Отчет по лабораторной работе №2

Дискреционное разгарничение прав в Linux. Основныет атрибуты

Бурдина Ксения Павловна

2022 Sep 15th

Содержание

# 1 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.

# 2 Ход выполнение лабораторной работы

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

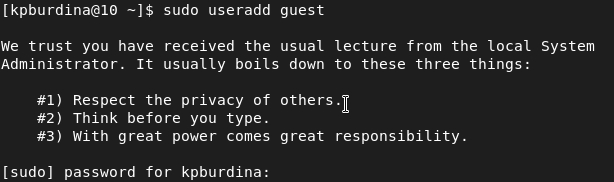


рис 1. Создание учетной записи

1. Зададим пароль для пользователя guest (используя учётную запись администратора):

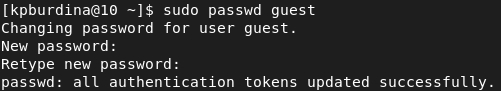


рис 2. Задание пароля для пользователя

1. Войдем в систему от имени пользователя guest:

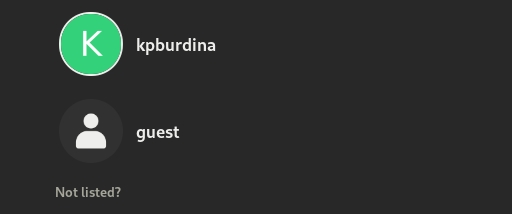


рис 3. Вход от имени guest

1. Определим директорию, в которой мы находимся, командой pwd. Сравнивая с приглашением командной строки, мы видим, что она является домашней директорией:

рис 4. Определение директории

рис 4. Определение директории

1. Уточним имя нашего пользователя командой whoami. Увидим, что мы действительно зашли под именем guest.
2. Уточним имя нашего пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gid и groups принимают значение 1001, запомним его:

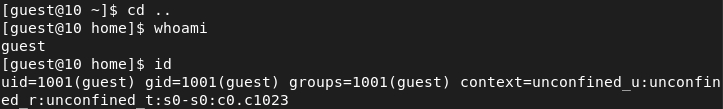


рис 5. Информация о пользователе по whoami и id

Сравним вывод id с выводом команды groups:

рис 6. Вывод groups

рис 6. Вывод groups

1. Сравнивая полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки, видим, что они совпадают.
2. Просмотрим файл /etc/passwd:

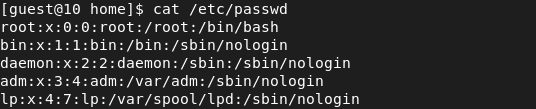


рис 7. Просмотр файла (н)

рис 8. Просмотр файла (к)

рис 8. Просмотр файла (к)

Найдем в нём свою учётную запись. Она у нас находится в самом конце. Видим, что uid пользователя и gid пользователя совпадают со значениями, найденными в предыдущих пунктах.

Мы также можем получить вывод команды с помощью программы grep в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания. Такой вывод будет выглядеть следующим образом:

рис 9. Вывод информации с помощью grep

рис 9. Вывод информации с помощью grep

1. Определим существующие в системе директории:

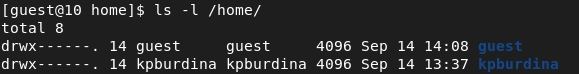


рис 10. Просмотр директорий

У нас имеются поддиректории наших учетных записей. Видим, что у обоих пользователей установлены права на чтение, изменение и выполнение только для самого пользователя.

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

рис 11. Просмотр информации командой lsattr

рис 11. Просмотр информации командой lsattr

Можем увидеть, что расширенные атрибуты у директории отсутствуют. Также видно, что на недоступен просмотр расширенных атрибутов директорий других пользователей.

1. Создадим в домашней директории поддиректорию dir1 и определим командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1:

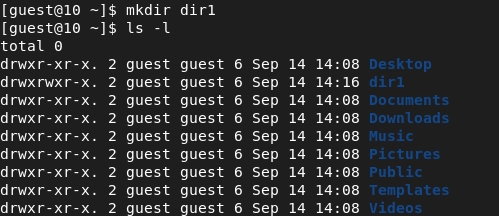


рис 12. Создание поддиректории и просмотр ls -l



рис 13. Просмотр командой lsattr

Видим, что у нас в созданной поддиректории имеются права на чтение, исполнение и редактирование у пользователя и группы, а у остальных только на чтение и исполнение.

