Информационная безопасность

Лабораторная работа №5

Матюшкин Денис Владимирович (НПИбд-02-21)

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 Теоретическое введение

VirtualBox (Oracle VM VirtualBox) — программный продукт виртуализации для операционных систем Windows, Linux, FreeBSD, macOS, Solaris/OpenSolaris, ReactOS, DOS и других [1].

Rocky Linux — дистрибутив Linux, разработанный Rocky Enterprise Software Foundation. Предполагается, что это будет полный бинарно-совместимый выпуск, использующий исходный код операционной системы Red Hat Enterprise Linux (RHEL) [2].

# 3 Ход работы

## 3.1 Создание программы

1. Войдите в систему от имени пользователя guest.
2. Создайте программу simpleid.c (рис. 1).

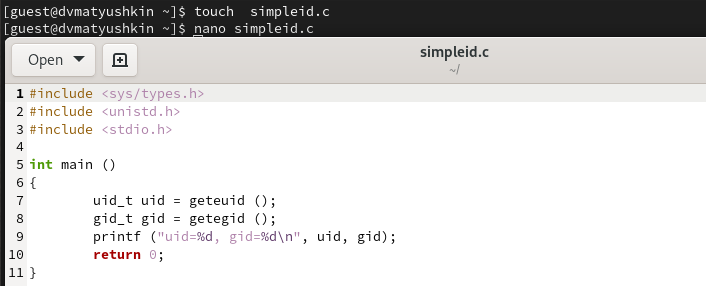


Рис. 1: simpleid.c

1. Скомплилируйте программу и убедитесь, что файл программы создан. Выполните программу simpleid и выполните системную программу id (рис. 2). Полученные результаты совпадают.

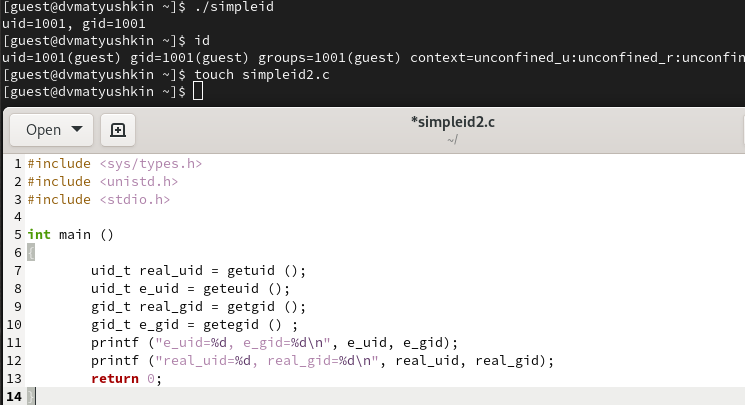


Рис. 2: Выполнение программы simpleid

1. Усложните программу, добавив вывод действительных идентификаторов (рис. 2).
2. Скомпилируйте и запустите simpleid2.c (рис. 3).

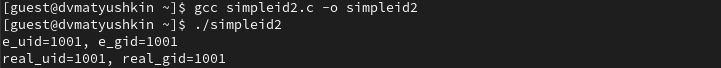


Рис. 3: Выполнение программы simpleid2

1. От имени суперпользователя выполните команды (рис. 4). Эти команды меняют владельца файла и устанавливают SetUID бит.

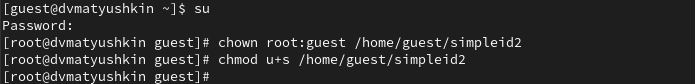


Рис. 4: Выполнение команд

1. Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2. Запустите simpleid2 и id (рис. 5).

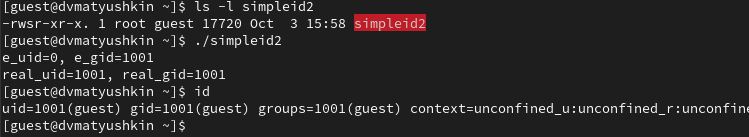


Рис. 5: Проверка атрибутов и запуск программы

1. Проделайте тоже самое относительно SetGID-бита (рис. 6 и 7).

Рис. 6: Установка SetGID-бита

Рис. 6: Установка SetGID-бита

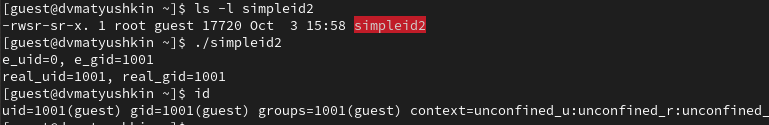


Рис. 7: Проверка атрибутов и запуск программы

1. Создайте программу readfile.c. Откомпилируйте её (рис. 8).

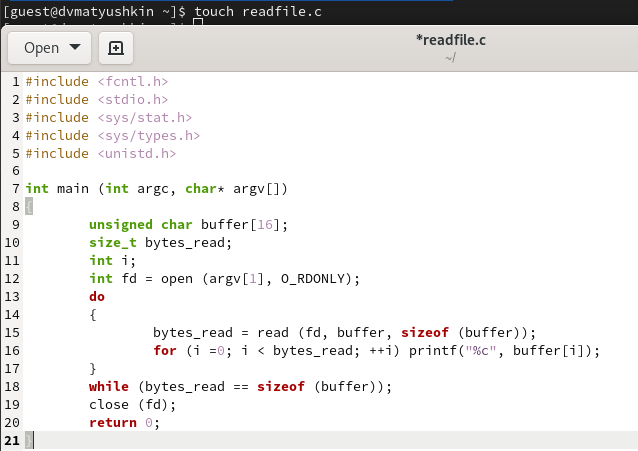


Рис. 8: readfile.c

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. 9).

