Отчёт по лабораторной работе №5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

дисциплина: Информационная безопасность

Рыбалко Элина Павловна

Содержание

# Цель работы

Изучить механизмы 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.

# Техническое обеспечение

Лабораторная работа подразумевает наличие на виртуальной машине VirtualBox операционной системы Linux (дистрибутив Rocky или CentOS). Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (http://www.gentoo.ru/); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: /afs/dk.sci.pfu.edu.ru/common/files/iso/.

# Объект/Предмет исследования

Операционная система Linux и расширенные атрибуты.

# Теоретическое введение

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

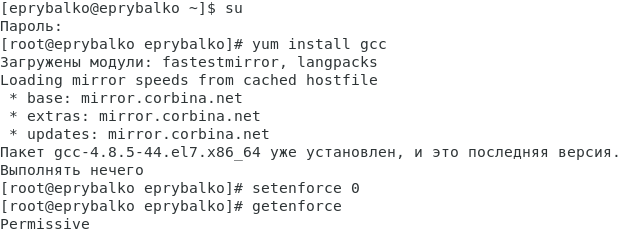
Один из подходов к разграничению доступа — так называемый дискреционный (от англ, discretion — чье-либо усмотрение) — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. [[2]](#список-литературы).

# Выполнение лабораторной работы

## 1. Подготовка лабораторного стенда

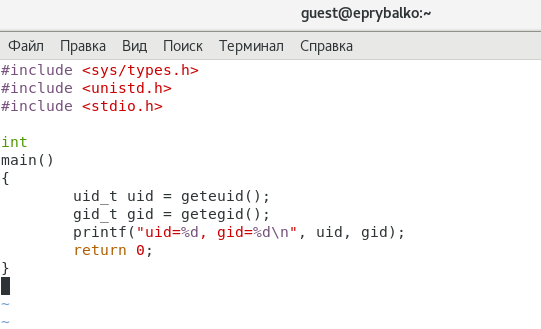
1. Убедиться, что в системе установлен компилятор gcc (см. рис. -@fig:001).
2. Отключите систему запретов до очередной перезагрузки системы командой setenforce 0. После этого команда getenforce должна выводить Permissive (см. рис. -@fig:001).



Подготовка лабораторного стенда

## 2. Создание программы

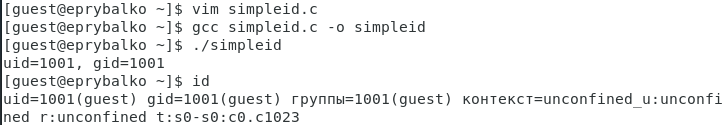
1. Войдите в систему от имени пользователя guest (см. рис. -@fig:002).
2. Создайте программу simpleid.c (см. рис. -@fig:002).



Создание программы simpleid.c

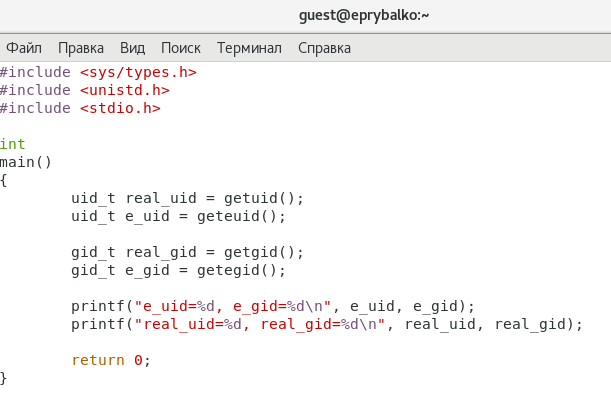
1. Скомплилируйте программу и убедитесь, что файл программы создан: gcc simpleid.c -o simpleid (см. рис. -@fig:003).
2. Выполните программу simpleid: ./simpleid (см. рис. -@fig:003).
3. Выполните системную программу id: id и сравните полученный вами результат с данными предыдущего пункта задания (см. рис. -@fig:003).

Результаты совпадают.



