Лабораторная работа № 3

Дискреционноеразграничение прав в Linux. Два пользователя

Аксёнова Алина Владимировна

Содержание

# Цель работы

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

# Задание

Закрепить дискреционное разграничение прав для групп в Linux.

# Теоретическое введение

Linux в целом и Ubuntu в частности - системы многопользовательские, т.е. на одном компьютере может быть несколько различных пользователей, каждый со своими собственными настройками, данными и правами доступа к различным системным функциям.Кроме пользователей в Linux для разграничения прав существуют группы. Каждая группа так же как и отдельный пользователь обладает неким набором прав доступа к различным компонентам системы и каждый пользователь-член этой группы автоматически получает все права группы. То есть группы нужны для группировки пользователей по принципу одинаковых полномочий на какие-либо действия, вот такая тавтология. Каждый пользователь может состоять в неограниченном количестве групп и в каждой группе может быть сколько угодно пользователей1). Один из подходов к разграничению доступа — так называемый дискреционный - предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют. Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. Чтобы получить доступ к файлам в Linux, используются разрешения. Эти разрешения назначаются трем объектам: файлу, группе и другому объекту. Для управления правами используется команда chmod. При использовании chmod в относительном режиме вы работаете с тремя индикаторами, чтобы указать, что вы хотите сделать. Сначала вы указываете, для кого вы хотите изменить разрешения. Для этого вы можете выбрать между пользователем (u), группой (g) и другими (o). Затем вы используете оператор для добавления или удаления разрешений из текущего режима или устанавливаете их абсолютно. В конце вы используете r(read), w(write) и x(execute), чтобы указать, какие разрешения вы хотите установить.При использовании chmod вы можете устанавливать разрешения для пользователя (user), группы (group) и других (other).Помимо основных разрешений, о которых вы только что прочитали, в Linux также есть набор расширенных разрешений. Это не те разрешения, которые вы устанавливаете по умолчанию, но иногда они предоставляют полезное дополнение.

# Ход работы

1. Заходим под учётной записью пользователя guest, созданной при выполнении предыдущей лабораторной работы (Рис. 1).

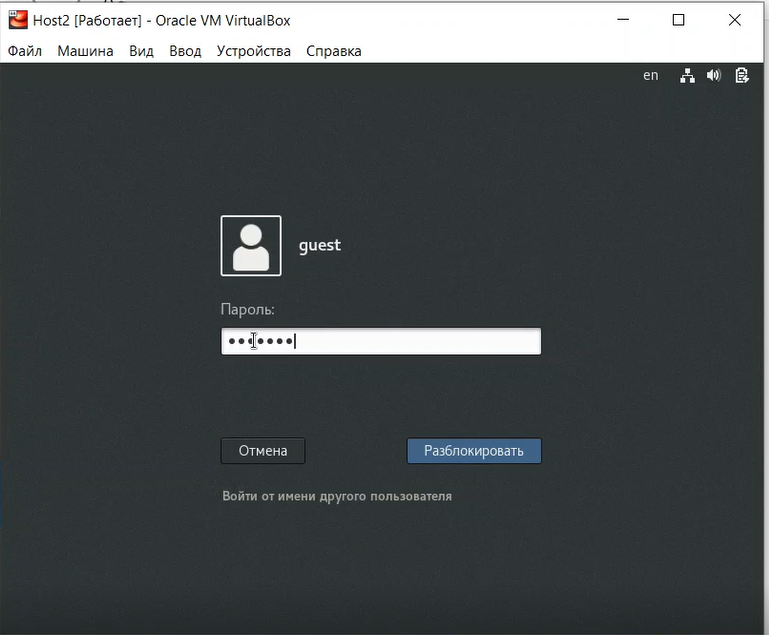


Figure 1: Вход в систему

1. Аналогично создаем второго пользователя guest2 (использую учётную запись администратора) и задаем пароль. (Рис. 2).

