

# Цель работы

---

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.

## Задание

---

## Выполнение лабораторной работы

---

Установил gcc с помощью команды `yum install gcc`.

Отменил на текущую сессию SELinux командой `setenforce 0`. Вошёл в систему от имени пользователя guest, создал программу `simpleid.c`.

Скомпилировал программу и убедился, что файл программы создан: `gcc simpleid.c -o simpleid`. Выполнил программу `simpleid`: `./simpleid`. Выполнил программу `id` и сравнил полученный результат с данными предыдущего пункта задания. Полученные значения `id` совпадают.

Усложнил программу, добавив вывод действительных идентификаторов, получившуюся программу назвал `simpleid2.c`.

Скомпилировал и запустил `simpleid2.c` `gcc simpleid2.c -o simpleid2`, а затем `./simpleid2`.

От имени суперпользователя выполнил команды: `chown root:guest /home/guest/simpleid2`, а затем `chmod u+s /home/guest/simpleid2`. Первая команда изменяет права на файл с `guest` на `root`. А затем устанавливает атрибут SetUID, который запускает программу не с правами пользователя, а с правами владельца файла. Затем выполнил проверку изменений с помощью команды `ls -l simpleid2`.

Запустил `simpleid2` и `id`: `./simpleid2`, `id`. При данном запуске выводы совпадают.

Проделал то же самое с атрибутом SetGID (установление прав для владеющей группы). Запустил файл. Теперь выводы для группы различны.

Создал программу `readfile.c`.

Откомпилировал программу: `gcc readfile.c -o readfile`. Сменил владельца у файла `readfile.c` и изменил права так, чтобы только суперпользователь(`root`) мог прочитать его, а `guest` не мог. Проверил, что пользователь `guest` не может прочитать файл `readfile.c`.

Сменил у программы `readfile` владельца и установил SetU'D-бит. Программа `readfile` может прочитать файл `readfile.c`. Программа `readfile` может прочитать файл `/etc/shadow`.

Исследование Sticky-бита. Узнал, установлен ли атрибут Sticky на директории `/tmp`, для чего выполнил команду `ls -l / | grep tmp`

От имени пользователя `guest` создал файл `file01.txt` в директории `/tmp`

со словом `test` `echo "test" > /tmp/file01.txt`. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные»: `ls -l`

`/tmp/file01.txt`, `chmod o+rw /tmp/file01.txt`, `ls -l /tmp/file01.txt`. От пользователя

`guest2` (не являющегося владельцем) попробовал прочитать файл `/tmp/file01.txt`: `cat`

`/tmp/file01.txt`, записать в файл `/tmp/file01.txt` текст `test3`, стерев при этом всю

имеющуюся в файле информацию командой `echo "test3" > /tmp/file01.txt`. Проверил содержимое файла командой `cat /tmp/file01.txt`, попробовал дозаписать в файл

`/tmp/file01.txt` слово `test2` командой `echo "test2" >> /tmp/file01.txt`, удалить файл

/tmp/file01.txt командой `rm /tmp/file01.txt` Файл удалить не удалось.

Повысил свои права до суперпользователя следующей командой `su -`

и выполнил после этого команду, снимающую атрибут `t` (Sticky-бит) с

директории /tmp: `chmod -t /tmp`. Затем попробовал выполнить все вышеперечисленные операции. Все удалось.

Повысил свои права до суперпользователя и вернул атрибут `t` на директорию /tmp: `su -`,  
`chmod +t /tmp`, `exit`.

I

```
[root@localhost iayukhnin]# sudo yum install gcc
Last metadata expiration check: 2:29:07 ago on Sat 10 Sep 2022 04:40:03 PM MSK.
Package gcc-11.2.1-9.4.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@localhost iayukhnin]# setenforce 0
[root@localhost iayukhnin]# su - guest
[guest@localhost ~]$ ls
tmp
[guest@localhost ~]$ touch simpleid.c
[guest@localhost ~]$ vim simpleid.c
[guest@localhost ~]$ gcc simpleid.c -o simpleid
[guest@localhost ~]$ ./simpleid
uid=1001, gid=1001
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

```
[guest@localhost ~]$ vim simpleid2.c
[guest@localhost ~]$ gcc simpleid2.c -o simpleid2
[guest@localhost ~]$ ./simpleid2
e uid=1001, e gid=1001
real uid=1001, real gid=1001
[guest@localhost ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 26008 Sep 10 19:12 simpleid2
[guest@localhost ~]$ ./simpleid2
e uid=0, e gid=1001
real uid=1001, real gid=1001
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$ vim readfile.c
[guest@localhost ~]$ gcc readfile.c -o readfile
[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@localhost ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Sep 10 19:14 tmp
[guest@localhost ~]$ echo "test" > /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Sep 10 19:17 /tmp/file01.txt
[guest@localhost ~]$ chmod o+rw /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Sep 10 19:17 /tmp/file01.txt
[guest@localhost ~]$ su - guest2
Password:
[guest2@localhost ~]$ cat /tmp/file01.txt
test
[guest2@localhost ~]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@localhost ~]$ cat /tmp/file01.txt
test
```

```

[guest2@localhost ~]$ echo "test2" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@localhost ~]$ cat /tmp/file01.txt
test
[guest2@localhost ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@localhost ~]$ cat /tmp/file01.txt
test
[guest2@localhost ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@localhost ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@localhost ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'?
[guest2@localhost ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@localhost ~]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Sep 10 19:18 tmp
[guest2@localhost ~]$

```

```

[iayukhnin@localhost ~]$ su
Password:
[root@localhost iayukhnin]# chown root:guest /home/guest/simpleid2
[root@localhost iayukhnin]# chmod u+s /home/guest/simpleid2
[root@localhost iayukhnin]# chown root:root /home/guest/readfile.c
[root@localhost iayukhnin]# chmod ugo-r
chmod: missing operand after 'ugo-r'
Try 'chmod --help' for more information.
[root@localhost iayukhnin]# chmod ugo-r /home/guest/readfile.c
[root@localhost iayukhnin]# chmod -t /tmp
[root@localhost iayukhnin]# chmod +t /tmp
[root@localhost iayukhnin]#

```

## Выводы

Изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

## Список литературы

- [Лабораторная работа №5](#)