Лабораторная работа №5

Информационная безопасность

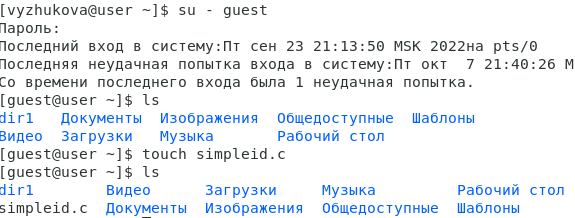
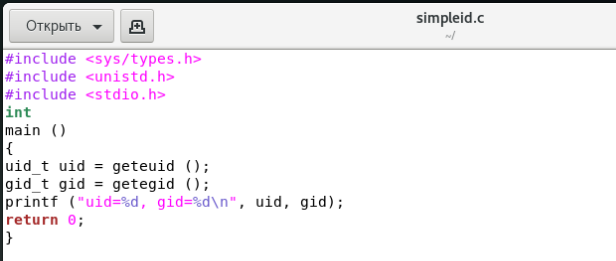
Жукова Виктория

Содержание

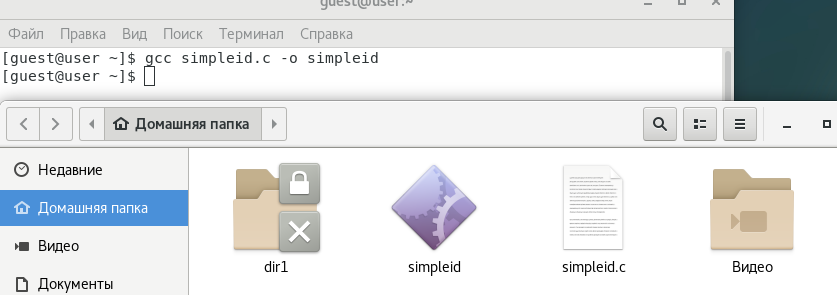
# Цель работы

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.

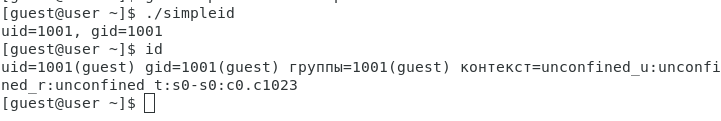
# Выполнение лабораторной работы

Вошла в систему от имени пользователя guest, создала программу simpleid.c. (рис. -@fig:002)  

