Отчет по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Бурдина Ксения Павловна

2022 Oct 5th

Содержание

# 1 Цель работы

Целью данной работы является 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.

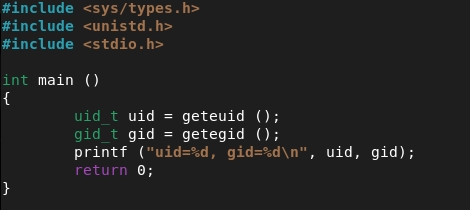
# 2 Ход выполнение лабораторной работы

## 2.1 Создание программы

1. Войдем в систему от имени пользователя guest
2. Создадим программу simpleid.c:

Создание программы simpleid.c

Создание программы simpleid.c



Листинг программы simpleid.c

1. Скомпилируем программу и убедимся, что файл программы создан:

Компиляция файла simpleid.c

Компиляция файла simpleid.c

1. Выполним программу simpleid:

Выполнение программы simpleid

Выполнение программы simpleid

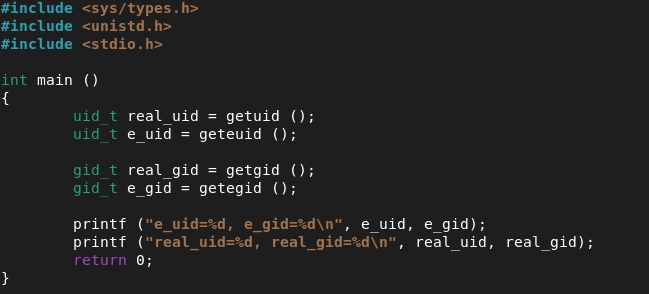
1. Выполним системную программу id:

Выполнение системной программы id

Выполнение системной программы id

Видим, что выводимые данные совпадают с данными из прошлого пункта.

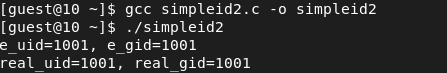
1. Усложним программу, добавив вывод действительных идентификаторов:



Листинг усложненной программы

Получившуюся пргограмму назовем simpleid2.c.

1. Скомпилируем и запустим simpleid2.c:



Компиляция и запуск simpleid2.c

1. От имени суперпользователя выполним команды:

Выполнение команд от имени суперпользователя

Выполнение команд от имени суперпользователя

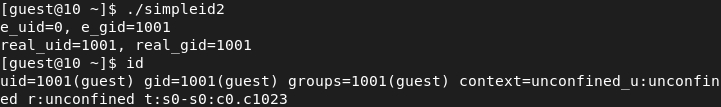
1. Для перехода в режим суперпользователя мы выполнили команду su. Если говорить про команду sudo, то ее следует использовать перед каждой командой, если работа производится от имени обычного пользователя, а команды возможны к выполнению только суперпользователем.
2. Выполним проверку правильности установки новых атрибутов и смены владельца файла simpleid2:

Проверка установки атбирутов и смены владельца simpleid2

Проверка установки атбирутов и смены владельца simpleid2

Видим, что владельцем файла указан root и у пользователя выставлен атрибут s.

1. Запустим simpleid2 и id:



Запуск simpleid2 и id

Видим, что у нас при запуске программы выводятся значения e\_uid, e\_gid, real\_uid и real\_gid, которые мы прописали в коде, а при просмотре информации выводятся действительные значения uid и gid.

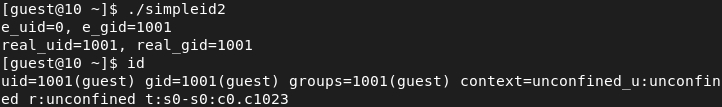
1. Проделаем то же самое относительно SetGID-бита [[1]](https://esystem.rudn.ru/pluginfile.php/1651889/mod_resource/content/2/005-lab_discret_sticky.pdf):

Изменение атрибутов файла для группы пользователей

Изменение атрибутов файла для группы пользователей

Проверка изменения атрибутов

Проверка изменения атрибутов

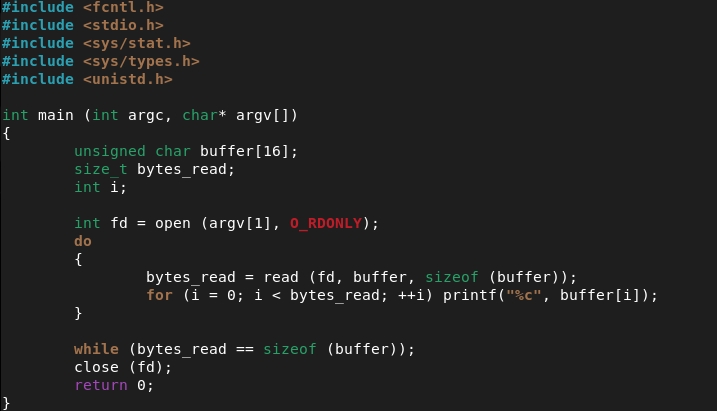


Запуск программы и id

1. Создадим программу readfile.c:

Создание программы readfile.c

Создание программы readfile.c



Листинг программы readfile.c

1. Откомпилируем программу readfile.c:

Компиляция программы readfile.c

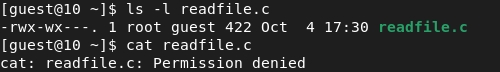
Компиляция программы readfile.c

1. Сменим владельца файла readfile.c и изменим права так, чтоб только суперпользователь мог прочитать его, а guest нет:

Изменение владельца и атрибутов файла readfile.c

Изменение владельца и атрибутов файла readfile.c

1. Проверим, что пользователь guest не может прочитать файл readfile.c:



