Учреждение образования
«Брестский государственный технический университет»
Кафедра ИИТ

Лабораторная работа №2
По дисциплине: «ОСиСП»
Тема: «ССЫЛКИ. ПРАВА ДОСТУПА.»

Выполнил:
Студент 2 курса
Группы ПО-7
Комиссаров А.Е.
Проверила:
Давидюк Ю.И.

2022

Цель: научиться работать с основными командами для ссылок и прав доступа на системе Linux.

Выполнение заданий:

Часть 1.

1. Изучить назначение и ключи команды ln.

- создать жесткую ссылку на файл.

~$ln file.txt myfile

Просмотреть содержимое файла, используя ссылку.

~$cat myfile

Удалить файл. Просмотреть содержимое файла.

~$rm file.txt

~$cat myfile

Объяснить результат – Содержимое файла вывелось на экран в полном его содержании, так как при удалении имени удаляется только связь, и только если связей больше нет, то удаляется весь файл.

- создать жесткую ссылку на каталог. Объяснить результат;

~$ mkdir dir1

~$ ln dir1 newdir

"Не допускается создавать жёсткие ссылки на каталоги"

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

Создать ссылку на файл. Просмотреть содержимое файла, используя ссылку. Удалить файл. Просмотреть содержимое файла.

~$ ln -s file2 newfile2

~$ cat newfile2

Получим содержимое

~$ rm file2

~$ cat newfile2

«Нет такого файла или каталога».

Создать ссылку на каталог.

~$ ln -s dir1 newdir1

~$ ls newdir1

Символьные ссылки содержат только имя и путь к файлу, соответственно при удалении оригинального файла, содержимое файла по ссылке получить не получится.

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

~$ ln file2.txt myfile1
~$ ln -s file2.txt myfile2
~$ ls -i file2.txt
~$ ls -i myfile1

Жесткие ссылки и имя файла равноправны, и изменение любых данных распространяется на ссылку и на файл, по результатам команд Inod у них одинаковый.

~$ ls -i myfile2
У символьной ссылки и файла разный inod.

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.

~$ man ls

«-l use a long listing format»

Права каталогов /etc и /bin:

```
andrey@andrey-VirtualBox:~$ ls -ld /etc
drwxr-xr-x 132 root root 12288 кра 14 14:42 /etc
andrey@andrey-VirtualBox:~$ ls -ld /bin
lrwxrwxrwx 1 root root 7 сак 23 16:12 /bin -> usr/bin
andrey@andrey-VirtualBox:~$ ls -ld ./
drwxr-xr-x 18 andrey andrey 4096 кра  5 21:44 ./
```

drwxr-xr-x : “директория, все права для владельца, отсутствует право на запись для группы и остальных пользователей”

lrwxrwxrwx : “символьная ссылка, все права (rwx) для всех пользователей”

~$ ls -l /etc

```
andrey@andrey-VirtualBox:~$ ls -l /etc
итого 1112
drwxr-xr-x  3 root root    4096 лют 23 11:50 acpi
-rw-r--r--  1 root root    3028 лют 23 11:47 adduser.conf
drwxr-xr-x  3 root root    4096 лют 23 11:48 alsa
drwxr-xr-x  2 root root    4096 кра  5 21:18 alternatives
-rw-r--r--  1 root root     401 лiп 16  2019 anacrontab
-rw-r--r--  1 root root     433 кас  2  2017 apg.conf
drwxr-xr-x  5 root root    4096 лют 23 11:48 apm
drwxr-xr-x  3 root root    4096 лют 23 11:50 apparmor
drwxr-xr-x  6 root root    4096 кра  5 20:57 apparmor.d
drwxr-xr-x  4 root root    4096 лют 23 11:50 apport
```

/etc – преобладают файлы с правами drwxr-xr-x (d – директория, rwx – для себя право на чтение, изменение и исполнение; r-xr-x - для группы и остальных право на чтение и исполнение).

~$ ls -l /bin

```
lrwxrwxrwx 1 root root 7 сак 23 16:12 /bin -> usr/bin
```

В каталоге /bin – lrwxrwxrwx (l – символическая ссылка, rwxrwxrwx – для себя, группы и остальных право на чтение, изменение и исполнение).

~$ ls -l ./

```
andrey@andrey-VirtualBox:~$ ls -l ./
итого 4744
drwxrwxr-x 4 andrey andrey    4096 кра  4 20:18  kom
-rw-rw-r-- 1 andrey andrey 4803796 сне  7 01:48  mkc
-rw-rw-r-- 1 andrey andrey      49 кра  5 00:15  myf
-rw------- 1 andrey andrey    1743 кра  5 21:29  roo
-rw-rw-r-- 1 andrey andrey    1452 кра  5 21:39  roo
-rw-rw-r-- 1 andrey andrey     416 кра  5 21:25  rou
-rw-rw-r-- 1 andrey andrey       0 кра  5 21:18  tex
drwxr-xr-x 2 andrey andrey    4096 сак 23 16:24  Вид
drwxr-xr-x 2 andrey andrey    4096 сак 23 16:24  Док
drwxr-xr-x 2 andrey andrey    4096 сак 23 16:24  Заг
drwxr-xr-x 2 andrey andrey    4096 сак 23 16:24  Изо
drwxr-xr-x 2 andrey andrey    4096 сак 23 16:24  Муз
drwxr-xr-x 2 andrey andrey    4096 сак 23 16:24  Общ
drwxr-xr-x 2 andrey andrey    4096 кра  4 19:34 'Раб
```

В домашнем каталоге больше всего – drwxr-xr-x (d – директория, rwx – для себя право на чтение, изменение и исполнение; r-xr-x - для группы и остальных право на чтение и исполнение).

