Лабораторная работа № 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Соболевский Денис Андреевич

Содержание

# Цель работы

Целью данной работы является получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# Задание

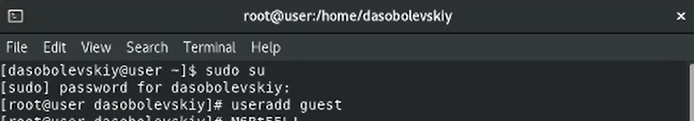
1. Создать новую учетную запись guest.
2. Выполнить операции в новой учетной записи.
3. Сформировать таблицу “Установленные права и разрешенные действия”.
4. Сформировать таблицу “Минимальные права для совершения операций”.

# Теоретическое введение

* Операционная система — это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.
* Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы.

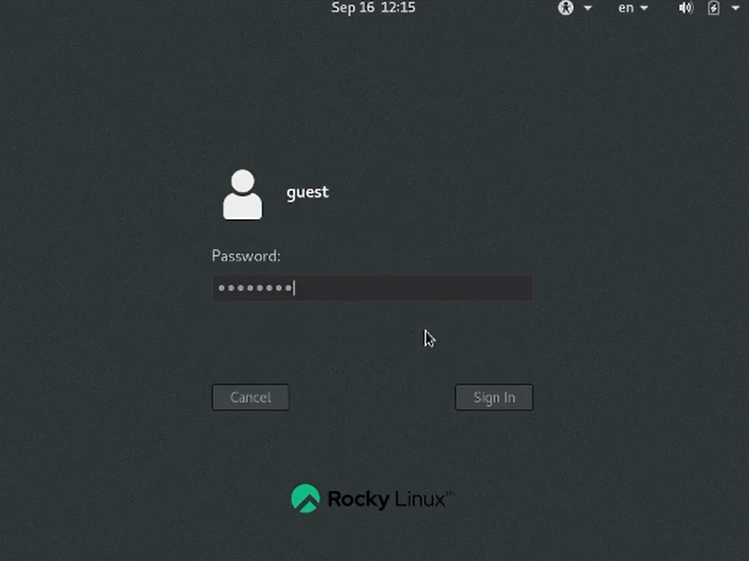
# Выполнение лабораторной работы

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



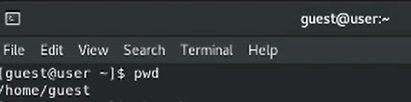
Создание и настройка новой учетной записи

1. Войдем в систему от имени пользователя guest



Вход в систему

1. Определим директорию, в которой мы находимся.



Определение директории

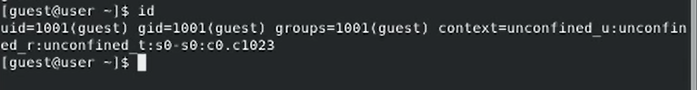
Мы находимся в домашней директории.

1. Уточним имя пользователя командой whoami.

Уточнение имени пользователя

Уточнение имени пользователя

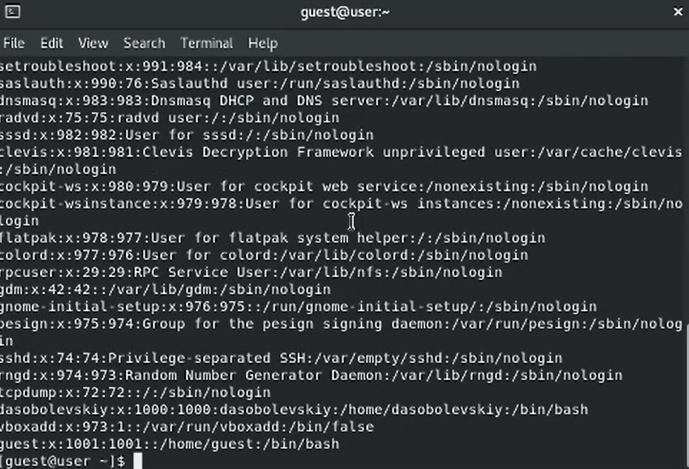
1. Уточним имя пользователя, его группу, а также группы, куда входит пользователь.



Уточнение информации о пользователе

Имя пользователя совпадает с приглашением в командной строке.

1. Просмотрим файл /etc/passwd.



Содержимое файла

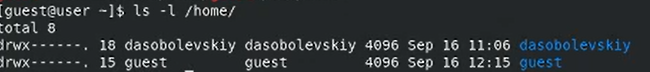
Найдем в нём свою учётную запись.

