Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра ИИТ

Лабораторная работа №2

за 4 семестр

По дисциплине: «ОСиСП»

Тема: «Ссылки. Права доступа»

Выполнил:

Студент 2 курса

Группы ПО-4(1)

Иваненко И. Л.

Проверил:

Давидюк Ю. И.

2021

Лабораторная работа №2

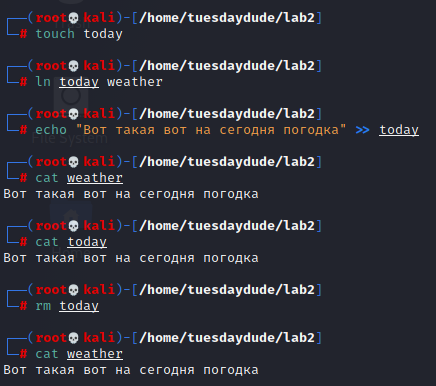
Ссылки. Права доступа

Цель работы: изучить работу с ссылками и правами ОС Linux.

Часть 1

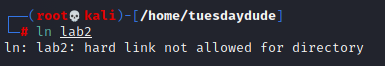
1. Изучить назначение и ключи команды ln. - создать жесткую ссылку на файл.

Просмотреть содержимое файла, используя ссылку. Удалить файл. Просмотреть содержимое файла. Объяснить результат.



В данном примере создано две жесткие ссылки на файл: today и weather. Жесткие ссылки равноправны, поэтому, удалив жесткую ссылку today, файл все еще можно просматривать, используя жесткую ссылку weather.

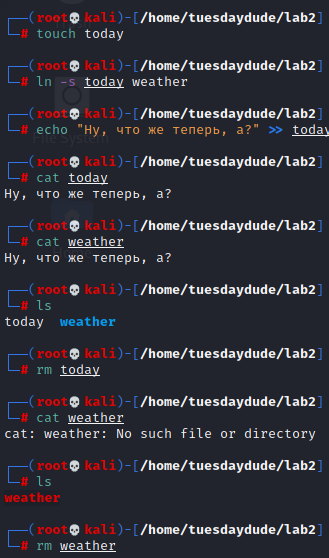
Создать жесткую ссылку на каталогю Объяснить результат.



Нельзя создавать жетские ссылки на каталоги.

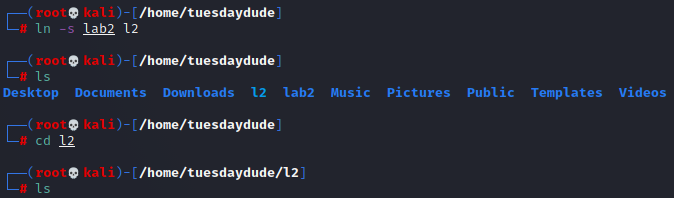
2. Выполнить все задания пункта 1, создавая не жесткие, а символьные ссылки.

Просмотреть содержимое файла, используя ссылку. Удалить файл. Просмотреть содержимое файла. Объяснить результат.



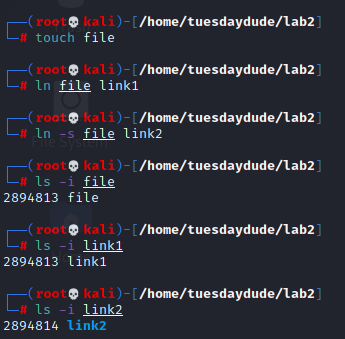
В отличие от жестких ссылок, после удаления указываемого ими файла символьные списки перестают работать, поэтому после удаления файла today ссылка weather перестала работать.

Создать ссылку на каталог



Также, в отличие от жестких ссылок, символьные ссылки позволяют создавать ссылки на каталоги.

3. Создать жесткую и символьную ссылки на файл. С помощью команды ls просмотреть inod файла и ссылок. Объяснить результат.



Поскольку жесткие ссылки между собой равноправны, то у жесткой ссылки и файла inod одинаков. У символьной ссылки inod отличается.

Часть 2

1. Изучите при помощи man опцию -l команды ls. Просмотрите права каталогов/etc, /bin и домашнего каталога. Просмотрите права файлов, содержащиеся в этих каталогов. Выявите тенденции (файлов с какими правами в каких каталогах больше). Сделайте вывод.