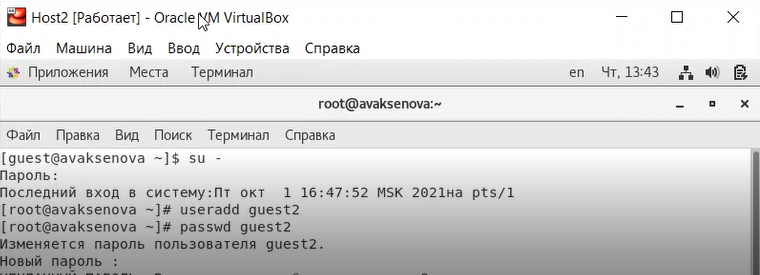


Figure 2: Пароль для новой учетной записи

1. Добавляем пользователя guest2 в группу guest. (Рис. 3).

Figure 3: Добаление в группу

Figure 3: Добаление в группу

1. Осуществляем вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли и.Для обоих пользователей командой pwd определяем директорию, в которой мы находимся. (Рис. 4).

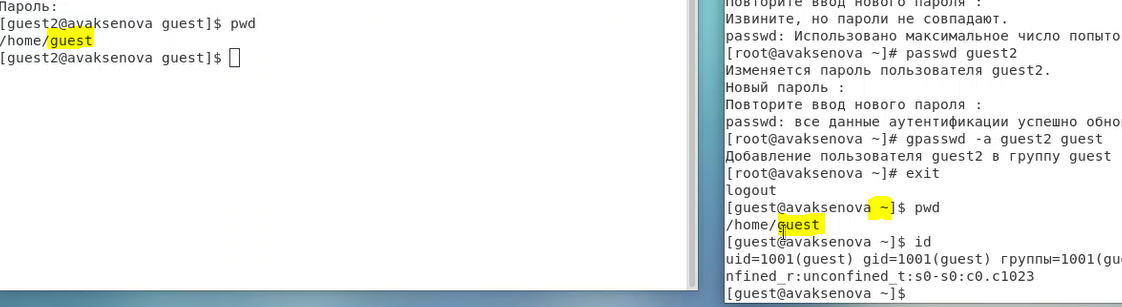


Figure 4: Определение домашней директории

1. Уточните имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравните вывод команды groups с выводом команд id -Gn и id -G, а также с содержимым файла /etc/group.(Рис. 5, 6, 7).

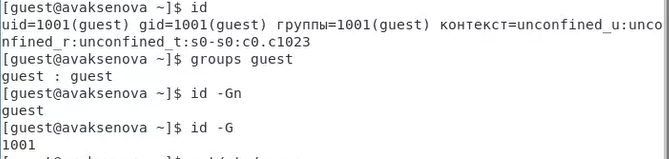


Figure 5: Уточнение id пользователя guest

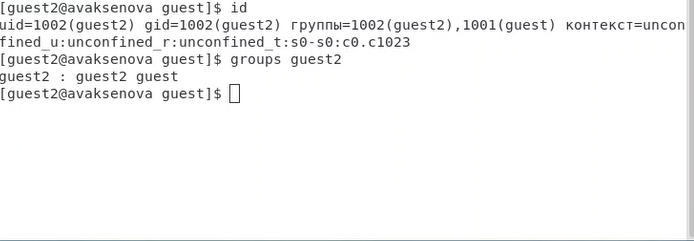


Figure 6: Уточнение id пользователя guest1

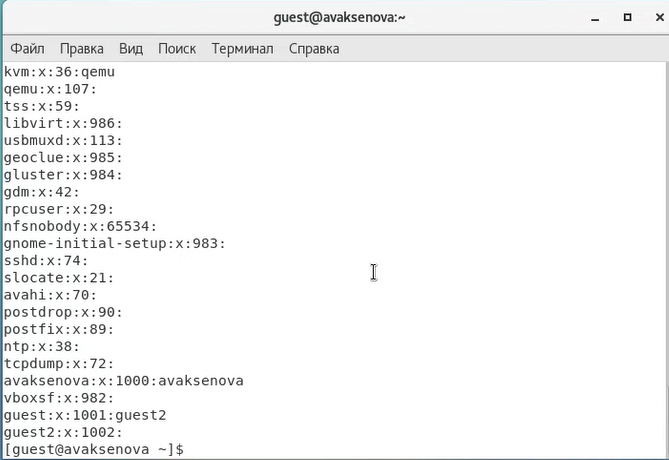


Figure 7: Уточнение id пользователя guest

1. От имени пользователя guest2 выполняем регистрацию пользователя guest2 в группе guest командой newgrp guest. (Рис. 8).