Компиляция программы simpleid.c

1. Усложните программу, добавив вывод действительных идентификаторов. Получившуюся программу назовите simpleid2.c (см. рис. -@fig:004 и рис. -@fig:005).



Создание программы simpleid2.c

Создание программы simpleid2.c

Создание программы simpleid2.c

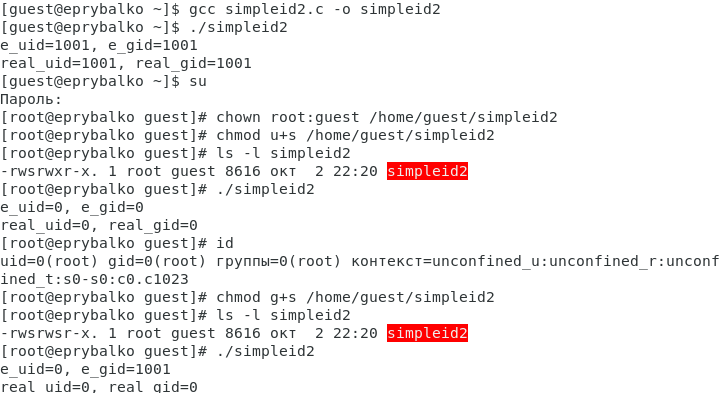
1. Скомпилируйте и запустите simpleid2.c (см. рис. -@fig:006).
2. От имени суперпользователя выполните команды (см. рис. -@fig:006).
3. Используйте sudo или повысьте временно свои права с помощью su (см. рис. -@fig:006).

Первая команда меняет владельца файла simpleid2 на группу guest. Вторая команда меняет права доступа к файлу simpleid2 для пользователя и установленные атрибуты SUID или SGID позволяют запускать файл на выполнение с правами владельца файла или группы соответственно.

1. Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2 (см. рис. -@fig:006).
2. Запустите simpleid2 и id (см. рис. -@fig:006).

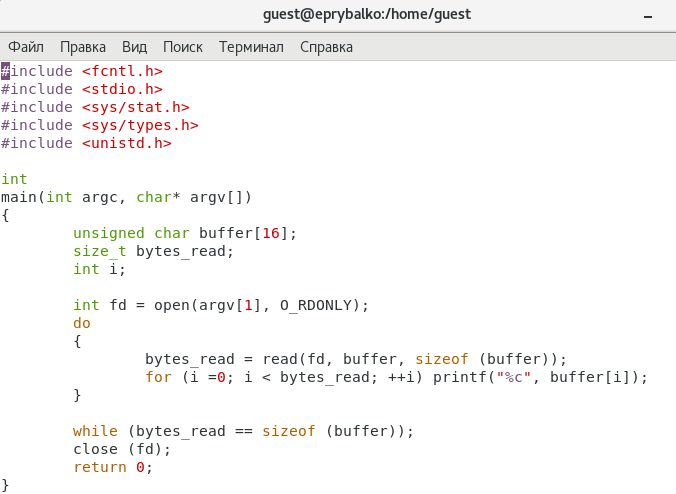
Результаты совпадают.

1. Проделайте тоже самое относительно SetGID-бита (см. рис. -@fig:006).



Компиляция simpleid2.c и изменение прав

1. Создайте программу readfile.c (см. рис. -@fig:007).



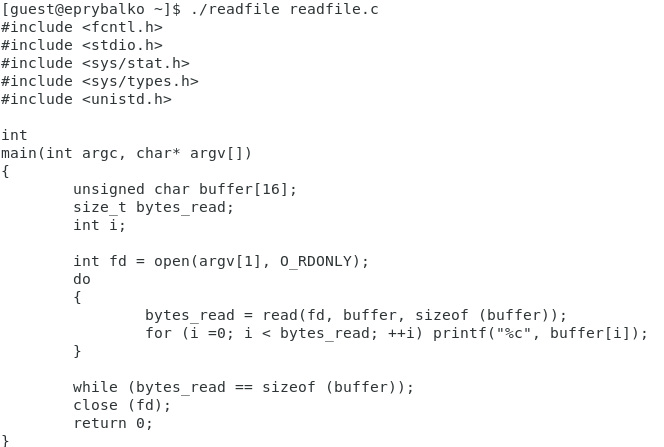
Создание программы readfile.c

1. Откомпилируйте её (см. рис. -@fig:008).
2. 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 (см. рис. -@fig:008).
3. Проверьте, что пользователь guest не может прочитать файл readfile.c (см. рис. -@fig:008).
4. Смените у программы readfile владельца и установите SetU’D-бит (см. рис. -@fig:008).



Компиляция readfile.c и изменение прав

1. Проверьте, может ли программа readfile прочитать файл readfile.c (см. рис. -@fig:009).



Проверка чтения файла readfile.c

1. Проверьте, может ли программа readfile прочитать файл /etc/shadow (см. рис. -@fig:010).

Программа может прочитать файлы.



Проверка чтения файла /etc/shadow

## 3. Исследование Sticky-бита

1. Выясните, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду ls -l / | grep tmp (см. рис. -@fig:011).
2. От имени пользователя guest создайте файл file01.txt в директории /tmp со словом test (см. рис. -@fig:011).
3. Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные» (см. рис. -@fig:011).
4. От пользователя guest2 (не являющегося владельцем) попробуйте прочитать файл /tmp/file01.txt (см. рис. -@fig:011).
5. От пользователя guest2 попробуйте дозаписать в файл (см. рис. -@fig:011).

Выполнить операцию удалось.

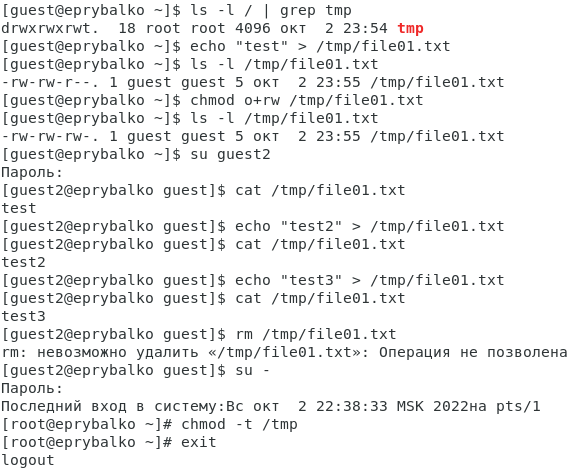
1. Проверьте содержимое файла командой cat /tmp/file01.txt (см. рис. -@fig:011).
2. От пользователя guest2 попробуйте записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой echo “test3” > /tmp/file01.txt (см. рис. -@fig:011).

Выполнить операцию удалось.

1. Проверьте содержимое файла командой cat /tmp/file01.txt (см. рис. -@fig:011).
2. От пользователя guest2 попробуйте удалить файл /tmp/file01.txt командой rm /tmp/fileOl.txt (см. рис. -@fig:011).

Выполнить операцию не удалось.

1. Повысьте свои права до суперпользователя следующей командой su и выполните после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp (см. рис. -@fig:011).
2. Покиньте режим суперпользователя командой exit (см. рис. -@fig:011).



Чтение и запись файла с атрибутом Sticky-бит

1. От пользователя guest2 проверьте, что атрибута t у директории /tmp нет (см. рис. -@fig:012).
2. Повторите предыдущие шаги (см. рис. -@fig:012).

Удалось перезаписать файл и также удалить его.

1. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем? (см. рис. -@fig:012).

Выполнить операцию удалось.

1. Повысьте свои права до суперпользователя и верните атрибут t на директорию /tmp (см. рис. -@fig:012).



