Отчёт Лабораторной работы №5

По дисциплине Информационная безопасность

Прокошев Никита Евгеньевич

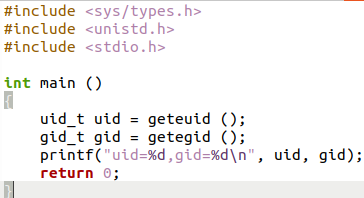
Содержание

# Цель работы

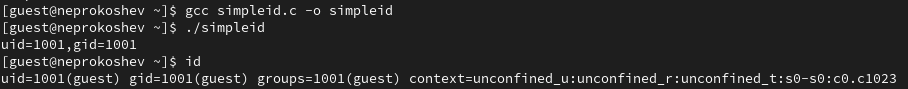
Цель: Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в кон- соли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Выполнение лабораторной работы

1. Входим в систему от имени пользователя guest и создаём программу simpleid.c (@pic:001, @pic:002).

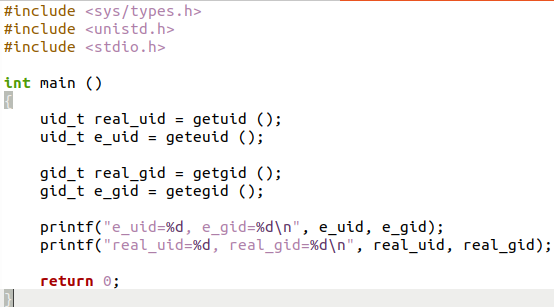
Создаём программу simpleid.c. 

1. Скомплилируем и выполним программу simpleid.c и системную программу id и сравним полученные результаты (@pic:003).

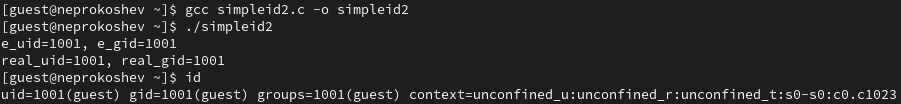


Компилируем и выполняем программу simpleid.c.

1. Усложним программу, добавив вывод действительных идентификато- ров и назовём её simpleid2.c (@pic:004, @pic:005).

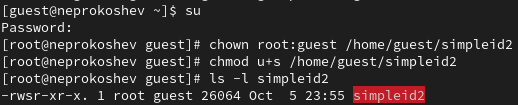
Создаём программу simpleid2.c. 

1. Скомпилируем и запустим simpleid2.c (@pic:006).



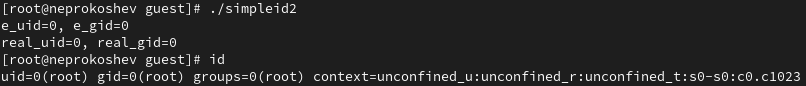
Компилируем и выполняем программу simpleid2.c.

1. От имени суперпользователя выполним команды и выполним проверку правильности установки новых атрибутов и смены владельца файла simpleid2.c (@pic:007).



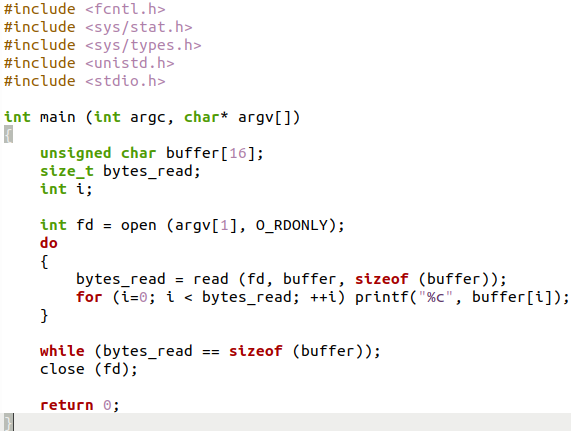
Выполняем команды и проверяем правильность установки атрибутов.

1. Запустим simpleid2.c и id и сравним результаты (@pic:008).



Выполняем программу simpleid2.c.

1. Создадим программу readfile.c (@pic:009, @pic:010).

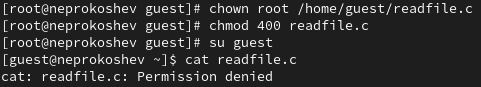
Создаём программу readfile.c. 

1. Скомпилируем файл readfile.c (@pic:011).

Компилируем программу readfile.c.

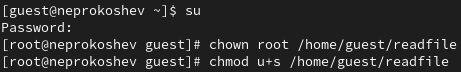
Компилируем программу readfile.c.

1. Сменим владельца у файла readfile.c и изменим права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог. Проверим, что пользователь guest не может прочитать файл readfile.c (@pic:012).



Меняем владельца файла и его права

1. Сменим у программы readfile владельца и установим SetUID-бит (@pic:013). Проверим, может ли программа readfile прочитать файлы readfile.c и /etc/shadow? (@pic:014, @pic:015).

1. Выясним, установлен ли атрибут Sticky на директории /tmp (@pic:016).

Проверям Sticky-атрибут.

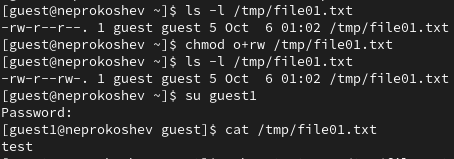
Проверям Sticky-атрибут.

1. От имени пользователя guest создаём файл file01.txt в директории /tmp со словом “test” (@pic:017).

Создаём файл file01.txt.

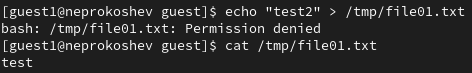
Создаём файл file01.txt.

1. Просмотрим атрибуты у только что созданного файла и разрешим чте- ние и запись для категории пользователей «все остальные». От пользователя guest1 попробуем прочитать файл file01.txt (@pic:018).



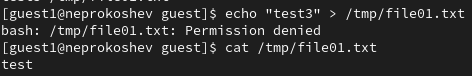
Изменяем атрибуты и читаем файл.

1. От пользователя guest2 попробуем дозаписать в файл /tmp/file01.txt слово “test2” и проверим содержимое файла (@pic:019).



Дозаписываем слово и проверям файл.

1. От пользователя guest2 попробуем записать в файл /tmp/file01.txt слово “test3”, стерев при этом всю имеющуюся в файле информацию и проверим содержимое файла (@pic:020).



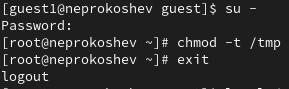
Дозаписываем слово и проверяем файл.

1. От пользователя guest2 попробуем удалить файл /tmp/file01.txt (@pic:021).

Пробуем удалить файл.

Пробуем удалить файл.

1. Повышаем свои права до суперпользователя и выполняем после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp. После покидаем режим суперпользователя (@pic:022).



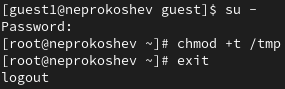
Снимаем атрибут t.

1. От пользователя guest2 проверяем, что атрибута t у директории /tmp нет. Повторим предыдущие шаги. Видим, что теперь мы можем удалить этот файл, но не более (@pic:023).



Повторяем действия без атрибута t.

1. Повышаем свои права до суперпользователя и возвращаем атрибут t на ди- ректорию /tmp (@pic:024).



Возвращаем атрибут t.

# Выводы

В ходе данной лабораторной работы были изучены механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получены практические навыки работы в консоли с дополнительными атрибутами. Рассмотрены работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Список литературы