Отчёт по лабораторной работе №5

Дисциплина: Информационная безопасность

Шапошникова Айталина Степановна, НПИбд-02-18

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

5.3.1. Создание программы

1. Вошли в систему от имени пользователя guest.
2. Создали программу simpleid.c (рис. 1).

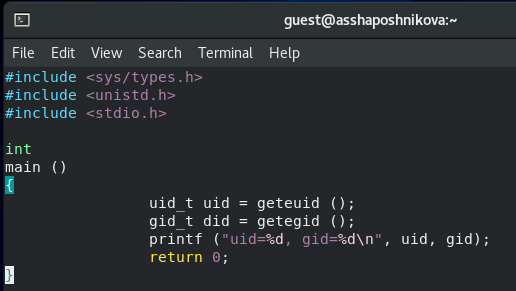


Figure 1: Программа simpleid.c

1. Скомплилировали программу и убедились, что файл программы создан (рис. 2).

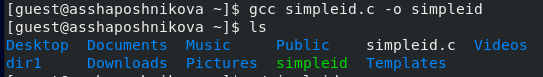


Figure 2: Компиляция программы

1. Выполнили программу simpleid (рис. 3).

Figure 3: Выполнение программы simpleid

Figure 3: Выполнение программы simpleid

1. Выполнили системную программу id (рис. 4).

Figure 4: Программа id

Figure 4: Программа id

1. Усложнили программу, добавив вывод действительных идентификаторов (рис. 5). Получившуюся программу назвали simpleid2.c.

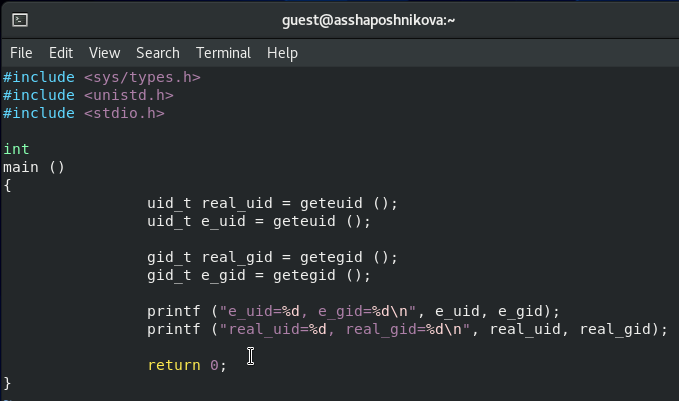


Figure 5: Усложнение программы

1. Скомпилировали и запустили simpleid2.c (рис. 6).

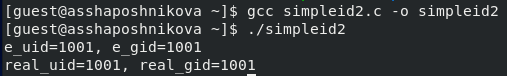


Figure 6: Программа simpleid2.c

1. От имени суперпользователя выполнили команды (рис. 7).

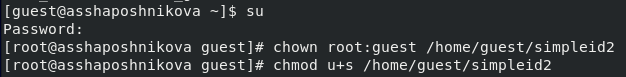


Figure 7: Изменение прав программы

1. Повысили временно свои права с помощью su.
2. Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2 (рис. 8).

Figure 8: Проверка

Figure 8: Проверка

1. Запустили simpleid2 и id (рис. 9).

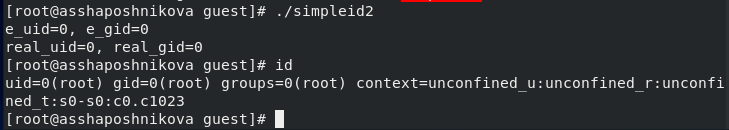


Figure 9: Запуск simpleid2 и id

1. Проделали тоже самое относительно SetGID-бита (рис. 10).

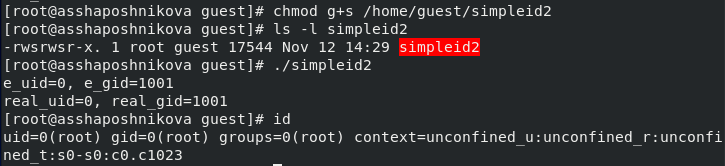


Figure 10: SetGID-бита

1. Создайли программу readfile.c (рис. 11).