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

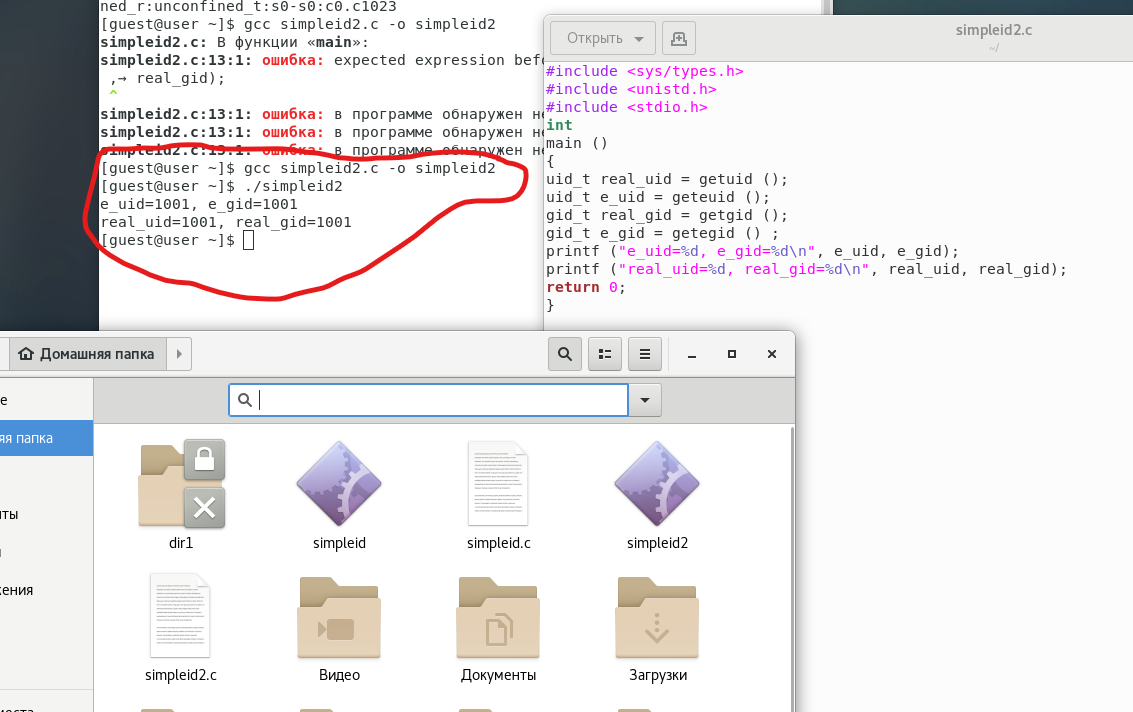


Компиляция



Сравнение результатов программы и команды

Усложнила программу, добавив вывод действительных идентификаторов, получившуюися программу назвала simpleid2.c. Скомпилировала и запустила simpleid2.c gcc simpleid2.c -o simpleid2, а затем ./simpleid2. (рис. -@fig:005)



Компиляция и запуск simpleid2.c

От имени суперпользователя выполнила 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. (рис. -@fig:006)

Выполнение команд

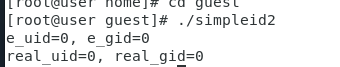
Выполнение команд

Затем выполнила проверку изменений с помощью команды ls -l simpleid2.

