Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.

Алхимова Дарья Сергеевна НБИ-01-19[1]

4 октября, 2022

[1]Российский Университет Дружбы Народов

Информация

Докладчик

- Алхимова Дарья Сергеевна
- студентка 4 курса
- группы НБИбд-01-19
- Российский университет дружбы народов
- 1032191645@rudn.ru

Цель работы

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

Выполнение лабораторной работы

Создала файл

Вошла в систему от имени пользователя guest и создала программу simpleid.c.

```
[guest1@dsalkhimova ~]$ touch simpleid.c
[guest1@dsalkhimova ~]$ ls
simpleid.c
[guest1@dsalkhimova ~]$ nano simpleid.c
```

Рис. 1: Создание файла программы

Выполнение лабораторной работы

Скомплилировала программу

Убедилась, что файл программы создан

```
[guest1@dsalkhimova ~]$ gcc simpleid.c -o simpleid
[guest1@dsalkhimova ~]$ ls
simpleid  simpleid.c
```

Рис. 2: Проверка наличия файла

Выполнение лабораторной работы

Сравнила вывод программ simpleid и id

Вывод программ сходится - они передают одинаковые параметры пользователя и его группы.

```
[guest1@dsalkhimova ~]$ ./simpleid
uid=1001, gid=1001
[guest1@dsalkhimova ~]$ id
uid=1001(guest1) gid=1001(guest1) groups=1001(guest1) context=unc
onfined u:unconfined r:unconfined t:s0-s0:c0.c1023
```

Рис. 3: Сравнения вывода программ simpleid и id

Выполнение лабораторной работы

Усложнила программу

Добавила в программу вывод действительных идентификаторов и сохранила как новый файл

```
[guest1@dsalkhimova ~]$ touch simpleid2.c
[guest1@dsalkhimova ~]$ ls
simpleid  simpleid2.c  simpleid.c
```

Рис. 4: Добавление в программу действительных индентификаторов

Выполнение лабораторной работы

Запустила программу

Скомпилировала и запустила simpleid2.c

```
[guest1@dsalkhimova ~]$ gcc simpleid2.c -o simpleid2
[guest1@dsalkhimova ~]$ ls
simpleid  simpleid2  simpleid2.c  simpleid.c
[guest1@dsalkhimova ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

Рис. 5: Компилирование и запуск программы simpleid2

Выполнение лабораторной работы

Изменила владельца файла

От имени суперпользователя выполнила команду `chown root:guest /home/guest/simpleid2`

```
[root@dsalkhimova guest1]# chown root:guest1 /home/guest1/simple
d2
[root@dsalkhimova guest1]# ls
simpleid  simpleid2  simpleid2.c  simpleid.c
[root@dsalkhimova guest1]# ls -l
total 32
-rwxrwxr-x. 1 guest1 guest1 8512 Oct  4 14:22 simpleid
-rwxrwxr-x. 1 root   guest1 8616 Oct  4 14:28 simpleid2
-rw-rw-r--. 1 guest1 guest1  335 Oct  4 14:28 simpleid2.c
-rw-rw-r--. 1 guest1 guest1  177 Oct  4 14:22 simpleid.c
```

Рис. 6: Смена владельца файла

Выполнение лабораторной работы

Изменила права файла

От имени суперпользователя выполнила команду `chmod u+s /home/guest/simpleid2`

```
[root@dsalkhimova guest1]# chmod u+s /home/guest1/simpleid2
[root@dsalkhimova guest1]# ls -l
total 32
-rwxrwxr-x. 1 guest1 guest1 8512 Oct  4 14:22 simpleid
-rwsrwxr-x. 1 root   guest1 8616 Oct  4 14:28 simpleid2
-rw-rw-r--. 1 guest1 guest1  335 Oct  4 14:28 simpleid2.c
-rw-rw-r--. 1 guest1 guest1  177 Oct  4 14:22 simpleid.c
```

Рис. 7: Смена прав файла

Выполнение лабораторной работы

Сравнила вывод программ simpleid и id

Результаты вывода сходятся.

```
[root@dsalkhimova guest1]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@dsalkhimova guest1]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:uncc
fined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 8: Сравнения вывода программ simpleid2 и id

Выполнение лабораторной работы

Повторила действия для SetGID-бита

```
[root@dsalkhimova guest1]# chmod g+s /home/guest1/simpleid2
[root@dsalkhimova guest1]# ls -l
total 32
-rwxrwxr-x. 1 guest1 guest1 8512 Oct  4 14:22 simpleid
-rwsrwsr-x. 1 root   guest1 8616 Oct  4 14:28 simpleid2
-rw-rw-r--. 1 guest1 guest1  335 Oct  4 14:28 simpleid2.c
-rw-rw-r--. 1 guest1 guest1  177 Oct  4 14:22 simpleid.c
[root@dsalkhimova guest1]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@dsalkhimova guest1]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:uncon
fined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 9: Повтор операций для SetGID-бита

Выполнение лабораторной работы

Сменила владельца и права у readfile.c

Изменила права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог

```
[root@dsalkhimova guest1]# chmod ugo-r readfile.c
[root@dsalkhimova guest1]# ls -l
total 48
-rwxr-xr-x. 1 root        root   8552 Oct  4 14:50 readfile
--w-------. 1 dsalkhimova root    395 Oct  4 14:49 readfile.c
-rwxrwxr-x. 1 guest1      guest1 8512 Oct  4 14:22 simpleid
-rwsrwsr-x. 1 root        guest1 8616 Oct  4 14:28 simpleid2
-rw-rw-r--. 1 guest1      guest1  335 Oct  4 14:28 simpleid2.c
-rw-rw-r--. 1 guest1      guest1  177 Oct  4 14:22 simpleid.c
```

Рис. 10: Смена прав readfile.c

Выполнение лабораторной работы

Проверила доступ к readfile.c

Проверила, что пользователь guest не может прочитать файл readfile.c

```
[root@dsalkhimova guest1]# su guest1
[guest1@dsalkhimova ~]$ cat readfile.c
cat: readfile.c: Permission denied
```

Рис. 11: Проверка доступа guest к readfile

Выполнение лабораторной работы

Сменила у программы readfile владельца

```
[guest1@dsalkhimova ~]$ su
Password:
[root@dsalkhimova guest1]# chown dsalkhimova readfile
[root@dsalkhimova guest1]# ls -l
total 48
-rwxr-xr-x. 1 dsalkhimova root   8552 Oct  4 14:50 readfile
--w-------. 1 dsalkhimova root    395 Oct  4 14:49 readfile.c
-rwxrwxr-x. 1 guest1      guest1 8512 Oct  4 14:22 simpleid
-rwsrwsr-x. 1 root        guest1 8616 Oct  4 14:28 simpleid2
-rw-rw-r--. 1 guest1      guest1  335 Oct  4 14:28 simpleid2.c
-rw-rw-r--. 1 guest1      guest1  177 Oct  4 14:22 simpleid.c
```

Рис. 12: Смена владельца readfile

Выполнение лабораторной работы

Установила SetU’D-бит у программы readfile

```
[root@dsalkhimova guest1]# chmod u+s readfile
[root@dsalkhimova guest1]# ls -l
total 48
-rwsr-xr-x. 1 dsalkhimova root   8552 Oct  4 14:50 readfile
--w-------. 1 dsalkhimova root    395 Oct  4 14:49 readfile.c
-rwxrwxr-x. 1 guest1      guest1 8512 Oct  4 14:22 simpleid
-rwsrwsr-x. 1 root        guest1 8616 Oct  4 14:28 simpleid2
-rw-rw-r--. 1 guest1      guest1  335 Oct  4 14:28 simpleid2.c
-rw-rw-r--. 1 guest1      guest1  177 Oct  4 14:22 simpleid.c
```

Рис. 13: Смена прав readfile

Выполнение лабораторной работы

Проверка атрибута Sticky на директории /tmp

Выяснила, установлен ли атрибут Sticky на директории /tmp

Рис. 14: Проверка атрибута Sticky

Выполнение лабораторной работы

Создала файл file01.txt

От имени пользователя guest создала файл file01.txt в директории /tmp со словом test

```
[guest1@dsalkhimova ~]$ cat /tmp/file01.txt
test
```

Рис. 15: Просмотр file01.txt

Выполнение лабораторной работы

Просмотр атрибутов file01.txt

Разрешила чтение и запись для категории пользователей «все остальные»

```
[guest1@dsalkhimova ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest1 guest1 5 Oct  4 15:04 /tmp/file01.txt
[guest1@dsalkhimova ~]$ chmod i+rw /tmp/file01.txt
chmod: invalid mode: ‘i+rw’
Try 'chmod --help' for more information.
[guest1@dsalkhimova ~]$ chmod o+rw /tmp/file01.txt
[guest1@dsalkhimova ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest1 guest1 5 Oct  4 15:04 /tmp/file01.txt
```

Рис. 16: Просмотр и изменение атрибутов file01.txt

Выполнение лабораторной работы

Прочитала file01.txt от пользователя guest2

От пользователя guest2 (не являющегося владельцем) успешно прочитала файл /tmp/file01.txt