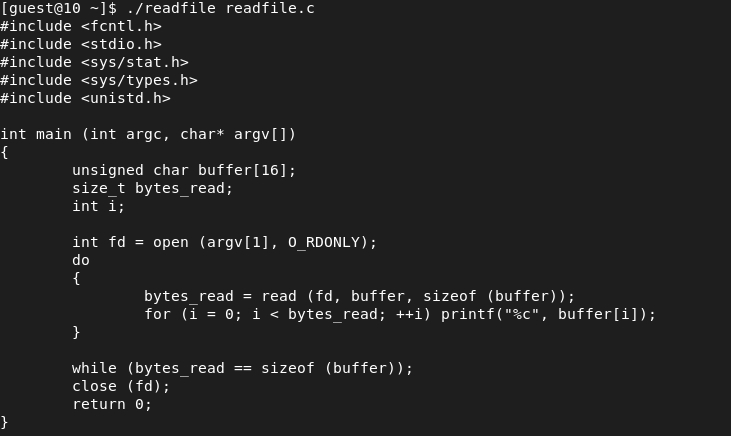
Проверка невозможности чтения файла readfile.c

1. Сменим у программы readfile владельца и установим SetUID-бит:

Смена владельца readfile и установка SetUID-бита

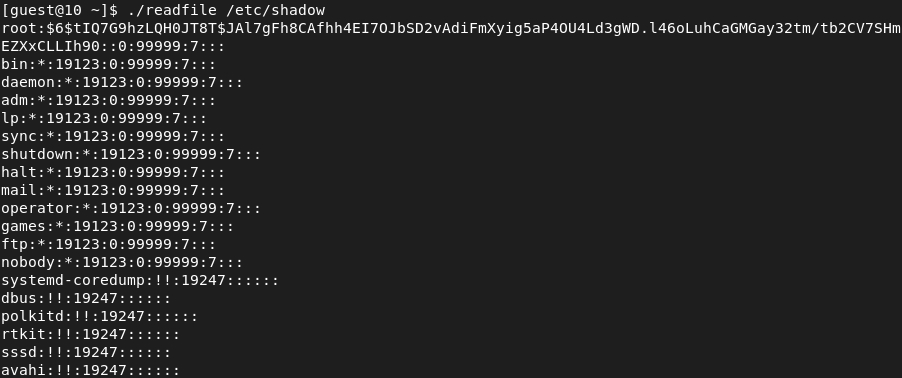
Смена владельца readfile и установка SetUID-бита

1. Проверим, что программа может прочитать файл readfile:



Проверка возможности чтения файла readfile

1. Проверим, что программа readfile может прочитать файл /etc/shadow:



Чтение файла /etc/shadow

Можем заметить, что SetUID-бит позволяет пользователю запускать исполняемый файл с правами владельца этого файла.

## 2.2 Исследование Sticky-бита

1. Выясним, установлен ли атрибут Sticky на директории /tmp:

Проверка установки атрибута Sticky

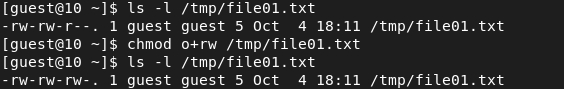
Проверка установки атрибута Sticky

1. От имени пользователя guest создадим файл file01.txt в директории /tmp со словом test:

Создание файла file01.txt

Создание файла file01.txt

1. Просмотрим атрибуты у только что созданного файла и расширим чтение и запись для категории пользователей “все остальные”:



Просмотр и изменение атрибутов файла file01.txt

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

Попытка чтения файла от имени guest2

Попытка чтения файла от имени guest2

1. От пользователя guest2 попробуем дозаписать в файл /tmp/file01.txt слово test2:

Дозапись в файл слова test2

Дозапись в файл слова test2

1. Проверим содержимое файла file01.txt:

Проверка содержимого файла

Проверка содержимого файла

1. От пользователя guest2 попробуем записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию:

Запись в файл слова test3

Запись в файл слова test3

1. Проверим содержимое файла:

Проверка содержимого файла

Проверка содержимого файла

1. От пользователя guest2 попробуем удалить файл /tmp/file01.txt:

Попытка удаления файла

Попытка удаления файла

Мы получили отказ в выполнении действия.

1. Повысим свои права до суперпользователя командой su - и выполним после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp:

Снятие атрибута t с директории /tmp

Снятие атрибута t с директории /tmp

1. Покинем режим суперпользователя:

Покидание режима суперпользователя

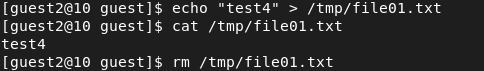
Покидание режима суперпользователя

1. От пользователя guest2 проверим, что атрибута t у директории /tmp нет:

Проверка отсутствия атрибута t

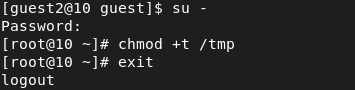
Проверка отсутствия атрибута t

1. Повторим предыдущие шаги:



Выполнение команд со снятым атрибутом t

1. Видим, что теперь мы можем удалить файл file01.txt. Суть в том, что атрибут t как Sticky-бит устанавливает такие права, что файл с данным битом может удалить только тот пользователь, который является владельцем файла [[2]](https://zalinux.ru/?p=6440).
2. Повысим свои права до суперпользователя и вернем атрибут t на директорию /tmp:



Возврат атрибута t на директорию

# 3 Выводы

В ходе работы мы 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.

# 4 Список литературы

1. Методические материалы курса [[1]](https://esystem.rudn.ru/pluginfile.php/1651889/mod_resource/content/2/005-lab_discret_sticky.pdf)
2. Электронный источник “Атрибуты файлов в Linux” [[2]](https://zalinux.ru/?p=6440)