Учетная запись guest в файле /etc/passwd

Учетная запись guest в файле /etc/passwd

uid = 1001, gid = 1001. Совпадают со значениями, полученными в предыдущих пунктах.

1. Определим существующие в системе директории.



Существующие в системе директории

Получили список поддиректорий директории /home. На обеих директориях установлены права drwx——.

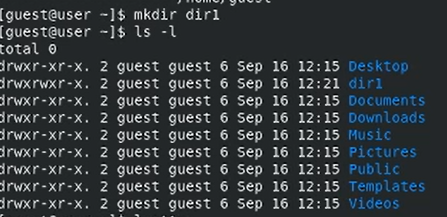
1. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home.

Расширенные атрибуты

Расширенные атрибуты

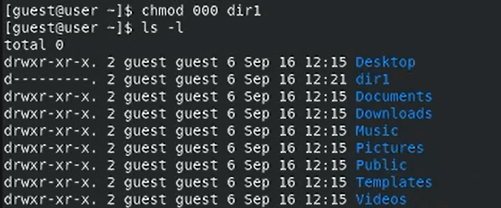
Удалось увидеть расширенные атрибуты директории текущего пользователя. Не удалось увидеть атрибуты директории другого пользователя.

1. Создадим в домашней директории поддиректорию dir1 и выведем права доступа и расширенные атрибуты.



Создание поддиректории

1. Снимем с директории dir1 все атрибуты командой chmod 000 dir1.



Снятие всех атрибутов

1. Попытаемся создать в директории dir1 файл file1.

Создание file1

Создание file1

Мы получили отказ, так как у нас нет прав на создание. Из-за этого файл не был создан.

1. Заполним таблицу «Установленные права и разрешённые действия».

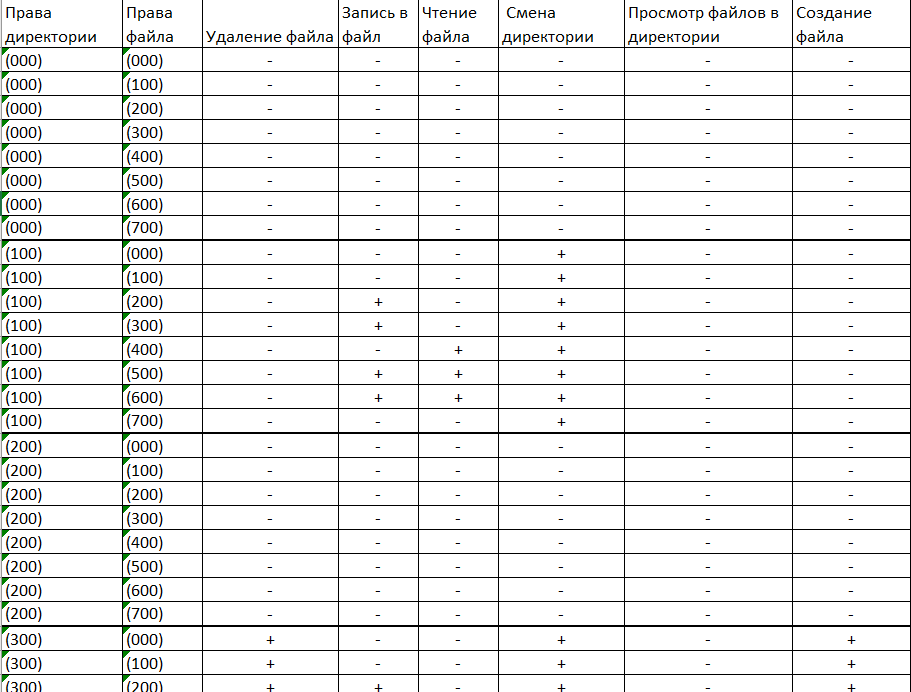


Таблица 2.1

1. Заполним таблицу «Минимальные права для совершения операций».

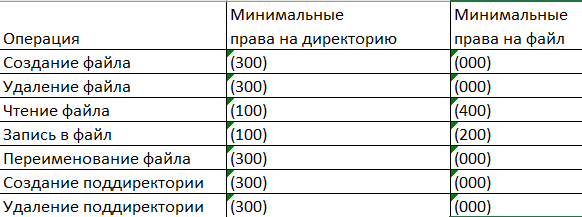


Таблица 2.2

# Выводы

В данной лабораторной работе были изучены средства ограничения прав для отдельных учетных записей.

# Список литературы

[1] https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux

[2] https://wiki.astralinux.ru/kb/diskretsionnye-i-mandatnye-razgranicheniya-dostupa-k-resursu-samba-158603114.html