Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя.

Пономарева Лилия Михайловна

Содержание

# Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей[[1]](#список-литературы).

# 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 к объектам, которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ, которые работают от лица псевдопользовательских учетных записей.

В рамках дискреционного разграничения доступа каждому файлу назначен пользователь-владелец и группа-владелец файла.

В метаданных каждого объекта содержится список разрешений на доступ к нему для разных категорий субъектов.

Атрибуты Minimal ACL поддерживают три базовых класса субъектов доступа к файлу (класс All объединяет все три класса):

User access (u) – доступ для владельца файла;  
Group access (g) – доступ для группы, владеющей файлом;  
Other access (o) – доступ для остальных пользователей (кроме пользователя root);  
All access (a) – доступ для всех субъектов доступа (u, g, o).

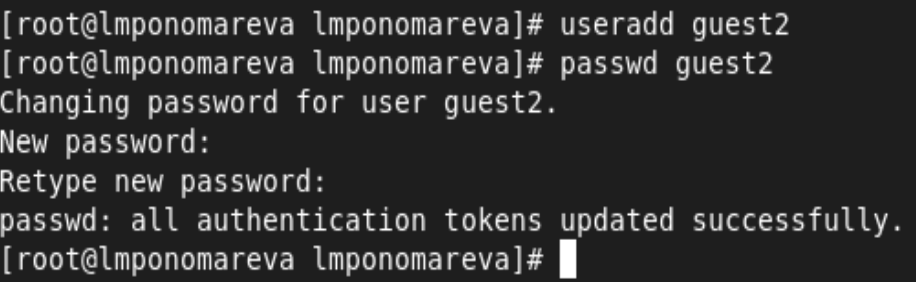
Для каждого из этих классов определены три типа разрешений:  
На чтение содержимого файла (read) – символ «r».  
На запись внутри файла или изменения его содержимого (write) – символ «w».  
На исполнение файла (если это бинарный исполняемый файл или файл сценария интерпретатора (execute)) – символ «x».

Для директорий трактовка типов разрешений иная:  
r – разрешение на «открытие» директории, то есть на чтение списка файлов, которые содержит эта директория.  
w – разрешение на модификацию этого списка файлов (создание/удаление/переименование/перемещение) файлов этой директории.  
x – разрешение на «исполнение» директории, то есть на возможность перейти в нее.

Чтобы изменить расширения для определенного файла используется команда chmod с соответствующими аргументами.

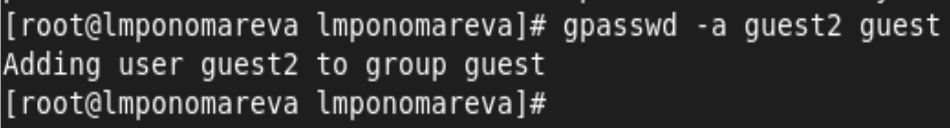
# Выполнение лабораторной работы

1. Создала учётную запись пользователя guest2, используя учётную запись администратора([рис. 1](../../image/1.png))  
   useradd guest2  
   passwd guest



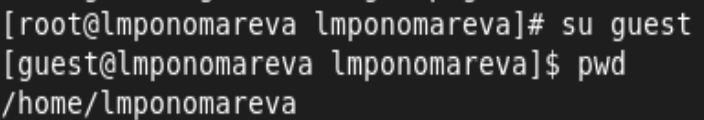
Создание нового пользователя

1. Добавила пользователя guest2 в группу guest([рис. 2](../../image/2.png))  
   gpasswd -a guest2 guest

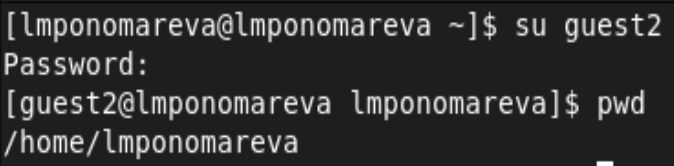


Добавления пользователя в группу

1. Вошла в систему от двух пользователей на двух разных консолях и командой pwd определила директорию, в которой нахожусь([рис. 3](../../image/3.png) и [рис. 4](../../image/4.png))



Пользователь guest



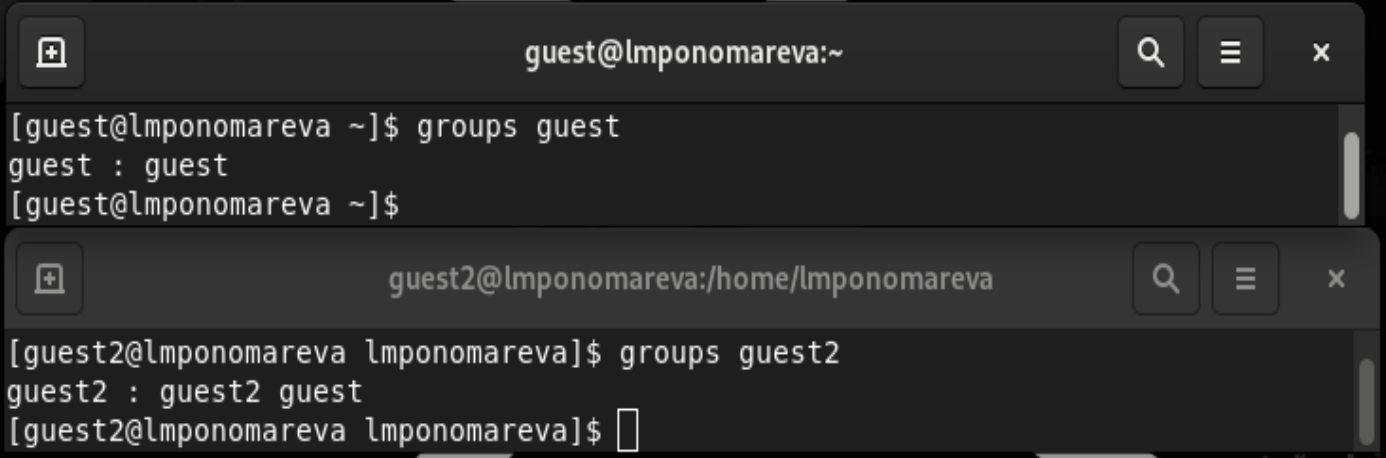
Пользователь guest2

1. Уточнила имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам([рис. 5](../../image/5.png))



Имя, группа пользователя

Определила командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2([рис. 6](../../image/6.png))



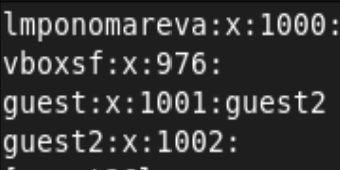
Имя, группа пользователя

Сравнила вывод команды groups с выводом команд id -Gn и id -G([рис. 7](../../image/7.png))



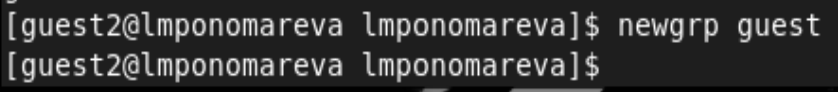
Команда id -Gn и id -G

1. Сравнила полученную информацию с содержимым файла /etc/group([рис. 8](../../image/8.png))



Файл /etc/group

1. От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest командой newgrp guest([рис. 9](../../image/9.png))



Регистрация пользователя в группе

1. От имени пользователя guest изменила права директории /home/guest, разрешив все действия для пользователей группы: chmod g+rwx /home/guest([рис. 10](../../image/10.png))

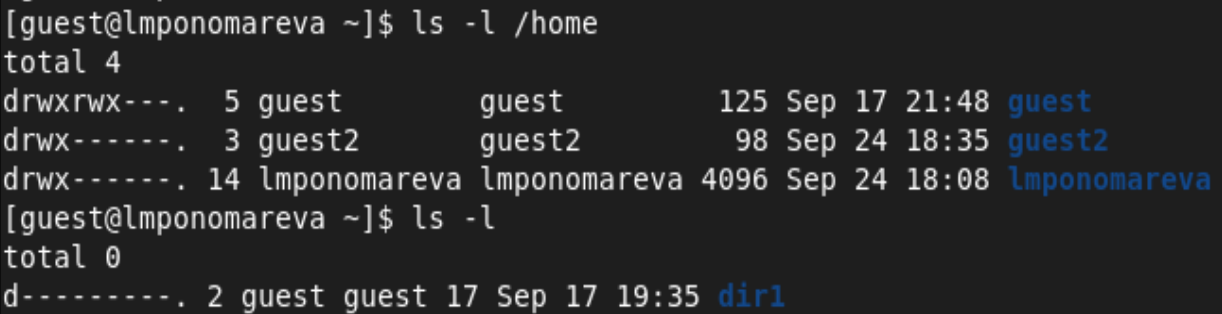
Изменение прав директории /home/guest

Изменение прав директории /home/guest

1. От имени пользователя guest сняла с директории /home/guest/dir1 все атрибуты командой chmod 000 dirl([рис. 11](../../image/11.png)), и проверила правильность снятия атрибутов([рис. 12](../../image/12.png))

Снятие атрибутов с директории /home/guest/dir1

Снятие атрибутов с директории /home/guest/dir1



Проверка значений атрибутов

Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнила табл. 1, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».

