Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Аксёнова Алина Владимировна

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.

# Задание

Закрепить дискреционное разграничение прав в Linux с дополнительными атрибутами.

# Теоретическое введение

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов. Один из подходов к разграничению доступа — так называемый дискреционный - предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют. Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. Чтобы получить доступ к файлам в Linux, используются разрешения. Эти разрешения назначаются трем объектам: файлу, группе и другому объекту. Для управления правами используется команда chmod. При использовании chmod в относительном режиме вы работаете с тремя индикаторами, чтобы указать, что вы хотите сделать. Сначала вы указываете, для кого вы хотите изменить разрешения. Для этого вы можете выбрать между пользователем (u), группой (g) и другими (o). Затем вы используете оператор для добавления или удаления разрешений из текущего режима или устанавливаете их абсолютно. В конце вы используете r(read), w(write) и x(execute), чтобы указать, какие разрешения вы хотите установить.При использовании chmod вы можете устанавливать разрешения для пользователя (user), группы (group) и других (other).Помимо основных разрешений, о которых вы только что прочитали, в Linux также есть набор расширенных разрешений. Это не те разрешения, которые вы устанавливаете по умолчанию, но иногда они предоставляют полезное дополнение.

# Ход работы

1. Готовим систему и входим из-под пользователя guest. Пишем программу simpleid.c. Компилируем программу, запускаем, видим вывод uid и gid пользователя, сравниваем вывод с id (все совпадает). (Рис. 1, 2,3).

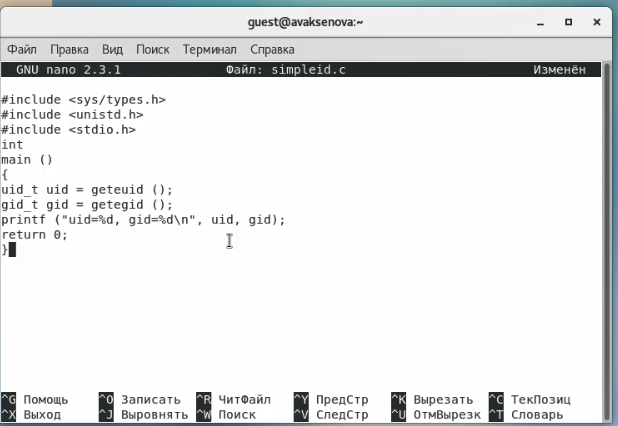


Figure 1: Листинг simpleid.c

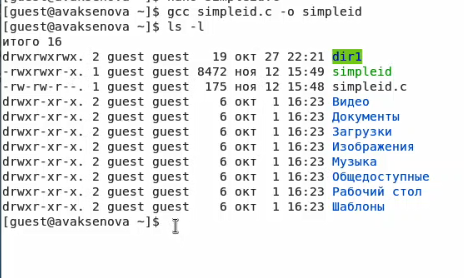


Figure 2: Запуск simpleid.c

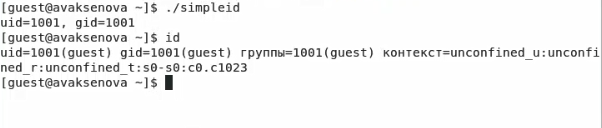


Figure 3: Сверка simpleid.c и id

1. Усложняем программу и запускаем её. (Рис. 4, 5).



Figure 4: Листинг simpleid2.c

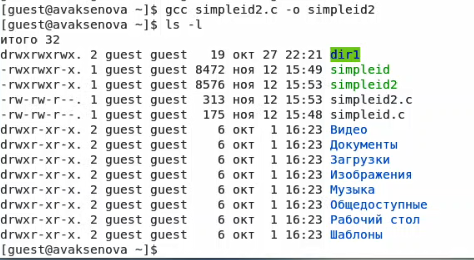


Figure 5: Запуск simpleid2.c

1. Из-под суперпользователя меняем владельца и добавляем SetUID бит на файл. Проверяем правильность и запускаем программу еще раз. еuid возвращает id владельца, а real\_uid возвращает uid запускающего пользователя.(Рис. 6, 7, 8).

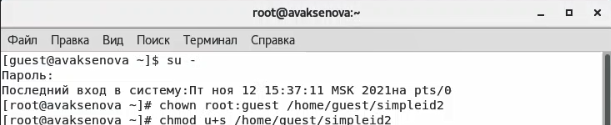


Figure 6: Смена владельца и добавление SetUID бита

Figure 7: Запуск simpleid2.c

Figure 7: Запуск simpleid2.c

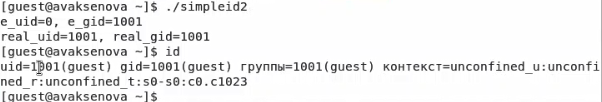


Figure 8: Сверка simpleid2.c и id

1. Теперь добавим на файл SetGID бит с проделаем все то же самое. (Рис. 9, 10).



Figure 9: Добавление SetGID бита

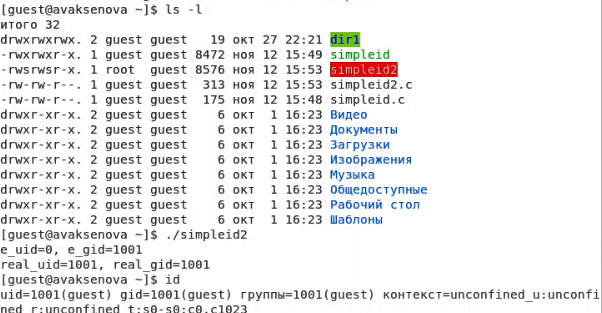


Figure 10: Запуск simpleid2.c

1. Пишем программу readfile.c. (Рис. 11).

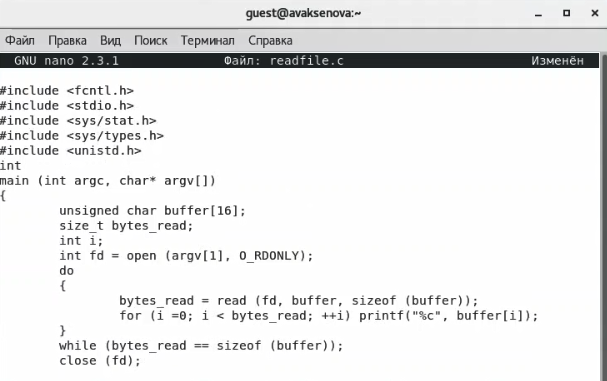


Figure 11: Код программы

6.Компилируем программу. (Рис. 12).

Figure 12: Компиляция

Figure 12: Компиляция

1. Меняем владельца у файла readfile.c и запрещаем чтение всем, кроме суперпользователя. Проверяем, что guest не может читать. Меняем владельца у программы readfile и добавляем SetUID бит на неё. (Рис. 13, 14, 15).

Figure 13: Смена владельца readfile.c

Figure 13: Смена владельца readfile.c

Figure 14: Проверка на cat из-под guest’a

Figure 14: Проверка на cat из-под guest’a

Figure 15: Смена владельца readfile и SetUID

Figure 15: Смена владельца readfile и SetUID

1. Проверяем, может ли программа readfile прочитать файл readfile.c и файл /etc/shadow. Да, может. Хотя сам пользователь вручную не мог. Всё дело в том, что при вызове программы права пользователя повышаются SetUID битом до прав владельца, который может читать файлы (суперпользователь в нашем случае). (Рис. 16, 17).

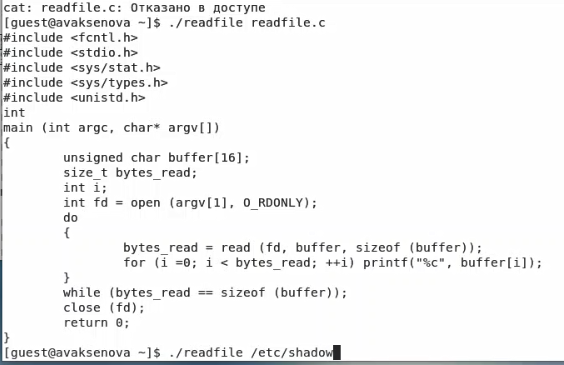


Figure 16: Чтение readfile.c программой readfile



Figure 17: Чтение /etc/shadow программой readfile

1. Проверяем Sticky бит. Для этого создаем файл, которому даем rw права для others и пишем туда слово test. Теперь пробуем выполнить дозапись в файл, перезапись файла и его удаление. Всё, кроме удаления, прошло успешно. (Рис. 18, 19, 20, 21, 22).



Figure 18: Создание файла

Figure 19: Правка прав файла

Figure 19: Правка прав файла

Figure 20: Проверка прав

Figure 20: Проверка прав

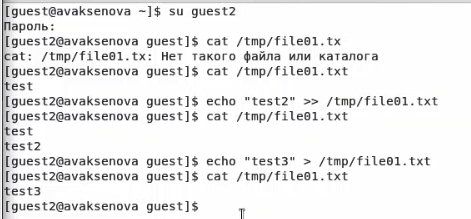


Figure 21: Тестирование файла

Figure 22: Попытка удаления файла

Figure 22: Попытка удаления файла

1. Повышаем права до суперпользователя и удаляем Sticky-бит с папки /tmp. Повторяем наши тесты. Теперь прошли все команды, включая удаление файла. Таким образом, пользователь, не являющийся владельцем файла, смог его удалить, так как Sticky-бит не был настроен. Возвращаем Sticky-бит на папку /tmp. (Рис. 23, 24, 25).

Figure 23: Удаление Sticky-бита

Figure 23: Удаление Sticky-бита

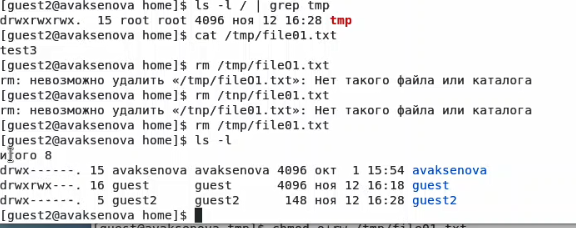


Figure 24: Повторное тестирование файла

Figure 25: Возвращение Sticky-бита

Figure 25: Возвращение Sticky-бита

# Выводы

В результате выполнения данной работы были изучены механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Кроме того, получены практические навыки работы в консоли с дополнительными атрибутами, рассмотрена работа механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Библиографический список

1. Острейковский В. А. Информатика: учеб. для вузов / В. А. Острейковский. - 4-е изд., стер. - М.: Высш. шк., 2007. - 511 с.
2. Права в Linux [Электронный ресурс]. – Режим доступа : https://habr.com/ru/post/469667/, свободный. – Загл. с экрана.
3. Права доступа Unix, SUID, SGID, Sticky биты [Электронный ресурс]. – Режим доступа : https://help.ubuntu.ru/wiki/%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%BD%D1%8B%D0%B5\_%D0%BF%D1%80%D0%B0%D0%B2%D0%B0\_unix, свободный. – Загл. с экрана.