Лабораторная работа №2

Дисциплина: Операционные системы

Коновалова Татьяна Борисовна

Содержание

# 1 Цель работы

Цель данной лабораторной работы — Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# 2 Теоретические данные

Рассмотрим три параметра доступа для каждого файла в ОС Linux:

1.Чтение - разрешить доступ к получению содержимого файла, но записывать нельзя. Для каталога позволяет получить список файлов и каталогов, которые в нём располагаются;

2.Запись - разрешить записывать данные в файл или изменять уже имеющиеся. Также можно создавать и менять файлы и каталоги;

3.Выполнение - нельзя выполнить программу, если у неё нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система понимает, что этот файл нужно запустить как программу.

Атрибуты — это набор основных девяти битов, определяющих какие из пользователей обладают правами на чтение, запись и исполнение. Первые три бита отвечают права доступа владельца, вторые — для группы пользователей, последние — для всех остальных пользователей в системе.

Установка атрибутов производится командой chmod. Установка бита чтения (r) позволяет сделать файл доступным для чтения. Наличие бита записи (w) позволяет изменять файл. Установка бита запуска (x) позволяет запускать файл на исполнение.

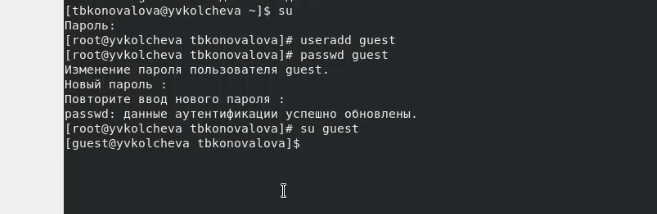
Более подробно см. в (**gnu-doc:bash?**).

# 3 Задание

1.Создать нового пользователя в Виртуальной машине, установить для него пароль. 2.Заполнить таблицу «Установленные права и разрешённые действия» (см. табл. 2.1) 3.На основании заполненной таблицы 2.1 определить те или иные минимально необходимые права для выполнения операций внутри директории. Заполнить таблицу «Минимальные права для совершения операций» 2.2.

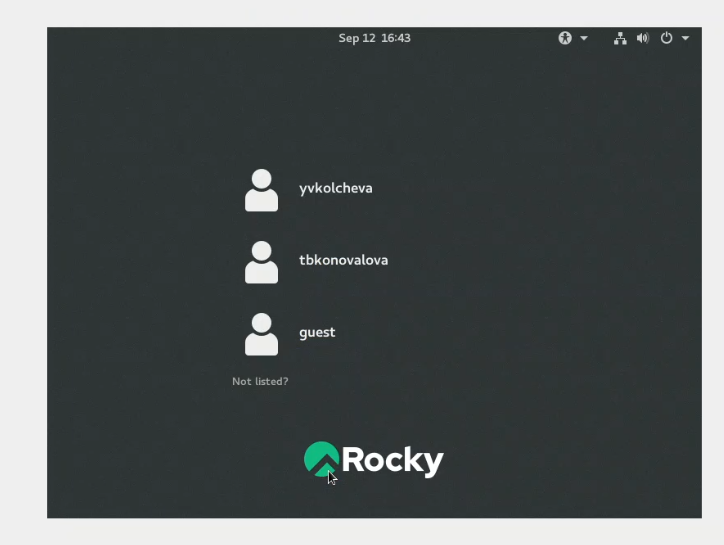
# 4 Выполнение лабораторной работы

1). Создала нового пользователя guest командой useradd, затем устанавила для него пароль с помощью команды passwd guest (рис. [??]).

