Отчет по лабораторной работе №5

Информационная безопасность

Байрамгельдыев Довлетмурат

Содержание

# 1 Цель работы

* Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов
* Получение практических навыков работы в консоли с дополнительными атрибутами

# 2 Задание

* Написание программ
* Изменение владельца файлов и прав доступа на файлы
* Установка и снятие Sticky-бита и проверка доступных действий

# 3 Теоретическое введение

Setuid –– это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла. Другими словами, использование этого бита позволяет нам поднять привилегии пользователя в случае, если это необходимо. Классический пример использования этого бита в операционной системе это команда sudo.

На месте, где обычно установлен классический бит x (на исполнение), выставлен специальный бит s. Это позволяет обычному пользователю системы выполнять команды с повышенными привилегиями без необходимости входа в систему как root, зная пароль пользователя root.

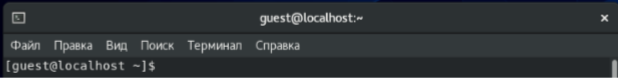
Принцип работы Setgid очень похож на setuid с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

Последний специальный бит разрешения – это Sticky Bit . В случае, если этот бит установлен для папки, то файлы в этой папке могут быть удалены только их владельцем. Пример использования этого бита в операционной системе это системная папка /tmp . Эта папка разрешена на запись любому пользователю, но удалять файлы в ней могут только пользователи, являющиеся владельцами этих файлов.

Более подробно о см. в [**lab-theory?**,**ruvds?**].

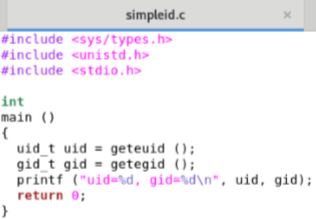
# 4 Выполнение лабораторной работы

В качестве первого шага лабораторной работы осуществил вход от лица пользователя guest и создал файл simpleid.c (рис. ??).

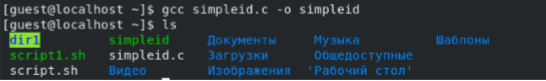


Создание файла

Далее написал программу, которая выводит информацию об идентификаторах пользователя и группы (рис. ??). Скомпилировал эту программу (рис. ??).



Программа 1

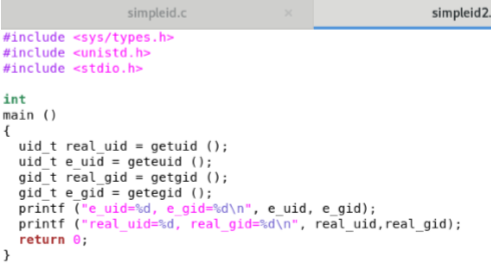


Компиляция программы 1

Выполнил эту программу и сравнил ее вывод с результатом работы системной команды id (рис. ??)(рис. ??).

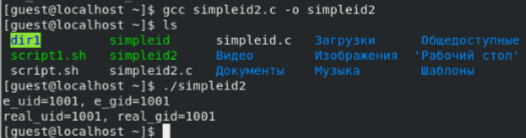
Запуск программы 1 Запуск программы 1

Модифицировал программу, чтобы она выводила также действительные идентификаторы (рис. ??).

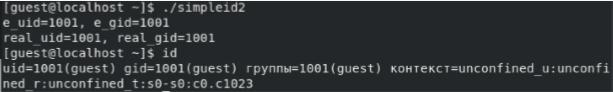


Программа 2

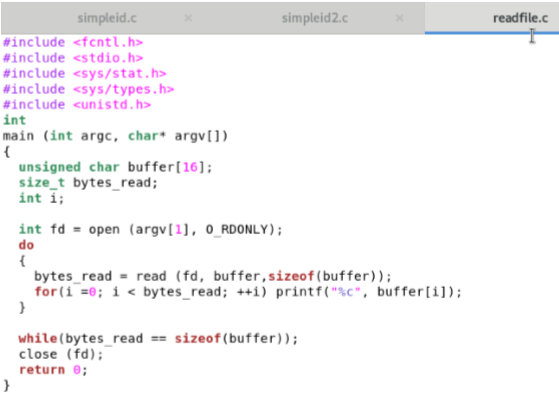
Скомпилировал и запустил модифицированную программу (рис. ??).