Figure 8: Регистрация в группе

Figure 8: Регистрация в группе

1. От имени пользователя guest изменяем права директории /home/guest, разрешив все действия для пользователей группы: chmod g+rwx /home/guest, а также снимаем с директории /home/guest/dir1 все атрибуты командой chmod 000 dirl[2]. (Рис. 9).

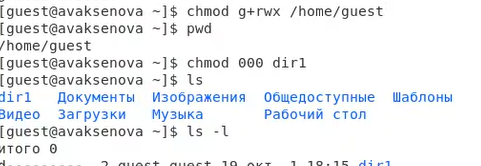


Figure 9: Изсенение прав директории

1. Заполняем таблицу «Установленные права и разрешённые действия», выполняя действия от имени guest и делая проверку от пользователя guest2, определяем опытным путём, какие операции разрешены, а какие нет.Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-». При заполнении таблицы рассматриваем не все атрибуты файлов и директорий, а лишь «первые три»: г, w, х, для «владельца». В итоге рассматриваем 64 варианта[1]. (Рис. 10, 11).

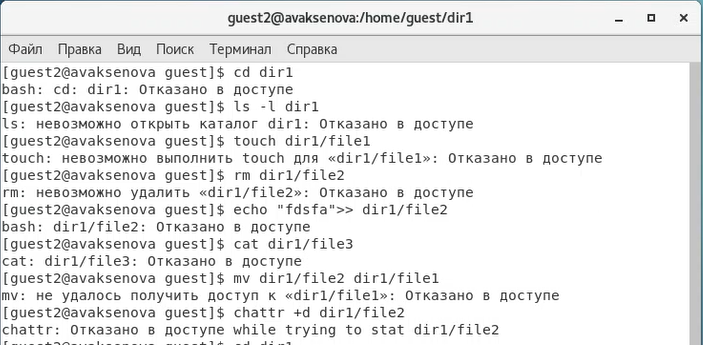


Figure 10: Процесс проверки разрешенных операций

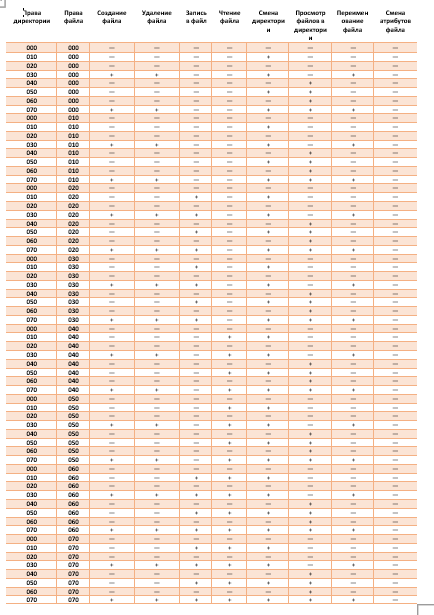


Figure 11: Заполненная таблица

1. На основании заполненной таблицы определяем те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1, внося данные во вторую таблицу[3]. (Рис. 12).



Figure 12: Проверка минимально необходимых прав для выполнения операций внутри директории

# Выводы

В результате выполнения данной работы были приобретены практические навыки работы в консоли с атрибутами файлов для группы.

# Библиографический список

1. Острейковский В. А. Информатика: учеб. для вузов / В. А. Острейковский. - 4-е изд., стер. - М.: Высш. шк., 2007. - 511 с.
2. Права в Linux [Электронный ресурс]. – Режим доступа : https://habr.com/ru/post/469667/, свободный. – Загл. с экрана.
3. Дискреционное разграничение доступа Linux [Электронный ресурс]. – Режим доступа : https://debianinstall.ru/iskretsionnoe-razgranichenie-dostupa-linux/, свободный. – Загл. с экрана.