Отчёт по лабораторной работе №5

Основы информационной безопасности

Надежда Александровна Рогожина

Содержание

# 1 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.

# 2 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.

root@ruvds-hrc [~]# which sudo /usr/bin/sudo  
root@ruvds-hrc [~]# ls -l /usr/bin/sudo  
-rwsr-xr-x 1 root root 125308 Feb 20 14:15 /usr/bin/sudo

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

Принцип работы Setgid очень похож на setuid с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом. Иллюстрирует работу этого бита команда crontab:

root@ruvds-hrc [~]# which crontab  
/usr/bin/crontab  
root@ruvds-hrc [~]# ls -l /usr/bin/crontab  
-rwxr-sr-x 1 root crontab 34021 Feb 12 2017 /usr/bin/crontab

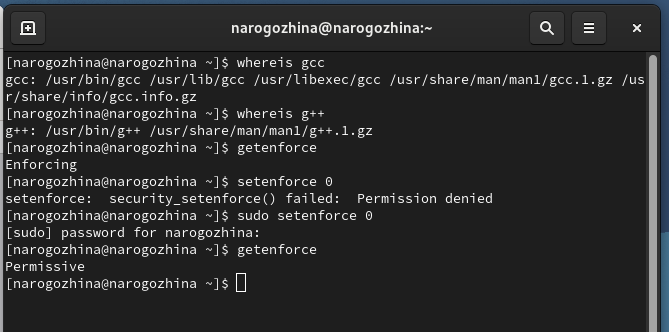
Последний специальный бит разрешения – это Sticky Bit . В случае, если этот бит установлен для папки, то файлы в этой папке могут быть удалены только их владельцем. Пример использования этого бита в операционной системе это системная папка /tmp . Эта папка разрешена на запись любому пользователю, но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

root@ruvds-hrc [~]# ls -ld /tmp  
drwxrwxrwt 8 root root 4096 Mar 25 10:22 /tmp

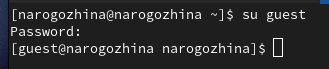
Символ «t» указывает, что на папку установлен Sticky Bit.

# 3 Выполнение лабораторной работы

1. Войдем в систему от имени пользователя guest (рис. [??], [??]).



Вход в систему



Вход в систему

1. Создадим файл simpleid.c (рис. [??]).



simpleid.c

1. Скомпилируем и убедимся, что файл программы создан (рис. [??], рис. [??]).

компиляция

компиляция

проверка работоспособности

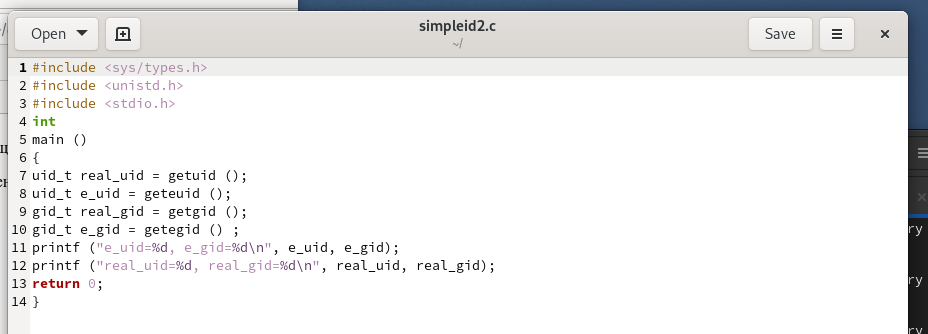
проверка работоспособности

1. Выполните системную команду id и сравните с результатом вывода нашей программы (рис. [??]).

id

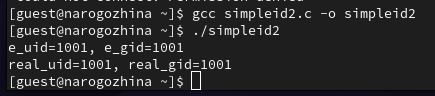
id

1. Программа simpleid2.c (рис. [??]).



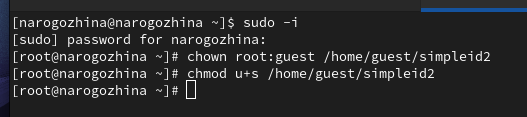
simpleid2.c

1. Компиляция и выполнение (рис. [??]).



simpleid2

1. Смена владельца и прав (рис. [??]).



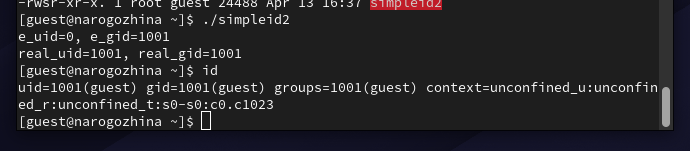
смена прав от root

1. Проверка (рис. [??]).

