

Лабораторная работа №3

Настройка прав доступа

Сидорова А.В.

Российский университет дружбы народов, Москва, Россия

Информация

- Сидорова Арина Валерьевна
- студентка НПИбд-02-24
- ст.б. 1132242912
- Российский университет дружбы народов

Вводная часть

Управление правами доступа к файлам и каталогам является фундаментальным аспектом информационной безопасности в многопользовательских операционных системах, к которым относятся все дистрибутивы Linux. Неправильная настройка прав может привести к утечке конфиденциальной информации, её повреждению или удалению.

Объект исследования

- Механизмы управления правами доступа в операционной системе Linux.

Предмет исследования

Практическая реализация разграничения прав доступа с использованием базовых разрешений

- Получение практических навыков настройки базовых и специальных прав доступа для групп пользователей в ОС Linux;
- На практике освоить управление базовыми разрешениями;
- Освоить управление специальными разрешениями;
- Освоить управление расширенными разрешениями;

Выполнение лабораторной работы

Управление базовыми разрешениями

Откроем терминал с учетной записью root. В корневом каталоге создадим каталоги /data/main/ и /data/third. Проверим, кто является владельцем этих каталогов.

```
avsidorova@avsidorova:~$ sudo i
[sudo] пароль для avsidorova:
sudo: i: команда не найдена
avsidorova@avsidorova:~$ sudo -i
root@avsidorova:~# mkdir -p /data/main /data/third
root@avsidorova:~# ls -Al /data
итого 0
drwxr-xr-x. 2 root root 6 сен 19 07:32 main
drwxr-xr-x. 2 root root 6 сен 19 07:32 third
```

Рис. 1: main,third

Изменим владельцев

Изменим владельцев этих каталогов с root на main и third соответственно.

```
root@avsidorova:~# chgrp main /data/main  
root@avsidorova:~# chgrp third /data/third
```

Рис. 2: изменим владельцев

```
root@avsidorova:~# ls -Al /data  
итого 0  
drwxr-xr-x. 2 root main  6 сен 19 07:32 main  
drwxr-xr-x. 2 root third 6 сен 19 07:32 third
```

Рис. 3: проверяю владельцев

Установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям группам. После этого проверим установленные права.

```
root@avsidorova:~# chmod 770 /data/main
root@avsidorova:~# chmod 770 /data/third
root@avsidorova:~# ls -Al /data
итого 0
drwxrwx---. 2 root main  6 сен 19 07:32 main
drwxrwx---. 2 root third 6 сен 19 07:32 third
```

Рис. 4: chmod

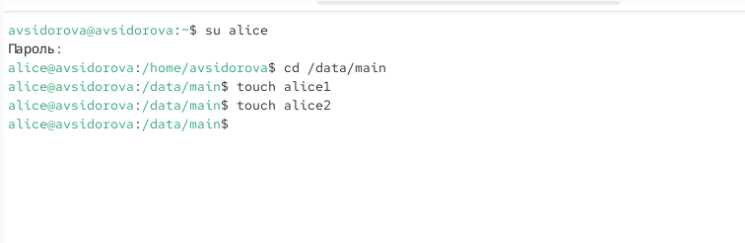
Перейдем в другой терминал, под пользователем bob в каталоге /data/main создадим файл emptyfile. Создался файл под пользователем bob, так как у группы есть права доступа. Перейдем в каталог /data/third и создадим файл emptyfile, нам отказано в доступе, так как группа не имеет прав

```
root@avsidorova:~# su - bob
bob@avsidorova:~$ cd /data/main
bob@avsidorova:/data/main$ touch emptyfile
bob@avsidorova:/data/main$ ls -Al
итого 0
-rw-r--r--. 1 bob bob 0 сен 19 07:35 emptyfile
bob@avsidorova:/data/main$ cd /data/third
-bash: cd: /data/third: Отказано в доступе
bob@avsidorova:/data/main$ █
```

Рис. 5: emptyfile

Управление специальными разрешениями

Откроем новый терминал под пользователем Alice. Перейдем в каталог /data/main и создадим два файла alice1, alice2



```
avsidorova@avsidorova:~$ su alice
Пароль:
alice@avsidorova:/home/avsidorova$ cd /data/main
alice@avsidorova:/data/main$ touch alice1
alice@avsidorova:/data/main$ touch alice2
alice@avsidorova:/data/main$
```

Рис. 6: alice1, alice2

Видим два файла, созданные пользователем alice. Попробуем удалить файлы, принадлежащие пользователю alice. Создадим два файла, которые будут принадлежать пользователю bob (bob1, bob2)

```
bob@avsidorova:/data/main$ ls -Al
итого 0
-rw-r--r--. 1 alice alice 0 сен 19 07:39 alice1
-rw-r--r--. 1 alice alice 0 сен 19 07:39 alice2
-rw-r--r--. 1 bob  bob  0 сен 19 07:35 emptyfile
bob@avsidorova:/data/main$ rm -f alice*
bob@avsidorova:/data/main$ ls -Al
итого 0
-rw-r--r--. 1 bob bob 0 сен 19 07:35 emptyfile
bob@avsidorova:/data/main$ touch bob1
bob@avsidorova:/data/main$ touch bob2
bob@avsidorova:/data/main$
```

Рис. 7: bob1, bob2

В терминале под пользователем root установим для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы



```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# chmod g+s,o+t /data/main
root@avsidorova:~#
```