Чтение и запись файла без атрибута Sticky-бит

# Вывод

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

# Список литературы

1. [Лабораторная работа №5](https://docs.yandex.ru/docs/view?tm=1664733659&tld=ru&lang=ru&name=005-lab_discret_sticky.pdf&text=Лабораторная%20работа%20№%205.%20Дискреционное%20разграничение%20прав%20в%20Linux.%20Исследование%20влияния%20дополнительных%20атрибутов%205.1.%20Цель%20работы%20Изучение%20механизмов%20изменения%20идентификаторов%2C%20применения%20SetUID-%20и%20Sticky-битов.%20Получение%20практических%20навыков%20работы%20в%20консоли%20с%20дополнительными%20атрибутами.%20Рассмотрение%20работы%20механизма%20смены%20идентификатора%20процессов%20пользователей%2C%20а%20также%20влияние%20бита%20Sticky%20на%20зап&url=https%3A%2F%2Fstud-sci.rudn.ru%2Fpluginfile.php%2F8543%2Fmod_resource%2Fcontent%2F2%2F005-lab_discret_sticky.pdf&lr=213&mime=pdf&l10n=ru&sign=f43a062c6ea217358bc63468bfe94d93&keyno=0&serpParams=tm%3D1664733659%26tld%3Dru%26lang%3Dru%26name%3D005-lab_discret_sticky.pdf%26text%3D%25D0%259B%25D0%25B0%25D0%25B1%25D0%25BE%25D1%2580%25D0%25B0%25D1%2582%25D0%25BE%25D1%2580%25D0%25BD%25D0%25B0%25D1%258F%2B%25D1%2580%25D0%25B0%25D0%25B1%25D0%25BE%25D1%2582%25D0%25B0%2B%25E2%2584%2596%2B5.%2B%25D0%2594%25D0%25B8%25D1%2581%25D0%25BA%25D1%2580%25D0%25B5%25D1%2586%25D0%25B8%25D0%25BE%25D0%25BD%25D0%25BD%25D0%25BE%25D0%25B5%2B%25D1%2580%25D0%25B0%25D0%25B7%25D0%25B3%25D1%2580%25D0%25B0%25D0%25BD%25D0%25B8%25D1%2587%25D0%25B5%25D0%25BD%25D0%25B8%25D0%25B5%2B%25D0%25BF%25D1%2580%25D0%25B0%25D0%25B2%2B%25D0%25B2%2BLinux.%2B%25D0%2598%25D1%2581%25D1%2581%25D0%25BB%25D0%25B5%25D0%25B4%25D0%25BE%25D0%25B2%25D0%25B0%25D0%25BD%25D0%25B8%25D0%25B5%2B%25D0%25B2%25D0%25BB%25D0%25B8%25D1%258F%25D0%25BD%25D0%25B8%25D1%258F%2B%25D0%25B4%25D0%25BE%25D0%25BF%25D0%25BE%25D0%25BB%25D0%25BD%25D0%25B8%25D1%2582%25D0%25B5%25D0%25BB%25D1%258C%25D0%25BD%25D1%258B%25D1%2585%2B%25D0%25B0%25D1%2582%25D1%2580%25D0%25B8%25D0%25B1%25D1%2583%25D1%2582%25D0%25BE%25D0%25B2%2B5.1.%2B%25D0%25A6%25D0%25B5%25D0%25BB%25D1%258C%2B%25D1%2580%25D0%25B0%25D0%25B1%25D0%25BE%25D1%2582%25D1%258B%2B%25D0%2598%25D0%25B7%25D1%2583%25D1%2587%25D0%25B5%25D0%25BD%25D0%25B8%25D0%25B5%2B%25D0%25BC%25D0%25B5%25D1%2585%25D0%25B0%25D0%25BD%25D0%25B8%25D0%25B7%25D0%25BC%25D0%25BE%25D0%25B2%2B%25D0%25B8%25D0%25B7%25D0%25BC%25D0%25B5%25D0%25BD%25D0%25B5%25D0%25BD%25D0%25B8%25D1%258F%2B%25D0%25B8%25D0%25B4%25D0%25B5%25D0%25BD%25D1%2582%25D0%25B8%25D1%2584%25D0%25B8%25D0%25BA%25D0%25B0%25D1%2582%25D0%25BE%25D1%2580%25D0%25BE%25D0%25B2%252C%2B%25D0%25BF%25D1%2580%25D0%25B8%25D0%25BC%25D0%25B5%25D0%25BD%25D0%25B5%25D0%25BD%25D0%25B8%25D1%258F%2BSetUID-%2B%25D0%25B8%2BSticky-%25D0%25B1%25D0%25B8%25D1%2582%25D0%25BE%25D0%25B2.