Лабораторная работа 5

Юдин Герман Станиславович, НФИбд-01-19

Содержание

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

дисциплина: Информационная безопасность

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Юдин Герман Станиславович

Группа: НФИбд-01-19

МОСКВА

2022 г.

# 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.

Принцип работы Setgid очень похож на setuid с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

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.

# 3 **Выполнение лабораторной работы**

1. Создал файл simpleid.c, который скомпилировал и запустил. Выполнил команду id и сравнил вывод. Вывело одинаковую информацию (Рис fig. 1).



Figure 1: simpleid

1. Усложнил программу в файле simpleid2.c, также скомпилировал и запустил (Рис fig. 2). На этот раз выдаёт две идентификатора пользователя и 2 идентификатора группы.

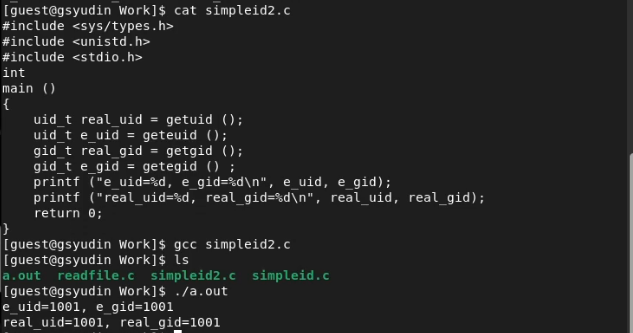


Figure 2: simpleid2

1. От имени суперпользователя изменил владельца файла на рута и добавил S бит на пользователя (Рис fig. 3). Проверил корректность установленного бита (Рис fig. 4).

Figure 3: change parameters

Figure 3: change parameters

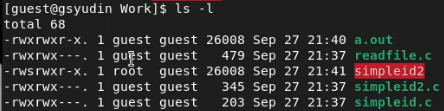


Figure 4: ls -l

1. При запуске от guest выдаёт следующую информацию. Здесь мы видим, что e\_uid стал 0 (Рис fig. 5), что означает, что файл запустился от имени владельца, то есть root.

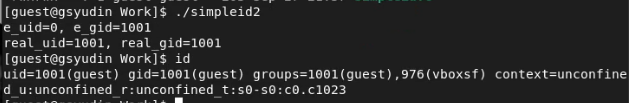


Figure 5: start simpleid2

1. Создал новый файл readfile.c, который предназначен для чтения файлов (Рис fig. 6). Сделал так, чтобы другой файл мог проитать root, но не мог guest (Рис fig. 7).

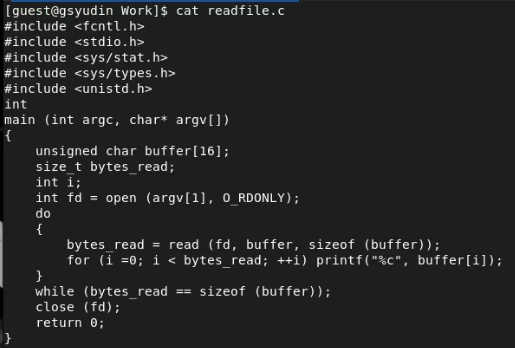


Figure 6: readfile

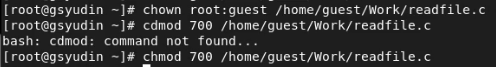


Figure 7: change file

1. Попытался прочитать с guest, но доступ закрыт (Рис fig. 8 и fig. 9).

Figure 8: try read

Figure 8: try read

Figure 9: error

Figure 9: error

1. Сменил владельца файла и установил SetU’D-бит (Рис fig. 10). На этот раз от пользователя guest имеется доступ ко всем файлам, к которым есть доступ у root (Рис fig. 11). Set биты позволяют делать действия относительно владельца файла, то есть файлы запускаются от лица владельца файла, и если владелец может прочитать какой-то файл, а тот кто запускает нет, то с помощью set бита есть возможность прочитать файл даже у пользователя не имеющего возможности прочитать данный файл.

Figure 10: root access

Figure 10: root access



Figure 11: read with readfile

1. Посмотерл атрибуты на каталоге /tmp (Рис fig. 12).

Figure 12: ls tmp

Figure 12: ls tmp

1. Создал в данном каталоге файл от пользователя guest (Рис fig. 13).

Figure 13: echo file

Figure 13: echo file

1. Посмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные» (Рис fig. 14).

Figure 14: rw for other

Figure 14: rw for other

1. От пользователя guest2 попробовал дозаписать файл. Попробовал перезаписать файл. Все действия выполнились (Рис fig. 15).

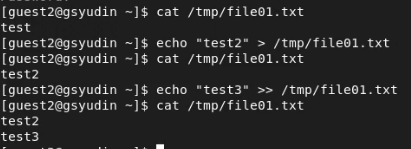


Figure 15: add text, change text

1. Попробовал удалить файл (Рис fig. 16).

Figure 16: rm file fail

Figure 16: rm file fail

1. От прав администратора снял t бит с директории /tmp (Рис fig. 17).

Figure 17: -t /tmp

Figure 17: -t /tmp

1. Повторил предыдущие шаги от guest2. На этот раз смог удалить файл (Рис fig. 18).

Figure 18: rm file success

Figure 18: rm file success

1. Вернул t бит обратно.

# 4 Вывод

Выполнив данную лабораторную работу, я 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.

# 5 Список литературы

1. Кулябов, Д.С. - Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов https://esystem.rudn.ru/pluginfile.php/1651889/mod\_resource/content/2/005-lab\_discret\_sticky.pdf