При этом видим, что доступа к расширенным атрибутам у нас нет.

1. Снимем с директории dir1 все атрибуты командой chmod 000 dir1 и проверим правильность выполнения команды:

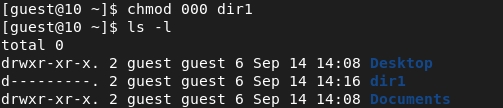


рис 14. Снятие атрибутов с директории

1. Попытаемся создать в директории dir1 файл file1, однако получим отказ в выполнении операции по созданию файла, так как мы сбросили права на исполнение директории dir1. С помощью команды убедились, что файл file1 не находится внутри директории dir1:

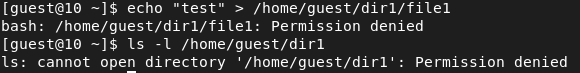


рис 15. Попытка создания файла в директории dir1

1. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет (https://esystem.rudn.ru/pluginfile.php/1651883/mod\_resource/content/6/002-lab\_discret\_attr.pdf)[1].

Мы рассматриваем первые три атрибута, которые относятся к владельцу. Это 64 варианта.

Проведем действия с атрибутами директории 700 и атрибутами файла с 000 до 700.

Нам требуется для каждого возможного варианта проверить, будет ли выполняться создание и удаление файла, запись в файл, его чтение, смена директории, просмотр файлов в директории, возможно ли будет переименовывать файл, а также изменять его атрибуты.

Установим атрибуты директории dir1 как 700:



рис 16. Действия при атрибутах dir1(700) и file(700)

рис 17. Действия при атрибутах dir1(700) и file(700)

рис 17. Действия при атрибутах dir1(700) и file(700)

По умолчанию у нас атрибуты созданного файла были 700. Мы видим, что у нас возможны все действия с файлом, просмотр и изменение атрибутов, смена директории, а также просмотр файлов в ней. Занесем эти данные в таблицу.

Теперь изменим атрибуты файла на 000 и проведем все действия с ними:

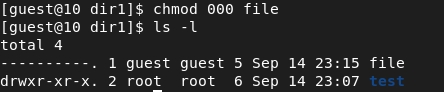


рис 18. Действия при атрибутах dir1(700) и file(000)

У нас нет никаких прав на работу с файлом, поэтому мы можем создать новый файл, удалить файл и поработать с директорией, в которой у нас есть все права: сменить, просмотреть содержимое, переименовать файлы, сменить атрибуты файлам.

Изменим атрибуты файла на 100:

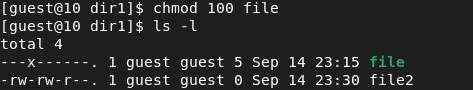


рис 19. Действия при атрибутах dir1(700) и file(100)

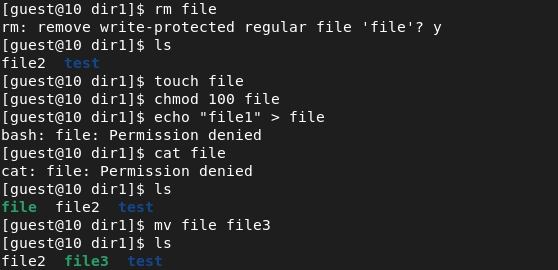


рис 20. Действия при атрибутах dir1(700) и file(100)

Видим, что у нас появилась возможность на исполнение файла, но мы по прежнему не смодем записать в него данные или прочитать.

Изменим атрибуты файла на 200:

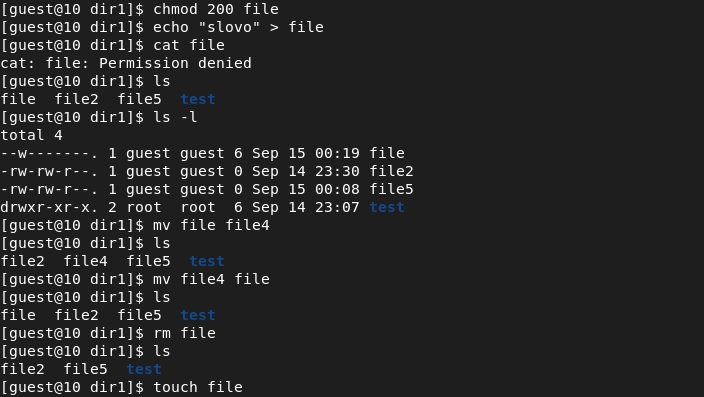


рис 21. Действия при атрибутах dir1(700) и file(200)

Теперь мы имеем право сделать запись в файл, поскольку появилась возможность редактирования файла, но по прежнему нет права на чтение.

Изменим атрибуты на 300:

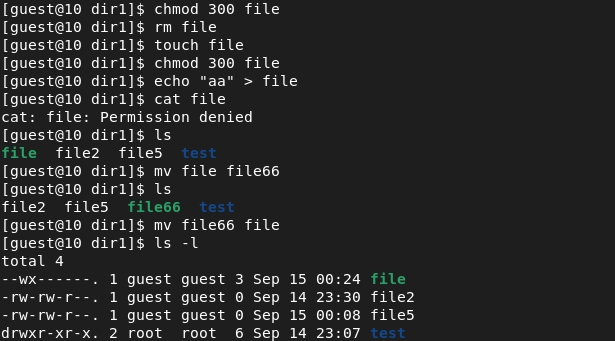


рис 22. Действия при атрибутах dir1(700) и file(300)

У нас также имеется возможность исполнения файла и редактирования.

Изменим атрибуты на 400:

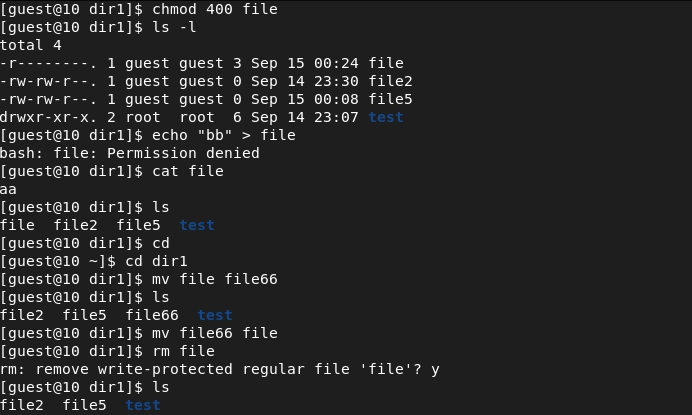


рис 23. Действия при атрибутах dir1(700) и file(400)

Теперь у нас есть право на чтение файла, но нет возможности редактирования.

Посмотрим возможности работы с атрибутами файла 500:

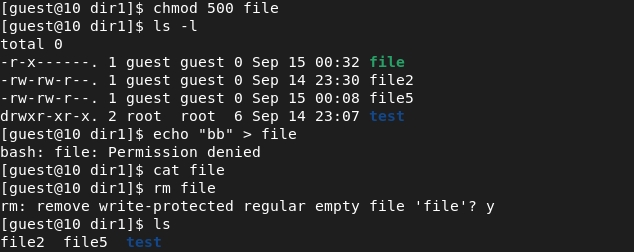


рис 24. Действия при атрибутах dir1(700) и file(500)

Мы можем исполнять и читать файл, однако у нас нет права на редактирование.

Завершим просмотр директории dir1 с атрибутами 700 просмотром возможностей файла с атрибутами 600:

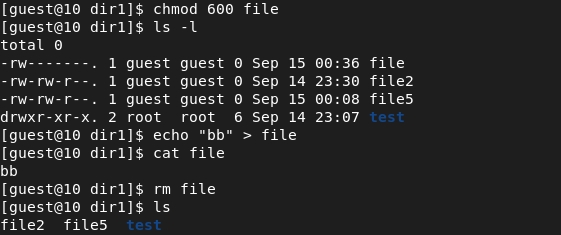


рис 25. Действия при атрибутах dir1(700) и file(600)

Видим, что мы можем и прочитать файл, и изменить его. Нет права лишь на исполнение.