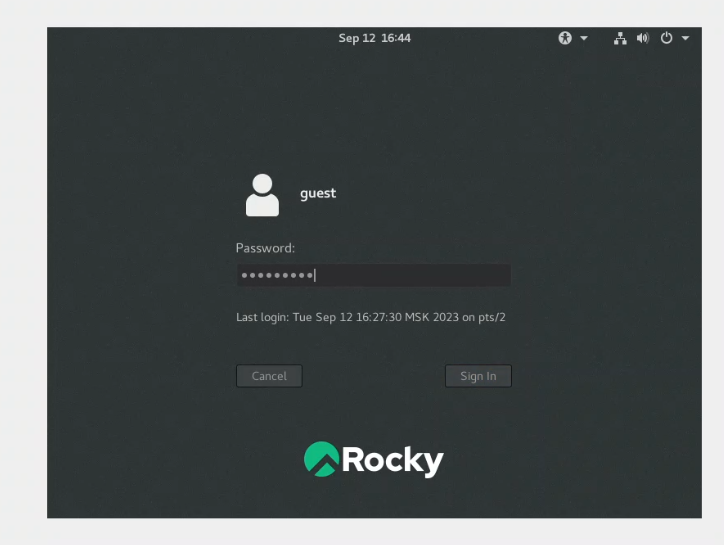


Новый пользователь в Виртуальной машине

2). Зашла в систему от имени пользователя guest, используя только что придуанный пароль (рис. [??]) и (рис. [??]).

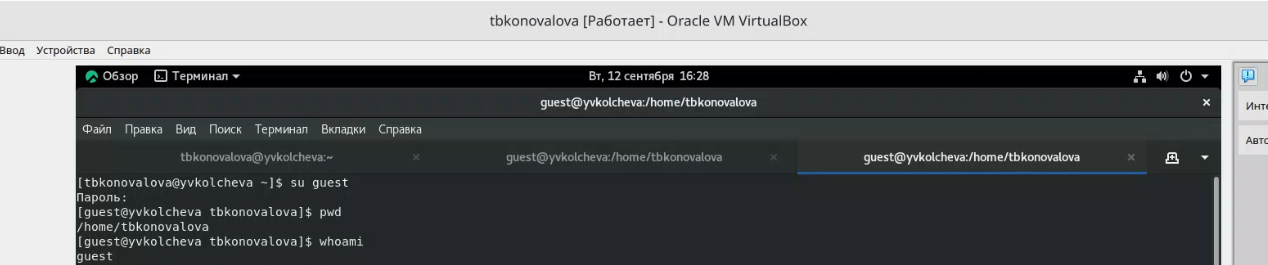


Захожу в систему от имени нового пользователя



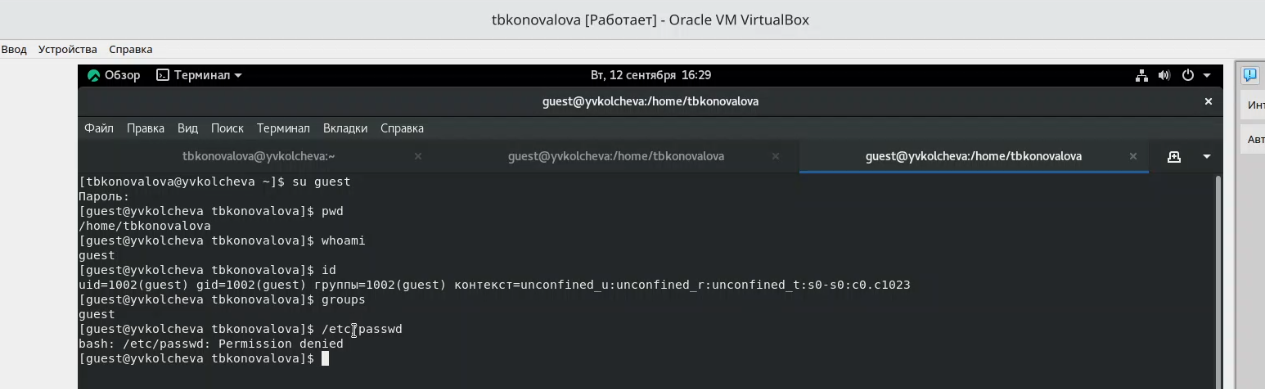
Захожу в систему от имени нового пользователя

3). Выполнила команду pwd, которая показывает, что мы находимся в домашнем каталоге пользователя guest. Уточнила имя пользователя командой whoami, ожидаемо получаем вывод guest (рис. [??]).



