**Лабораторная работа N° 2**

Информационная безопасность

Леон Фернандо Хосе Фернандо | НПМбд02-20

Содержание

[1Цель работы 2](#_Toc145794353)

[2 Теоретическое введение 2](#_Toc145794354)

[3 Выполнение лабораторной работы 3](#_Toc145794355)

[4 Выводы 9](#_Toc145794356)

[5 Список Литературы 10](#_Toc145794357)

# **1 Цель работы**

Приобретение практического опыта в управлении атрибутами файлов с помощью консоли, а также углубление теоретического понимания дискреционного контроля доступа в современных системах с открытым исходным кодом, особенно в тех, которые построены на операционной системе Linux.

# **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**

В ранее проведенной лабораторной работе операционная система установила учетную запись пользователя для "guest" с помощью команды "sudo useradd guest" и установила пароль для этого пользователя с помощью команды "sudo passwd guest".

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Вошел в систему от имени пользователя ‘guest’

Изображение выглядит как текст, снимок экрана, программное обеспечение, Операционная система

Автоматически созданное описание

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

Автоматически созданное описание

Используя команду "pwd", я определил, что нахожусь в каталоге /home/guest, который также является моим домашним каталогом. Это соответствует командной строке.

Я подтвердил свое имя пользователя с помощью команды "whoami" и получил вывод: ‘guest’.

С помощью команды "id" я идентифицировал свое имя пользователя как "гость" с uid = 1001 (гость) и gid = 1001 (гость). Затем я сравнил эту информацию с выводом команды "группы", которая отображала "гость". Мой пользователь принадлежит только к одной группе, которая состоит из самого пользователя, поэтому выходные данные команд "id" и "groups" совпадают. Данные, отображаемые в командной строке, совпадают с полученной информацией.

Затем я просмотрел файл /etc/passwd, используя команду "cat /etc/passwd".

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Я нашел свою учетную запись пользователя в самом конце файла /etc/passwd. uid равен 1001, а gid равен 1001, что соответствует информации, которую мы получили ранее.

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

Автоматически созданное описание

Я просмотрел каталоги в системе, используя команду "ls -l /home/". Мне удалось получить список подкаталогов в каталоге /home. Эти каталоги имеют разрешения на чтение, запись и выполнение, установленные для пользователя (для группы и других пользователей разрешения на доступ не установлены).

Я также проверил наличие расширенных атрибутов, установленных в подкаталогах, расположенных в каталоге /home, используя команду "lsattr /home". Я мог наблюдать только расширенные атрибуты в каталоге, связанном с учетной записью пользователя, которую я в данный момент использую в системе.

Я создал подкаталог с именем "dir1" в моем домашнем каталоге, используя команду "mkdir dir1". Затем я проверил установленные на нем права доступа и расширенные атрибуты. Разрешения следующие: чтение, запись и выполнение доступны для пользователя и группы, в то время как для других предоставляются только разрешения на чтение и выполнение. Для этого каталога не заданы расширенные атрибуты.

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

Автоматически созданное описание

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, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

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

Автоматически созданное описание

Заполним таблицу «Установленные права и разрешённые действия» 3.1.

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

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

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

Чтение файла: “cat /home/guest/dir1/file1”

Смена директории: “cd dir1”

Просмотр файлов в директории: “ls dir1”

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

Смена атрибутов файла: “chattr -a /home/guest/dir1/file1”

В случае успеха будет записывать +, в случае ошибки доступа будем записывать -. Соберём данные в таблицу 1.

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 (100) | (000) | - | - | - | - | + | - | - | - |
| d -w- (200) | (000) | - | - | - | - | - | - | - | - |
| d -wx (300) | (000) | + | + | - | - | + | - | + | - |
| d r– (400) | (000) | - | - | - | - | - | + | - | - |
| d r-x (500) | (000) | - | - | - | - | + | + | - | - |
| d rw- (600) | (000) | - | - | - | - | - | + | - | - |
| d rwx (700) | (000) | + | + | - | - | + | + | + | - |
| d (000) | –x (100) | - | - | - | - | - | - | - | - |
| d –x (100) | –x (100) | - | - | - | - | + | - | - | - |
| d -w- (200) | –x (100) | - | - | - | - | - | - | - | - |
| d -wx (300) | –x (100) | + | + | - | - | + | - | + | - |
| d r– (400) | –x (100) | - | - | - | - | - | + | - | - |
| d r-x (500) | –x (100) | - | - | - | - | + | + | - | - |
| d rw- (600) | –x (100) | - | - | - | - | - | + | - | - |
| d rwx (700) | –x (100) | + | + | - | - | + | + | + | - |
| d (000) | -w- (200) | - | - | - | - | - | - | - | - |
| d –x (100) | -w- (200) | - | - | + | - | + | - | - | - |
| d -w- (200) | -w- (200) | - | - | - | - | - | - | - | - |
| d -wx (300) | -w- (200) | + | + | + | - | + | - | + | - |
| d r– (400) | -w- (200) | - | - | - | - | - | + | - | - |
| d r-x (500) | -w- (200) | - | - | + | - | + | + | - | - |
| d rw- (600) | -w- (200) | - | - | - | - | - | + | - | - |
| d rwx (700) | -w- (200) | + | + | + | - | + | + | + | - |
| d (000) | -wx (300) | - | - | - | - | - | - | - | - |
| d –x (100) | -wx (300) | - | - | + | - | + | - | - | - |
| d -w- (200) | -wx (300) | - | - | - | - | - | - | - | - |
| d -wx (300) | -wx (300) | + | + | + | - | + | - | + | - |
| d r– (400) | -wx (300) | - | - | - | - | - | + | - | - |
| d r-x (500) | -wx (300) | - | - | + | - | + | + | - | - |
| d rw- (600) | -wx (300) | - | - | - | - | - | + | - | - |
| d rwx (700) | -wx (300) | + | + | + | - | + | + | + | - |
| d (000) | r– (400) | - | - | - | - | - | - | - | - |
| d –x (100) | r– (400) | - | - | - | + | + | - | - | + |
| d -w- (200) | r– (400) | - | - | - | - | - | - | - | - |
| d -wx (300) | r– (400) | + | + | - | + | + | - | + | + |
| d r– (400) | r– (400) | - | - | - | - | - | + | - | - |
| d r-x (500) | r– (400) | - | - | - | + | + | + | - | + |
| d rw- (600) | r– (400) | - | - | - | - | - | + | - | - |
| d rwx (700) | r– (400) | + | + | - | + | + | + | + | + |
| d (000) | r-x (500) | - | - | - | - | - | - | - | - |
| d –x (100) | r-x (500) | - | - | - | + | + | - | - | + |
| d -w- (200) | r-x (500) | - | - | - | - | - | - | - | - |
| d -wx (300) | r-x (500) | + | + | - | + | + | - | + | + |
| d r– (400) | r-x (500) | - | - | - | - | - | + | - | - |
| d r-x (500) | r-x (500) | - | - | - | + | + | + | - | + |
| d rw- (600) | r-x (500) | - | - | - | - | - | + | - | - |
| d rwx (700) | r-x (500) | + | + | - | + | + | + | + | + |
| d (000) | rw- (600) | - | - | - | - | - | - | - | - |
| d –x (100) | rw- (600) | - | - | + | + | + | - | - | + |
| d -w- (200) | rw- (600) | - | - | - | - | - | - | - | - |
| d -wx (300) | rw- (600) | + | + | + | + | + | - | + | + |
| d r– (400) | rw- (600) | - | - | - | - | - | + | - | - |
| d r-x (500) | rw- (600) | - | - | + | + | + | + | - | + |
| d rw- (600) | rw- (600) | - | - | - | - | - | + | - | - |
| d rwx (700) | rw- (600) | + | + | + | + | + | + | + | + |
| d (000) | rwx (700) | - | - | - | - | - | - | - | - |
| d –x (100) | rwx (700) | - | - | + | + | + | - | - | + |
| d -w- (200) | rwx (700) | - | - | - | - | - | - | - | - |
| d -wx (300) | rwx (700) | + | + | + | + | + | - | + | + |
| d r– (400) | rwx (700) | - | - | - | - | - | + | - | - |
| d r-x (500) | rwx (700) | - | - | + | + | + | + | - | + |
| d rw- (600) | rwx (700) | - | - | - | - | - | + | - | - |
| d rwx (700) | rwx (700) | + | + | + | + | + | + | + | + |

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 (300) | — (000) |
| Удаление файла | d -wx (300) | — (000) |
| Чтение файла | d –x (100) | r– (400) |
| Запись в файл | d –x (100) | -w- (200) |
| Переименование файла | d -wx (300) | — (000) |
| Создание поддиректории | d -wx (300) | — (000) |
| Удаление поддиректории | d -wx (300) | — (000) |

# **4 Выводы**

В ходе этой лабораторной работы я приобрел практические навыки работы с атрибутами файлов в консоли. Я также укрепил свое теоретическое понимание дискреционного контроля доступа в современных системах с открытым исходным кодом, основанных на операционной системе Linux.

# **5 Список Литературы**

1. Права доступа к файлам в Linux [Электронный ресурс]. 2019. URL: https: //losst.ru/prava-dostupa-k-fajlam-v-linux.
2. Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006
3. Практические аспекты сетевой безопасности. Сетевая безопасность. Межсетевые экраны. (В. Иванов, МГУ)