Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.

Монастырская Кристина Владимировна

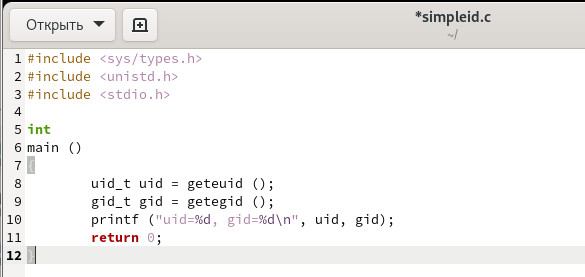
Содержание

# 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 [[1]](#список-литературы).

# Выполнение лабораторной работы

1. Вошла в систему от имени пользователя guest.
2. Создала программу simpleid.c ([рис. 1](../images/1.jpg)).



Код программы simpleid.c

1. Скомплилировала программу и убедилась, что файл программы создан.([рис. 2](../images/2.jpg))

Компилирование программы simpleid

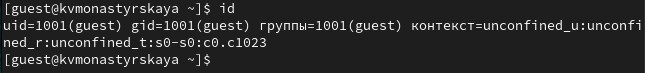
Компилирование программы simpleid

1. Выполнила программу simpleid ([рис. 3](../images/3.jpg)).

Выполнение программы simpleid

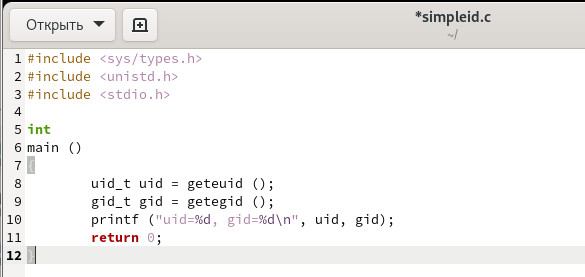
Выполнение программы simpleid

1. Выполнила системную программу id и сравнила полученный результат с данными предыдущего пункта задания.([рис. 4](../images/4.jpg))



Выполнение id

1. Усложнила программу, добавив вывод действительных идентификаторов. Получившуюся программу назвала simpleid2.c([рис. 5](../images/5.jpg))



Код программы simpleid2.c

1. Скомпилируйте и запустите simpleid2.c:([рис. 6](../images/6.jpg))([рис. 7](../images/7.jpg))

Компиляция simpleid2 Выполнение simpleid2

1. От имени суперпользователя выполнила команды([рис. 8](../images/8.jpg)):

Смена владельца и атрибутов

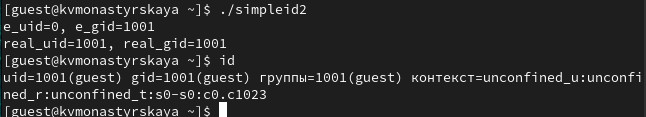
Смена владельца и атрибутов

1. Выполнила проверку правильности установки новых атрибутов и сменила владельца файла simpleid2:([рис. 2](../images/9.jpg))

Проверка установки новых атрибутов

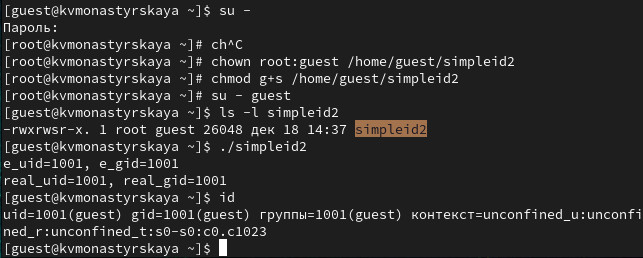
Проверка установки новых атрибутов

1. Запустила simpleid2 и id([рис. 10](../images/11.jpg))



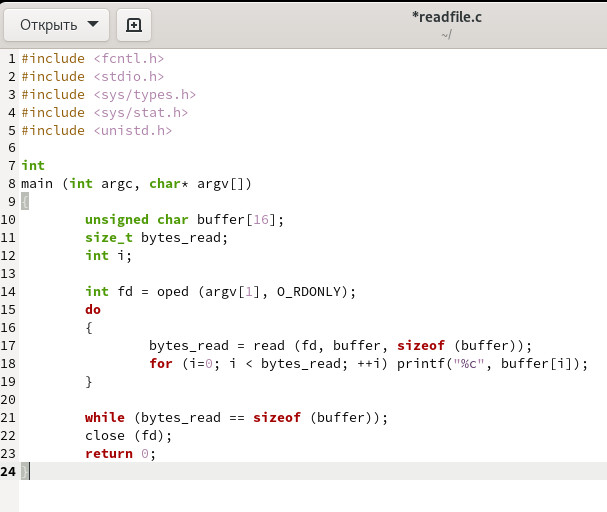
Код программы simpleid.c

1. Проделала тоже самое относительно SetGID-бита.([рис. 11](../images/12.jpg))



SetGID-бит

1. Создала программу readfile.c([рис. 12](../images/13.jpg)):



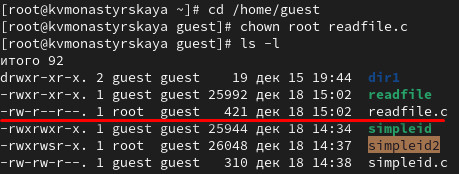
Программа readfile.c

1. Откомпилировала её.([рис. 13](../images/14.jpg))