Рис. 9: Смена владельца и установка SetUID

Рис. 9: Смена владельца и установка SetUID

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

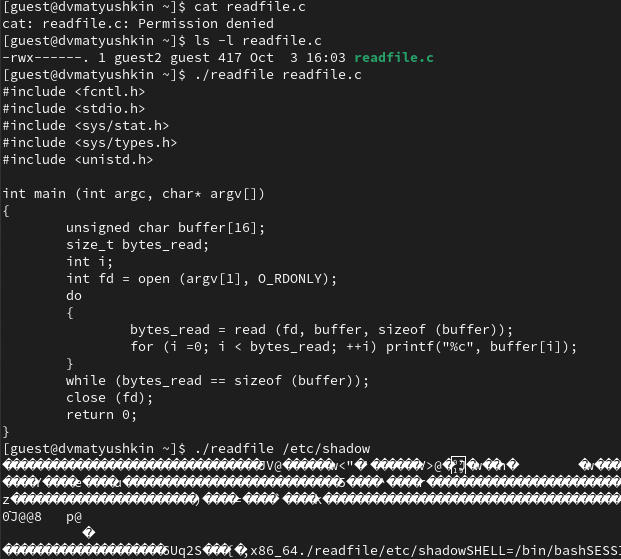


Рис. 10: Проверка

1. Смените у программы readfile владельца и установите SetUID-бит (рис. 9).
2. Проверьте, может ли программа readfile прочитать файл readfile.c (рис. 10).
3. Проверьте, может ли программа readfile прочитать файл /etc/shadow (рис. 10).

Команды выполняются, т.к. Setuid – это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.

## 3.2 Исследование Sticky-бита

1. Выясните, установлен ли атрибут Sticky на директории /tmp (рис. 11).
2. От имени пользователя guest создайте файл file01.txt в директории /tmp со словом test (рис. 11).
3. Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные» (рис. 11).

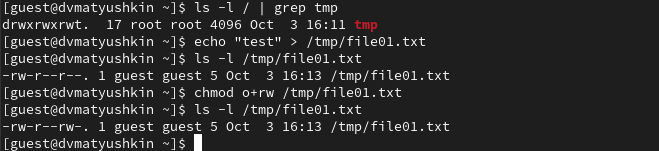


Рис. 11: Работа в директории /tmp

1. От пользователя guest2 (не являющегося владельцем) попробуйте прочитать файл /tmp/file01.txt (рис. 12).
2. От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 (рис. 12).
3. Проверьте содержимое файла командой (рис. 12).
4. От пользователя guest2 попробуйте записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию (рис. 12).
5. Проверьте содержимое файла командой (рис. 12).
6. От пользователя guest2 попробуйте удалить файл /tmp/file01.txt (рис. 12).

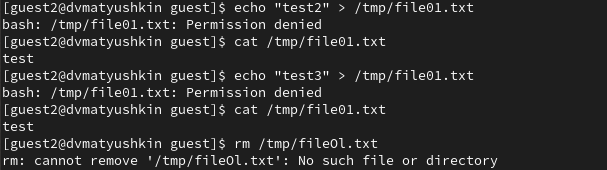


Рис. 12: Работа с файлом file01.txt

Удалить файл нам не получилось.

1. Повысьте свои права до суперпользователя и выполните после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp. После покиньте режим суперпользователя (рис. 13).

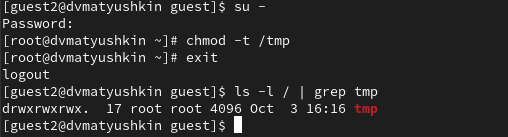


Рис. 13: Снятие Sticky-бит с директории /tmp

1. От пользователя guest2 проверьте, что атрибута t у директории /tmp нет (рис. 13).
2. Повторите предыдущие шаги. Теперь можем все то же самое, но еще и удалять файл (рис. 14).

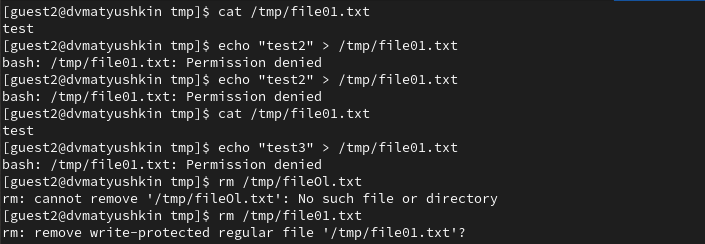


Рис. 14: Повторение действий с file01.txt

1. Повысьте свои права до суперпользователя и верните атрибут t на директорию /tmp (рис. 15).



Рис. 15: Возвращение Sticky-бит в директорию /tmp

# 4 Выводы

В ходе данной лабораторной работы мы изучили механизм изменения идентификаторов, применение 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

1. VirtualBox Documentation [Электронный ресурс]. Oracle, 2024. URL: <https://www.virtualbox.org/wiki/Documentation>.

2. Rocky Documentation [Электронный ресурс]. Rocky Enterprise Software Foundation, 2024. URL: <https://docs.rockylinux.org/ru/>.