Установленные права и разрешённые действия для групп

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение из файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d--- | ---- | - | - | - | - | - | - | - | - |
| d--x | ---- | - | - | - | - | + | - | - | - |
| d-w- | ---- | - | - | - | - | - | - | - | - |
| d-wx | ---- | + | + | - | - | + | - | + | - |
| dr-- | ---- | - | - | - | - | - | + | - | - |
| dr-x | ---- | - | - | - | - | + | + | - | - |
| drw- | ---- | - | - | - | - | - | + | - | - |
| drwx | ---- | + | + | - | - | + | + | + | - |
| d--- | ---x | - | - | - | - | - | - | - | - |
| d--x | ---x | - | - | - | - | + | - | - | - |
| d-w- | ---x | - | - | - | - | - | - | - | - |
| d-wx | ---x | + | + | - | - | + | - | + | - |
| dr-- | ---x | - | - | - | - | - | + | - | - |
| dr-x | ---x | - | - | - | - | + | + | - | - |
| drw- | ---x | - | - | - | - | - | + | - | - |
| drwx | ---x | + | + | - | - | + | + | + | - |
| d--- | --w- | - | - | - | - | - | - | - | - |
| d--x | --w- | - | - | + | - | + | - | - | - |
| d-w- | --w- | - | - | - | - | - | - | - | - |
| d-wx | --w- | + | + | + | - | + | - | + | - |
| dr-- | --w- | - | - | - | - | - | + | - | - |
| dr-x | --w- | - | - | + | - | + | + | - | - |
| drw- | --w- | - | - | - | - | - | + | - | - |
| drwx | --w- | + | + | + | - | + | + | + | - |
| d--- | --wx | - | - | - | - | - | - | - | - |
| d--x | --wx | - | - | + | - | + | - | - | - |
| d-w- | --wx | - | - | - | - | - | - | - | - |
| d-wx | --wx | + | + | + | - | + | - | + | - |
| dr-- | --wx | - | - | - | - | - | + | - | - |
| dr-x | --wx | - | - | + | - | + | + | - | - |
| drw- | --wx | - | - | - | - | - | + | - | - |
| drwx | --wx | + | + | + | - | + | + | + | - |
| d--- | -r-- | - | - | - | - | - | - | - | - |
| d--x | -r-- | - | - | - | + | + | - | - | - |
| d-w- | -r-- | - | - | - | - | - | - | - | - |
| d-wx | -r-- | + | + | - | + | + | - | + | - |
| dr-- | -r-- | - | - | - | - | - | + | - | - |
| dr-x | -r-- | - | - | - | + | + | + | - | - |
| drw- | -r-- | - | - | - | - | - | + | - | - |
| drwx | -r-- | + | + | - | + | + | + | + | - |
| d--- | -r-x | - | - | - | - | - | - | - | - |
| d--x | -r-x | - | - | - | + | + | - | - | - |
| d-w- | -r-x | - | - | - | - | - | - | - | - |
| d-wx | -r-x | + | + | - | + | + | - | + | - |
| dr-- | -r-x | - | - | - | - | - | + | - | - |
| dr-x | -r-x | - | - | - | + | + | + | - | - |
| drw- | -r-x | - | - | - | - | - | + | - | - |
| drwx | -r-x | + | + | - | + | + | + | + | - |
| d--- | -rw- | - | - | - | - | - | - | - | - |
| d--x | -rw- | - | - | + | + | + | - | - | - |
| d-w- | -rw- | - | - | - | - | - | - | - | - |
| d-wx | -rw- | + | + | + | + | + | - | + | - |
| dr-- | -rw- | - | - | - | - | - | + | - | - |
| dr-x | -rw- | - | - | + | + | + | + | - | - |
| drw- | -rw- | - | - | - | - | - | + | - | - |
| drwx | -rw- | + | + | + | + | + | + | + | - |
| d--- | -rwx | - | - | - | - | - | - | - | - |
| d--x | -rwx | - | - | + | + | + | - | - | - |
| d-w- | -rwx | - | - | - | - | - | - | - | - |
| d-wx | -rwx | + | + | + | + | + | - | + | - |
| dr-- | -rwx | - | - | - | - | - | + | - | - |
| dr-x | -rwx | - | - | + | + | + | + | - | - |
| drw- | -rwx | - | - | - | - | - | + | - | - |
| drwx | -rwx | + | + | + | + | + | + | + | - |

1. На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнила табл. 2

Минимальные права для совершения операций от имени пользователей входящих в группу

| Операция | Права на директорию | Права на файл |
| --- | --- | --- |
| Создание файла | d-wx | --- |
| Удаление файла | d-wx | --- |
| Чтение файла | d--x | r-- |
| Запись в файл | d--x | -w- |
| Переименование файла | d-wx | --- |
| Создание поддиректории | d-wx | --- |
| Удаление поддиректории | d-wx | --- |

# Выводы

Получили навыки работы в консоли с атрибутами файлов для групп пользователей.

# Список литературы

1. [Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3](https://search.rsl.ru/ru/record/01000682756).