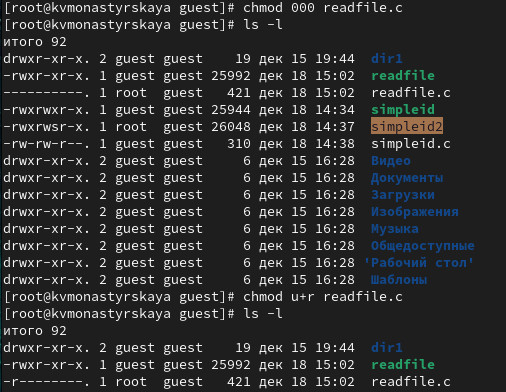
Компилирование readfile

Компилирование readfile

1. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог.([рис. 14](../images/15.jpg))([рис. 15](../images/16.jpg))



Смена владельца readfile.c



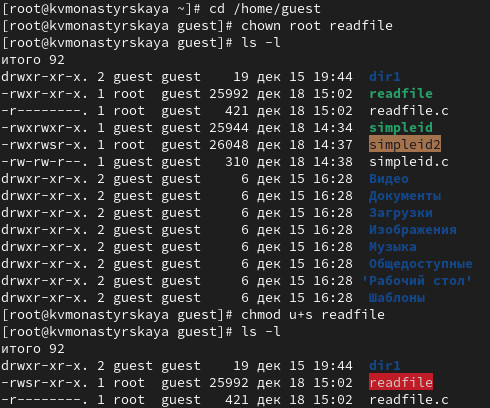
Изменение атрибутов readfile.c

1. Проверила, что пользователь guest не может прочитать файл readfile.c.([рис. 16](../images/17.jpg))

Проверка чтения файла

Проверка чтения файла

1. Сменила у программы readfile владельца и установила SetU’D-бит([рис. 17](../images/18.jpg))



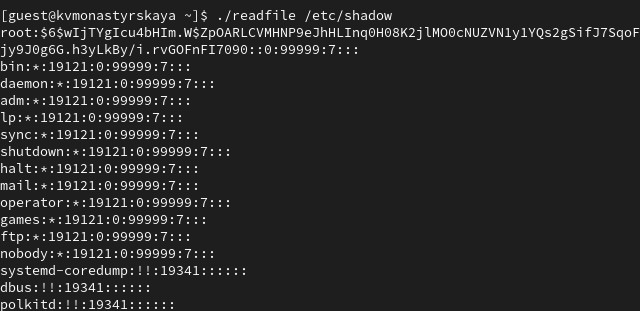
Смена владельца и установка SetU’D-бита

1. Проверила, может ли программа readfile прочитать файл readfile.c([рис. 18](../images/19.jpg))



Чтение файла readfile.c программой readfile

1. Проверила, может ли программа readfile прочитать файл /etc/shadow([рис. 19](../images/20.jpg))



Чтение файла /etc/shadow программой из readfile

1. Выяснила, установлен ли атрибут Sticky на директории /tmp ([рис. 20](../images/21.jpg))

Атрибут Sticky на директории /tmp

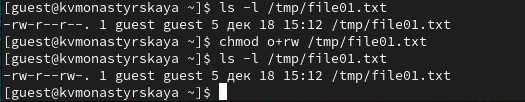
Атрибут Sticky на директории /tmp

1. От имени пользователя guest создала файл file01.txt в директории /tmp со словом test: echo “test” > /tmp/file01.txt([рис. 21](../images/22.jpg))

Создание файла file01.txt в директории /tmp

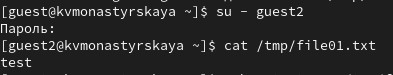
Создание файла file01.txt в директории /tmp

1. Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные»([рис. 22](../images/23.jpg)): ls -l /tmp/file01.txt chmod o+rw /tmp/file01.txt ls -l /tmp/file01.txt



Чтение и запись для категории пользователей «все остальные»

1. От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt([рис. 23](../images/24.jpg)):



Чтение файла /tmp/file01.txt

1. От пользователя guest2 попробовала дозаписать в файл /tmp/file01.txt слово test2 командой echo “test2” > /tmp/file01.txt([рис. 24](../images/25.jpg))

Дозапись файла /tmp/file01.txt

Дозапись файла /tmp/file01.txt

1. От пользователя guest2 попробовала записать в файл /tmp/file01.txtслово test3, стерев при этом всю имеющуюся в файле информацию командой echo “test3” > /tmp/file01.txt([рис. 25](../images/27.jpg))

Перезапись файла /tmp/file01.txt

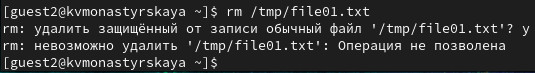
Перезапись файла /tmp/file01.txt

1. Проверила содержимое файла([рис. 26](../images/28.jpg))

Проверка содержимого файла /tmp/file01.txt

Проверка содержимого файла /tmp/file01.txt

1. От пользователя guest2 попробовала удалить файл /tmp/file01.txt([рис. 27](../images/29.jpg))

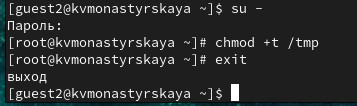


Попытка удаления файла /tmp/file01.txt

1. Повысила свои права до суперпользователя следующей командой([рис. 28](../images/1.jpg)) su - и выполнила после этого команду, снимающую атрибут t (Sticky-бит) сдиректории /tmp: chmod -t /tmp
2. Повторила предыдущие шаги([рис. 29](../images/30.jpg))

[Проверка атрибутов]](../images/30.jpg){ #fig:029 width=80% height=80% }

1. Теперь можем удалять файлы находящиеся в каталоге tmp.
2. Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp([рис. 30](../images/31.jpg)): su - chmod +t /tmp exit



Проверка атрибутов

# Выводы

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.

# Список литературы

1. [Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3](https://search.rsl.ru/ru/record/01000682756).