Лабораторнаяработа No 3

Дискреционное разграничение прав в Linux. Два пользователя

Белкина Анастасия Михайловна

Содержание

[Цель работы 1](#_Toc85047300)

[Задание 1](#_Toc85047301)

[Теоретическое введение 2](#_Toc85047302)

[Выполнение лабораторной работы 3](#_Toc85047303)

[Выводы 4](#_Toc85047304)

# Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

# Задание

1. Добавить пользователя guest2
2. Создать пароль для пользователя guest2
3. Добавить guest2 в группу guest
4. Опытным путём заполнить таблицу “Установленные права и разрешённые действия”
5. На основании заполненной таблицы определить те или иные минимально необходимые права для выполнения операций внутри директории

# Теоретическое введение

В операционной системе Linux есть много отличных функций безопасности, но она из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо.

И это очень важно, потому что локальный доступ к файлам для всех программ и всех пользователей позволил бы вирусам без проблем уничтожить систему. Но новым пользователям могут показаться очень сложными новые права на файлы в linux, которые очень сильно отличаются от того, что мы привыкли видеть в Windows. В этой статье мы попытаемся разобраться в том как работают права файлов в linux, а также как их изменять и устанавливать.

Изначально каждый файл имел три параметра доступа. Вот они:

Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;

Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги;

Выполнение - вы не можете выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу.

Но все эти права были бы бессмысленными, если бы применялись сразу для всех пользователей. Поэтому каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение. Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу. Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла. Именно с помощью этих наборов полномочий устанавливаются права файлов в linux. Каждый пользователь может получить полный доступ только к файлам, владельцем которых он является или к тем, доступ к которым ему разрешен. Только пользователь Root может работать со всеми файлами независимо от их набора их полномочий.

Но со временем такой системы стало не хватать и было добавлено еще несколько флагов, которые позволяют делать файлы не изменяемыми или же выполнять от имени суперпользователя

# Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя guest (использую учётную запись администратора): useradd guest

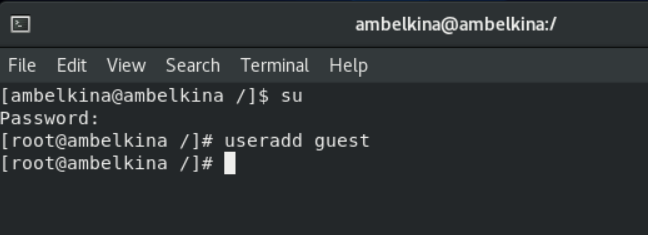


Рис.1 Создался юзер guest

1. Задала пароль для пользователя guest (используя учётную запись администратора): passwd guest

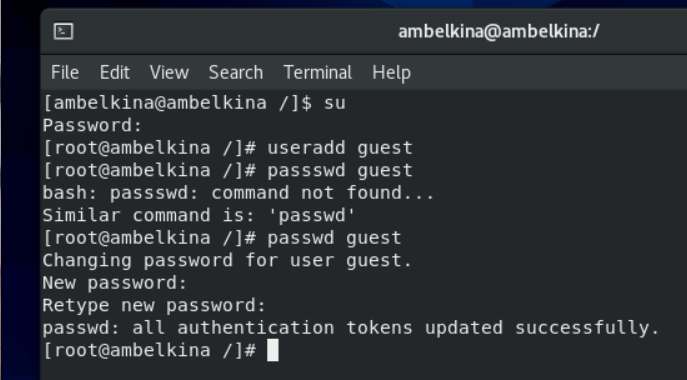


Рис.2 Задала пароль

1. Аналогично создала второго пользователя guest2.