проверка

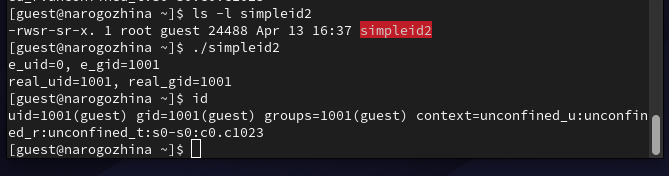
проверка

1. Запуск двух команд (рис. [??]).



id VS simpleid2

1. То же самое, только для SetGID-бита (рис. [??]).



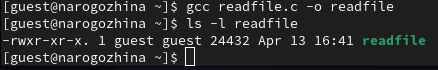
SetGID-бит

1. Программа readfile (рис. [??]).



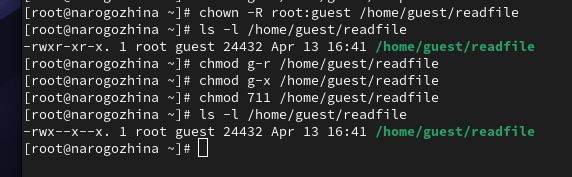
readfile

1. Компиляция и проверка прав (рис. [??]).



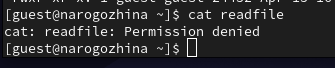
компиляция и проверка прав

1. Смена владельца и прав у readfile (рис. [??]).



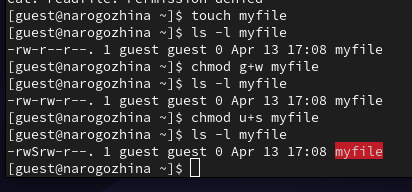
Смена владельца и прав

1. Попытка прочитать (рис. [??]).



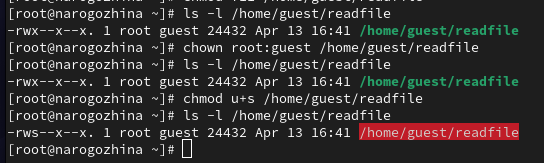
попытка №1

1. Пример работы SetUID-бита (рис. [??]).



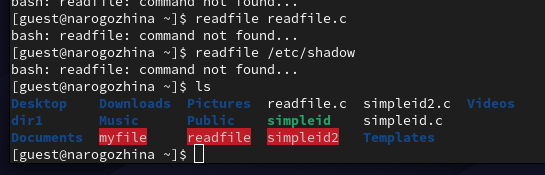
SetUID

1. Смена прав и владельца файла readfile (рис. [??]).



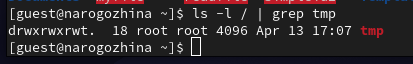
смена владельца и прав

1. Попытка прочитать файлы (рис. [??]).



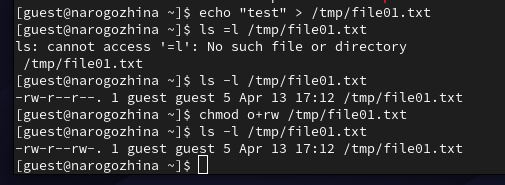
попытка №2

1. Права доступа директории /tmp (рис. [??]).



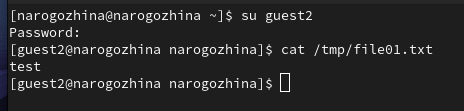
/tmp

1. Попытка записи в новый файл и просмотр его атрибутов (рис. [??]).



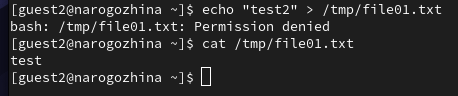
file01.txt

1. Вход от имени guest2 (рис. [??]).



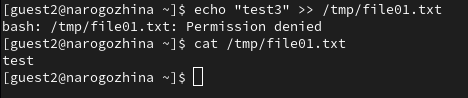
guest2

1. Попытка дозаписи в файл (рис. [??]).



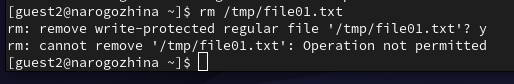
попытка №3

1. Попытка перезаписи файла (рис. [??]).



попытка №4

1. Попытка удаления файла (рис. [??]).



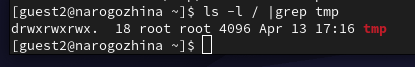
попытка №5

1. Смена прав директории (рис. [??]).

смена прав /tmp

смена прав /tmp

1. Проверка (рис. [[1](#fig:027)]).

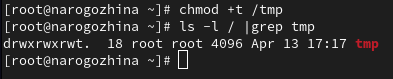


1. Повторение всех предыдущих действий (рис. [??]).



повтор

1. Возвращение прав обратно (рис. [??]).



возвращение прав

# 4 Выводы

В ходе работы мы изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, получили практические навыки работы в консоли с дополнительными атрибутами, а также рассмотрели работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Список литературы