Лабораторная работа №5

Информационная безопасность

Доре Стевенсон Эдгар

Содержание

[Цель работы 1](#_Toc116161044)

[Задание 1](#_Toc116161045)

[Выполнение лабораторной работы 1](#_Toc116161046)

[Выводы 6](#_Toc116161047)

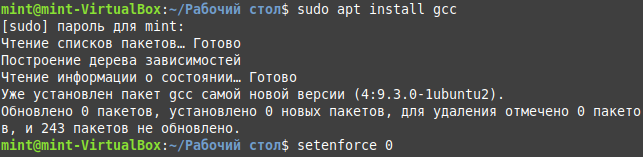
# Цель работы

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

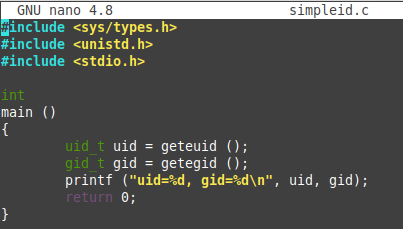
# Выполнение лабораторной работы

Установил gcc с помощью команды yum install gcc. (рис. @fig:001)



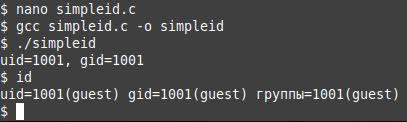
Установка gcc

Отменил на текущую сессию SELinux командой setenforce 0. Вошёл в систему от имени пользователя guest, создал программу simpleid.c. (рис. @fig:002)



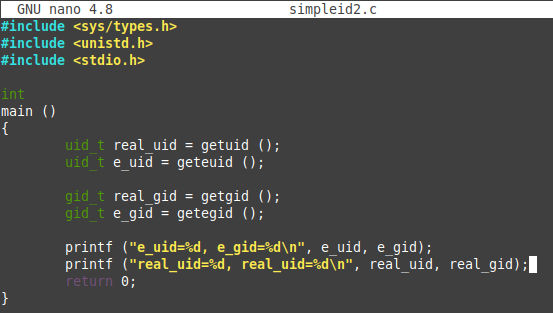
Код программы simpleid.c

Скомпилировал программу и убедился, что файл программы создан: gcc simpleid.c -o simpleid. Выполнил программу simpleid: ./simpleid. Выполнил программу id и сравнил полученный результат с данными предыдущего пункта задания. Полученные значения id совпадают. (рис. @fig:003)



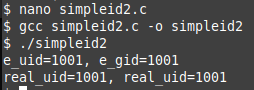
Сравнение результатов программы и команды

Усложнил программу, добавив вывод действительных идентификаторов, получившуюися программу назвал simpleid2.c. (рис. @fig:004)



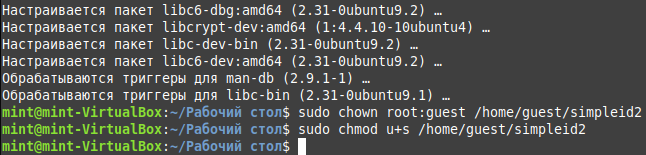
Код программы simpleid2.c

Скомпилировал и запустил simpleid2.c gcc simpleid2.c -o simpleid2, а затем ./simpleid2. (рис. @fig:005)



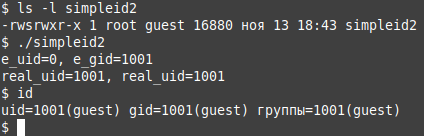
Компиляция и запуск simpleid2.c

От имени суперпользователя выполнил команды: chown root:guest /home/guest/simpleid2, а затем chmod u+s /home/guest/simpleid2. Первая команда изменяет права на файл с guest на root. А затем устанавливает атрибут SetUID, который запускает программу не с правами пользователя, а с правами владельца файла. Затем выполнил проверку изменений с помощью команды ls -l simpleid2. (рис. @fig:006)



Добавление SetUID

Запустил simpleid2 и id: ./simpleid2, id. При данном запуску выводы совпадают. (рис. @fig:007)



Сверка результата программы и кода

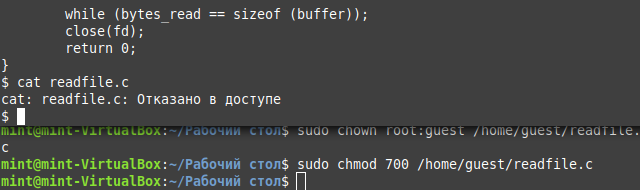
Проделал то же самое с атрибутом SetGID (установление прав для владеющей группы). Запустил файл. Теперь выводы для группы различны.

Создал программу readfile.c. (рис. @fig:008)



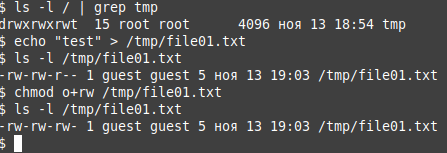
Код программы readfile.c

Откомпилировал программу: gcc readfile.c -o readfile. Сменил владельца у файла readfile.c и изменил права так, чтобы только суперпользователь(root) мог прочитать его, a guest не мог. Проверил, что пользователь guest не может прочитать файл readfile.с (рис. @fig:009)



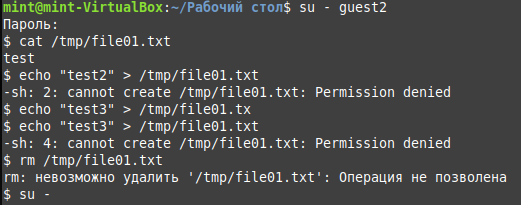
Проверка чтения файла

Сменил у программы readfile владельца и установил SetU’D-бит. Программа readfile может прочитать файл readfile.c. Программа readfile может прочитать файл /etc/shadow. Исследование Sticky-бита. Узнал, установлен ли атрибут Sticky на директории /tmp, для чего выполнил команду ls -l / | grep tmp (рис. @fig:010)



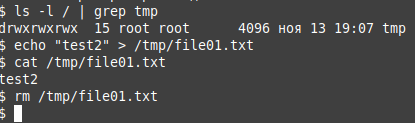
Проверка атрибутов

От имени пользователя guest создал файл file01.txt в директории /tmp со словом test echo "test" > /tmp/file01.txt. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные»: ls -l /tmp/file01.txt, chmod o+rw /tmp/file01.txt, ls -l /tmp/file01.txt. От пользователя guest2 (не являющегося владельцем) попробовал прочитать файл /tmp/file01.txt: cat /tmp/file01.txt, записать в файл /tmp/file01.txt текст test3, стерев при этом всю имеющуюся в файле информацию командой echo "test3" > /tmp/file01.txt. Проверил содержимое файла командой cat /tmp/file01.txt, попробовал дозаписать в файл /tmp/file01.txt слово test2 командой echo "test2" >> /tmp/file01.txt, удалить файл /tmp/file01.txt командой rm /tmp/file01.txt Файл удалить не удалось. (рис. @fig:011)



Проверка от guest2

Повысил свои права до суперпользователя следующей командой su - и выполнил после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: chmod -t /tmp. Затем попробовал выполнить все вышеперечисленные операции. Все удалось. (рис. @fig:012)



Проверка после снятия Sticky атрибута

Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp: su -, chmod +t /tmp, exit.

# Выводы

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