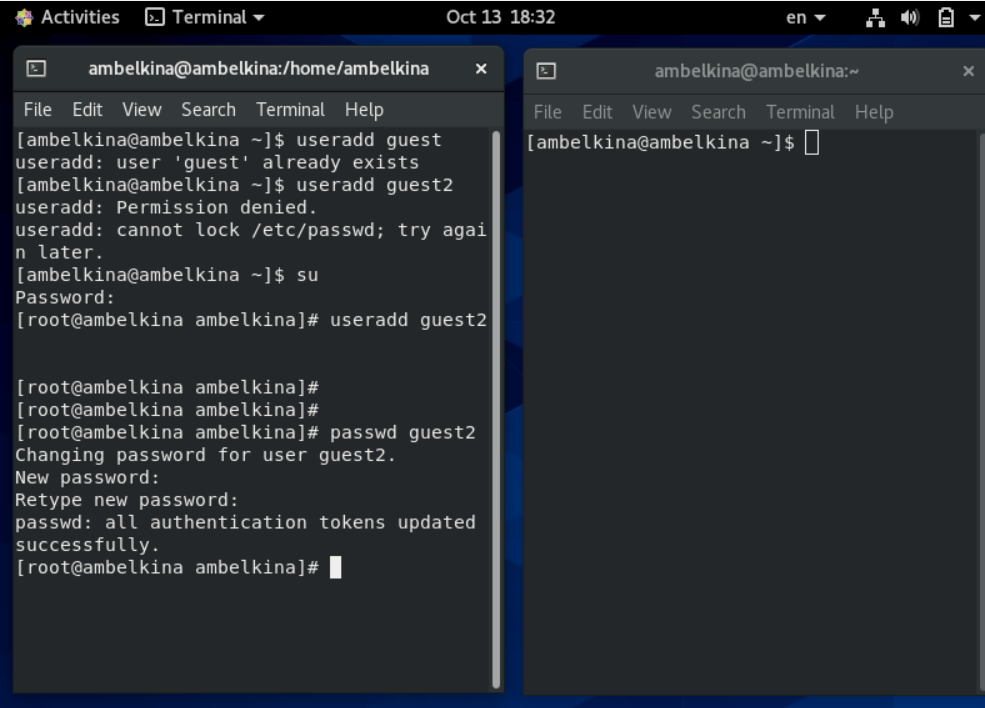


Рис.3 Создался второй юзер

1. Добавила пользователя guest2 в группу guest: gpasswd -a guest2 guest

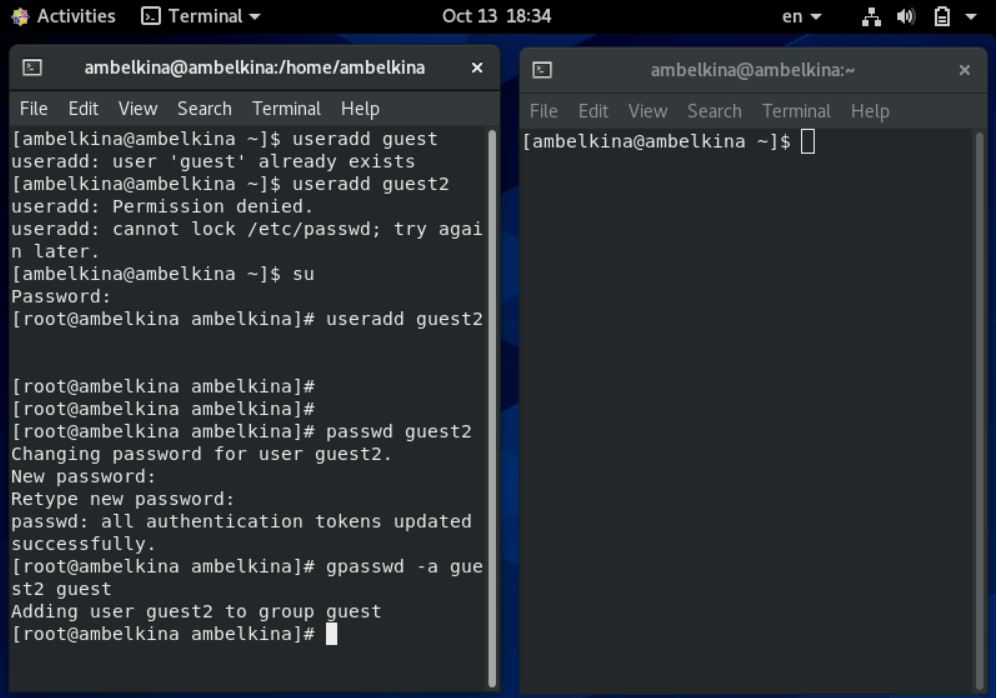


Рис.4 Добавение в группу

1. Осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли.

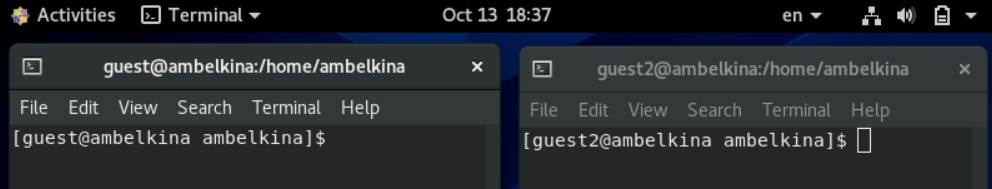


Рис.5 Две консоли

1. Для обоих пользователей командой pwd определила директорию, в которой нахожусь.

