Отчёт по лабораторной работе №2

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

# 1 Цель работы

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

# 2 Задания

1. Знакомство с пользователями и их аттрибутами
2. Заполнение таблиц 2.1 и 2.2

# 3 Выполнение лабораторной работы

## 3.1 Знакомство с пользователями и их аттрибутами

Добавляю нового пользователя - guest, затем задаю ему пароль (рис. 1).

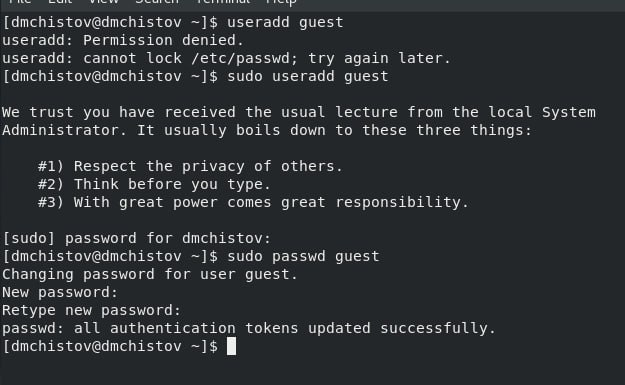


Рис. 1: Новый пользователь

Видно, что новый пользователь успешно создан. Захожу в него. (рис. 2).

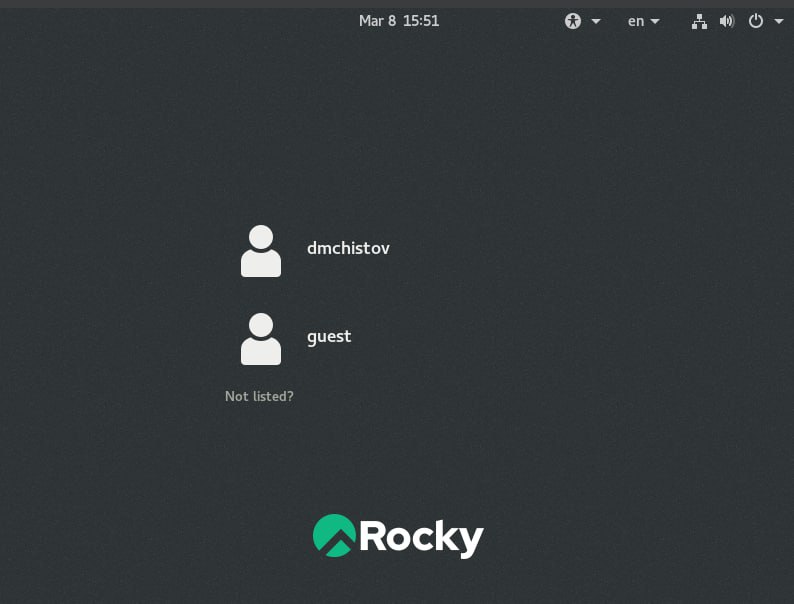


Рис. 2: Новый пользователь успешно создан

Командой pwd определяю своё местоположение в файловой системе - я нахожусь в домашнем каталоге пользователя guest, это также можно было определить по значку ~ в командной строке (рис. 3).

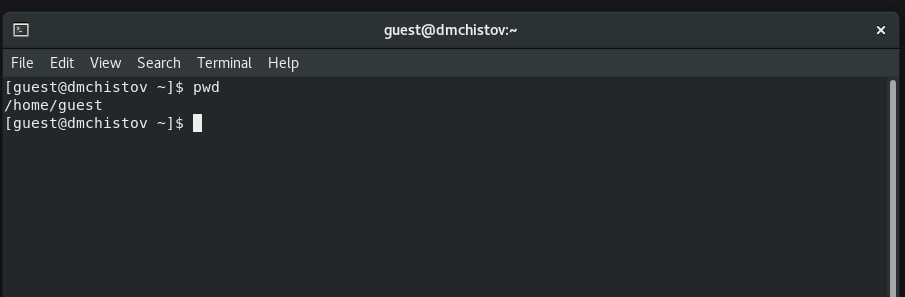


Рис. 3: Команда pwd

Командой whoami, уточняю имя пользователя - guest (рис. 4).

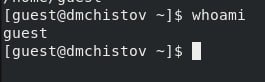


Рис. 4: Имя пользователя

Командой id получаю информацию о uid и gid - таким образом я получил id пользователя и его группы, затем командой groups вывожу группу - там также указана группа guest (рис. 5).

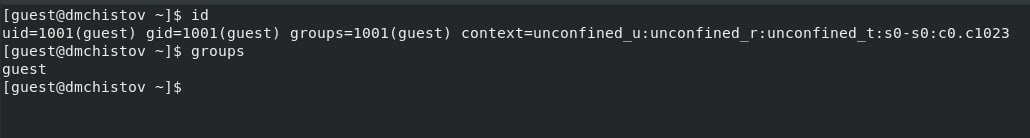


Рис. 5: Группы, пользователи и их ID

Командой cat /etc/passwd | grep guest (grep guest пишу, чтобы прочитать информацию исключительно о нашем пользователе - guest) определяю uid и gid пользователя, сравниваю их с выводом команды id, всё совпадает (рис. 6).

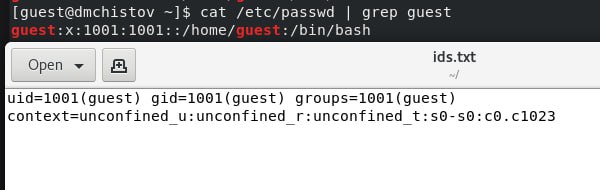


Рис. 6: Пользователи, группы и их ID

Командой ls -l /home/ определяю существующие в ситеме директории - определил, что в home теперь домашняя директория пользователя guest и домашняя директория пользователя dmchistov - моего основого пользователя. Права у каждых директорий стоят полные для пользователей (700) (рис. 7).

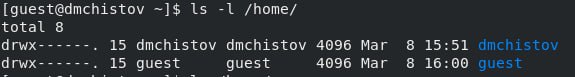


Рис. 7: Директории пользователей

Командой lsattr определяю расширенные атрибуты каждой директории внутри /home, однако мне не удалось узнать об аттрибутах директории dmchistov, т.к. это другой пользователь, зато получилось узнать об аттрибутах пользователя guest (рис. 8).

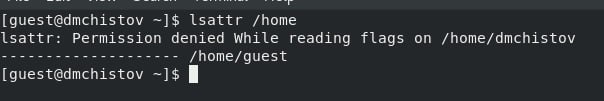


Рис. 8: Аттрибуты пользователей

Создаю директорию dir1 и командой ls -l узнаю о её правах (рис. 9).

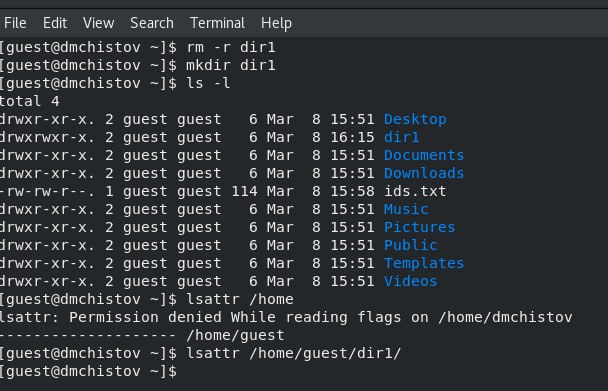


Рис. 9: Аттрибуты dir1

Командой chmod 000 dir1, снимаю все атрибуты с директории dir1, командой ls -l подтверждаю, что у директории больше нет никаких прав (рис. 10).

