Отчет по лабораторной работе 5

Дисциплина: Информационная безопасность

Дяченко Злата Константиновна, НФИбд-03-18

Прагматика выполнения лабораторной работы

Данная лабораторная работа выполнялась мной для приобретения практических навыков работы в консоли с дополнительными атрибутами файлов и исследования их влияния.

Цель выполнения лабораторной работы

Изучить механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получить практических навыков работы в консоли с дополнительными атрибутами. Рассмотреть работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Задачи выполнения лабораторной работы

Создать и скомпилировать программу simpleid.c и убедиться, что файл программы создан (рис. 1).

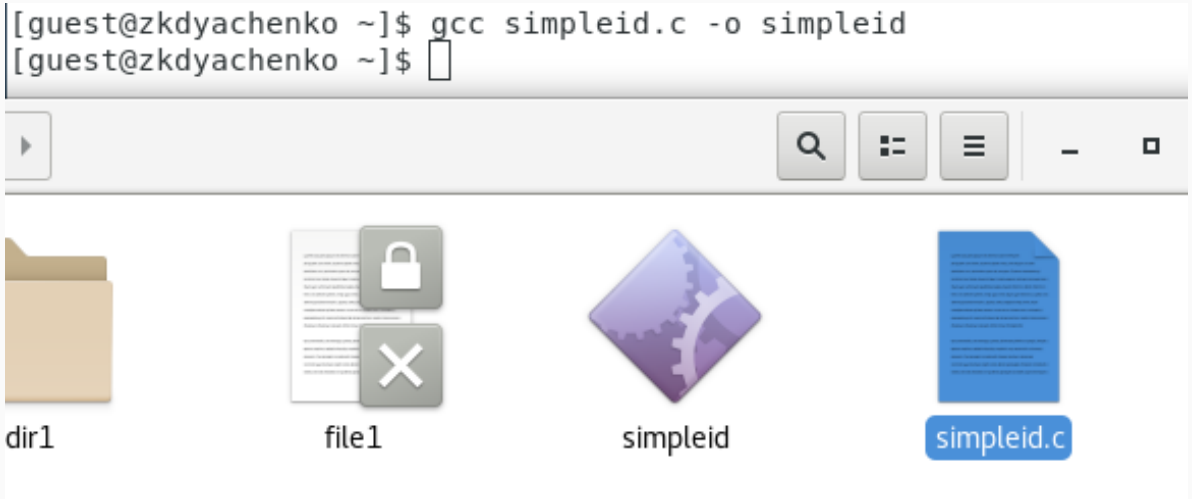

Figure 1: Компиляция программы

Задачи выполнения лабораторной работы

Выполнить программу simpleid и системную программу id (рис. 2).

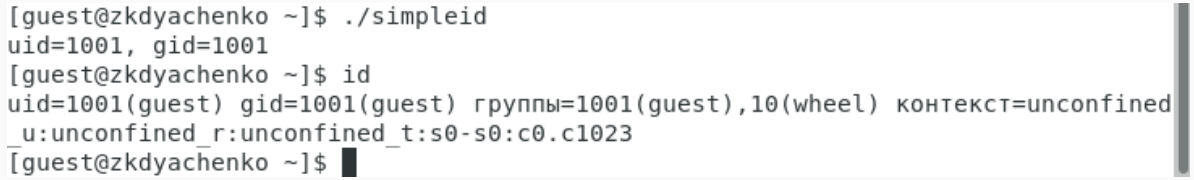

Figure 2: Результат выполнения программы simpleid и системной программы id

Задачи выполнения лабораторной работы

Усложнить программу, добавив вывод действительных идентификаторов, назвать новую программу simpleid2.c. Скомпилировать и запустить simpleid2.c (рис. 3).

```
[guest@zkdyachenko ~]$ gcc simpleid2.c -o simpleid2
[guest@zkdyachenko ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@zkdyachenko ~]$
```

Figure 3: Результат выполнения программы simpleid2

Задачи выполнения лабораторной работы

От имени суперпользователя выполнить команду chown, чтобы изменить владельца (пользователя и группу) файла simpleid2 и chmod u+s, чтобы установить SetUID (рис. 4).

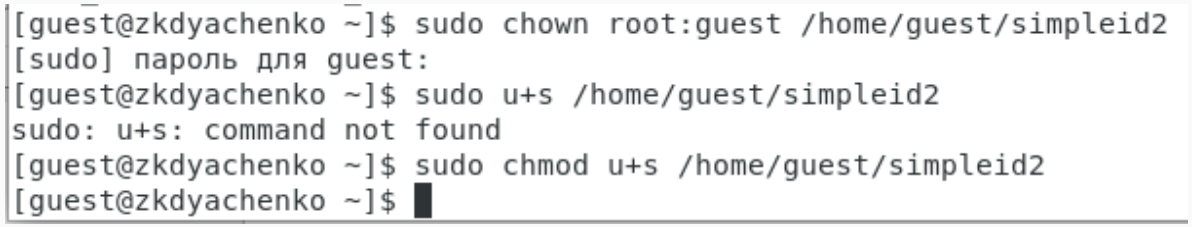

Figure 4: Выполнение команд

Задачи выполнения лабораторной работы

Выполнить проверку правильности установки новых атрибутов и смены владельца файла simpleid2. А затем запустить simpleid2 и id (рис. 5).

```
[guest@zkdyachenko ~]$ ls -l simpleid2
-rwsrwxr-x. 1 root guest 8576 ноя 11 18:25 simpleid2
[guest@zkdyachenko ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@zkdyachenko ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel) контекст=unconfined
_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@zkdyachenko ~]$
```

Figure 5: Выполнение программы simpleid2 после смены владельца файла

Задачи выполнения лабораторной работы

Проделать тоже самое относительно SetGID-бита (рис. 6).

```
[guest@zkdyachenko ~]$ sudo chown guest:root /home/guest/simpleid2
[guest@zkdyachenko ~]$ sudo chmod g+s /home/guest/simpleid2
[guest@zkdyachenko ~]$ ls -l simpleid2
-rwxrwsr-x. 1 guest root 8576 ноя 11 18:25 simpleid2
[guest@zkdyachenko ~]$ ./simpleid2
e_uid=1001, e_gid=0
real_uid=1001, real_gid=1001
[guest@zkdyachenko ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel) контекст=unconfined
_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@zkdyachenko ~]$
```

Figure 6: Установка SetGID-бита и выполнение программы simpleid2

Задачи выполнения лабораторной работы

Создать программу readfile.c и откомпилировать ее. Сменить владельца у файла readfile.c и изменить права так, чтобы только суперпользователь мог прочитать его, а guest не мог. Проверить, что пользователь guest не может прочитать файл readfile.c (рис. 7).

```
[guest@zkdyachenko ~]$ gcc readfile.c -o readfile
[guest@zkdyachenko ~]$ sudo chown guest2:guest /home/guest/readfile.c
[sudo] пароль для guest:
[guest@zkdyachenko ~]$ sudo chmod ug-r /home/guest/readfile.c
[guest@zkdyachenko ~]$ ls -l readfile.c
--w--w-r--. 1 guest2 guest 407 ноя 11 18:41 readfile.c
[guest@zkdyachenko ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@zkdyachenko ~]$
```

Figure 7: Новый владелец readfile.c

Задачи выполнения лабораторной работы

Сменить у программы readfile владельца и установить SetUID-бит (рис. 8).

```
[guest@zkdyachenko ~]$ sudo chown guest2:guest /home/guest/readfile
[sudo] пароль для guest:
[guest@zkdyachenko ~]$ sudo chmod u+s /home/guest/readfile
[guest@zkdyachenko ~]$
```

Figure 8: Смена владельца и установка SetUID-бита

Задачи выполнения лабораторной работы

Проверить, что программа readfile не может прочитать файл readfile.c (рис. 9).

Figure 9: Попытка прочитать readfile.c

Задачи выполнения лабораторной работы

Проверить, что программа readfile не может прочитать файл /etc/shadow (рис. 10).

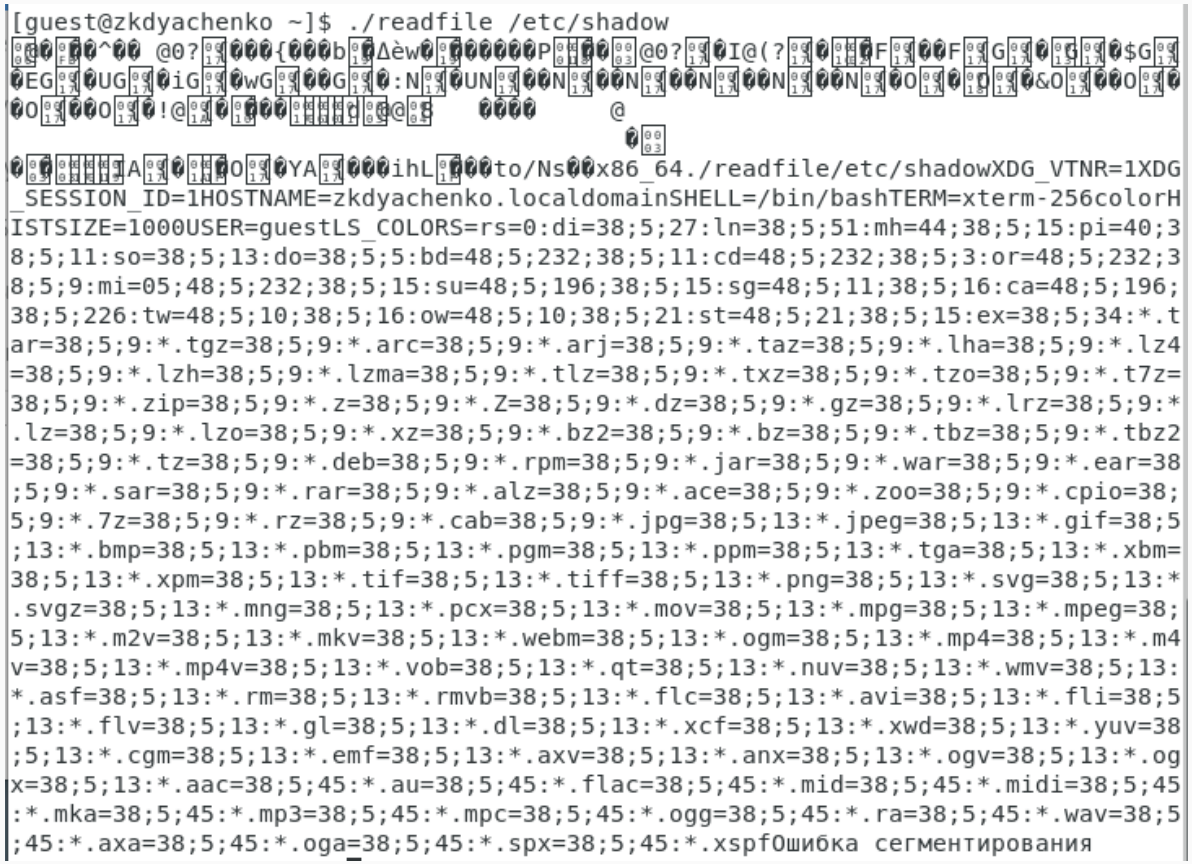

Figure 10: Попытка прочитать /etc/shadow

Задачи выполнения лабораторной работы

Выяснить, что установлен атрибут Sticky на директории /tmp (рис. 11). От имени пользователя guest создать файл file01.txt в директории /tmp со словом test. Просмотреть атрибуты у только что созданного файла и разрешить чтение и запись для категории пользователей «все остальные».

```
[guest@zkdyachenko ~]$ ls -l / | grep tmp
drwxrwxrwt.  16 root root 4096 ноя 11 19:01 tmp
[guest@zkdyachenko ~]$ echo "test" > /tmp/file01.txt
[guest@zkdyachenko ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 ноя 11 19:07 /tmp/file01.txt
[guest@zkdyachenko ~]$ chmod o+rw /tmp/file01.txt
[guest@zkdyachenko ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 ноя 11 19:07 /tmp/file01.txt
[guest@zkdyachenko ~]$
```

Figure 11: Создание файла и установка атрибутов

Задачи выполнения лабораторной работы

От пользователя guest2 прочитать файл /tmp/file01.txt. Проверить, возможно ли дозаписать в файл слово test2, перезаписать файл словом test3 (рис. 12).

```
[guest2@zkdyachenko ~]$ cat /tmp/file01.txt
test
[guest2@zkdyachenko ~]$ echo "test2" >> /tmp/file01.txt
[guest2@zkdyachenko ~]$ cat /tmp/file01.txt
test
test2
[guest2@zkdyachenko ~]$ echo "test3" > /tmp/file01.txt
[guest2@zkdyachenko ~]$ cat /tmp/file01.txt
test3
[guest2@zkdyachenko ~]$
```

Figure 12: Изменение файла /tmp/file01.txt от имени пользователя guest2

Задачи выполнения лабораторной работы

От пользователя guest2 попробовать удалить файл /tmp/file01.txt. Повысить свои права до суперпользователя и выполнить после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp. (рис. 13)

```
[guest2@zkdyachenko ~]$ rm /tmp/file01.txt
rm: невозможно удалить «/tmp/file01.txt»: Операция не позволена
[guest2@zkdyachenko ~]$ su -
Пароль:
Последний вход в систему:Чт ноя 11 17:52:44 MSK 2021на pts/0
[root@zkdyachenko ~]# chmod -t /tmp
[root@zkdyachenko ~]# exit
logout
[guest2@zkdyachenko ~]$
```

Figure 13: Снятие Sticky-бита

Задачи выполнения лабораторной работы

От пользователя guest2 проверить, что атрибута t у директории /tmp нет. От пользователя guest2 попробовать прочитать файл /tmp/file01.txt, дозаписать в файл слово test2, записать только слово test3, удалить файл от имени guest2 (рис. 14).

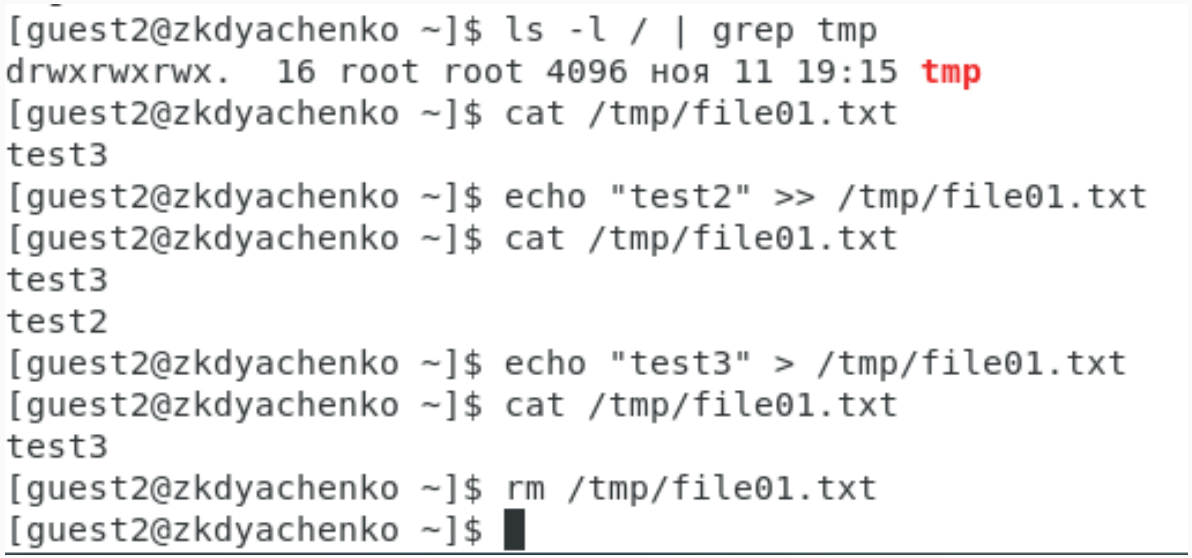

Figure 14: Удаление файла от имени guest2

Задачи выполнения лабораторной работы

Повысить свои права до суперпользователя и вернуть атрибут t на директорию /tmp (рис. 15).

```
[guest2@zkdyachenko ~]$ su -
Пароль:
Последний вход в систему:Чт ноя 11 19:15:02 MSK 2021на pts/0
[root@zkdyachenko ~]# chmod +t /tmp
[root@zkdyachenko ~]# exit
logout
[guest2@zkdyachenko ~]$
```

Figure 15: Возвращение атрибута t

Результаты выполнения лабораторной работы

В результате выполнения работы я изучила механизмы изменения идентификаторов, применение SetUID- и Sticky-битов. Были получены практические навыки работы в консоли с дополнительными атрибутами и рассмотрена работа механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.