**Лабораторная работа N° 3**

Информационная безопасность

Леон Фернандо Хосе Фернандо | НПМбд02-20

**Содержание**

[**1 Цель работы 2**](#_Toc145794353)

[**2 Теоретическое введение 2**](#_Toc145794354)

[**3 Выполнение лабораторной работы 3**](#_Toc145794355)

[**4 Выводы 9**](#_Toc145794356)

[**Список Литературы 10**](#_Toc145794357)

**Список иллюстраций**

[Figure 1. Создание пользователя и добавление его в группу 5](#_Toc146148371)

[Figure 2. Проверка, в какие группы входят пользователи 6](#_Toc146148372)

[Figure 3.Просмотр файла /etc/group 7](#_Toc146148373)

[Figure 4.Изменение атрибутов 8](#_Toc146148374)

# **1 Цель работы**

Получение практического опыта работы с атрибутами файлов для групп пользователей в консоли.

# **2 Теоретическое введение**

Операционная система Linux предлагает множество надежных функций безопасности, но одной из наиболее важных является система прав доступа к файлам. На ранних стадиях разработки каждый файл был наделен тремя параметрами доступа. Вот они:

* Чтение - Разрешение на чтение позволяет получить доступ к содержимому файла, но не разрешает запись. Для каталогов это позволяет выводить список файлов и подкаталогов, содержащихся внутри.
* Запись - Затем разрешение "Запись" дает возможность создавать новые данные в файле, редактировать существующие данные, создавать новые файлы и изменять как файлы, так и каталоги.
* Выполнение - невозможно запустить программу, если у нее нет флага выполнения. Этот атрибут установлен для всех программ и скриптов, и именно с помощью этого флага система определяет, что файл должен выполняться как программа.

Каждый файл имеет три категории пользователей, для которых могут быть настроены различные комбинации прав доступа:

* Владелец - набор разрешений для владельца файла, пользователя, который его создал или в настоящее время назначен его владельцем. Как правило, владелец обладает полными правами, включая чтение, запись и выполнение.
* Группа - любая группа пользователей, существующая в системе и связанная с файлом. Однако, как правило, это только одна группа, часто группа владельца, хотя файлу можно назначить другую группу.
* Другие - все пользователи, кроме владельца и пользователей, принадлежащих к группе файла.

Команды, которые могут понадобиться при работе с правами доступа:

* “ls -l” - для просмотра прав доступа к файлам и каталогам
* “chmod категория действие флаг файл или каталог” - для изменения прав доступа к файлам и каталогам (категорию действие и флаг можно заменить на набор из трех цифр от 0 до 7)

Значения флагов прав:

* — - нет никаких прав
* –x - разрешено только выполнение файла, как программы, но не изменение и не чтение
* -w- - разрешена только запись и изменение файла
* -wx - разрешено изменение и выполнение, но в случае с каталогом, невозможно посмотреть его содержимое
* r– - права только на чтение
* r-x - только чтение и выполнение, без права на запись
* rw- - права на чтение и запись, но без выполнения
* rwx - все права

# **3 Выполнение лабораторной работы**

При настройке, выполненной во время предыдущего лабораторного сеанса, операционная система установила учетную запись пользователя с именем "guest2" (поскольку пользователь "гость" уже был создан в предыдущем лабораторном сеансе). Это было достигнуто с помощью команды "sudo useradd guest 2", за которой последовала установка пароля для пользователя "guest2" с помощью команды "sudo passwd guest2". Кроме того, я добавил пользователя "guest2" в группу "guest", используя команду "sudo gpasswd -a guest2".

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Figure . Создание пользователя и добавление его в группу

Затем я инициировал вход в систему для двух пользователей на двух отдельных консолях, используя команды "su - guest" и "подзапрос 2". Я определил, используя команду "pwd", что оба пользователя находились в своих соответствующих домашних каталогах, что соответствовало указаниям командной строки. Я проверил имена пользователей с помощью команды "whoami", получив "guest" и "guest2" соответственно. Используя команды "groups guest" и "groups guest2", я установил, что пользователь "guest" является членом группы "guest", в то время как пользователь "guest2" является частью обеих групп "guest" и "guest2". Я сравнил эту информацию с выводами команд "id -Gn guest", "id -Gn guest2", "id -G guest" и "id -G guest2". Данные совпали, за исключением второй команды "id -G", которая отображала номера групп 1001 и 1002, которые также являются точными. Я удалил все атрибуты из каталога "dir1" с помощью команды "chmod 000 dir1" и проверил его статус с помощью команды "ls -l". Действительно, все атрибуты были удалены. Я попытался создать файл с именем "file1" в каталоге "dir1", используя команду "echo 'test' > /home/guest/dir1/file1". Однако эта операция завершилась неудачей, поскольку мы ранее удалили доступ на запись в каталог. Следовательно, файл не был создан. Изначально я даже не мог открыть каталог с помощью команды "ls -l /home/guest/dir1" по той же причине. Чтобы устранить это, я изменил права доступа, снова использовал команду, а затем смог просмотреть содержимое каталога, подтвердив, что файл не был создан.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Figure . Проверка, в какие группы входят пользователи

Просмотрел файл /etc/group командой “cat /etc/group”, данные этого файла совпадают с полученными ранее.

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Автоматически созданное описание

Figure .Просмотр файла /etc/group

От имени пользователя "guest2" я зарегистрировал этого пользователя в группе "гость", используя команду "newgrp guest". После этого, используя учетные данные пользователя "guest", я изменил разрешения каталога "/home/guest", предоставив все действия пользователям в группе с помощью команды "chmod g+rwx /home/guest".

Используя ту же учетную запись пользователя "guest", я удалил все атрибуты из каталога "/home/guest/dir1" командой "chmod 000 dir1" и проверил правильное удаление атрибутов с помощью команды "ls -l".

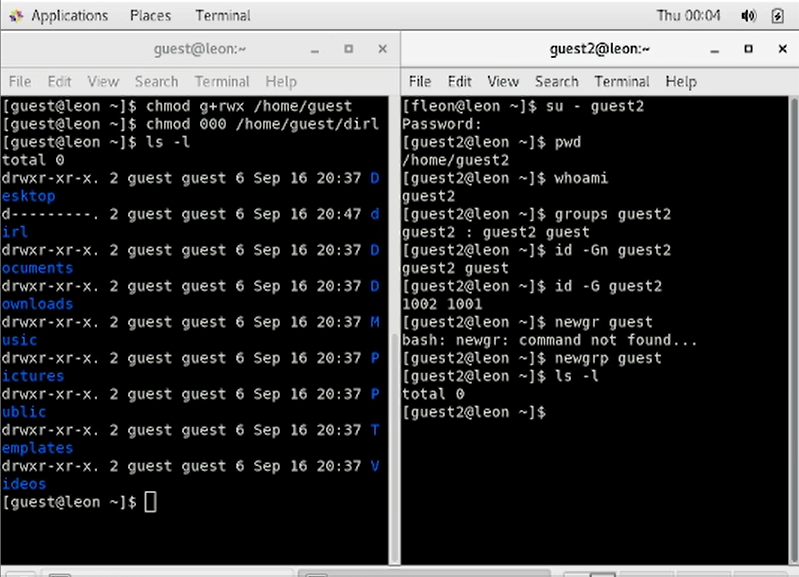


Figure .Изменение атрибутов

Теперь давайте заполним таблицу "Установленные разрешения и разрешенные действия" в разделе 3, изменив атрибуты каталога и файла от имени пользователя "guest" и проведя проверку с точки зрения пользователя "guest2".

Создание файла: “echo”текст” > /home/guest/dir1/file2”

Удаление файла: “rm -r /home/guest/dir1/file1”

Войти в файл: “echo”textnew” > /home/guest/dir1/file1”

Имя пользователя: “cat /home/guest/dir1/file1”

Смена директории: “cd /home/guest/dir1”

Просмотрев в директории: “ls /home/guest/dir1”

Переименование файла: “mv /home/guest/dir1/file1 filenew”

Ссылка на скачивание: “chattr -a /home/guest/dir1/file1”

Установленные права и разрешённые действия

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
| d (000) | (000) | - | - | - | - | - | - | - | - |
| d –x (010) | (000) | - | - | - | - | + | - | - | - |
| d -w- (020) | (000) | - | - | - | - | - | - | - | - |
| d -wx (030) | (000) | + | + | - | - | + | - | + | - |
| d r– (040) | (000) | - | - | - | - | - | + | - | - |
| d r-x (050) | (000) | - | - | - | - | + | + | - | - |
| d rw- (060) | (000) | - | - | - | - | - | + | - | - |
| d rwx (070) | (000) | + | + | - | - | + | + | + | - |
| d (000) | –x (010) | - | - | - | - | - | - | - | - |
| d –x (010) | –x (010) | - | - | - | - | + | - | - | - |
| d -w- (020) | –x (010) | - | - | - | - | - | - | - | - |
| d -wx (030) | –x (010) | + | + | - | - | + | - | + | - |
| d r– (040) | –x (010) | - | - | - | - | - | + | - | - |
| d r-x (050) | –x (010) | - | - | - | - | + | + | - | - |
| d rw- (060) | –x (010) | - | - | - | - | - | + | - | - |
| d rwx (070) | –x (010) | + | + | - | - | + | + | + | - |
| d (000) | -w- (020) | - | - | - | - | - | - | - | - |
| d –x (010) | -w- (020) | - | - | + | - | + | - | - | - |
| d -w- (020) | -w- (020) | - | - | - | - | - | - | - | - |
| d -wx (030) | -w- (020) | + | + | + | - | + | - | + | - |
| d r– (040) | -w- (020) | - | - | - | - | - | + | - | - |
| d r-x (050) | -w- (020) | - | - | + | - | + | + | - | - |
| d rw- (060) | -w- (020) | - | - | - | - | - | + | - | - |
| d rwx (070) | -w- (020) | + | + | + | - | + | + | + | - |
| d (000) | -wx (030) | - | - | - | - | - | - | - | - |
| d –x (010) | -wx (030) | - | - | + | - | + | - | - | - |
| d -w- (020) | -wx (030) | - | - | - | - | - | - | - | - |
| d -wx (030) | -wx (030) | + | + | + | - | + | - | + | - |
| d r– (040) | -wx (030) | - | - | - | - | - | + | - | - |
| d r-x (050) | -wx (030) | - | - | + | - | + | + | - | - |
| d rw- (060) | -wx (030) | - | - | - | - | - | + | - | - |
| d rwx (070) | -wx (030) | + | + | + | - | + | + | + | - |
| d (000) | r– (040) | - | - | - | - | - | - | - | - |
| d –x (010) | r– (040) | - | - | - | + | + | - | - | + |
| d -w- (020) | r– (040) | - | - | - | - | - | - | - | - |
| d -wx (030) | r– (040) | + | + | - | + | + | - | + | + |
| d r– (040) | r– (040) | - | - | - | - | - | + | - | - |
| d r-x (050) | r– (040) | - | - | - | + | + | + | - | + |
| d rw- (060) | r– (040) | - | - | - | - | - | + | - | - |
| d rwx (070) | r– (040) | + | + | - | + | + | + | + | + |
| d (000) | r-x (050) | - | - | - | - | - | - | - | - |
| d –x (010) | r-x (050) | - | - | - | + | + | - | - | + |
| d -w- (020) | r-x (050) | - | - | - | - | - | - | - | - |
| d -wx (030) | r-x (050) | + | + | - | + | + | - | + | + |
| d r– (040) | r-x (050) | - | - | - | - | - | + | - | - |
| d r-x (050) | r-x (050) | - | - | - | + | + | + | - | + |
| d rw- (060) | r-x (050) | - | - | - | - | - | + | - | - |
| d rwx (070) | r-x (050) | + | + | - | + | + | + | + | + |
| d (000) | rw- (060) | - | - | - | - | - | - | - | - |
| d –x (010) | rw- (060) | - | - | + | + | + | - | - | + |
| d -w- (020) | rw- (060) | - | - | - | - | - | - | - | - |
| d -wx (030) | rw- (060) | + | + | + | + | + | - | + | + |
| d r– (040) | rw- (060) | - | - | - | - | - | + | - | - |
| d r-x (050) | rw- (060) | - | - | + | + | + | + | - | + |
| d rw- (060) | rw- (060) | - | - | - | - | - | + | - | - |
| d rwx (070) | rw- (060) | + | + | + | + | + | + | + | + |
| d (000) | rwx (070) | - | - | - | - | - | - | - | - |
| d –x (010) | rwx (070) | - | - | + | + | + | - | - | + |
| d -w- (020) | rwx (070) | - | - | - | - | - | - | - | - |
| d -wx (030) | rwx (070) | + | + | + | + | + | - | + | + |
| d r– (040) | rwx (070) | - | - | - | - | - | + | - | - |
| d r-x (050) | rwx (070) | - | - | + | + | + | + | - | + |
| d rw- (060) | rwx (070) | - | - | - | - | - | + | - | - |
| d rwx (070) | rwx (070) | + | + | + | + | + | + | + | + |

На основании этой таблицы создадим другую, в которой опишем минимальные требования на права и директорию для выполнения тех или иных действий. Внесём проанализированные данные в таблицу.

*Минимальные права для совершения операций*

|  |  |  |
| --- | --- | --- |
| Операция | Минимальные права на директорию | Минимальные права на файл |
| Создание файла | d -wx (030) | — (000) |
| Удаление файла | d -wx (030) | — (000) |
| Чтение файла | d –x (010) | – (040) |
| Запись в файл | d –x (010) | - (020) |
| Переименование файла | d -wx (030) | — (000) |
| Создание поддиректории | d -wx (030) | — (000) |
| Удаление поддиректории | d -wx (030) | — (000) |

# **4 Выводы**

Во время выполнения этой лабораторной работы я приобрел практические навыки работы с атрибутами файлов для групп пользователей в консоли.

# **5 Список Литературы**

1. Права доступа к файлам в Linux [Электронный ресурс]. 2019. URL: https: //losst.ru/prava-dostupa-k-fajlam-v-linux.