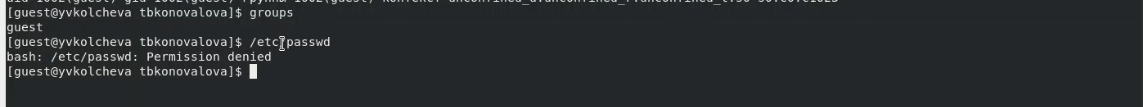
Работа в домашнем каталоге

4). C помощью команды id узнала, что uid = 1002, gid = 1002 (guest) (рис. [??]).



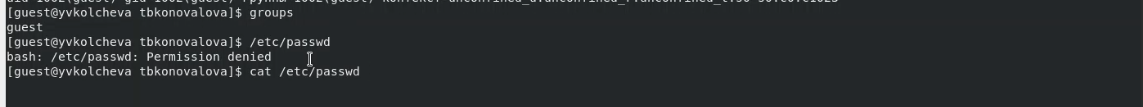
Команда id

5). Ввела команду groups и убедилась, что группа состоит из одного пользователя guest (рис. [??]).

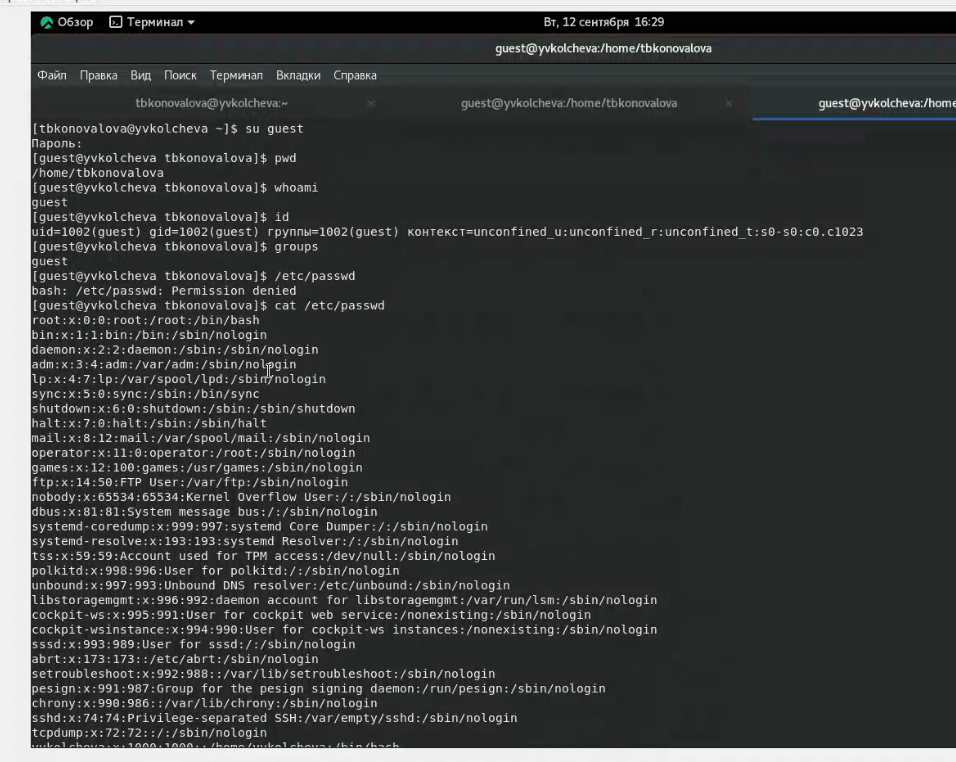


Команда groups

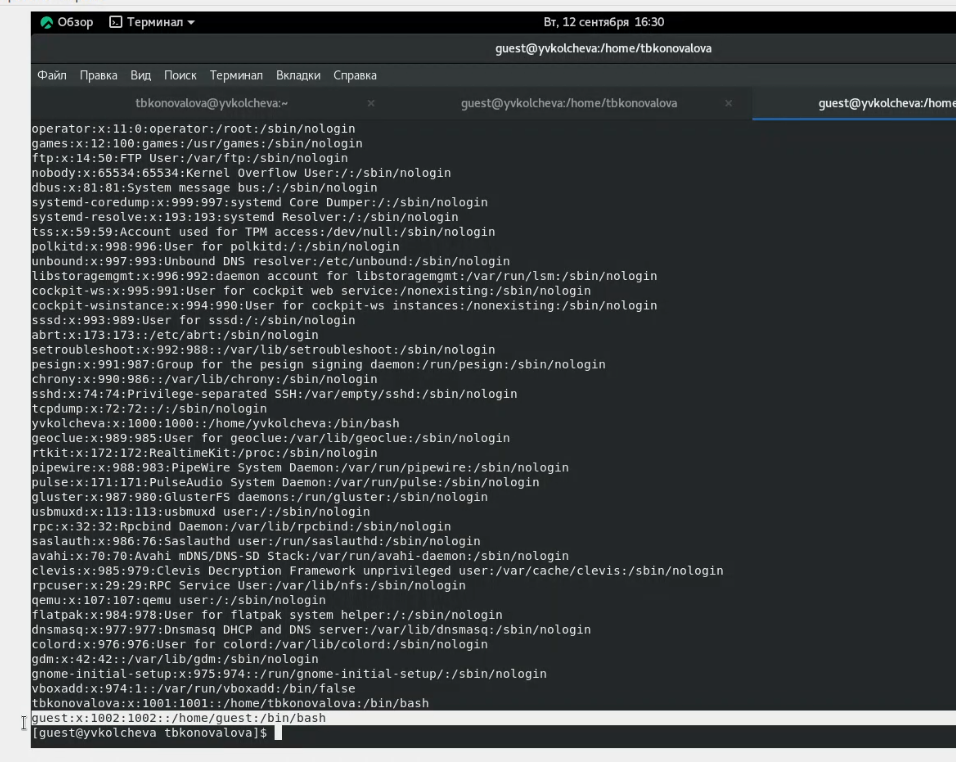
6). В содержимом файла /etc/passwd нашла информацию о пользователе, что соответствует данным, полученным с помощью команды id и pwd (рис. [??]), (рис. [??]), (рис. [??]).



