Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Азарцова Полина Валерьевна

Содержание

[Цель работы 1](#_Toc87714782)

[Задание 1](#_Toc87714783)

[Выполнение лабораторной работы 1](#_Toc87714784)

[Выводы 9](#_Toc87714785)

[Список литературы 9](#_Toc87714786)

# Цель работы

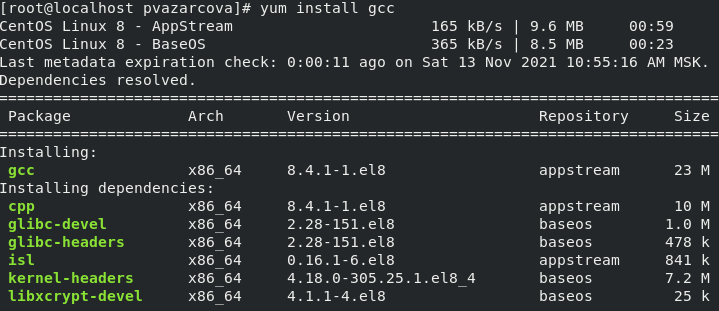
Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Задание

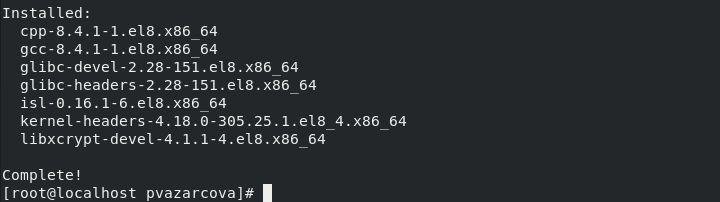
1. Подготовить к выполнению лабораторной необходимые средства разработки.
2. По порядку выполнить все пункты из раздела “создание программы”.
3. По порядку выполнить все пункты из раздела “исследование Sticky-бита”.

# Выполнение лабораторной работы

1.1 Установила компилятор gcc с помощью команды ‘yum install gcc’. (рис - @fig:001, рис - @fig:002).



Установка gcc



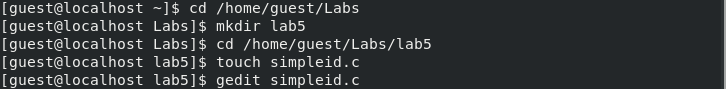
Удачное зашершение установки gcc

1.2 Отключила систему защиты SELinux на текущую сессию командой ‘setenforce 0’. Проверила выполнение командой ‘getenforce’, которая вывела Permissive (рис -@fig:003).

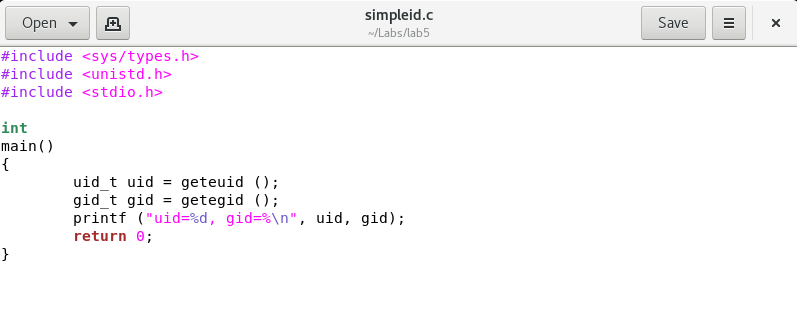
Отключение SELinux

Отключение SELinux

2.1 Вошла в систему от имени пользователя guest, создала программу simpleid.c и папку лабораторной с помощью команд ‘touch’ и ‘mkdir’. (рис -@fig:004, рис -@fig:005).



Создание программы simpleid.c



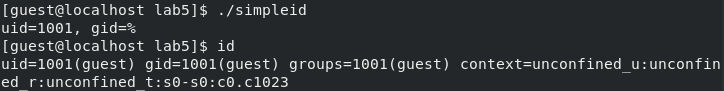
Код программы simpleid.c

2.2 Скомпилировала программу и убедилась, что файл программы создан с помощью программы ‘gcc simpleid.c -o simpleid’. (рис -@fig:006)

Компиляция программы

Компиляция программы

2.3 Выполнила программу simpleid с помощью ‘./simpleid’ и системную программу ‘id’ и сравнила полученный результат (рис. -@fig:007)



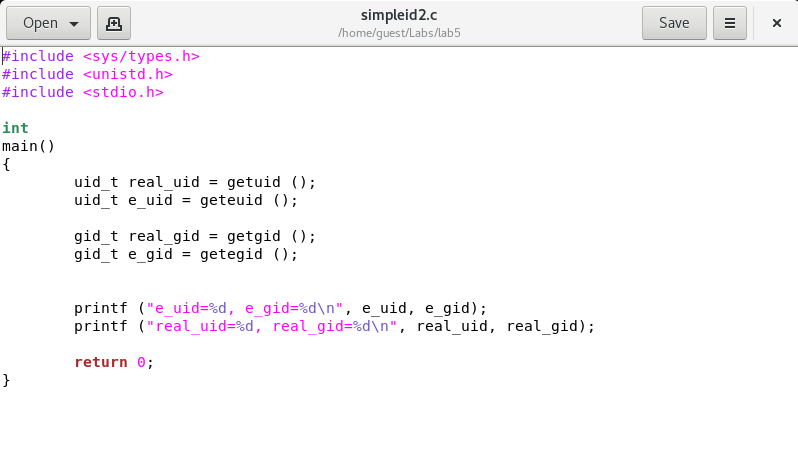
Сравнение ‘./simpleid’ и ‘id’

Полученные значения id совпадают.

2.4 Усложнила программу, добавив вывод действительных идентификаторов, назвала программу simpleid2. (рис -@fig:008, рис -@fig:009).

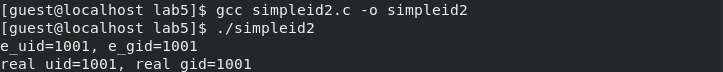
Создание программы

Создание программы



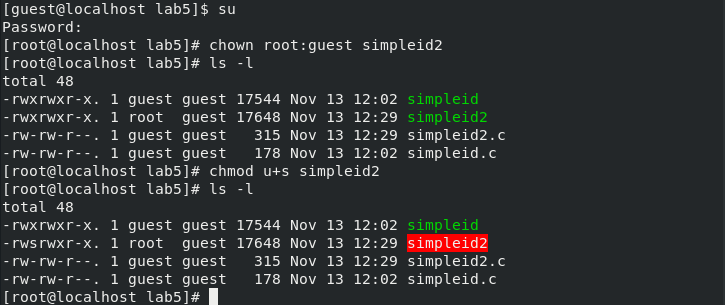
Усложненный код программы

2.5 Скомпилировала и запустила программу simpleid2. (рис. -@fig:010)



Компиляция и запуск simpleid2

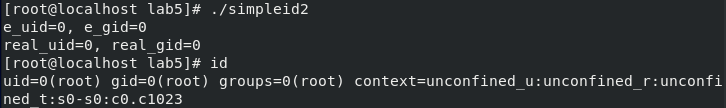
2.6 От имени суперпользователя выполнила команды: ‘chown root:guest /home/guest/simpleid2’ и ‘chmod u+s /home/guest/simpleid2’, а также выполнила проверку изменений с помощью команды ‘ls -l simpleid2’. (рис. -@fig:011)



Смена владельца и установка SetUID

Первая команда изменяет права на файл с guest на root. А затем устанавливает атрибут SetUID.

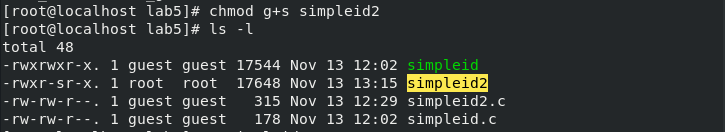
2.7 Запустила simpleid2 и id, сравнила полученные результаты. (рис. -@fig:012)



Сравнение ‘./simpleid2’ и ‘id’

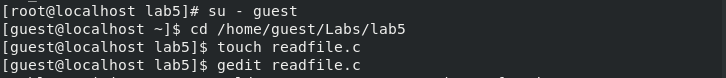
Полученные значения совпадают.

2.8 Проделала то же самое относительно SetGID (установление прав для владеющей группы). (рис -@fig:013)

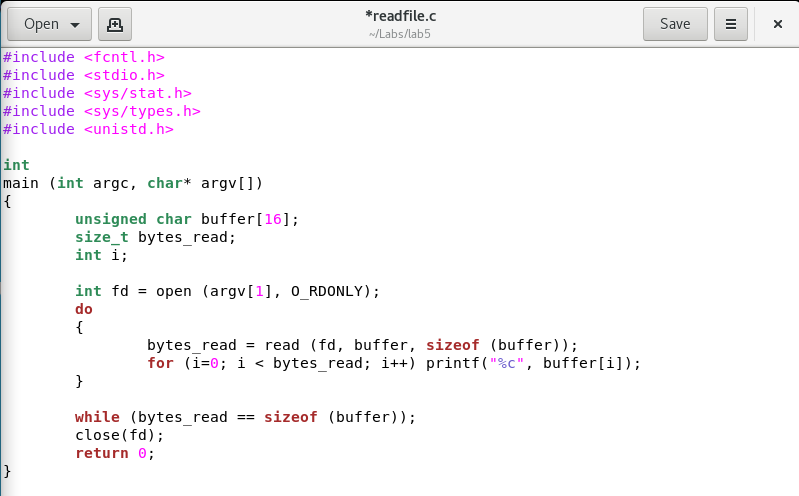


Установка SetGID

2.9 Создала программу readfile.c (рис -@fig:014, рис -@fig:015)



Создание readfile.c



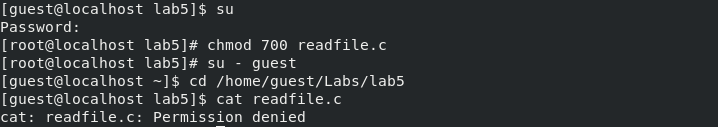
Код программы readfile.c

2.10 Откомпилировала программу readfile.c (рис -@fig:016).

Компиляция программы readfile.c

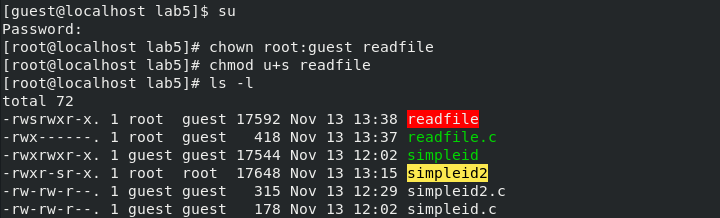
Компиляция программы readfile.c

2.11 Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь мог прочитать его, a guest не мог. Проверила, что пользователь guest не может прочитать файл readfile.c (рис -@fig:017)



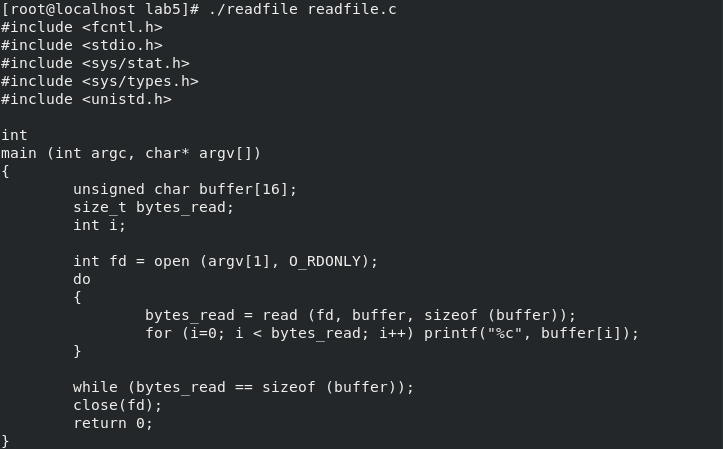
Смена владельца и изменение прав у readfile.c

2.12 Сменила у программы readfile владельца и установила SetUID (рис -@fig:018).



Смена владельца и установка SetUID

2.13 Проверила, может ли программа readfile прочитать файл readfile.c (рис -@fig:019).



Проверка, можел ли прочитать readfile.c

Может.

2.14 Проверила, может ли программа readfile прочитать файл /etc/shadow (рис -@fig:020).

Проверка, можел ли прочитать /etc/shadow

Проверка, можел ли прочитать /etc/shadow

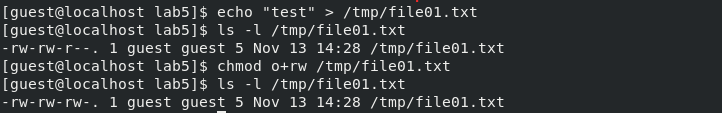
3.1 Выяснила, установлен ли атрибут Sticky на директории /tmp, для чего выполнила команду ‘ls -l / | grep tmp’ (рис -@fig:021).

Ищем атрибут Sticky

Ищем атрибут Sticky

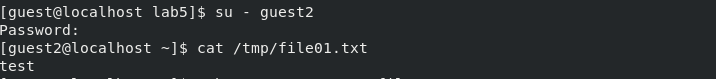
Установлен.

3.2 От имени пользователя guest создала файл file01.txt в директории /tmp со словом test, просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные» (рис -@fig:022).



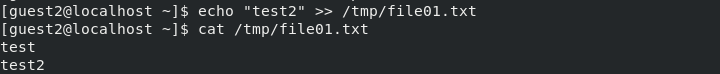
Создание file01.txt и установка на него атрибутов

3.3 От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt с помощью команды ‘cat /tmp/file01.txt’. Действие удалось. (рис -@fig:023).



Чтение файла

3.4 От пользователя guest2 попробовала дозаписать в файл /tmp/file01.txt слово test2 командой ‘echo “test2” >> /tmp/file01.txt’ и проверила содержимое файла командой ‘cat /tmp/file01.txt’. Действие удалось. (рис -@fig:024).



Дозапись в файл

3.5 От пользователя guest2 попробовала записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой ‘echo “test3” > /tmp/file01.txt’. Действие удалось. (рис -@fig:025).

Перезапись файла

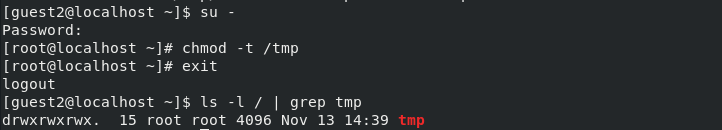
Перезапись файла

3.6 От пользователя guest2 попробовала удалить файл /tmp/file01.txt командой ‘rm /tmp/fileOl.txt’. Действие не удалось. (рис -@fig:026).

Удаление файла

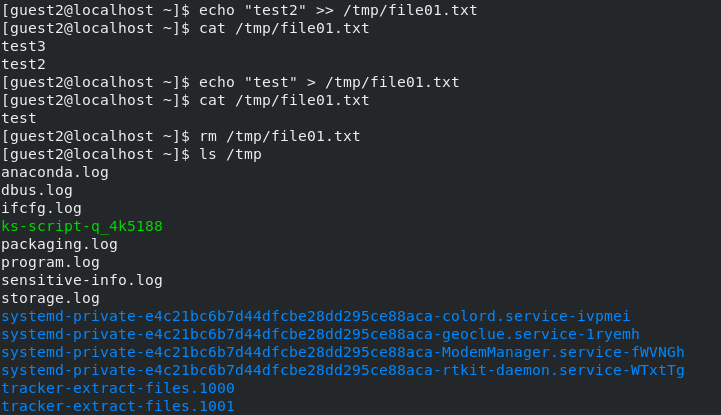
Удаление файла

3.7 Повысила свои права до суперпользователя командой ‘su -’ и выполнила команду ‘chmod -t /tmp’, снимающую атрибут t с директории /tmp. После покинула режим суперпользователя командой ‘exit’ и от пользователя guest2 с помощью команды ‘ls -l / | grep tmp’ проверила, что атрибута t у директории /tmp нет. (рис -@fig:027).



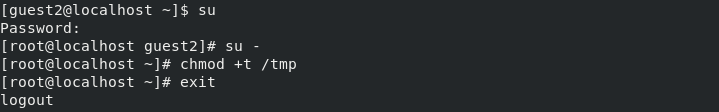
Снятие атрибута t (Sticky-бит)

3.8 Повторила предыдущие шаги: чтение файла, дозапись в файл, перезапись файла, удаление файла. Удалось всё, включая удаление файла от имени пользователя, не являющегося его владельцем (рис -@fig:028).



Повтор предыдущих шагов без атрибута t

3.9 Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp (рис -@fig:029).



Возвращение атрибута t

# Выводы

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

# Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 4. Дискреционное разграничение прав в Linux. Расширенные атрибуты