Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Павличенко Родион Андреевич

Содержание

Список иллюстраций

Список таблиц

1 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

2 Выполнение лабораторной работы

Вошли в систему от имени пользователя guest. Создали программу simpleid.c

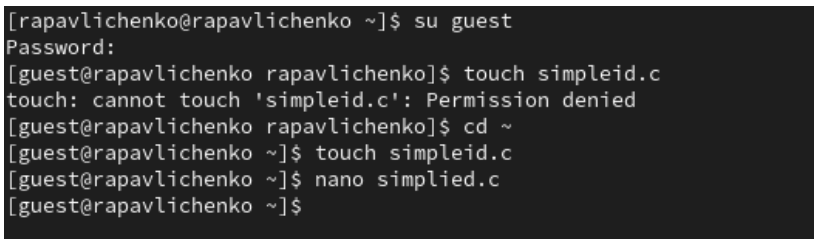

Рисунок 2.1: Создание simpleid

Скомплилировали программу и убедились, что файл программы создан. Выполнили программу simpleid. Выполнили системную программу id

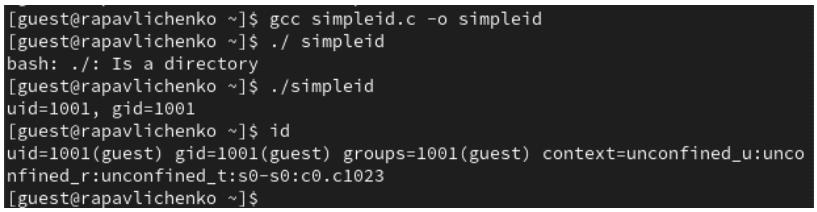

Рисунок 2.2: Работа с программой

Усложнили программу, добавив вывод действительных идентификаторо

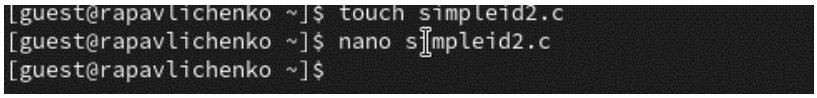

Рисунок 2.3: Усложнение программы

Скомпилировали и запустили simpleid2.c

Рисунок 2.4: Запуск

От имени суперпользователя выполнили команды: chown root:guest /home/guest/simpleid2; chmod u+s /home/guest/simpleid

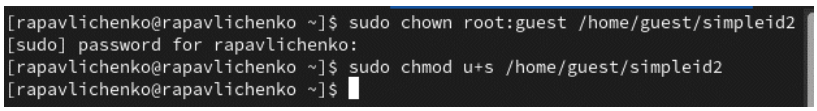

Рисунок 2.5: Выполнение команд

Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2. Запустили simpleid2 и id

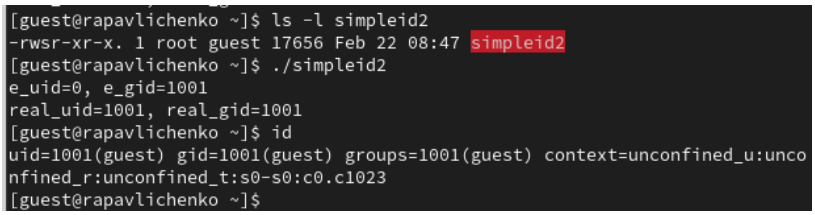

Рисунок 2.6: Проверка и запуск

Проделали тоже самое относительно SetGID-бита

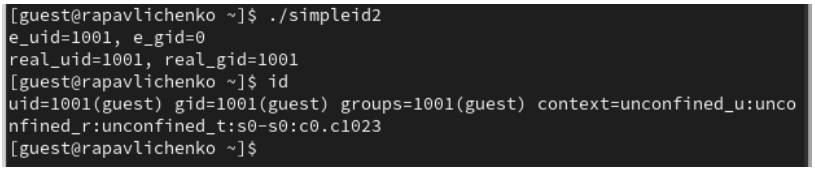

Рисунок 2.7: Работа с SetGID-битом

Создали программу readfile.c и откомпилировали ее

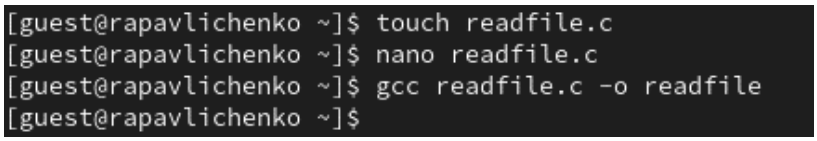

Рисунок 2.8: Создание новой программы

Сменили владельца у файла readfile.c и изменили права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог

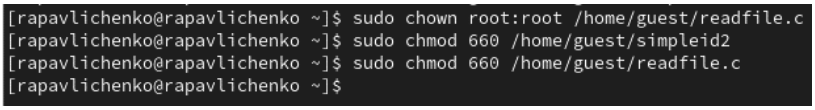

Рисунок 2.9: Смена владельца

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

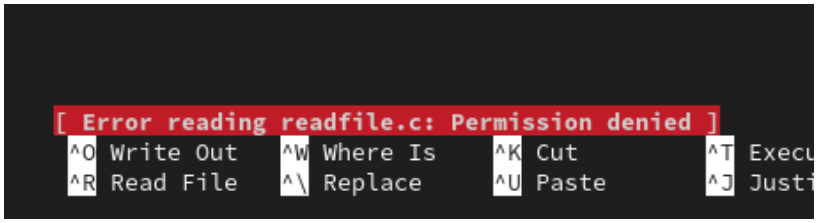

Рисунок 2.10: Проверка файла

Сменили у программы readfile владельца и установили SetU'D-бит

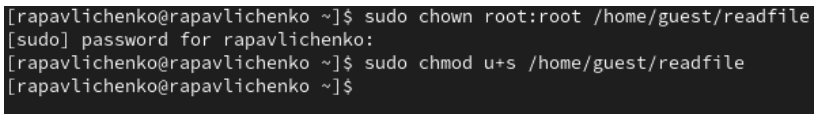

Рисунок 2.11: Смена владельца

Проверили, может ли программа readfile прочитать файл readfile.c. Она может

```
[guest@rapavlichenko ~]$ ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.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;
}
```

Рисунок 2.12: Чтение файла

Проверили, может ли программа readfile прочитать файл /etc/shadow. Она может

```
[guest@rapavlichenko ~]$ ./readfile /etc/shadow
root:$6$2DGS3DzNxjz4v3Ef$vb.9EXKNiZz2MHIQafBCOXhOHALYzBTpWyg1bbk1AhdtZwHdrd7
4gHHibEL8Rqn0EBN6mAk6/UXcvhX6.Ahge0::0:99999:7:::
bin:*:19820:0:99999:7:::
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:::
```

Рисунок 2.13: Чтение файла

Выяснили, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду ls -l / | grep tmp. От имени пользователя guest создали файл file01.txt в директории /tmp со словом test. Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные»

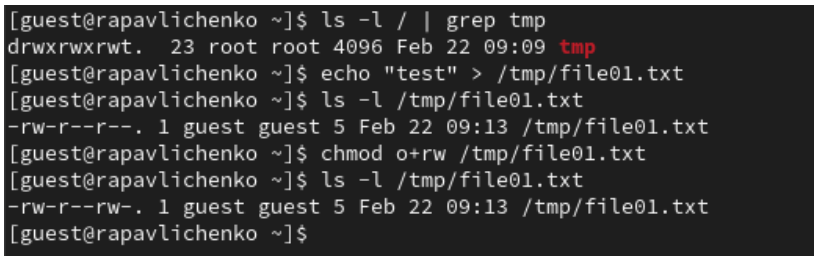

Рисунок 2.14: Работа с файлом file01.txt

От пользователя guest2 попробуйте прочитать файл /tmp/file01.txt. От пользователя guest2 попробовали дозаписать в файл /tmp/file01.txt слово test2. Операцию выполнить не удалось. Проверили содержимое файла командой cat /tmp/file01.txt. От пользователя guest2 попробовализаписать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию Выполнить операцию не удалось. Проверили содержимое файла командой cat /tmp/file01.txt