Запуск модифицированной программы

Передал право владения программой суперпользователю и наделил его правом на исполнение программы. Запустили программу и сверили результат с выводом команды id (рис. ??) (рис. ??). Запустил simpleid2 и id. Ничего не изменилось (рис. ??) Передача прав и перезапуск программы Передача прав и перезапуск программы 

Создал новую программу readfile, позволяющую прочесть содержимое файла (рис. ??).

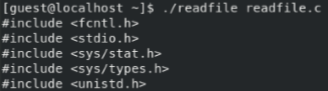
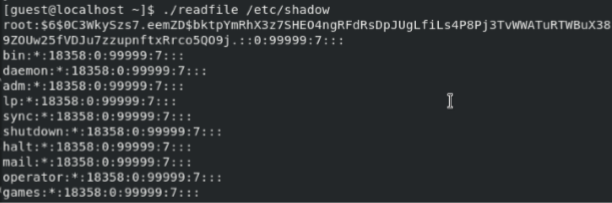


Программа 3

Скомпилировал ее, а затем поменял владельца файла readfile.c (рис. ??) и изменил права так, чтобы читать файл мог только суперпользователь. Проверил, может ли пользователь guest прочитать файл (рис. ??). Ему было отказано в доступе.

Смена владельца файла Смена прав и проверка

Передал право владения программой суперпользователю и проверили, может ли программа прочитать readfile.c (рис. ??) (рис. ??) и etc/shadow (рис. ??). Действия были выполнены успешно.

Смена владельца программой и чтение readfile.c  

Проверил, установлен ли Sticky-бит на директории tmp, создал file01.txt и передал категории пользователей “все остальные” право на чтение и запись (рис. ??) (рис. ??). Проверка наличия Sticky-бита и создание файла Проверка наличия Sticky-бита и создание файла

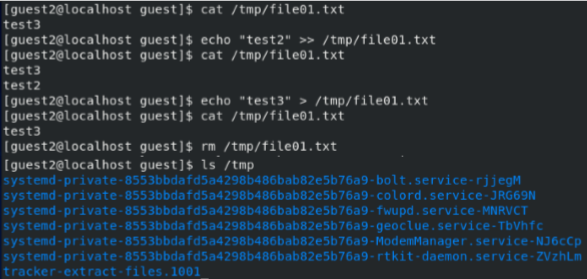
От лица пользователя guest2 (не являющегося владельцем файла) попробовал прочесть файл и записать туда новые данные (рис. ??) (рис. ??), а также удалить файл (рис. ??).

Попытка чтения и изменения Попытка чтения и изменения Попытка удаления

Снял с папки tmp атрибут Sticky (рис. ??) (рис. ??).

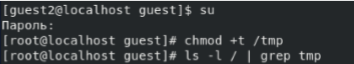
Снятие атрибута Sticky Снятие атрибута Sticky

От лица пользователя guest2 попробовал прочесть файл, произвести в него запись и удалить (рис. ??). Удаление файла прошло успешно.



Чтение, запись и удаление

Установил атрибут Sticky обратно на папку tmp (рис. ??) (рис. ??).

 Установка атрибута Sticky

# 5 Выводы

В результате лабораторной работы усовершенствовал навыки использования командой строки и изучил SetUID-, SetGID- и Sticky-биты.

# Список литературы

1. Дискреционное разграничение прав в Linux. Исследование влияния дополнитель ных атрибутов [Электронный ресурс]. URL: https://esystem.rudn.ru/mod/resource/v iew.php?id=1031377.
2. Использование SETUID, SETGID и Sticky Bit для расширенной настройки прав доступа в операционных системах Linux [Электронный ресурс]. URL: https://ruvd s.com/ru/helpcenter/suid-sgid-sticky-bit-linux/.