```
[root@dsalkhimova guest1]# su guest2
[guest2@dsalkhimova guest1]$ cd
[guest2@dsalkhimova ~]$ cat /tmp/file01.txt
test
```

Рис. 17: Чение file01.txt пользователем guest2

Выполнение лабораторной работы

Дозаписала в файл /tmp/file01.txt слово test2

От пользователя guest2 успешно дозаписала в файл /tmp/file01.txt слово test2 и проверила содержимое файла

```
[guest2@dsalkhimova ~]$ echo "test2" >> /tmp/file01.txt
[guest2@dsalkhimova ~]$ cat /tmp/file01.txt
test
test2
```

Рис. 18: Дозапись file01.txt пользователем guest2

Выполнение лабораторной работы

Очистила и дозаписала в файл /tmp/file01.txt слово test3

От пользователя guest2 успешно дозаписала в файл /tmp/file01.txt слово test3, стерев при этом все предыдущее содержимое файла

```
[guest2@dsalkhimova ~]$ echo "test3" > /tmp/file01.txt
[guest2@dsalkhimova ~]$ cat /tmp/file01.txt
test3
```

Рис. 19: Дозапись с удалением file01.txt пользователем guest2

Выполнение лабораторной работы

Попробовала удалить file01.txt

Операция запрещена

```
[guest2@dsalkhimova ~]$ rm /tmp/file01.txt
rm: cannot remove ‘/tmp/file01.txt’: Operation not permitted
```

Рис. 20: Удаление file01.txt пользователем guest2

Выполнение лабораторной работы

Удалила атрибут t с file01.txt

От суперпользователя сняла атрибут t (Sticky-бит) с директории /tmp и проверила атрибуты file01.txt от пользователя guest2

```
[guest2@dsalkhimova ~]$ su -
Password:
Last login: Tue Oct  4 15:07:38 MSK 2022 on pts/0
[root@dsalkhimova ~]# chmod -t /tmp
[root@dsalkhimova ~]# exit
logout
[guest2@dsalkhimova ~]$ ls -l / | grep tmp
drwxrwxrwx.  25 root root 4096 Oct  4 15:11 tmp
```

Рис. 21: Снятие атрибута Sticky

Выполнение лабораторной работы

Повторила предыдущие шаги без атрибута t

Изменений нет, кроме того, что теперь удалось удалить файл file01.txt от имени guest2

```
[guest2@dsalkhimova ~]$ cat /tmp/file01.txt
test3
[guest2@dsalkhimova ~]$ echo "test2" >> /tmp/file01.txt
[guest2@dsalkhimova ~]$ cat /tmp/file01.txt
test3
test2
[guest2@dsalkhimova ~]$ echo "test" > /tmp/file01.txt
[guest2@dsalkhimova ~]$ cat /tmp/file01.txt
test
[guest2@dsalkhimova ~]$ rm /tmp/file01.txt
[guest2@dsalkhimova ~]$ ls -l
total 0
[guest2@dsalkhimova ~]$ ls -l /tmp
total 564
drwx------. 2 guest2      guest2          25 Oct  4 12:25 ssh-
5j0i1Kzws
drwx------. 2 dsalkhimova dsalkhimova     24 Oct  4 13:34 ssh-
4KFnNc8kz
drwx------. 2 guest1      guest1          25 Oct  4 12:37 ssh-
FUKoOeJoL
drwx------. 3 root        root            17 Oct  4 13:32 syst
```

Выполнение лабораторной работы

Вернула атрибут t на директорию /tmp от суперпользователя

```
[guest2@dsalkhimova ~]$ su -
Password:
Last login: Tue Oct  4 15:17:21 MSK 2022 on pts/0
[root@dsalkhimova ~]# chmod +t /tmp
[root@dsalkhimova ~]# ls -l / | grep tmp
drwxrwxrwt.  25 root root 4096 Oct  4 15:20 tmp
[root@dsalkhimova ~]# exit
logout
[guest2@dsalkhimova ~]$
```

Рис. 22: Возвращение атрибута Sticky на директрорию /tmp

Вывод

В процессе выполнения данной лабораторной работы я научилась работать с механизмами изменения идентификаторов, применением SetUID- и Sticky-битов. Получила практических навыков работы в консоли с дополнительными атрибутами. Рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.