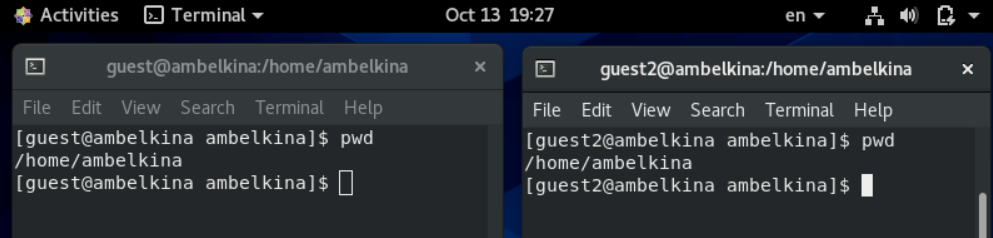


Рис.6 Определенные директории

1. Уточнила имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определила командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравнила вывод команды groups с выводом команд id -Gn и id -G.

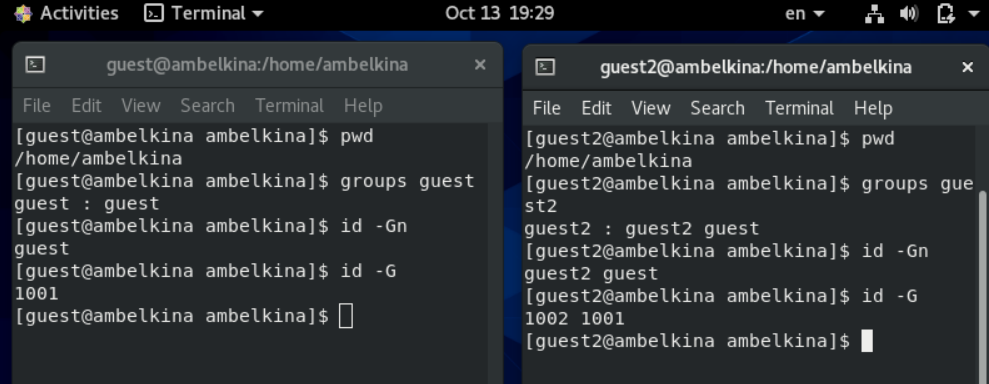


Рис.7 Имена пользователей и группы

1. Сравнила полученную информацию с содержимым файла /etc/group. Просмотрела файл командой cat /etc/group

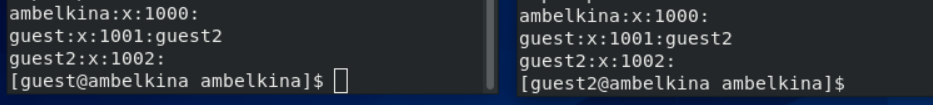


Рис.8 Данные из файла etc/passwd

1. От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest командой newgrp guest

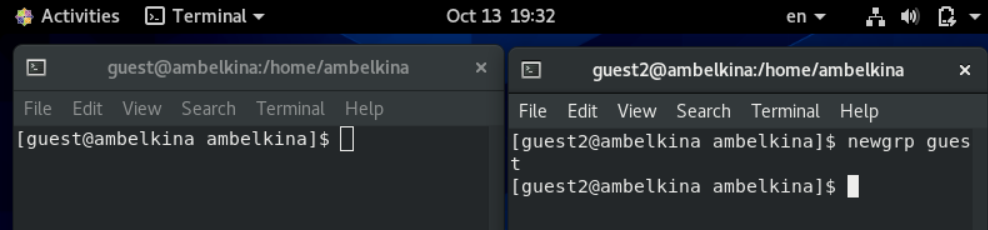


Рис.9 Заререстрирован пользователь

1. От имени пользователя guest изменила права директории /home/guest, разрешив все действия для пользователей группы: chmod g+rwx /home/guest

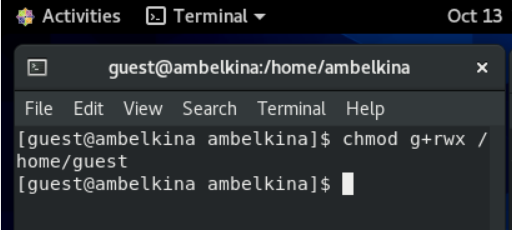


Рис.10 Измененные права директории

1. От имени пользователя guest сняла с директории /home/guest/dir1 все атрибуты командой chmod 000 dirl и проверила правильность снятия атрибутов.