Работа в содержимом файле /etc/passwd



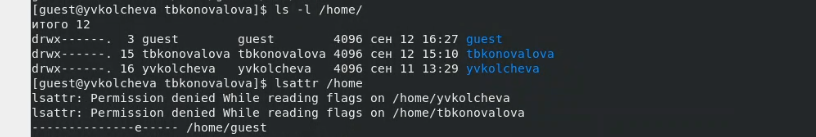
Работа в содержимом файле /etc/passwd



Работа в содержимом файле /etc/passwd

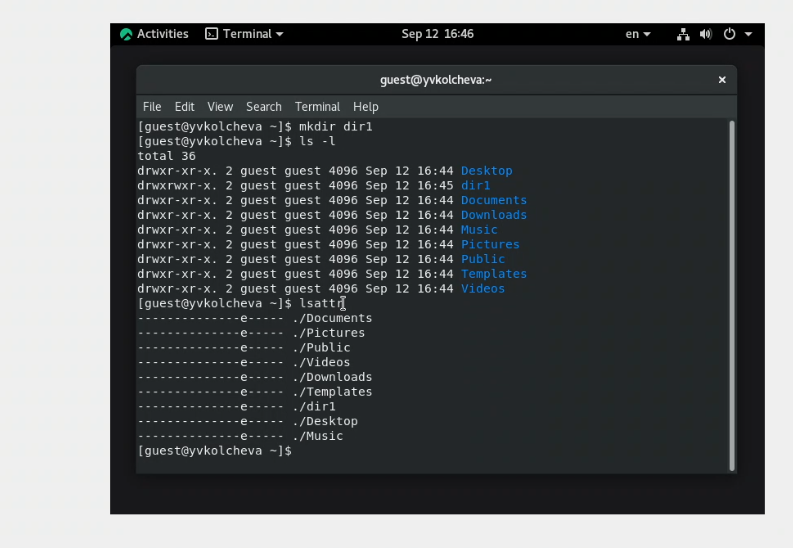
7). Определила содержимое каталога /home. С помощью команды ls -l /home/ я убедилась, что у меня есть домашние директории с их атрибутами rwx в первом бите для каждой. С помощью команды lsattr /home рассмотрела расширенные атрибуты текущего пользователя (рис. [??]).