%2B%25D0%259F%25D0%25BE%25D0%25BB%25D1%2583%25D1%2587%25D0%25B5%25D0%25BD%25D0%25B8%25D0%25B5%2B%25D0%25BF%25D1%2580%25D0%25B0%25D0%25BA%25D1%2582%25D0%25B8%25D1%2587%25D0%25B5%25D1%2581%25D0%25BA%25D0%25B8%25D1%2585%2B%25D0%25BD%25D0%25B0%25D0%25B2%25D1%258B%25D0%25BA%25D0%25BE%25D0%25B2%2B%25D1%2580%25D0%25B0%25D0%25B1%25D0%25BE%25D1%2582%25D1%258B%2B%25D0%25B2%2B%25D0%25BA%25D0%25BE%25D0%25BD%25D1%2581%25D0%25BE%25D0%25BB%25D0%25B8%2B%25D1%2581%2B%25D0%25B4%25D0%25BE%25D0%25BF%25D0%25BE%25D0%25BB%25D0%25BD%25D0%25B8%25D1%2582%25D0%25B5%25D0%25BB%25D1%258C%25D0%25BD%25D1%258B%25D0%25BC%25D0%25B8%2B%25D0%25B0%25D1%2582%25D1%2580%25D0%25B8%25D0%25B1%25D1%2583%25D1%2582%25D0%25B0%25D0%25BC%25D0%25B8.%2B%25D0%25A0%25D0%25B0%25D1%2581%25D1%2581%25D0%25BC%25D0%25BE%25D1%2582%25D1%2580%25D0%25B5%25D0%25BD%25D0%25B8%25D0%25B5%2B%25D1%2580%25D0%25B0%25D0%25B1%25D0%25BE%25D1%2582%25D1%258B%2B%25D0%25BC%25D0%25B5%25D1%2585%25D0%25B0%25D0%25BD%25D0%25B8%25D0%25B7%25D0%25BC%25D0%25B0%2B%25D1%2581%25D0%25BC%25D0%25B5%25D0%25BD%25D1%258B%2B%25D0%25B8%25D0%25B4%25D0%25B5%25D0%25BD%25D1%2582%25D0%25B8%25D1%2584%25D0%25B8%25D0%25BA%25D0%25B0%25D1%2582%25D0%25BE%25D1%2580%25D0%25B0%2B%25D0%25BF%25D1%2580%25D0%25BE%25D1%2586%25D0%25B5%25D1%2581%25D1%2581%25D0%25BE%25D0%25B2%2B%25D0%25BF%25D0%25BE%25D0%25BB%25D1%258C%25D0%25B7%25D0%25BE%25D0%25B2%25D0%25B0%25D1%2582%25D0%25B5%25D0%25BB%25D0%25B5%25D0%25B9%252C%2B%25D0%25B0%2B%25D1%2582%25D0%25B0%25D0%25BA%25D0%25B6%25D0%25B5%2B%25D0%25B2%25D0%25BB%25D0%25B8%25D1%258F%25D0%25BD%25D0%25B8%25D0%25B5%2B%25D0%25B1%25D0%25B8%25D1%2582%25D0%25B0%2BSticky%2B%25D0%25BD%25D0%25B0%2B%25D0%25B7%25D0%25B0%25D0%25BF%26url%3Dhttps%253A%2F%2Fstud-sci.rudn.ru%2Fpluginfile.php%2F8543%2Fmod_resource%2Fcontent%2F2%2F005-lab_discret_sticky.pdf%26lr%3D213%26mime%3Dpdf%26l10n%3Dru%26sign%3Df43a062c6ea217358bc63468bfe94d93%26keyno%3D0)
2. [Дискреционное разграничение доступа Linux](https://debianinstall.ru/diskretsionnoe-razgranichenie-dostupa-linux/)
3. [Руководство по формуле Cmd Markdown](https://russianblogs.com/article/26051452570/)
4. [Руководство по оформлению Markdown файлов](https://gist.github.com/Jekins/2bf2d0638163f1294637)