Основы информационной безопасности

Лабораторная работа № 3. Дискреционное разграничение прав в Linux. Два пользователя

Подлесный Иван Сергеевич

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

В установленной операционной системе создайте учётную запись пользователя guest(рис. fig. 1)

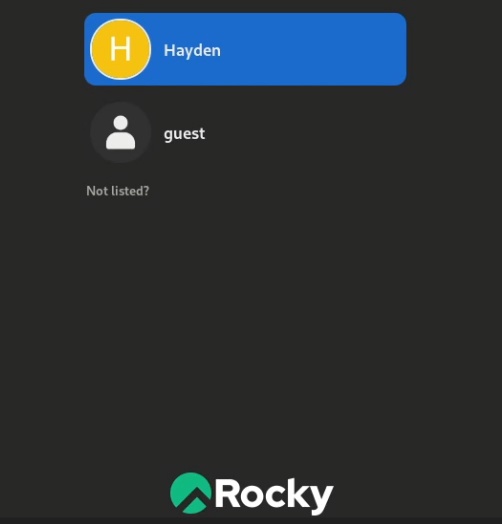


Рис. 1: первый пункт был выполнен еще в Лабораторной Работе №2

В установленной при выполнении предыдущей лабораторной работы ОС создадим учетную запись ползователя guest2 и добавляем его в группу guest(рис. fig. 2)

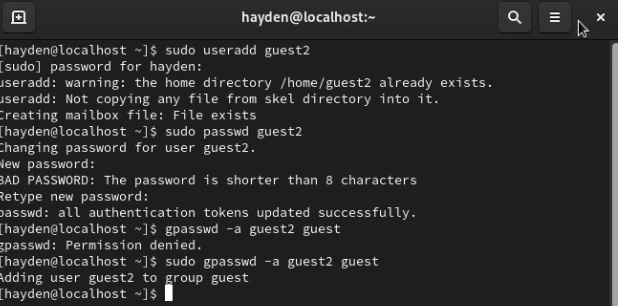


Рис. 2: Создание нового пользователся guest2 и добавление его в группу guest

Осуществим вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. Для обоих пользователей командой pwd определим директорию, в которой находимся, увидим, что она совпадает с приглашениями командной строки. Уточните имя нашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определим командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Увидим, что guest принадлежит одной группе guet c ig 2001, а двум группам guest и guest2 с id 1001 и 1002. С помощью команд id -Gn и id -G можно увидеть только id существующиз групп и название соответственно(рис. fig. 3)

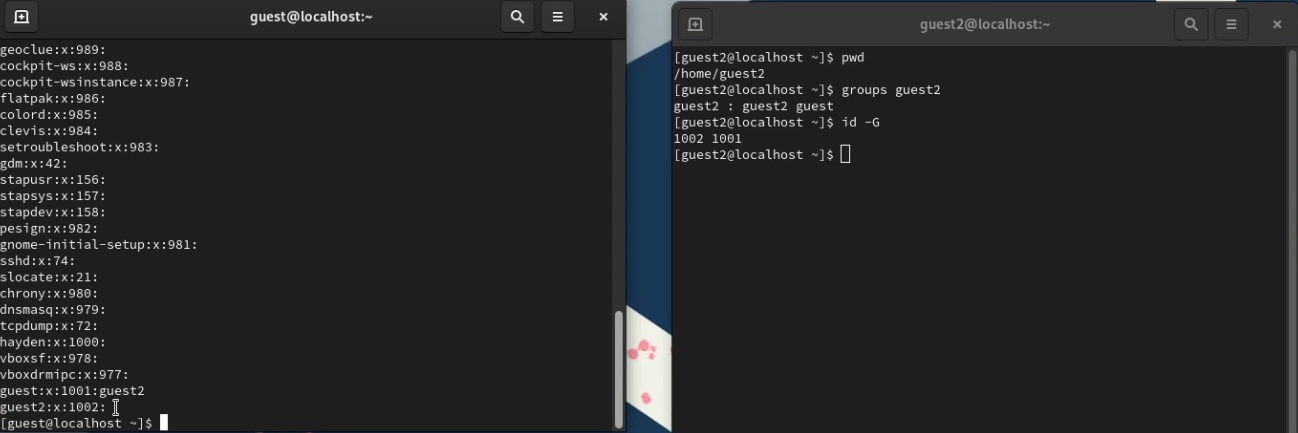


Рис. 3: Просмотр информации о группах пользователей

Посмотрев информацию о группа этих пользователей в файле /etc/group получим аналогичную информацию(рис. fig. 4)

От имени пользователя guest2 выполните регистрацию пользователя guest2 в группе guest командой newgrp guest.

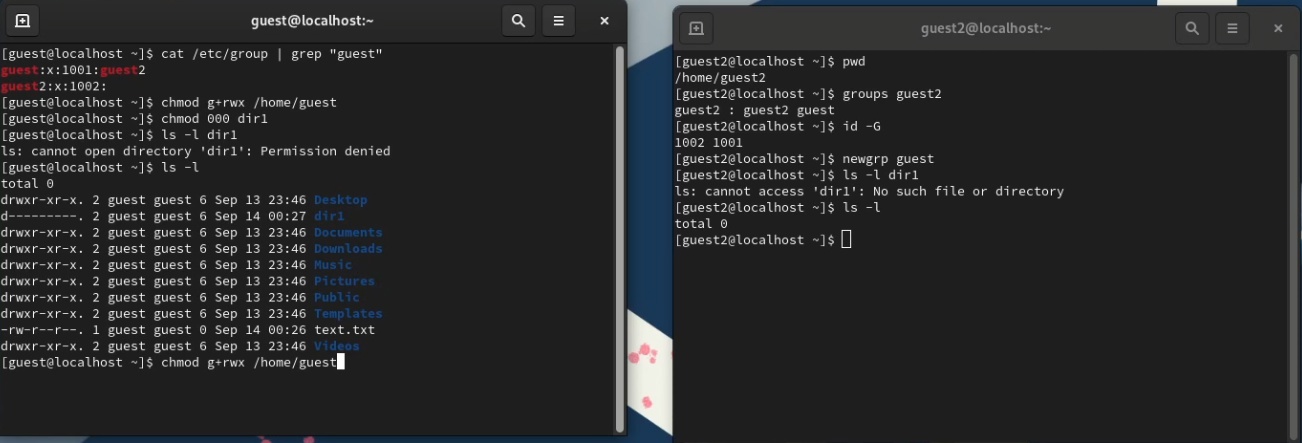


Рис. 4: Просмотр информации о группах пользователей в файле /etc/group

От имени пользователя guest изменим права директории /home/guest, разрешив все действия для пользователей группы и снимем с директории /home/guest/dir1 все атрибуты, затем проверим правильность атрибутов(рис. fig. 5).

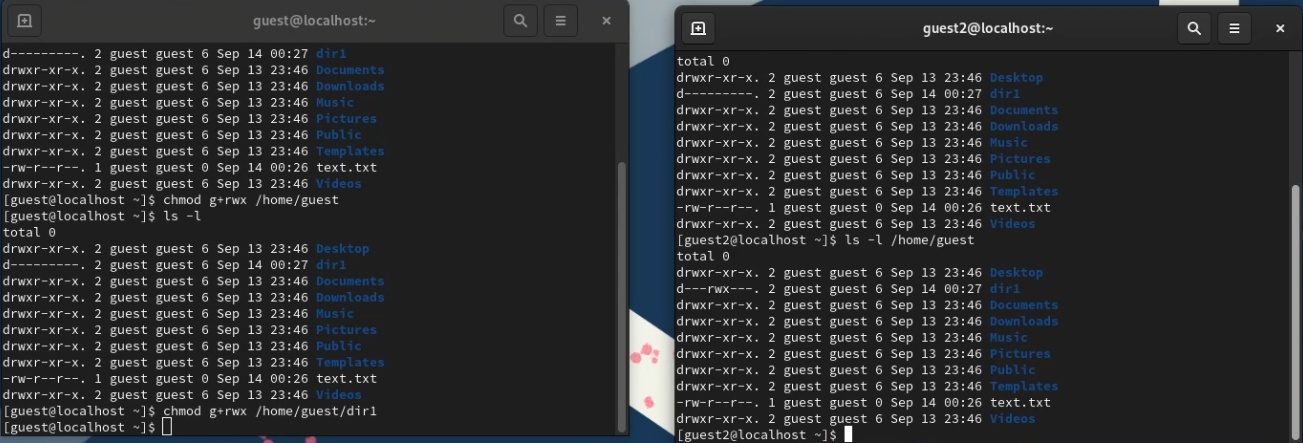


Рис. 5: Изменение прав доступа

В таблице приведены данные о том, какие операции разрешены, а какие нет для владельца данных.

Минимальные права для совершения операций

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

При сравнении с таблицей в лабораторной работе №2 можно увидеть, что отличие состоит только в том, что не владелец файла никогда не имеет прав на изменение его атрибутов. Менять права доступа (записывать в inode) может владелец файла или администратор. Члены группы файла никаких особых прав на inode не имеют. Пользователь может отобрать у себя собственные права на чтение и запись в файл, но право на запись в inode (в т.ч. право на смену прав) сохраняется у владельца файла при любых обстоятельствах. Пользователь не может передать право собственности на файл другому пользователю и не может забрать право собственности на файл у другого пользователя.

# 3 Выводы

В результате выполнения работы были приобретены практические навыки работы в консоли с атрибутами файлов для групп пользователей.