Лабораторная работа № 5.

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Диана Алексеевна Садова

Содержание

# 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 Последовательность выполнения работы

## 2.1 Создание программы

1. Войдите в систему от имени пользователя guest.(рис. 1).

Заходим в систему пользователя guest

Рис. 1: Заходим в систему пользователя guest

1. Создайте программу simpleid.c:(рис. 2),(рис. 3).

Создаем файл с именем simpleid

Рис. 2: Создаем файл с именем simpleid



Рис. 3: Код

1. Скомплилируйте программу и убедитесь, что файл программы создан:(рис. 4).

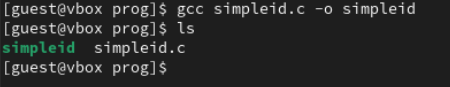


Рис. 4: Скомплилируем программу

1. Выполните программу simpleid:(рис. 5).

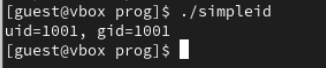


Рис. 5: Выполняем код

1. Выполните системную программу id:(рис. 6).

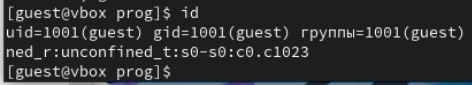


Рис. 6: Выполняем системную программу id

и сравните полученный вами результат с данными предыдущего пункта задания.

Записи идентичны.

1. Усложните программу, добавив вывод действительных идентификаторов:(рис. 7).



Рис. 7: Код

Получившуюся программу назовите simpleid2.c.

1. Скомпилируйте и запустите simpleid2.c:(рис. 8).

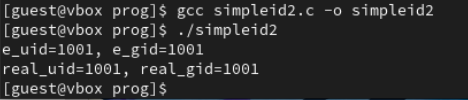


Рис. 8: Скомплилируем программу

1. От имени суперпользователя выполните команды:(рис. 9).

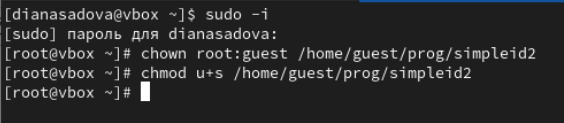


Рис. 9: Выполняем команды

1. Используйте sudo или повысьте временно свои права с помощью su.(рис. 10).

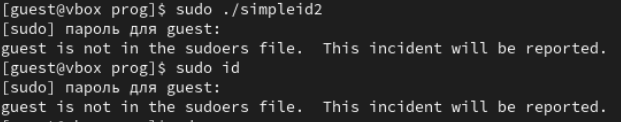


Рис. 10: Переходим в режим суперпользователя

Поясните, что делают эти команды.

Мы пытаемся запустить код в файле simpleid2.c от имени суперпользователя.

1. Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2:(рис. 11).

Проверяем правильности новых атрибутов

Рис. 11: Проверяем правильности новых атрибутов

1. Запустите simpleid2 и id:(рис. 12).

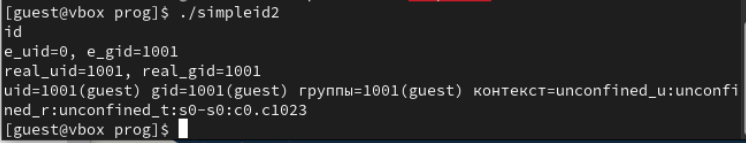


Рис. 12: Запускаем simpleid2 и id

Сравните результаты.

simpleid2 - выдает только информацию о id (номер).

id - дает больше информации об пользователе и его группах.

1. Проделайте тоже самое относительно SetGID-бита.
2. Создайте программу readfile.c:(рис. 13).

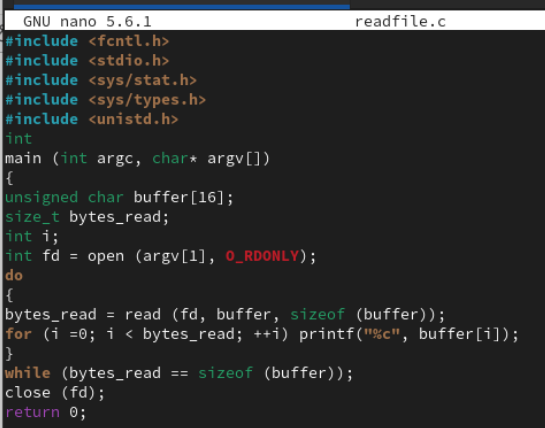


Рис. 13: Код

1. Откомпилируйте её.(рис. 14).

Скомплилируем программу

Рис. 14: Скомплилируем программу

1. Смените владельца у файла readfile.c (или любого другого текстового файла в системе) и измените права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог.(рис. 15).

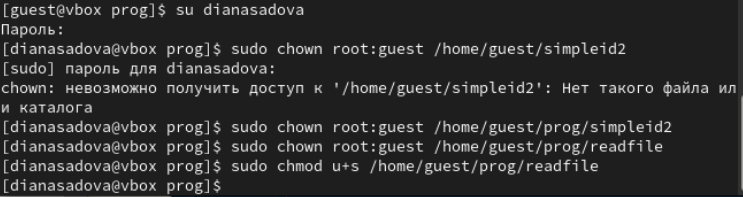


Рис. 15: Меняем прова доступа

1. Проверьте, что пользователь guest не может прочитать файл readfile.c.(рис. 16).

Проверяем, что guest не может прочитать файл

Рис. 16: Проверяем, что guest не может прочитать файл

1. Смените у программы readfile владельца и установите SetU’D-бит.(рис. 17).

Снимаем у readfile владельца

Рис. 17: Снимаем у readfile владельца

1. Проверьте, может ли программа readfile прочитать файл readfile.c?(рис. 18).

Проверяем может ли readfile прочитать файл readfile.c

Рис. 18: Проверяем может ли readfile прочитать файл readfile.c

1. Проверьте, может ли программа readfile прочитать файл /etc/shadow?(рис. 19).

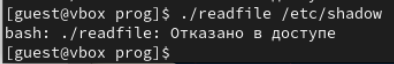


Рис. 19: Проверяем может ли readfile прочитать файл /etc/shadow

## 2.2 Исследование Sticky-бита

1. Выясните, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду(рис. 20).

Определяем установлин ли атрибут Sticky

Рис. 20: Определяем установлин ли атрибут Sticky

1. От имени пользователя guest создайте файл file01.txt в директории /tmp со словом test:(рис. 21).

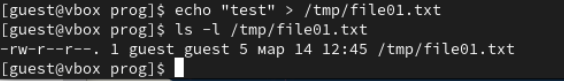


Рис. 21: Создаем файл file01.txt

1. Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные»:(рис. 22).

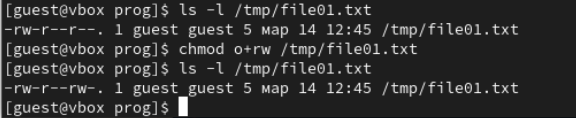


Рис. 22: Просматриваем все атрибуты

1. От пользователя guest2 (не являющегося владельцем) попробуйте прочитать файл /tmp/file01.txt:(рис. 23).

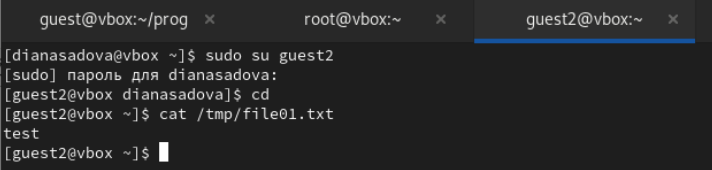


Рис. 23: Пробуем читать файл от guest2

1. От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 командой(рис. 24).

Пробуем чтото дописать в файл

Рис. 24: Пробуем чтото дописать в файл

Удалось ли вам выполнить операцию?

Нет. Отказано в доступе.

1. Проверьте содержимое файла командой(рис. 25).

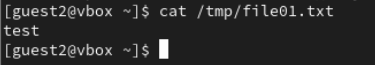


Рис. 25: Проверяем содержимое файла

1. От пользователя guest2 попробуйте записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой(рис. 26).

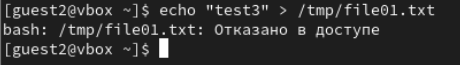


Рис. 26: Пробуем чтото дописать в файл

Удалось ли вам выполнить операцию?

Нет. Отказано в доступе.

1. Проверьте содержимое файла командой(рис. 27).

Проверяем содержимое файла

Рис. 27: Проверяем содержимое файла

1. От пользователя guest2 попробуйте удалить файл /tmp/file01.txt командой(рис. 28).

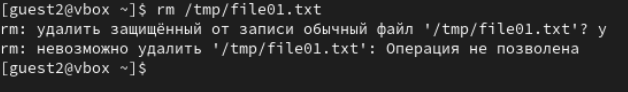


Рис. 28: Пробуем удалить файл

Удалось ли вам удалить файл?

Нет. Отказано в доступе.

1. Повысьте свои права до суперпользователя следующей командой su - и выполните после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp:(рис. 29).

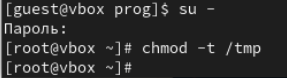


Рис. 29: Переходим в режим суперпользователя и снимаем атрибут

1. Покиньте режим суперпользователя командой(рис. 30).

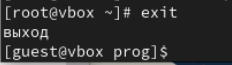


Рис. 30: Выходим из режима суперпользователя

1. От пользователя guest2 проверьте, что атрибута t у директории /tmp нет:(рис. 31).



Рис. 31: Проверяем наличие атрибута t

1. Повторите предыдущие шаги. Какие наблюдаются изменения?(рис. 32).

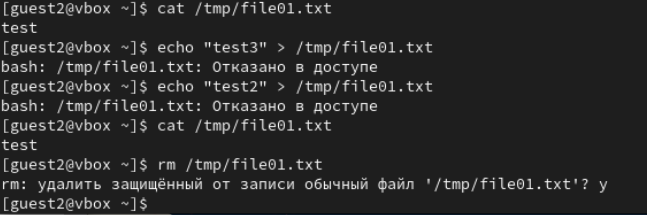


Рис. 32: Повторяем предыдущие шаги

1. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем? Ваши наблюдения занесите в отчёт.

Да, мы смогли удалить файл

1. Повысьте свои права до суперпользователя и верните атрибут t на директорию /tmp:(рис. 33).

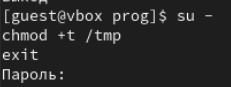


Рис. 33: Возращаем предыдущие шаги

# 3 Выводы

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

Получили практические навыки 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