Практическая работа «Права доступа к файлам и каталогам»

В этой практической работе будут рассмотрены как базовые, так и расширенные права доступа к файлам. Вы будете отображать права доступа к файлам, устанавливать основные права доступа (чтение, запись и выполнение) и устанавливать расширенные права доступа (setuid, setgid и sticky bit).

Кроме того, вы отобразите и установите значение umask, которое определяет разрешения по умолчанию для новых файлов и каталогов.

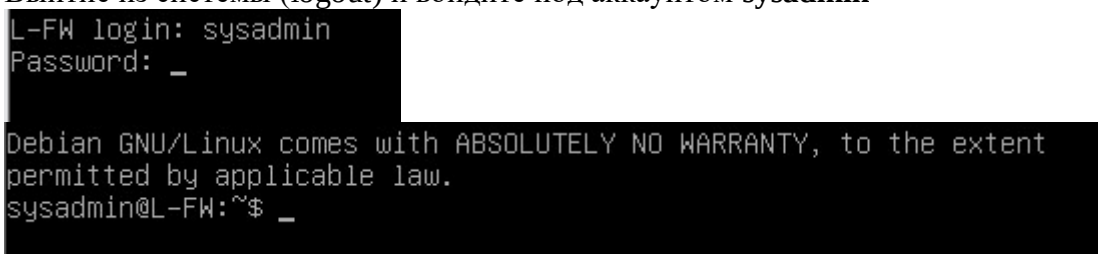
Создайте пользователя **sysadmin:class**

```
useradd –m –s /bin/bash sysadmin
```

Установите для пользователя пароль

```
passwd sysadmin
Введите пароль: class
Повторите пароль: class
```

Выйтие из системы (logout) и войдите под аккаунтом **sysadmin**



Выполните следующую команду, чтобы получить подробную информацию о файле **/etc/shadow**:

```
ls -l /etc/shadow
```

Обратите внимание, что владельцем этого файла является пользователь "root" , а владельцем группы является группа "shadow". Владелец пользователя имеет разрешение на чтение и запись, группы владельца имеет только разрешение на чтение, а обычные пользователи не имеют разрешения.

Выполните следующую команду, чтобы попытаться просмотреть файл /etc/shadow:

```
more /etc/shadow
```

Команда не выполнена, потому что только пользователь **root** и члены группы **shadow** могут просматривать содержимое этого файла.

Выполните следующую команду, чтобы перейти к учетной записи root:

```
su – root
```

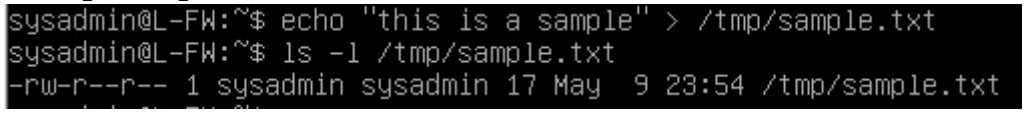
Введите пароль root-а: toor

Создайте файл в каталоге /tmp, выполнив следующую команду:

```
echo "this is a sample" > /tmp/sample.txt
```

Просмотрите разрешения этого файла и обратите внимание, что все пользователи могут просматривать содержимое файла, поскольку все пользователи имеют разрешение на чтение для файла:

```
ls -l /tmp/sample.txt
```



Выполните следующую команду, чтобы вернуться к учетной записи sysadmin:

```
exit
```

Убедитесь, что учетная запись **sysadmin** может просматривать содержимое файла, выполнив следующую команду:

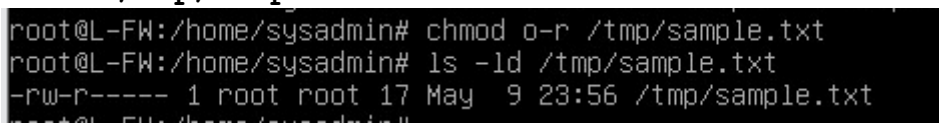
```
more /tmp/sample.txt
```

Выполните следующую команду, чтобы перейти к учетной записи root:

```
su
toor
```

Удалите возможность учетной записи **sysadmin** (которая принадлежит к набору разрешений «other») просматривать файл /tmp/sample.txt, выполнив следующую команду:

```
chmod o-r /tmp/sample.txt
ls -l /tmp/sample.txt
```




```
exit
```

Убедитесь, что учетная запись sysadmin **не может** просматривать содержимое файла, выполнив следующую команду:

```
more /tmp/sample.txt
```

Перейдите к учетной записи root

```
su
```

Выполните следующую команду, чтобы предоставить членам разрешения «others» установить возможность просмотра и изменения файла /tmp/sample.txt:

```
chmod o+rw /tmp/sample.txt
```

Выйдите из учетной записи root

```
exit
```

Убедитесь, что учетная запись sysadmin может изменять содержимое файла, выполнив следующую команду:

```
echo "well done" >> /tmp/sample.txt
```

Убедитесь, что учетная запись sysadmin **может** просматривать содержимое файла, выполнив следующую команду:

```
more /tmp/sample.txt
```

