Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Галиева Аделина Руслановна

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 Выполнение лабораторной работы

1. Для выполнения части заданий требуются средства разработки приложений. Проверяем наличие установленного компилятора gcc -v: компилятор обнаружен.
2. Чтобы система защиты SELinux не мешала выполнению заданий работы, отключили систему запретов до очередной перезагрузки системы командой setenforce 0.
3. Команда getenforce вывела Permissive.

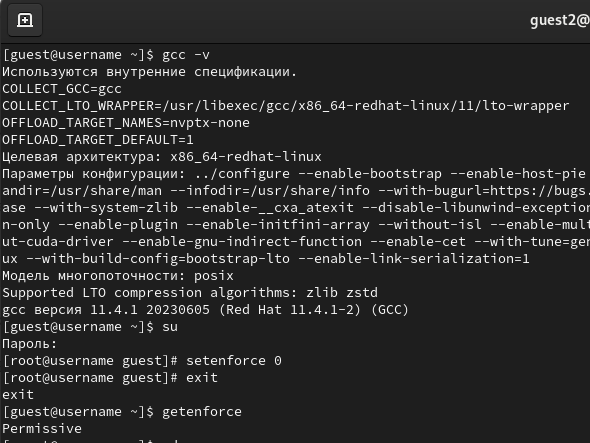


Рис. 1: Подготовка

1. Входим в систему от имени пользователя guest.
2. Создаем команду simpleid.c.



Рис. 2: Программа simpleid.c

1. Компилируем программу и убеждаемся, что файл программы создан.
2. Выполняем программу simpleid.
3. Выполняем системную программу id и gid совпадает в обеих программах.

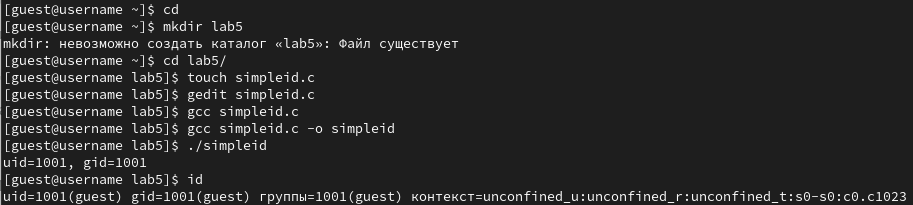


Рис. 3: Результат программы simpleid

1. Усложняем программу, добавив вывод действительных идентификаторов.

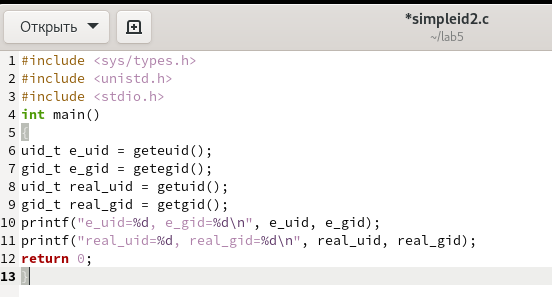


Рис. 4: Программа simpleid2

1. Компилируем и запускаем simpleid2.c.
2. От имени суперпользователя выполняем команды: chown root:guest /home/guest/simpleid2, chmod u+s /home/guest/simpleid2
3. Используем su для повышения прав до суперпользователя.
4. Выполняем проверку правильности установки новых атрибутов и смены владельца файла simpleid2.
5. Запускаем simpleid2 и id. Результат выполнения программ теперь немного отличается.
6. Проделаем тоже самое относительно SetGID-бита.

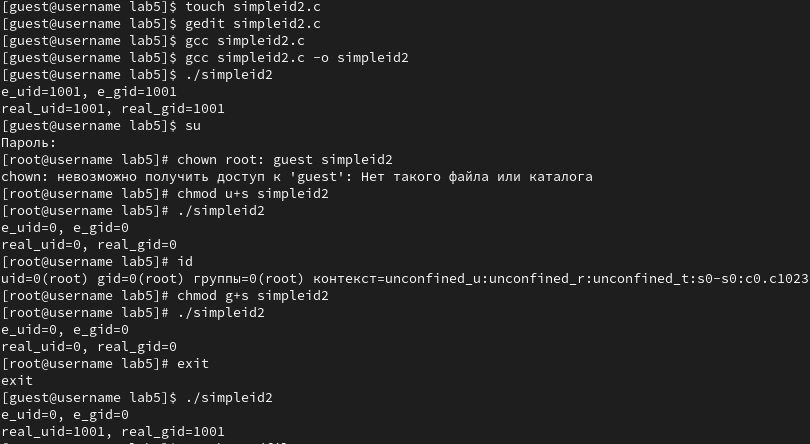


Рис. 5: Результат программы simpleid2

1. Создаем программу readfile.c.