В каталоге /etc больше файлов с разрешением drwxr-xr-x.

drwxr-xr-x: Все пользователи могут читать данный каталог, но изменять его может только владелец

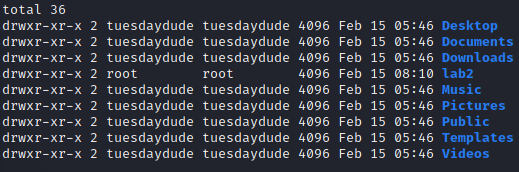


В каталоге /bin больше всего файлов lrwxrwxrwx и -rwxr-xr-x

lrwxrwxrwx: l – символическая ссылка, все пользователи имеют право на запись, чтение и исполнение.

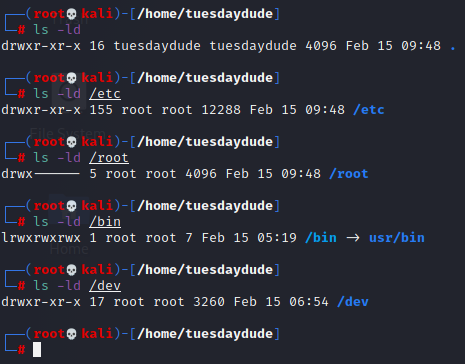
-rwxr-xr-x: Обычный файл. Все пользователи могут читать данный файл, но изменять его может только владелец

Домашний каталог:

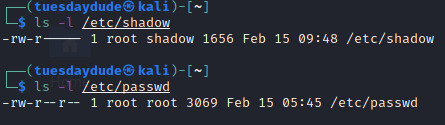


Содержит только файлы с разрешением drwxr-xr-x: Все пользователи могут читать данный каталог, но изменять его может только владелец

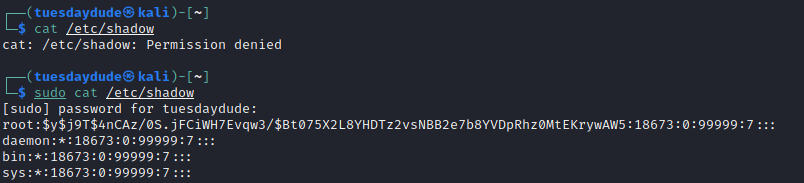
2. Изучите материал, посвящѐнный пользователям и группам пользователей. Изучите руководство по командам chown и chgrp. Выясните, кто является владельцем и к какой группе владельцов принадлежат файлы вашего домашнего каталога, каталогов /etc, /root, /bin и /dev.



3. Определите атрибуты файлов /etc/shadow и /etc/passwd

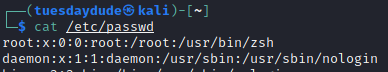


попробуйте вывести на экран содержимое этих файлов. Объясните результат.



Файл /etc/shadow(-rw-r-----) могут читать только пользователи root и пользователи группы shadow:





Файл /etc/passwd(-rw-r—r--) Могут читать все пользователи

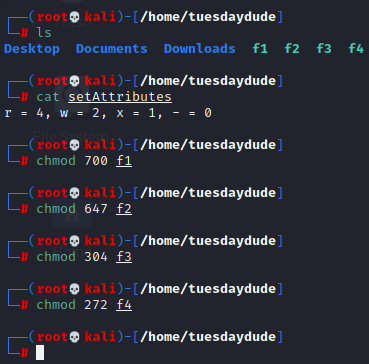
4. Изучите команду chmod. Создайте в домашнем каталоге любые четыре файла, установите при помощи восмеричных масок на каждый из них в отдельности следующие права:

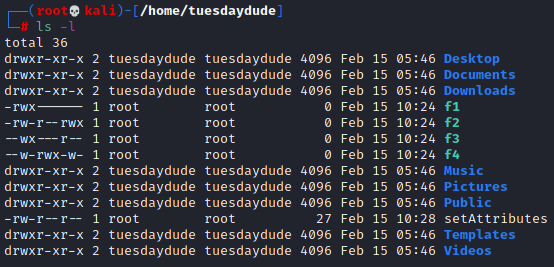
- для себя все права, для группы и остальных - никаких;

- для себя чтение и запись, для группы чтение, для остальных - все;

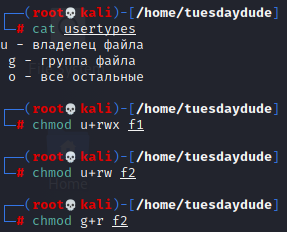
- для себя исполнение и запись, для группы никаких, для остальных чтение;

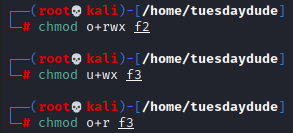
- для себя запись, для группы все, для остальных - только запись.