Почти во всех файлах присутствует право на чтение, а также для “владельца” присутствуют права RWX.

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.

```
andrey@andrey-VirtualBox:~$ ls -ld ./
drwxr-xr-x 18 andrey andrey 4096 кра  5 21:44 ./
andrey@andrey-VirtualBox:~$ ls -ld /etc
drwxr-xr-x 132 root root 12288 кра 14 14:42 /etc
andrey@andrey-VirtualBox:~$ ls -ld /root
drwx------ 4 root root 4096 сак 23 16:24 /root
andrey@andrey-VirtualBox:~$ ls -ld /bin
lrwxrwxrwx 1 root root 7 сак 23 16:12 /bin -> usr/bin
andrey@andrey-VirtualBox:~$ ls -ld /dev
drwxr-xr-x 20 root root 4100 кра 19 11:21 /dev
```

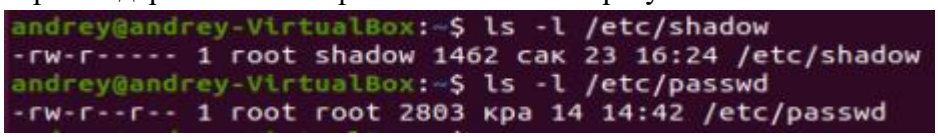
В каждом случае с новой строки выводится информация в таком порядке:

1. Права доступа
2. Количество жёстких ссылок
3. Владелец
4. Группа
5. Размер и т.д.

Для домашнего каталога владелец и группа это пользователь andrey (я).

Для /etc, /root, /bin и /dev владелец и группа это root – пользователь (система, супер-пользователь, который имеет полные права для изменения системных файлов).

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



~$ cat /etc/shadow

"Отказано в доступе".

~$ cat /etc/passwd

Здесь вывелось содержимое файла.

В первом случае вывело "Отказано в доступе" потому что в колонке "Other" (остальные пользователи) отсутствуют какие-либо права доступа (стоит три тире), значит доступ к файлу нам был закрыт.
Во втором же случае доступ для чтения (r--) открыт, поэтому мы смогли прочитать файл.

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;

~$ chmod 700 myfile1

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

~$ chmod 647 myfile2

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

~$ chmod 304 myfile3

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

~$ chmod 272 myfile4

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

~$ chmod a-rwx myfile1
~$ chmod u+rwx myfile1

~$ chmod a-rwx myfile2
~$ chmod u+rw myfile2
~$ chmod g+r myfile2
~$ chmod o+rwx myfile2

~$ chmod a-rwx myfile3
~$ chmod u+wx myfile3
~$ chmod g+rwx myfile3
~$ chmod o+r myfile3

~$ chmod a-rwx myfile4
~$ chmod u+w myfile4
~$ chmod g+rwx myfile4
~$ chmod o+w myfile4

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.

Номер зачетки: $200149_{10} = 0606725_8$
~$ chmod 060 myfile1
- - - - rw- - - -
~$ chmod 67 myfile2
- - - - rw- rwx
~$ chmod 25 myfile3
- - - - -w- r-x

File №	Данные маски	Права владельца	Права группы	Права остальных пользователей
Myfile1	Chmod 060	Никаких	Чтение и запись	Никаких
Myfile2	Chmod 67	Никаких	Чтение и запись	Все
Myfile3	Chmod 25	Никаких	Запись	Чтение и выполнение

7. В домашнем каталоге создайте файл и установите на него права так, чтобы его можно было только редактировать.
~$ nano file123.txt
~$ chmod 222 file123.txt

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.
~$ cp /bin/ls ./

~$ ls -l ls
“-rwxr-xr-x”
~$ chmod a-x ls
~$ ls -l ls
“-rw-r--r--"
~$ ./ls
“Отказано в доступе”

Так как мы убрали право на выполнение этого файла для владельца, группы и других, то мы не имеем право его выполнить, соответственно нам возвращается сообщение “отказано в доступе” при попытке его запуска.

9. Изучите на что влияют права доступа в случае каталогов. Попробуйте зайти в каталог /root, объясните результат и причину.
~$ cd /root
“Отказано в доступе”
~$ ls -ld /root
“drwx- - - - - -“ – У нас, как пользователя andrey недостаточно прав на чтение директории (владелец файла – root, то есть не мы, также в колонках group и other отсутствуют права доступа в принципе, значит нам запрещён доступ к каталогу).

Вывод: я научился работать с основными командами для ссылок и прав доступа на системе Linux.