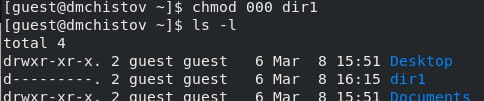


Рис. 10: Аттрибуты dir1 больше нет

Попытаюсь создать в директории dir1 файл, однако получаю отказ, т.к. ранее я снял все права доступа к этой директории, поэтому ни один пользователь не может получить доступ к этой папке, соответственно и не может создать файл (рис. 11).



Рис. 11: Не выходит создать файл в папке dir1

## 3.2 Заполнение таблиц 2.1 и 2.2

Теперь, перехожу к заполнению таблиц - требуется определить опытным путём, какие комбинации прав для файла и директории позволяет пользователю совершать те или иные действия с директориями и файлами внутри них.

## 3.3 Как работает системе нумерации прав

В интернете я нашёл удобную схему, которая показывает число и соответствуещее ему право (рис. 12):

1 - execute, 2 - write, 3 - write & execute, 4 - read, 5 - read & execute, 6 - read & write, 7 - read & write & execute

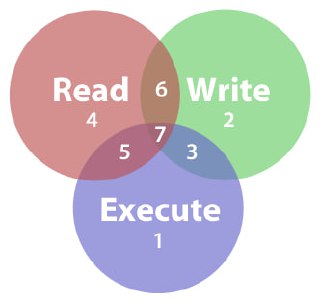


Рис. 12: Схема: Права и их нумерация

Пользуясь такой схемой, сначала я устанавливал права для директории, затем устанвалил каждый тип прав для файла, внутри этой директории и каждый проверял те или иные действия, затем заносил результат в таблицу. Затем задавал следующие права для директории, заново задавал права для файла и проверял операции. И так далее (рис. 13), (рис. 14), (рис. 15):