Проверка атрибутов

Проверка атрибутов

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



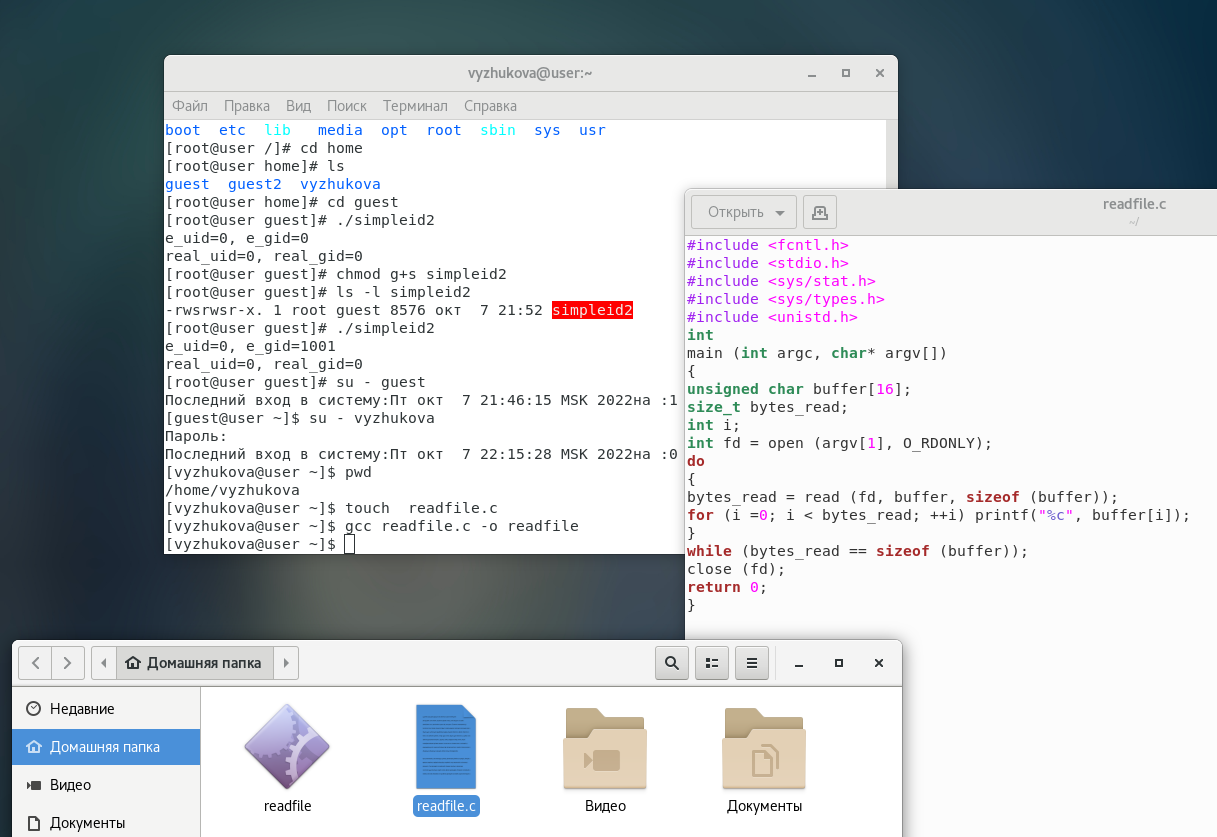
Сверка результата программы и кода

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



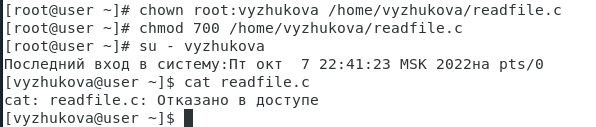
Тоже самое с атрибутом SetGID

Создала программу readfile.c. Откомпилировала программу: gcc readfile.c -o readfile.(рис. -@fig:008)



Код программы readfile.c

Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь(root) мог прочитать его, a vyzhukova не мог. Проверил, что пользователь vyzhukova не может прочитать файл readfile.с (рис. -@fig:009)



Проверка чтения файла

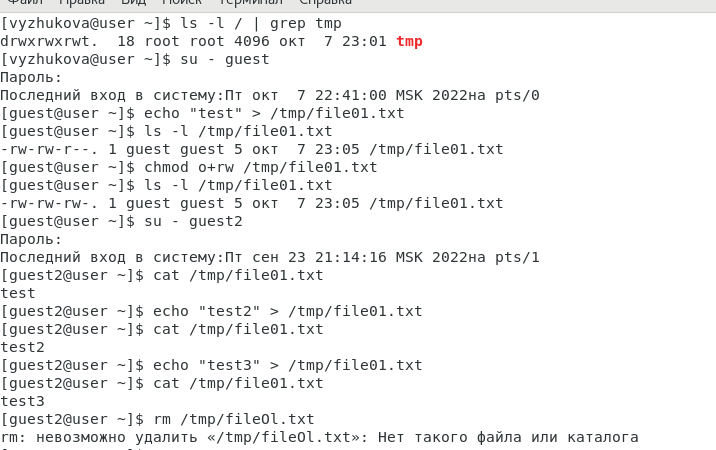
Сменила у программы readfile владельца и установил SetU’D-бит. Программа readfile может прочитать файл readfile.c. Программа readfile может прочитать файлы /etc/shadow. (рис. -@fig:010)



Чтение файлов

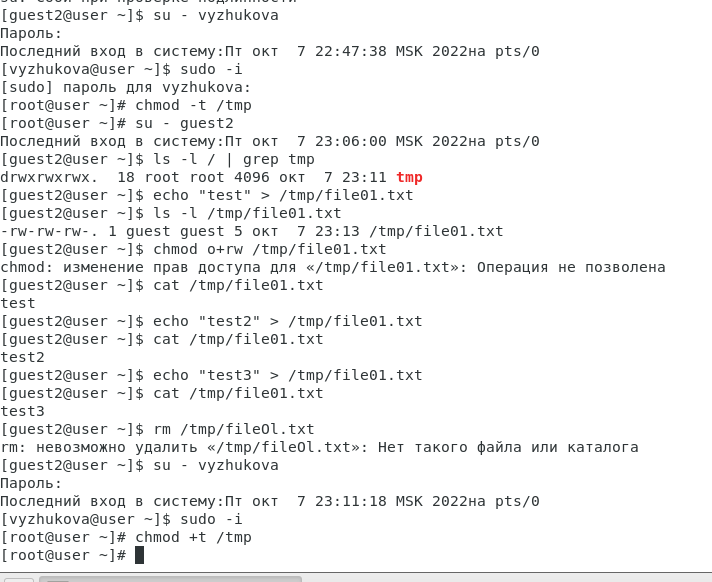
Исследование Sticky-бита. Узнал, установлен ли атрибут Sticky на директории /tmp, для чего выполнил команду ls -l / | grep tmp

От имени пользователя guest создала файл file01.txt в директории /tmp со словом test echo "test" > /tmp/file01.txt. Просмотрела атрибуты у только что созданного файла и разрешила 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) попробовала 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. Проверила содержимое файла командой cat /tmp/file01.txt, попробовала 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) Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp: su -, chmod +t /tmp, exit.



Проверка после снятия Sticky атрибута

# 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. [КОМАНДА CHATTR В LINUX](https://losst.ru/neizmenyaemye-fajly-v-linux)
2. [chattr](https://en.wikipedia.org/wiki/Chattr)