Рис. 8: chmod g+s o+t

В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4. Теперь мы увидели, что два созданных файла принадлежат группе main, которая является группой-владельцем каталога /data/main

```
alice@avsidorova:/data/main$ touch alice3
alice@avsidorova:/data/main$ touch alice4
alice@avsidorova:/data/main$ ls-l
bash: ls-l: команда не найдена...
^[A^Z
[1]+  Остановлен    ls-l
alice@avsidorova:/data/main$ ls -l
итого 0
-rw-r--r--. 1 alice main 0 сен 19 07:43 alice3
-rw-r--r--. 1 alice main 0 сен 19 07:43 alice4
-rw-r--r--. 1 bob   bob   0 сен 19 07:40 bob1
-rw-r--r--. 1 bob   bob   0 сен 19 07:40 bob2
-rw-r--r--. 1 bob   bob   0 сен 19 07:35 emptyfile
alice@avsidorova:/data/main$ █
```

В терминале под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob

```
alice@avsidorova:/data/main$ rm -rf bob*  
rm: невозможно удалить 'bob1': Операция не позволена  
rm: невозможно удалить 'bob2': Операция не позволена  
alice@avsidorova:/data/main$
```

Рис. 10: rm -rf bob*

Управление расширенными разрешениями с использованием списков ACL

Установим права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third. Используем команду getfacl, чтобы убедиться в правильности установки разре-

```
root@avsidorova:~# setfacl -m g:third:rx /data/main
root@avsidorova:~# setfacl -m g:main:rx /data/third
root@avsidorova:~# getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# flags: -st
user::rwx
group::rwx
group:third:r-x
mask::rwx
other::---
```



```
root@avsidorova:~# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rwx
```

Создадим новый файл с именем newfile1 в каталоге /data/main и проверим текущие назначения полномочий (user - чтения и редактирование; group, other - чтение). Выполним аналогичные действия в /data/third

```
root@avsidorova:~# touch /data/main/newfile1
root@avsidorova:~# getfacl /data/main/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile1
# owner: root
# group: main
user::rw-
group::r--
other::r--

root@avsidorova:~# █
```

Рис. 12: newfile1

Установим ACL по умолчанию для каталога /data/main. Добавим ACL по умолчанию для каталога /data/third. Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main.

```
root@avsidorova:~# setfacl -m d:g:third:rwX /data/main
root@avsidorova:~# setfacl -m d:g:main:rwX /data/third
root@avsidorova:~# touch /data/main/newfile2
root@avsidorova:~# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rw-
group::rw-                    #effective:rw-
group:third:rwX                #effective:rw-
mask::rw-
other::---
```

Используем `getfacl` для проверки текущих назначений полномочий. Выполним аналогичные действия для каталога `/data/third`.

```
-----  
root@avsidorova:~# touch /data/third/newfile2  
root@avsidorova:~# getfacl /data/third/newfile2  
getfacl: Removing leading '/' from absolute path names  
# file: data/third/newfile2  
# owner: root  
# group: root  
user::rw-  
group::rwx                               #effective:rw-  
group:main:rwx                           #effective:rw-  
mask::rw-  
other::---  
  
root@avsidorova:~# █
```

Рис. 15: ACL /data/third

Проверка полномочий

Для проверки полномочий группы third в каталоге /data/third войдем в другом терминале под учётной записью члена группы third. Проверим операции с файлами: rm /data/main/newfile1 - Успешно rm /data/main/newfile2 - Не хватает прав доступа Проверим, возможно ли осуществить запись в файл: echo "Hello, world" » /data/main/newfile1 - Не хватает прав доступа echo "Hello, world" » /data/main/newfile2 - Успешно

```
carol@avsidorova:~$ rm /data/main/newfile1
rm: удалить защищенный от записи пустой обычный файл '/data/main/newfile1'?
carol@avsidorova:~$ rm /data/main/newfile2
rm: невозможно удалить '/data/main/newfile2': Отказано в доступе
carol@avsidorova:~$ cd /data/main
carol@avsidorova:/data/main$ ls
alice3 alice4 bob1 bob2 emptyfile newfile1 newfile2
carol@avsidorova:/data/main$ ls -Al
итого 0
-rw-r--r--. 1 alice main 0 сен 19 07:43 alice3
-rw-r--r--. 1 alice main 0 сен 19 07:43 alice4
-rw-r--r--. 1 bob   bob   0 сен 19 07:40 bob1
-rw-r--r--. 1 bob   bob   0 сен 19 07:40 bob2
-rw-r--r--. 1 bob   bob   0 сен 19 07:35 emptyfile
-rw-r--r--. 1 root  main 0 сен 19 07:47 newfile1
-rw-rw----+ 1 root  main 0 сен 19 07:51 newfile2
carol@avsidorova:/data/main$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Отказано в доступе
carol@avsidorova:/data/main$ echo "Hello, world" >> /data/main/newfile2
```

Результаты

В ходе лабораторной работы были успешно получены практические навыки по управлению пользователями и группами в ОС Linux

- Базовые права доступа (chmod, chown, chgrp) являются основным и эффективным механизмом для разграничения доступа между тремя базовыми категориями: пользователем-владельцем, группой-владельцем и всеми остальными. ;
- Специальные атрибуты прав расширяют возможности базовой модели;
- Расширенные списки доступа (ACL) являются мощным инструментом для реализации сложных политик разграничения прав;
- Полученные навыки являются фундаментальными для дальнейшей деятельности в области системного администрирования и информационной безопасности.

...