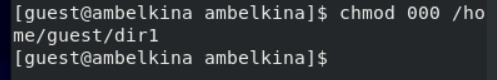
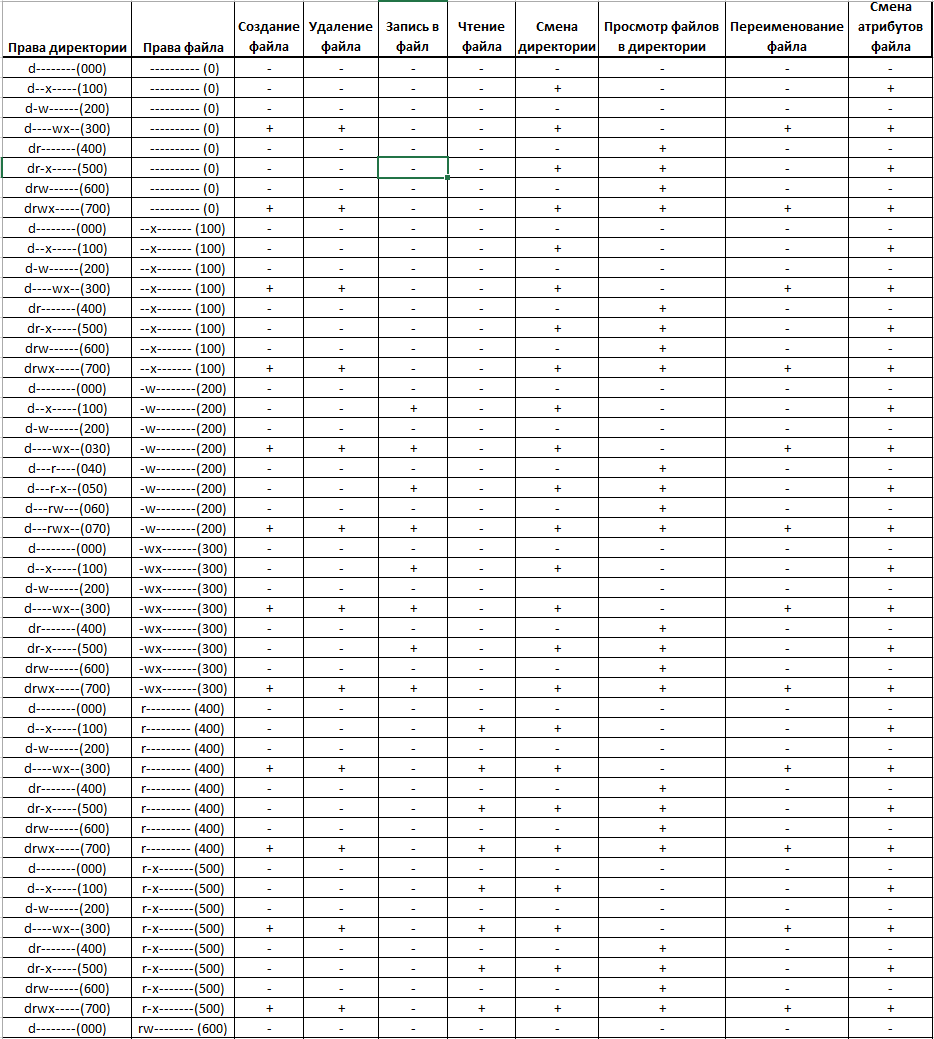


Рис.11 Снятые права

1. Заполнила таблицу «Установленные права и разрешённые действия», выполняя действия от имени от имени пользователя guest и делая проверку от пользователя guest2, определив опытным путём, какие операции разрешены, а какие нет.



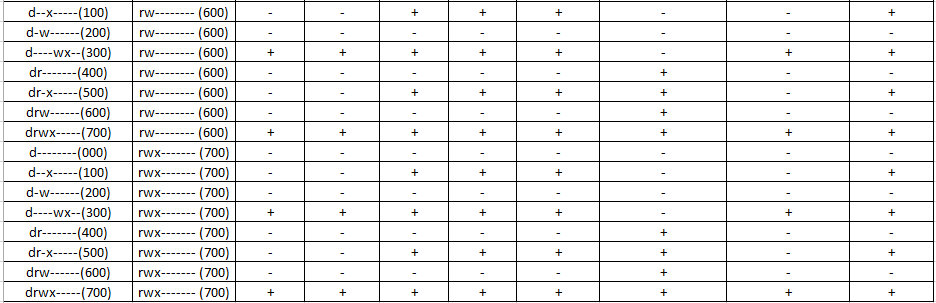


Табл.1 Установленные права и разрешённые действия

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

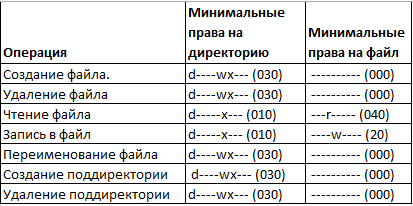


Табл.2 Минимально необходимые права

# Выводы

Получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.