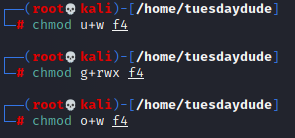


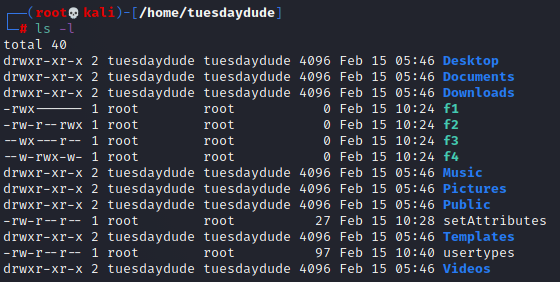


5. Выполните задание предыдущего пункта, используя в команде chmod только символы прав доступа.



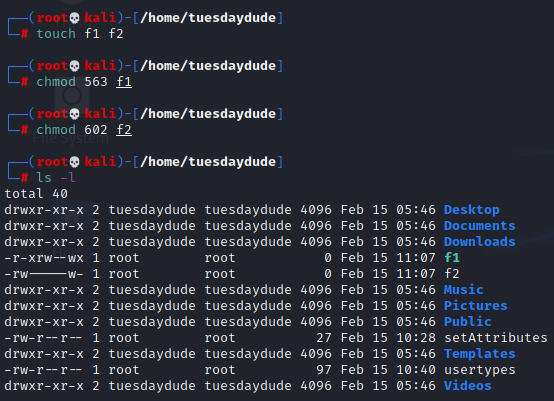






6. Переведите номер своей зачетной книжки в восьмеричную систему счисления, разбейте полученное значение на группы по 2-3 цифры и создайте файлы с правами доступа, выраженными полученными масками. Сопоставьте данные маски с символами прав доступа и объясните, какие операции с данными файлами доступны каким субъектам системы.

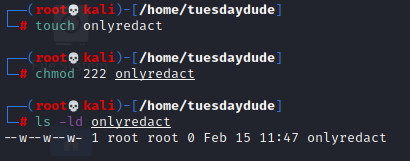
19033810 = 5636028 : (563)(602)



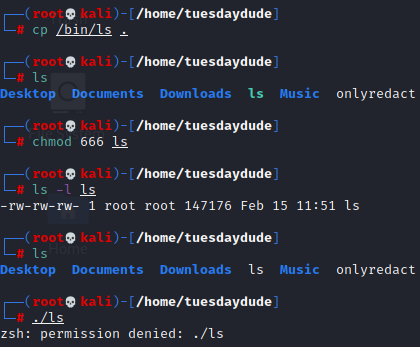
f1(-r-xrw--wx): Владелец файла может читать его. Члены группы владельцев могут записывать данные в файл, читать и исполнять его, остальные могут записывать данные в файл и исполнять его.

f2(-rw-----w-): Владелец файла может читать и записывать данные в файл, члены группы владельцев ничего не могут, остальные могут записывать данные в файл.

7. В домашнем каталоге создайте файл и установите на него права так, чтобы его можно было только редактировать.

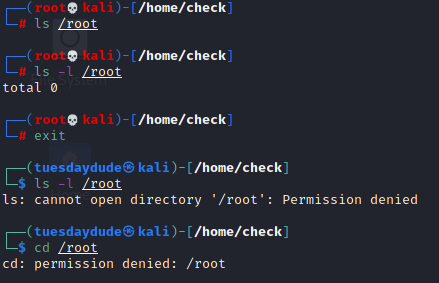


8. Скопируйте в свой домашний каталог файл ls из каталога /bin. Запретите выполнение этого файла и попробуйте выполнить именно его, а не исходный(!). Объясните результат.



Т.к. исполнение файла /home/tuesdaydude/ls запрещено, то и исполнить его невозможно.

9. Изучите на что влияют права доступа в случае каталогов. Попробуйте зайти в каталог /root, объясните результат и причину.





Что-либо делать с каталогом root может только пользователь root.

Вывод: Изучил работу с ссылками и правами Linux.