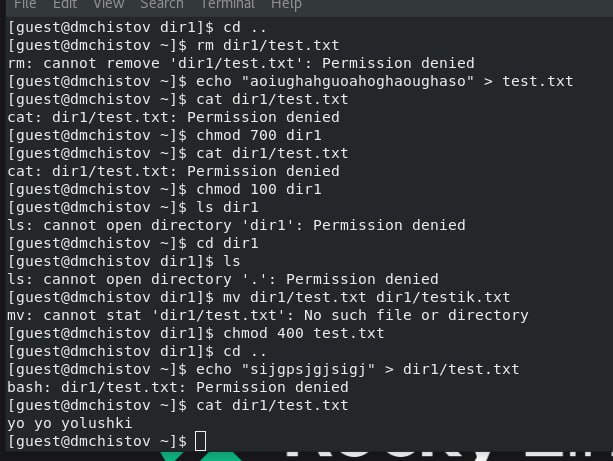


Рис. 13: Процесс заполнения таблицы 1

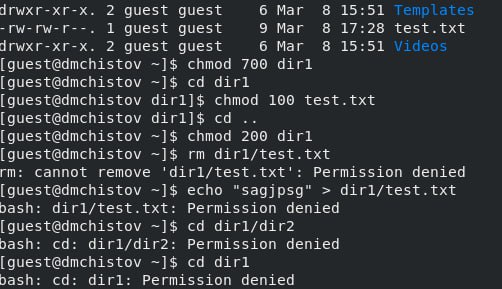


Рис. 14: Процесс заполнения таблицы 2

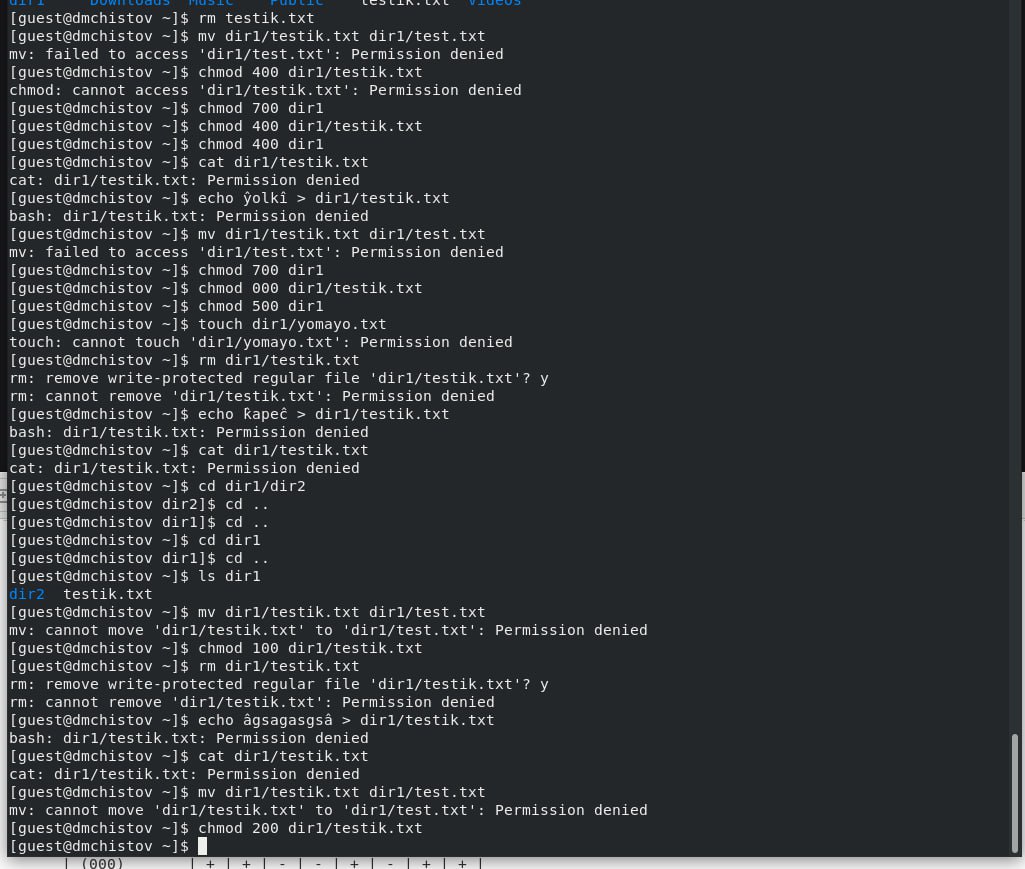


Рис. 15: Процесс заполнения таблицы 3

По итогу получилась вот такая таблица:

## 3.4 Таблица 2.1 “Установленные права и разрешённые действия”

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена аттрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d(000) | (000) | - | - | - | - | - | - | - | - |
| d(000) | (100) | - | - | - | - | - | - | - | - |
| d(000) | (200) | - | - | - | - | - | - | - | - |
| d(000) | (300) | - | - | - | - | - | - | - | - |
| d(000) | (400) | - | - | - | - | - | - | - | - |
| d(000) | (500) | - | - | - | - | - | - | - | - |
| d(000) | (600) | - | - | - | - | - | - | - | - |
| d(000) | (700) | - | - | - | - | - | - | - | - |
| d(100) | (000) | - | - | - | - | + | - | - | + |
| d(100) | (100) | - | - | - | - | + | - | - | + |
| d(100) | (200) | - | - | + | - | + | - | - | + |
| d(100) | (300) | - | - | + | - | + | - | - | + |
| d(100) | (400) | - | - | - | + | + | - | - | + |
| d(100) | (500) | - | - | - | + | + | - | - | + |
| d(100) | (600) | - | - | + | + | + | - | - | + |
| d(100) | (700) | - | - | + | + | + | - | - | + |
| d(200) | (000) | - | - | - | - | - | - | - | - |
| d(200) | (100) | - | - | - | - | - | - | - | - |
| d(200) | (200) | - | - | - | - | - | - | - | - |
| d(200) | (300) | - | - | - | - | - | - | - | - |
| d(200) | (400) | - | - | - | - | - | - | - | - |
| d(200) | (500) | - | - | - | - | - | - | - | - |
| d(200) | (600) | - | - | - | - | - | - | - | - |
| d(200) | (700) | - | - | - | - | - | - | - | - |
| d(300) | (000) | + | + | - | - | + | - | + | + |
| d(300) | (100) | + | + | - | - | + | - | + | + |
| d(300) | (200) | + | + | + | - | + | - | + | + |
| d(300) | (300) | + | + | + | - | + | - | + | + |
| d(300) | (400) | + | + | - | + | + | - | + | + |
| d(300) | (500) | + | + | - | + | + | - | + | + |
| d(300) | (600) | + | + | + | + | + | - | + | + |
| d(300) | (700) | + | + | + | + | + | - | + | + |
| d(400) | (000) | - | - | - | - | - | + | - | - |
| d(400) | (100) | - | - | - | - | - | + | - | - |
| d(400) | (200) | - | - | - | - | - | + | - | - |
| d(400) | (300) | - | - | - | - | - | + | - | - |
| d(400) | (400) | - | - | - | - | - | + | - | - |
| d(400) | (500) | - | - | - | - | - | + | - | - |
| d(400) | (600) | - | - | - | - | - | + | - | - |
| d(400) | (700) | - | - | - | - | - | + | - | - |
| d(500) | (000) | - | - | - | - | + | + | - | + |
| d(500) | (100) | - | - | - | - | + | + | - | + |
| d(500) | (200) | - | - | + | - | + | + | - | + |
| d(500) | (300) | - | - | + | - | + | + | - | + |
| d(500) | (400) | - | - | - | + | + | + | - | + |
| d(500) | (500) | - | - | - | + | + | + | - | + |
| d(500) | (600) | - | - | + | + | + | + | - | + |
| d(500) | (700) | - | - | + | + | + | + | - | + |
| d(600) | (000) | - | - | - | - | - | + | - | - |
| d(600) | (100) | - | - | - | - | - | + | - | - |
| d(600) | (200) | - | - | - | - | - | + | - | - |
| d(600) | (300) | - | - | - | - | - | + | - | - |
| d(600) | (400) | - | - | - | - | - | + | - | - |
| d(600) | (500) | - | - | - | - | - | + | - | - |
| d(600) | (600) | - | - | - | - | - | + | - | - |
| d(600) | (700) | - | - | - | - | - | + | - | - |
| d(700) | (000) | + | + | - | - | + | + | + | + |
| d(700) | (100) | + | + | - | - | + | + | + | + |
| d(700) | (200) | + | + | + | - | + | + | + | + |
| d(700) | (300) | + | + | + | - | + | + | + | + |
| d(700) | (400) | + | + | - | + | + | + | + | + |
| d(700) | (500) | + | + | - | + | + | + | + | + |
| d(700) | (600) | + | + | + | + | + | + | + | + |
| d(700) | (700) | + | + | + | + | + | + | + | + |

Опираясь на эту таблицу, я заполнил таблицу 2.2. Там просто требуется определить какие минимальные права нужны для файла и директории, чтобы выполнить ту или иную операцию. Заполнял просто определяя первую встретившуюся строчку, где стоит + для нужной мне операции, затем смотрел в ячейку с правами для директории и правами для файла.

В конце концов получилась вот такая таблица:

## 3.5 Таблица 2.2 “Минимальные права для совершения операций”

| Операция | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | 300 | 000 |
| Удаление файла | 300 | 000 |
| Чтение файла | 100 | 400 |
| Запись в файл | 100 | 200 |
| Переименование файла | 300 | 000 |
| Создание поддиректории | 300 | 000 |
| Удаление поддиректории | 300 | 000 |

# 4 Выводы

При выполнении данной лаборатоной работы я получил практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

# 5 Список литературы

[Лабораторная работы №2](https://esystem.rudn.ru/pluginfile.php/2580592/mod_resource/content/6/002-lab_discret_attr.pdf)