Перейдите к учетной записи root

```
su
```

Создайте каталог, выполнив следующую команду:

```
mkdir /tmp/data
```

Измените разрешения для каталога, чтобы только члены владельца группы и владелец пользователя имели доступ к этому каталогу:

```
chmod 770 /tmp/data
```

Проверьте измененные разрешения, выполнив следующую команду:

```
ls -ld /tmp/data
```

Скопируйте файл в этот каталог, чтобы убедиться, что текущий пользователь (пользователь **root**) может создавать файлы в этом каталоге. Напомним, что для успешного выполнения следующей команды пользователь должен иметь разрешение на запись и выполнение в каталоге:

```
cp /etc/hosts /tmp/data
ls /tmp/data
```

Выйдите из учетной записи root

```
exit
```

Выполните следующую команду. Эта команда должна завершиться сбоем, так как текущий пользователь не имеет прав доступа к этому каталогу:

```
ls /tmp/data
```

```
sysadmin@L-FW:~$ ls /tmp/data
ls: cannot open directory '/tmp/data': Permission denied
```

Использование setuid

Просмотрите права доступа к файлу /usr/bin/chfn, выполнив следующую команду:

```
sysadmin@L-FW:~$ ls -l /usr/bin/chfn
-rwsr-xr-x 1 root root 50040 May 17  2017 /usr/bin/chfn
```

Символ «**s**» в наборе разрешений владельца означают, что это файл **setuid**. При запуске эта программа может обращаться к файлам, как если бы программа запускалась от имени пользователя root (владельца файла). Эта конкретная команда позволяет пользователям изменять информацию в файле /etc/passwd.

Выполните следующую команду, чтобы изменить информацию вашей учетной записи:

chfn

Введите пароль пользователя sysadmin

class

Введите произвольные данные

Перейдите к учетной записи root

su

Измените файл /usr/bin/chfn, чтобы он больше не устанавливался, выполнив следующую команду:

chmod 0755 /usr/bin/chfn

Проверьте это изменение, выполнив следующую команду:

ls -l /usr/bin/chfn

```
root@L-FW:/home/sysadmin# chmod 0755 /usr/bin/chfn
root@L-FW:/home/sysadmin# ls -l /usr/bin/chfn
-rwxr-xr-x 1 root root 50040 May 17  2017 /usr/bin/chfn
```

Выйдите из учетной записи root

exit

Выполните следующую команду, чтобы попытаться изменить данные своей учетной записи:

chfn

Введите данные

```
sysadmin@L-FW:~$ chfn
Password:
Changing the user information for sysadmin
Enter the new value, or press ENTER for the default
        Full Name:
        Room Number []: 123
        Work Phone []: 123-123-123
        Home Phone []: 23
Cannot change ID to root.
```

Сообщение об ошибке указывает на то, что вы не можете использовать эту команду, поскольку она не может получить доступ к файлу **/etc/passwd** от имени пользователя **root**. Без разрешения **setuid** эта команда не будет работать для обычных пользователей.

Использование setugid

Перейдите к учетной записи root

su

Создайте каталог, выполнив следующую команду:

mkdir /tmp/test

Измените группе владельца этого нового каталога на группу "games", выполнив следующие команды:

chgrp games /tmp/test

ls -ld /tmp/test

```
root@L-FW:/home/sysadmin# mkdir /tmp/test
root@L-FW:/home/sysadmin# chgrp games /tmp/test
root@L-FW:/home/sysadmin# ls -ld /tmp/test
drwxr-xr-x 2 root games 4096 May 10 00:45 /tmp/test
```

Команда chgrp меняет групповое владение каталогом, как показано в выходных данных предыдущей команды **ls -ld**.

Обычно, создается новый файл, владельцем группы для нового файла становится основная группа. Создайте новый файл в этом каталоге и проверьте, выполнив следующие команды:

touch /tmp/test/file1.txt

ls -l /tmp/test/file1.txt

```
root@L-FW:/home/sysadmin# touch /tmp/test/file1.txt
root@L-FW:/home/sysadmin#
root@L-FW:/home/sysadmin# ls -l /tmp/test/file1.txt
-rw-r--r-- 1 root root 0 May 10 00:47 /tmp/test/file1.txt
```

Если каталог имеет установленное разрешение **setgid**, то все новые файлы будут принадлежать той же группе, которая владеет каталогом. Используйте следующие команды, чтобы установить разрешение **setgid** и проверить новое разрешение. Вы должны увидеть «**s**» в группе разрешений на выполнение:

chmod g+s /tmp/test

ls -ld /tmp/test

```
root@L-FW:/home/sysadmin# chmod g+s /tmp/test

lroot@L-FW:/home/sysadmin#
root@L-FW:/home/sysadmin# ls -ld /tmp/test

drwxr-sr-x 2 root games 4096 May 10 00:47 /tmp/test
```

Убедитесь, что разрешение **setgid** работает, выполнив следующие команды:

touch /tmp/test/file2.txt

ls -l /tmp/test/file2.txt

```
root@L-FW:/home/sysadmin# touch /tmp/test/file2.txt
root@L-FW:/home/sysadmin#
root@L-FW:/home/sysadmin# ls -l /tmp/test/file2.txt
-rw-r--r-- 1 root games 0 May 10 00:49 /tmp/test/file2.txt
```

Обратите внимание, что этот новый файл принадлежит группе "**games**", а не группе **root**.