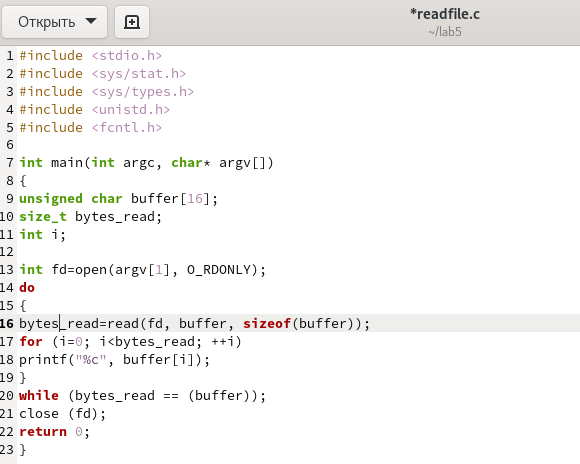


Рис. 6: Программа readfile

1. Откомпилируем её.
2. Сменили владельца у файла readfile.c и меняем права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог.
3. Проверяем, что пользователь guest не может прочитать файл readfile.c.
4. Меняем у программы readfile владельца и установите SetU’D-бит.
5. Проверяем, может ли программа readfile прочитать файл readfile.c.
6. Проверяем, может ли программа readfile прочитать файл /etc/shadow.

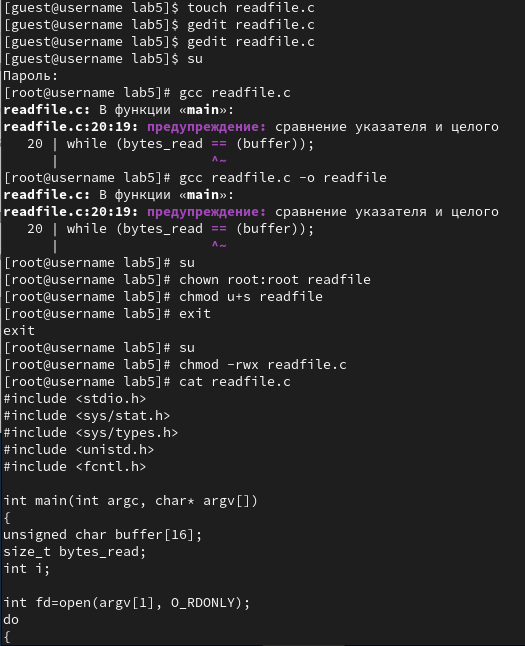


Рис. 7: Результат программы readfile

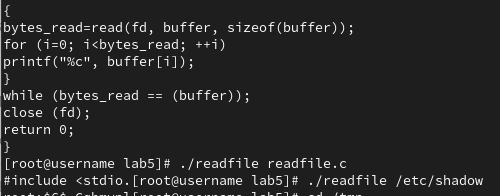


Рис. 8: Результат программы readfile

1. Выясняем, установлен ли атрибут Sticky на директории /tmp.
2. От имени пользователя guest создаем файл file01.txt в директории /tmp со словом test.
3. Просматриваем атрибуты у только что созданного файла и разрешаем чтение и запись для категории пользователей «все остальные». Первоначально все группы имели право на чтение, а запись могли осуществлять все, кроме “остальных пользователей”.
4. От пользователя guest2 (не являющегося владельцем) пробуем прочитать файл /tmp/file01.txt.
5. От пользователя guest2 пробуем дозаписать в файл /tmp/file01.txt слово test2.
6. Проверяем содержимое файла. В файле теперь записано test test2.
7. От пользователя guest2 пробуем записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию.
8. Проверяем содержимое файла командой cat /tmp/file01.txt.
9. От пользователя guest2 пробуем удалить файл /tmp/file01.txt командой rm /tmp/fileOl.txt. Получаем отказ.
10. От суперпользователя проверили, что атрибута t у директории /tmp нет.
11. Повторяем предыдущие шаги. Получилось удалить файл.
12. Удалось удалить файл от имени пользователя, не являющегося его владельцем.
13. Повышаем свои права до суперпользователя и возвращаем атрибут t на директорию /tmp.

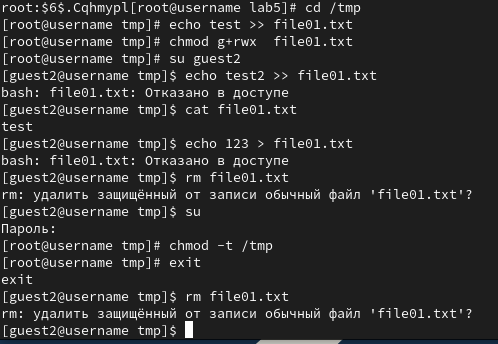


Рис. 9: Исследование Sticky-бит

# 3 Выводы

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