По аналогии проведем действия с другими атрибутами директории dir1 (от 000 до 600). По итогам заполним общую таблицу. Она выглядит следующим образом:

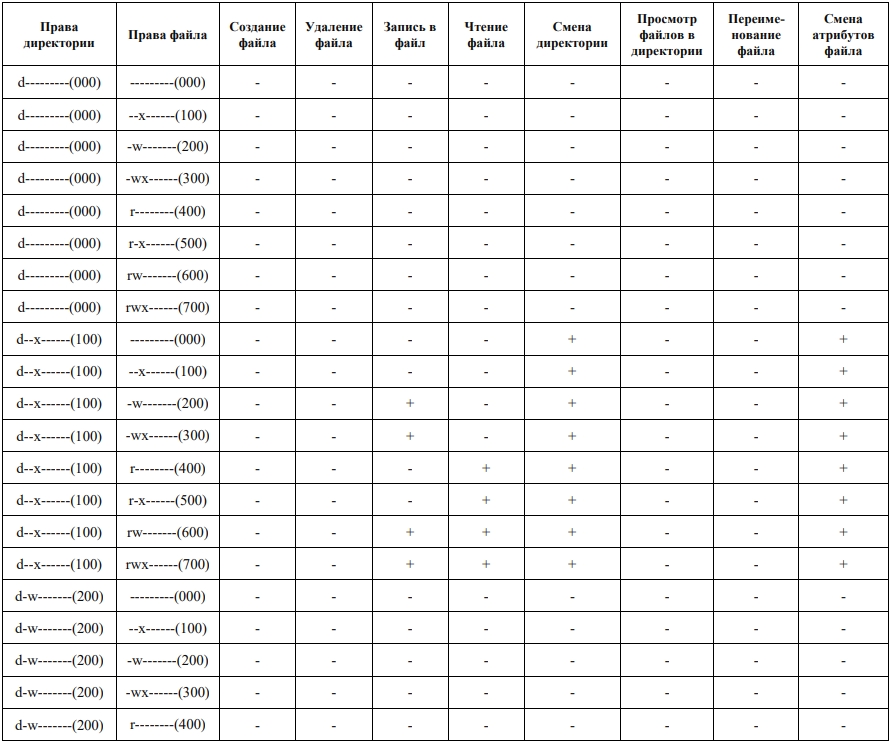


рис 26. Таблица прав и разрешений 1

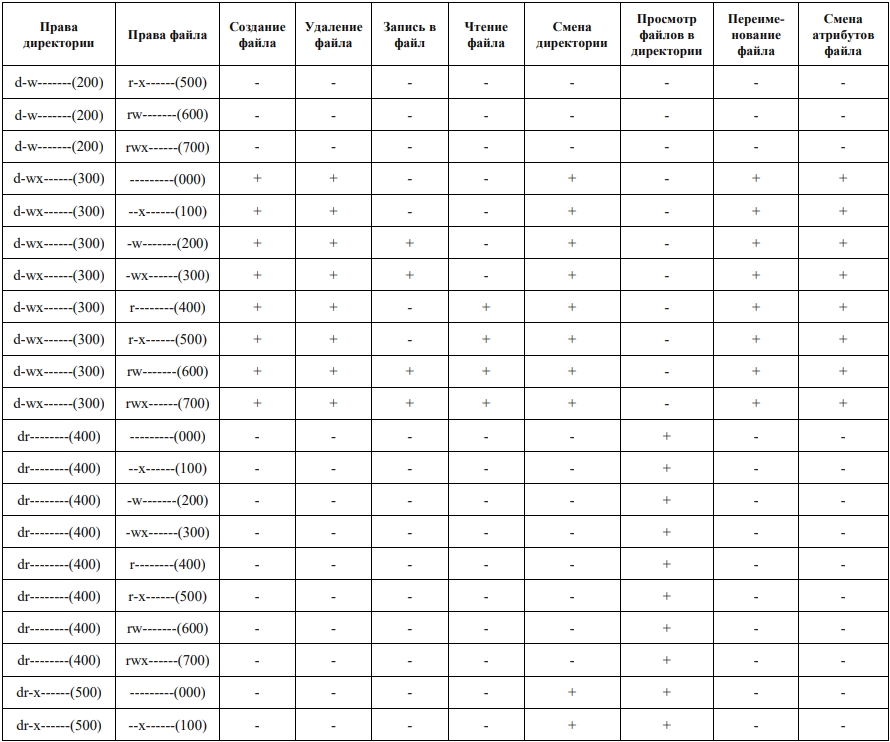


рис 27. Таблица прав и разрешений 2

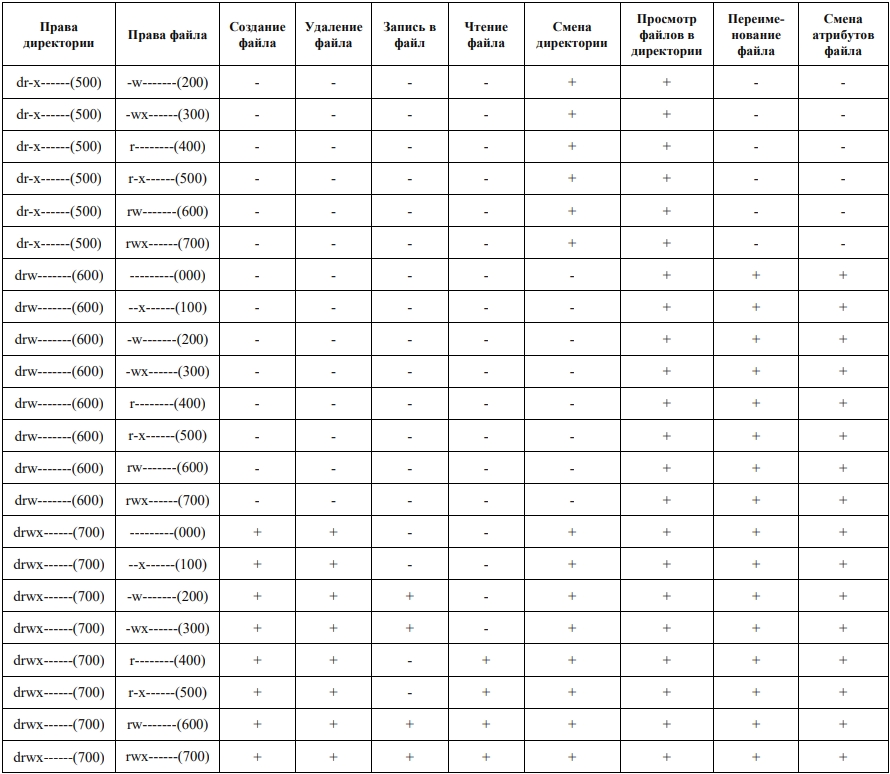


рис 28. Таблица прав и разрешений 3