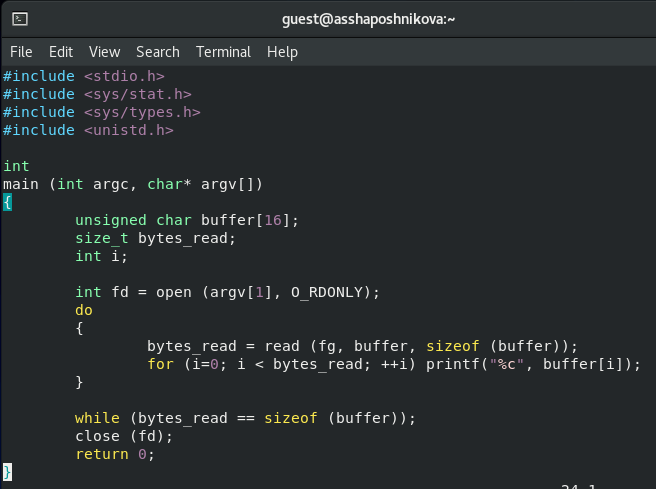


Figure 11: Программа readfile.c

1. Откомпилировали её (рис. 12).

Figure 12: Компиляция readfile.c

Figure 12: Компиляция readfile.c

1. Сменили владельца у файла readfile.c и изменили права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог (рис. 13).

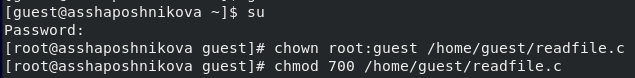


Figure 13: Права файла readfile.c

1. Проверили, что пользователь guest не может прочитать файл readfile.c (рис. 14).

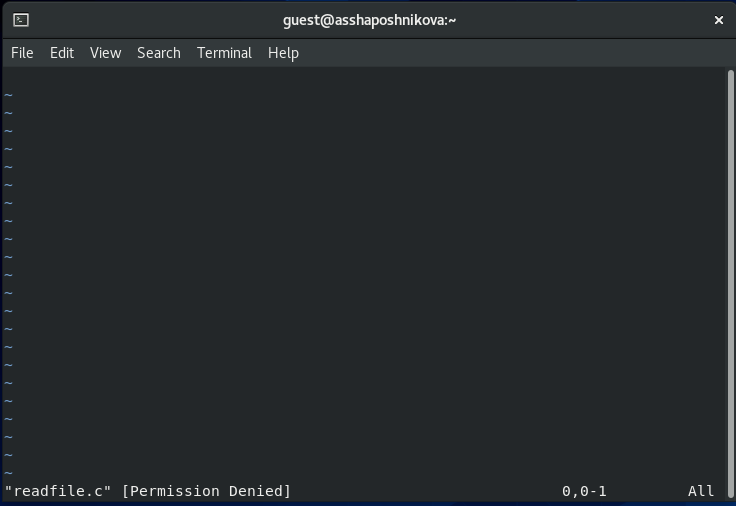


Figure 14: guest не может прочитать файл readfile.c

1. Сменили у программы readfile владельца и установили SetUID-бит (рис. 15).

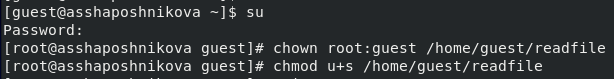


Figure 15: Права файла readfile.c

1. Проверили, может ли программа readfile прочитать файл readfile.c (рис. 16).

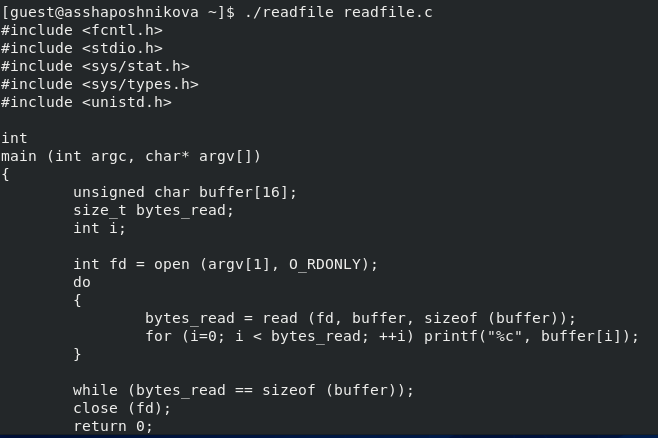


Figure 16: Права файла readfile.c

1. Проверили, может ли программа readfile прочитать файл /etc/shadow (рис. 17).

