:19973:!:!:

```

Рис. 4: setuid


```

[guest2@dmgeneralov ~]$ ls -l / |
> grep tmp
drwxrwxrwt. 18 root root 4096 окт  5 22:11 tmp
[guest2@dmgeneralov ~]$ echo "test" > /tmp/file01.txt
[guest2@dmgeneralov ~]$ ls -l /tmp/file01.txt
-rw-r--r-- 1 guest guest 5 окт  5 22:12 /tmp/file01.txt
[guest2@dmgeneralov ~]$ chmod 0+rw /tmp/file01.txt
chmod: неверный режим: «0+rw»
По команде «chmod --help» можно получить дополнительную информацию.
[guest2@dmgeneralov ~]$ chmod o+rw /tmp/file01.txt
[guest2@dmgeneralov ~]$ ls -l /tmp/file01.txt
-rw-r--r-- 1 guest guest 5 окт  5 22:12 /tmp/file01.txt
[guest2@dmgeneralov ~]$
[guest2@dmgeneralov ~]$
[guest2@dmgeneralov ~]$ ls -l /tmp/file01.txt
-rw-r--r-- 1 guest guest 5 окт  5 22:12 /tmp/file01.txt
[guest2@dmgeneralov ~]$ ls -l / | grep tmp
drwxrwxrwt. 19 root root 4096 окт  5 22:13 tmp
[guest2@dmgeneralov ~]$ rm /tmp/file01.txt
[guest2@dmgeneralov ~]$ echo "test1" > /tmp/file01.txt
[guest2@dmgeneralov ~]$ chmod o+rw /tmp/file01.txt
[guest2@dmgeneralov ~]$ echo "test1" > /tmp/file01.txt
[guest2@dmgeneralov ~]$ chmod o+rw /tmp/file01.txt
[guest2@dmgeneralov ~]$
[guest2@dmgeneralov ~]$ cat /tmp/file01.txt
test
[guest2@dmgeneralov ~]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@dmgeneralov ~]$ echo "test" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@dmgeneralov ~]$ rm /tmp/file01.txt
rm: удалить защищенный от записи обычный файл '/tmp/file01.txt'? y
rm: невозможно удалить '/tmp/file01.txt': Операция не разрешена
[guest2@dmgeneralov ~]$
[guest2@dmgeneralov ~]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@dmgeneralov ~]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@dmgeneralov ~]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@dmgeneralov ~]$ rm /tmp/file01.txt
rm: удалить защищенный от записи обычный файл '/tmp/file01.txt'? y
[guest2@dmgeneralov ~]$ cat /tmp/file01.txt
test1
[guest2@dmgeneralov ~]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@dmgeneralov ~]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@dmgeneralov ~]$ cat /tmp/file01.txt
test1
[guest2@dmgeneralov ~]$ rm /tmp/file01.txt
rm: удалить защищенный от записи обычный файл '/tmp/file01.txt'? y
[guest2@dmgeneralov ~]$ cat /tmp/file01.txt
cat: /tmp/file01.txt: Нет такого файла или каталога
[guest2@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$ sudo chmod -t /tmp

```

Рис. 5: sticky

Выводы

В этой лабораторной работе мы использовали механизмы sticky, setuid и setgid-битов, чтобы посмотреть на некоторые продвинутые механизмы работы с разрешениями файлов в Linux.