Список поддиректорий директории получить удалось. На директориях установлены права чтеня, записи и выполнения для самого пользователя (для группы и остальных пользователей никаких прав доступа нет). Удалось увидеть расширенные атрибуты только директории того пользователя, от имени которого я нахожусь в системе.



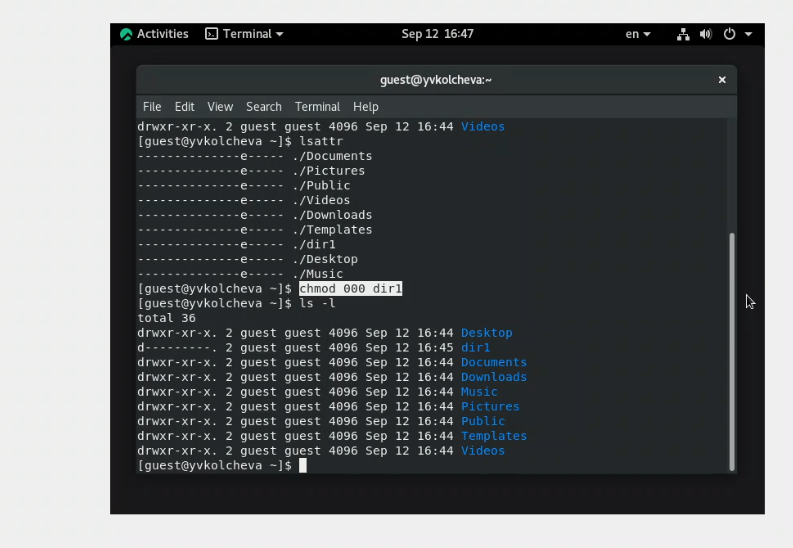
Работа с каталогом /home

8). Далее создала новый каталог dir1 и увидела, что у него больше атрибутов по сравнению со стандартными директориями (рис. [??]).



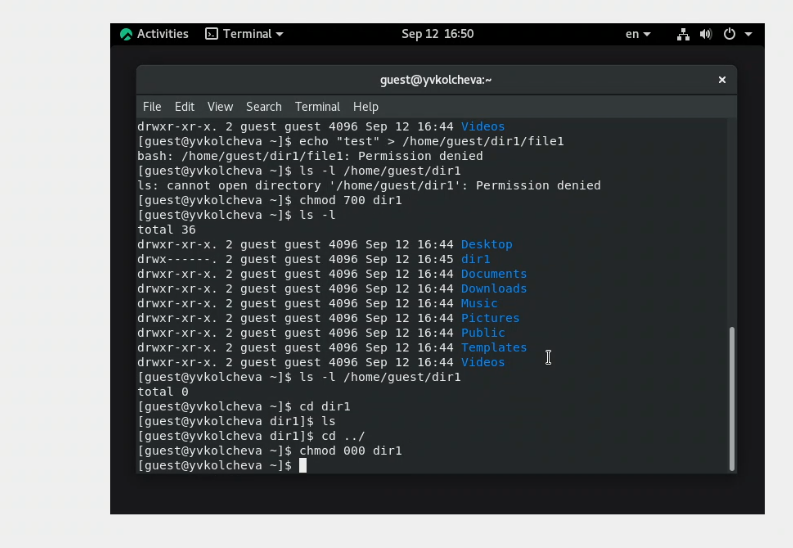
Новый каталог dir1

9). Поменяла директории dir1 атрибуты с помощью команды chmod 000. Далее, при попытке создать файл, вывыодит сообщение об ошибке, т.к. забрали права на всё у всех пользователей. Файл, соответственно, тоже не создаётся (рис. [??]).