Проанализировав данную таблицу, можем увидеть минимальные права, которые необходимы для совершения каждой из операций. Занесем данные наблюдения в таблицу:

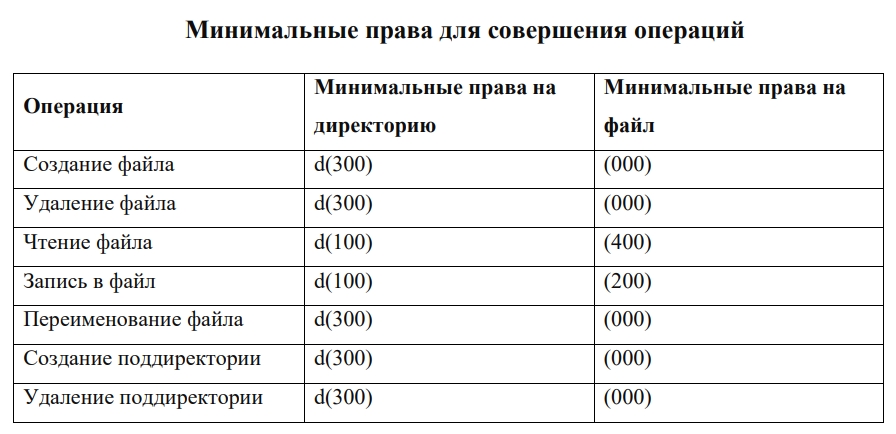


рис 29. Таблица минимальных прав для совершения операций

# 3 Выводы

В ходе работы мы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# 4 Список литературы

1. Методические материалы курса (https://esystem.rudn.ru/pluginfile.php/1651883/mod\_resource/content/6/002-lab\_discret\_attr.pdf)