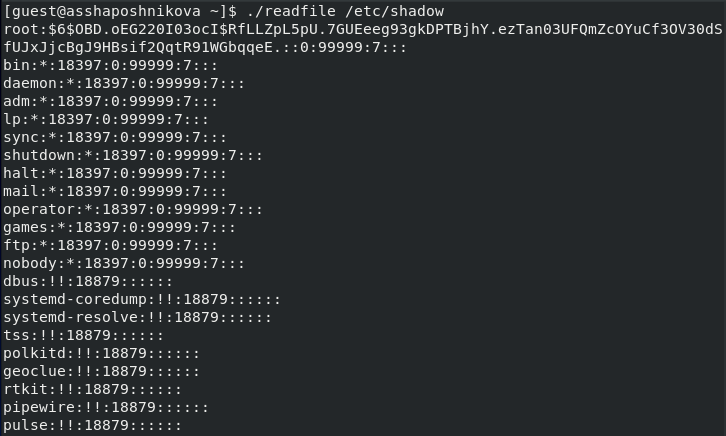


Figure 17: Права файла readfile.c

5.3.2. Исследование Sticky-бита

1. Выяснили, установлен ли атрибут Sticky на директории /tmp (рис. 18). Да, установлен.
2. От имени пользователя guest создали файл file01.txt в директории /tmp со словом test (рис. 18).

Figure 18: Атрибут Sticky и создание file01.txt

Figure 18: Атрибут Sticky и создание file01.txt

1. Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные» (рис. 19).

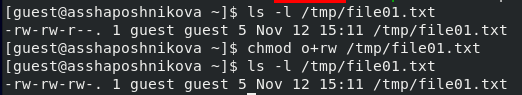


Figure 19: Атрибуты file01.txt

1. От пользователя guest2 (не являющегося владельцем) попробовали прочитать файл /tmp/file01.txt (рис. 20). Получилось.
2. От пользователя guest2 попробовали дозаписать в файл /tmp/file01.txt слово test2 (рис. 20). Получилось.
3. Проверили содержимое файла (рис. 20). Получилось.
4. От пользователя guest2 попробовали записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию (рис. 20). Получилось.
5. Проверили содержимое файла (рис. 20). Получилось.
6. От пользователя guest2 попробовали удалить файл /tmp/file01.txt (рис. 20). Не получилось.

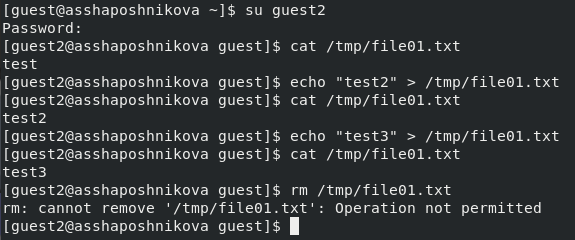


Figure 20: Проверка

1. Повысили свои права до суперпользователя и выполнили после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp (рис. 21).
2. Покинули режим суперпользователя (рис. 21).
3. От пользователя guest2 проверили, что атрибута t у директории /tmp нет (рис. 21).
4. Повторили предыдущие шаги (рис. 21).
5. Удалось удалить файл от имени пользователя, не являющегося его владельцемт (рис. 21).

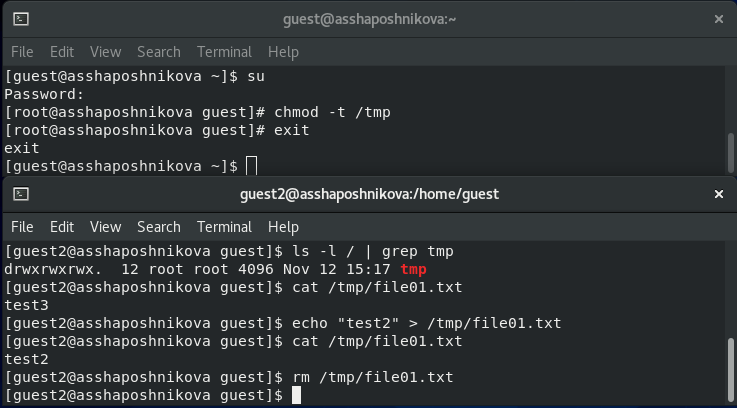


Figure 21: Проверка

1. Повысили свои права до суперпользователя и вернули атрибут t на директорию /tmp (рис. 22).

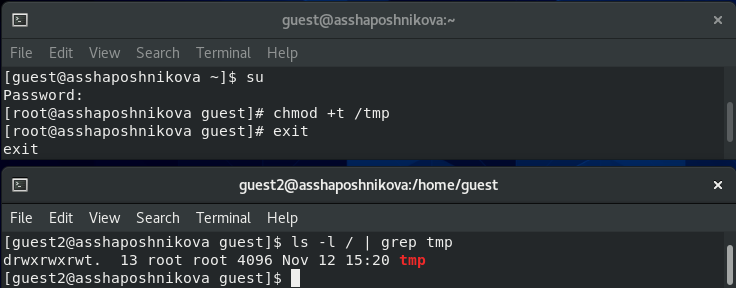


Figure 22: Возвращаем атрибут t

# Выводы

После выполнения лабораторной работы №5 мы изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Рассмотрели работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.