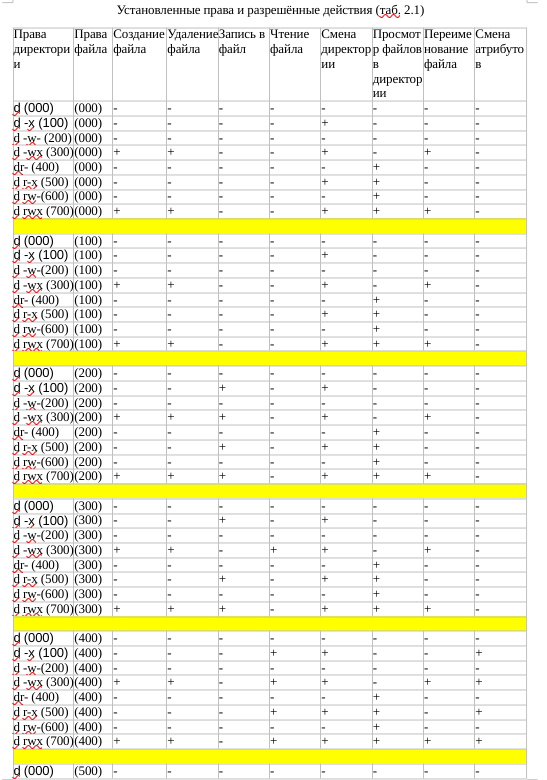
Меняем директории dir1 атрибуты

10). Рассмотрим, как влияют различные комбинации атрибутов файлов и директории на различные действия. Для этого буду создавать файл командой touch, удалять его командой rm, записывть в файл командой echo >, читать файл командой cat, менять директорию командой cd, просматривать директорию командой ls, а также переименовывать файл командой rename и менять атрибуты командой chattr (рис. [??]).

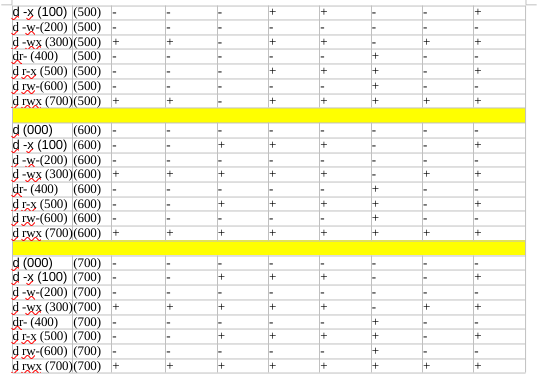


Рассматриваем различные комбинации атрибутов файлов

В случае успеха я ставила + в редактированную таблицу, ошибку обозначала -. Все данные я внесла в таблицу «Установленные права и разрешённые действия» (рис. [??]) и (рис. [??]).



Таблца 2.1 «Установленные права и разрешённые действия»



Таблца 2.1 «Установленные права и разрешённые действия»

11). На основании этой таблицы я заполнила вторую «Минимальные права для совершения операций». В данной таблице указала минимальные требования на права и директорию для выполнения тех или иных действий. Все данные я внесла в таблицу (рис. [??]).

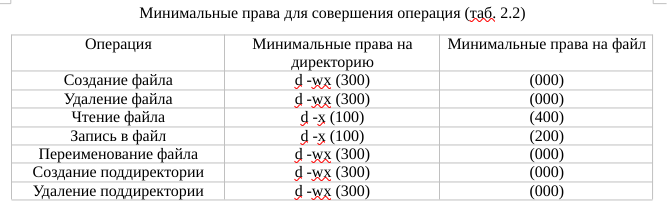


Таблица 2.2 «Минимальные права для совершения операций»

# 5 Выводы

Получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# 6 Библиография

СПИСОК ЛИТЕРАТУРЫ

1.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: http://bugtraq.ru/library/books/attack1/index.html

2.Теоеретические знания, приведённые в Лабораторной работе №2 - https://esystem.rudn.ru/pluginfile.php/2090123/mod\_resource/content/6/002-lab\_discret\_attr.pdf

3.Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

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

2.[Электронный ресурс] - доступ: https://debianinstall.ru/diskretsionnoe-razgranichenie-dostupa-linux/