Использование sticky bit

mkdir /pub

chmod 777 /pub

ls -ld /pub

Права доступа к этому новому каталогу позволят любому пользователю создавать и удалять файлы в каталоге. Чтобы проверить это, сначала создайте файл:

touch /pub/myfile
ls -l /pub

```
root@L-FW:/home/sysadmin# touch /pub/myfile
ls -l /puroot@L-FW:/home/sysadmin#
root@L-FW:/home/sysadmin# ls -l /pub
total 0
-rw-r--r-- 1 root root 0 May 10 00:52 myfile
```

Выйдите из учетной записи root

exit

Выполните следующую команду, чтобы удалить ранее созданный файл. Когда появится запрос «rm: удалить обычный пустой защищенный от записи файл` /pub/myfile '? », Ответьте **y**:

rm /pub/myfile
ls -l /pub

Обратите внимание, что пользователь **sysadmin** смог удалить файл, принадлежащий пользователю **root.** Это связано с тем, что разрешение на запись в каталог дает возможность добавлять и удалять файлы в каталоге.

Перейдите к учетной записи root

su

Добавьте разрешение «sticky bit» в каталог **/pub**, чтобы пользователи могли удалять в этом каталоге только те файлы, которыми они владеют:

chmod o+t /pub

```
root@L-FW:/home/sysadmin# chmod o+t /pub
root@L-FW:/home/sysadmin# ls -l /pub
total 0
-rw-r--r-- 1 root root 0 May 10 00:52 myfile
root@L-FW:/home/sysadmin# ls -ld /pub
drwxrwxrwt 2 root root 4096 May 10 00:52 /pub
```

Опять же, создайте файл в этом каталоге, который можно использовать для проверки нового набора разрешений:

touch /pub/myfile
ls -l /pub

Выйдите из учетной записи root

exit

Выполните следующие команды, чтобы попытаться удалить ранее созданный файл. Когда появится запрос «rm: удалить обычный пустой защищенный от записи файл` / pub / myfile '? », Ответьте y:

rm /pub/myfile
ls -l /pub

```
sysadmin@L-FW:~$ rm /pub/myfile
rm: remove write-protected regular empty file '/pub/myfile'? y
rm: cannot remove '/pub/myfile': Operation not permitted
sysadmin@L-FW:~$ ls -l /pub
total 0
-rw-r--r-- 1 root root 0 May 10 00:52 myfile
```

Использование umask

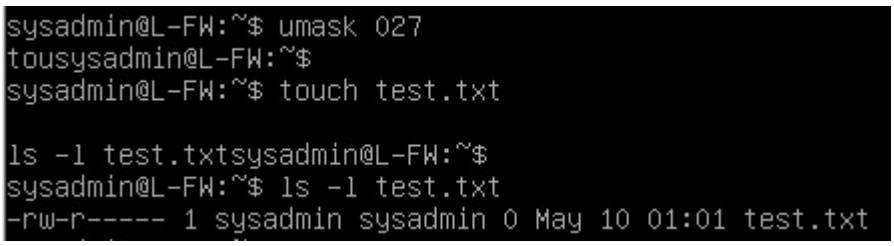
touch sample.txt
ls -l sample.txt

Обратите внимание, что разрешения по умолчанию для этого нового файла - «rw-rw-r--». Это результат значения **umask 022**. Выполните следующую команду, чтобы увидеть этот параметр:

umask

Выполните следующие команды, чтобы изменить настройку umask на **027** и убедиться, что новые файлы теперь имеют набор разрешений «rw-r -----»:

```
umask 027
touch test.txt
ls -l test.txt
```

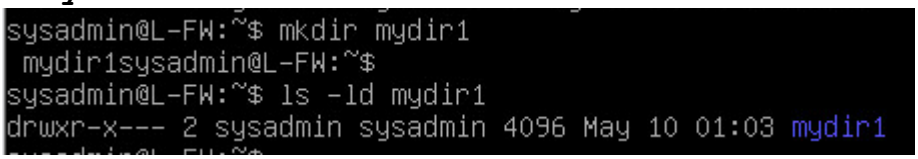


Помните, что значение umask влияет только на новые файлы и каталоги. Любой существующий файл никогда не будет зависеть от значения umask.

Значение umask предназначено для того, чтобы вам было проще указывать разрешения по умолчанию для новых файлов и каталогов. Выбирая хорошее значение umask, вы в будущем сэкономите много сил, поскольку вам не придется часто менять разрешения для новых файлов и каталогов.

Выполните следующие команды, чтобы создать новый каталог, и убедитесь, что значение umask 027 дает разрешения для новых каталогов «rwxr-x ---»:

```
mkdir mydir1
ls -ld mydir1
```



Выполните следующие команды, чтобы изменить umask на **002** и убедиться, что это приводит ко всем новым каталогам, имеющим набор разрешений «rwxrwxr-x»: