Министерство образования Республики Беларусь
учреждение образования
«Брестский государственный технический университет»
Кафедра ИИТ

Лабораторная работа № 2

«Интерфейс. Файлы. Команды»

Выполнил: студент 2-го курса
группы АС-65
Осовец М.М
Проверил: Степанчук В.И.

Брест 2024

Цель работы: научиться работать с жесткими и символическими ссылками и правами доступа в ОС Linux

Ход работы

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;
- создать жесткую ссылку на каталог. Объяснить результат;

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ echo "Это содержимое файла"
 > original.txt
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ln original.txt link.txt
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ cat link.txt
Это содержимое файла
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ rm original.txt
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ cat link.txt
Это содержимое файла
```

Результат: содержимое файла все ещё доступно через жесткую ссылку, так как ссылка указывает на ту же область памяти на диске, что и исходный файл. Жёсткая ссылка остаётся рабочей, даже если исходный файл был удалён, поскольку inode (дескриптор файла) продолжает существовать, пока хотя бы одна ссылка указывает на него.

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

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ echo  "Это содержимое файла
" > oridinal.txt
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ln -s oridinal.txt linkk.tx
t
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ cat link.txt
Это содержимое файла
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ rm oridinal.txt
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ cat linkk.txt
cat: linkk.txt: Нет такого файла или каталога
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$
```

Результат:Символическая (косвенная) ссылка содержит путевое имя файла, для которого она создается. Чтобы удалить файл, нужно удалить только прямые ссылки ,если остались символические ссылки, доступ к файлу по ним будет невозможен.

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

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ touch "main.txt"
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ln main.txt mainn.txt
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ln -s main.txt maine.txt
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -i maninn.txt maine.txt
```

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -i mainn.txt maine.txt
5015049 maine.txt  4982436 mainn.txt
```

Результат:Основное различие заключается в том, что жесткие ссылки указывают на одни и те же данные на диске, в то время как символические ссылки указывают на имя файла, и у них свои собственные метаданные.

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.

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ man ls
-l     use a long listing format
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -l /etc
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -l /bin
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -l ~
```

Вывод: В каталоге /bin файлы имеют права на выполнение для всех пользователей. Это общее правило для каталогов, содержащих программы. В каталоге /etc права более строгие файлы, и они не должны быть доступны для записи всем пользователям.В домашнем каталоге права доступа более гибкие, но, как правило, пользователи могут только читать и записывать свои файлы.

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.

Домашний каталог

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -ld ~
drwxr-x--- 33 mark mark 4096 окт 15 13:57 /home/mark
```

В этом каталоге владелец mark, группа mark

Каталог etc

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -ld /etc
drwxr-xr-x 146 root root 12288 окт 26 20:56 /etc
```

В этом каталоге владелец root, группа root

Каталог bin

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -ld /bin
lrwxrwxrwx 1 root root 7 апр 22  2024 /bin -> usr/bin
```

В этом каталоге владелец root, группа root

Каталог dev

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -ld /dev
drwxr-xr-x 20 root root 5560 окт 30 17:40 /dev
```

В этом каталоге владелец root, группа root

3. Определите атрибуты файлов /etc/shadow и /etc/passwd попробуйте вывести на экран содержимое этих файлов. Объясните результат.

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1368 сен  9 20:41 /etc/shadow
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2984 июл 23 23:14 /etc/passwd
```

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ cat /etc/shadow
cat: /etc/shadow: Отказано в доступе
```

Объяснение: /etc/passwd доступен для чтения всем пользователям, поскольку содержит общедоступную информацию, необходимую для идентификации пользователей./**etc/shadow** защищен, так как содержит конфиденциальные данные (хэши паролей), и доступен только пользователю root и группе shadow.

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.

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ touch ~/file1 ~/file2 ~/file3 ~/file4
```

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod 700 ~/file1
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod 674 ~/file2
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod 201 ~/file3
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod 263 ~/file4
```

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

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod u=rwx,g=,o= ~/file1
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod u=rw,g=r,o=rwx ~/file2
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod u=wx,g=,o=r ~/file3
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod u=w,g=rwx,o=w ~/file4
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$
```

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.

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ echo "ibase=10; obase=8; 230239" | bc
701537
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ touch ~/file_70 ~/file_15 ~/file_37
```

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod 70 ~/file_70
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod 15 ~/file_15
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod 37 ~/file_37
```

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

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ touch ~/edit_file
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod 222  ~/edit_file
```

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.

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ cp /bin/ls ~/
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ chmod a-x ~/ls
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ ~/ls
bash: /home/mark/ls: Отказано в доступе
```

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

```
mark@mark-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ cd /root
bash: cd: /root: Отказано в доступе
```

Обьяснение: Каталог /root является домашним каталогом пользователя root, и доступ к нему ограничен только для этого пользователя. Даже если у вас есть права на чтение файлов в этом каталоге (например, если бы у вас были права на чтение), у вас нет прав на выполнение (x) для входа в каталог. В Linux безопасность данных реализована через права доступа, и каталог /root предназначен для защиты конфиденциальной информации, хранящейся под управлением суперпользователя.

Вывод: в ходе работы мы научились использовать жесткие и символические ссылки, также научились работать с правами доступа, узнав о том какие права бывают и для чего они используются.