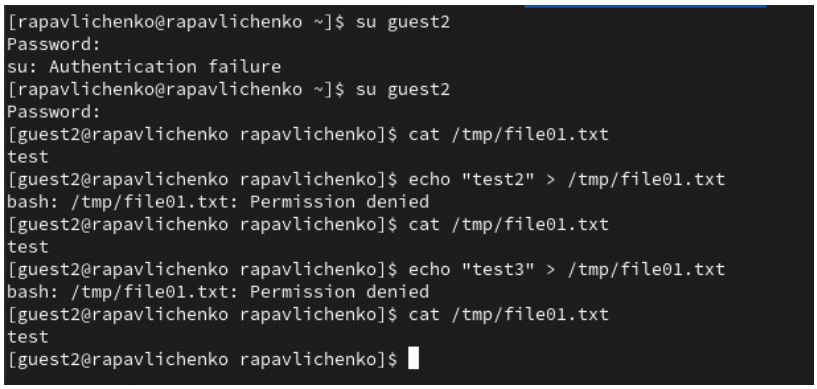

Рисунок 2.15: Работа с файлом file01.txt

От пользователя guest2 попробовали удалить файл /tmp/file01.txt командой rm /tmp/file01.txt. Не удалось удалить файл.

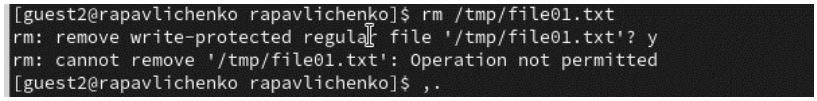

Рисунок 2.16: Удаление файла

Повысили свои права до суперпользователя и выполнили после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp. Покинули режим

суперпользователя командой exit. От пользователя guest2 проверили, что атрибута t у директории /tmp нет

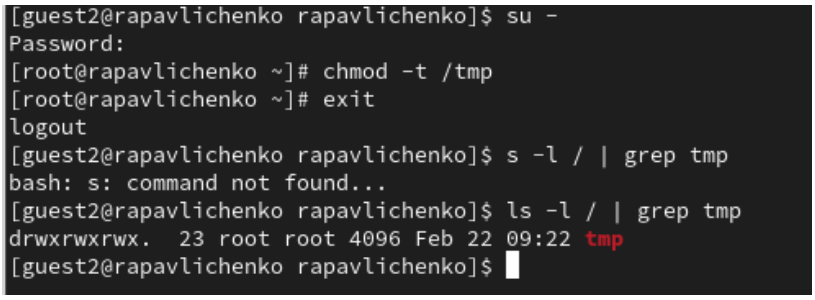

Рисунок 2.17: Работа с атрибутом t

Повторили предыдущие шаги. Все действия, кроме удаления выполнить не удалось.

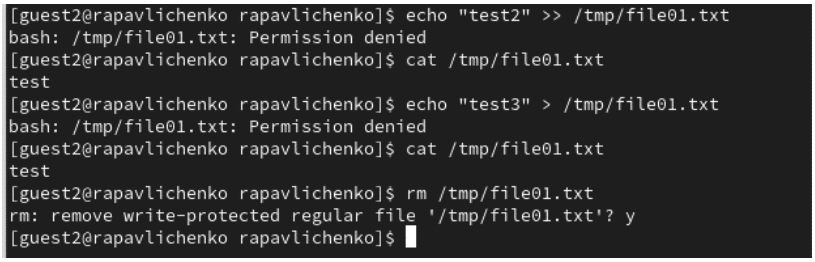

Рисунок 2.18: Повтор предыдущих шагов

Повысили свои права до суперпользователя и вернули атрибут t на директорию /tmp

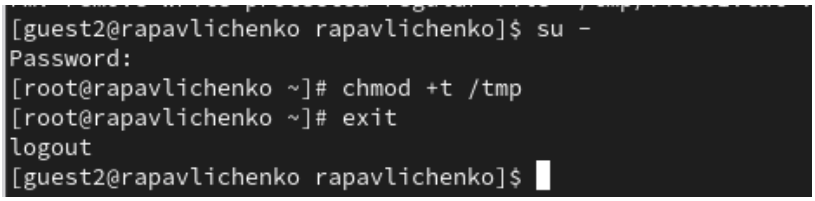

Рисунок 2.19: Возвращение атрибута t в дирректорию tmp

3 Выводы

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

Список литературы