Oтчёт по лабораторной работе

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Назарьева Алена Игоревна НФИбд-03-18

Содержание

# 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

# Выполнение лабораторной работы

Создание программы

1. Вошла в систему от имени пользователя guest.
2. Создала программу simpleid.c (рис. -fig. 1)



Figure 1: simpleid.c

1. Скомплилировала программу и убедилась, что файл программы создан
2. Выполнила программу simpleid
3. Выполнила системную программу id и сравнила полученный результат с данными предыдущего пункта задания. Данные совпадают (рис. -fig. 2)



Figure 2: пункты 3-5

1. Усложнила программу, добавив вывод действительных идентификаторов. Получившуюся программу назвала simpleid2.c. (рис. -fig. 3)

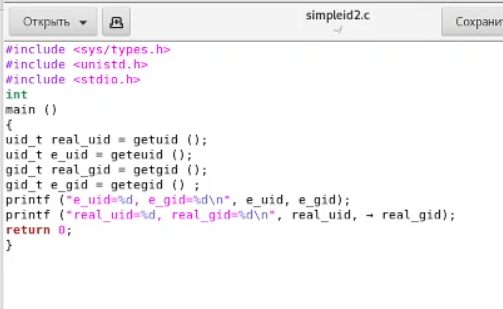


Figure 3: simpleid2.c

1. Скомпилировала и запустила simpleid2.c
2. От имени суперпользователя сменила у файла владельца и установила установите SetU’D-бит
3. Использовала sudo или повысила временно свои права с помощью su.(рис. -fig. 4)



Figure 4: пункты 7-9

1. Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2
2. Запустила simpleid2 и id. Результаты совпадают. (рис. -fig. 5)



Figure 5: пункты 10-11

1. Проделала тоже самое относительно SetGID-бита. (рис. -fig. 6)

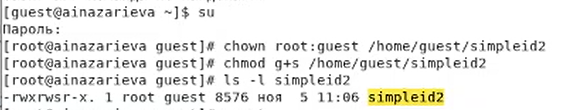


Figure 6: пункты 12-1

(рис. -fig. 7)



Figure 7: пункты 12-2

1. Создала программу readfile.c (рис. -fig. 8)

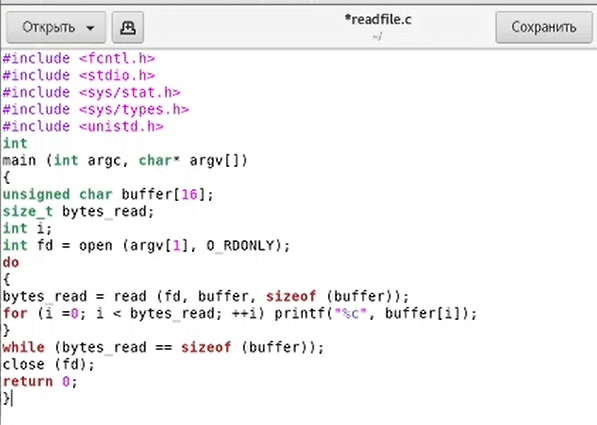


Figure 8: readfile.c

1. Откомпилировала её.
2. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь мог прочитать его, a guest не мог. (рис. -fig. 9)



Figure 9: пункты 14-15

1. Проверила, что пользователь guest не может прочитать файл readfile.c. (рис. -fig. 10)

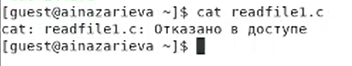


Figure 10: пункт 16

1. Сменила у программы readfile владельца и установила SetU’D-бит.
2. Проверила, может ли программа readfile прочитать файл readfile.c (рис. -fig. **¿fig:011?**)

 19. Проверила, может ли программа readfile прочитать файл /etc/shadow (рис. -fig. 11)

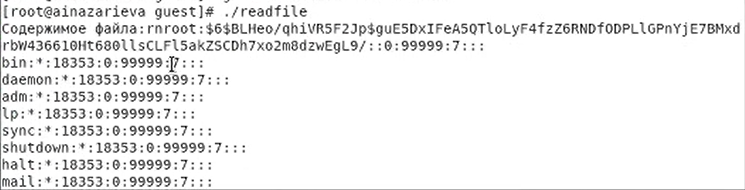


Figure 11: пункт 19

Так как владелец файла readfile root, а setuid являются флагами прав доступа в Unix, которые разрешают пользователям запускать исполняемые файлы с правами владельца исполняемого файла, то readfile смог прочитать и readfile.c и /etc/shadow

Исследование Sticky-бита

1. Выяснила, что установлен атрибут Sticky на директории /tmp
2. От имени пользователя guest создала файл file01.txt в директории /tmp со словом test
3. Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные» (рис. -fig. 12)



Figure 12: пункт 1-3

1. От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt
2. От пользователя guest2 не смогла дозаписать в файл.
3. Проверила содержимое файла
4. От пользователя guest2 записала в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию
5. Проверила содержимое файла
6. От пользователя guest2 не смогла удалить файл /tmp/file01.txt
7. Повысила свои права до суперпользователя следующей и выполнила после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp
8. Покинула режим суперпользователя
9. От пользователя guest2 проверила, что атрибута t у директории /tmp нет (рис. -fig. 13)

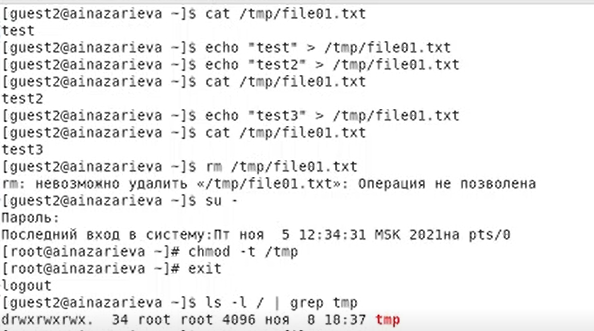


Figure 13: пункт 4-12

1. Повторила предыдущие шаги.
2. Мне удалось удалить файл от имени пользователя, не являющегося его владельцем Благодаря Sticky bit пользователи могут создавать файлы, читать и выполнять их, принадлежащие другим пользователям, но не могут удалять файлы, принадлежащие другим пользователям, даже если в каталоге есть разрешение 777. Если sticky bit не установлен, то юзер может удалить файл, так как он наследует разрешения родительского каталога.
3. Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp (рис. -fig. 14)



Figure 14: пункты 13-15

# Выводы

В результате выполнения работы я Изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов