

Информационная безопасность

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Выполнила: Халфина Айсылу Зуфаровна

Группа: НПМБд-02-19

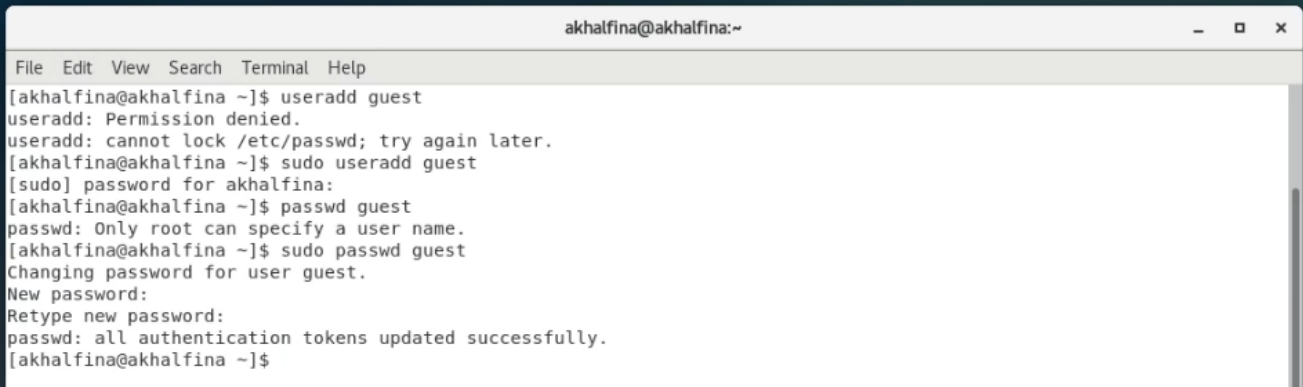
08.09.2022

Цель работы

1. Получение практических навыков работы в консоли с атрибутами файлов;
2. Закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Выполнение

Первым делом нам необходимо создать нового пользователя под именем **guest** и задать для него пароль. (Рис. 1)



```
akhalfina@akhalfina:~  
File Edit View Search Terminal Help  
[akhalfina@akhalfina ~]$ useradd guest  
useradd: Permission denied.  
useradd: cannot lock /etc/passwd; try again later.  
[akhalfina@akhalfina ~]$ sudo useradd guest  
[sudo] password for aklalfina:  
[akhalfina@akhalfina ~]$ passwd guest  
passwd: Only root can specify a user name.  
[akhalfina@akhalfina ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[akhalfina@akhalfina ~]$
```

Далее перезайдём в систему уже под новым пользователем. Откроем терминал и с помощью команды **pwd** проверим в какой директории находимся. Видим что это наша домашняя директория. (Рис. 2)

```
guest@akhalfina:~  
File Edit View Search Terminal Help  
[guest@akhalfina ~]$ pwd  
/home/guest  
[guest@akhalfina ~]$
```

Проверим имя текущего пользователя при помощи команды **whoami**. Затем посмотрим сводную информацию по нашему пользователю с помощью команды **id**. Видим что ID пользователя и ID группы соответствуют 1001. Так же посмотрим информацию по команде **groups**. Видим что по команде **id** вывод гораздо более полный. Команда **groups** показывает лишь имя группы, в которую входит пользователь. Так же можем заметить, что то, под каким пользователем мы сейчас залогинены, можно определить по командной строке. (Рис. 3)

```
guest@akhalfina:~  
File Edit View Search Terminal Help  
[guest@akhalfina ~]$ pwd  
/home/guest  
[guest@akhalfina ~]$ cd  
[guest@akhalfina ~]$ whoami  
guest  
[guest@akhalfina ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@akhalfina ~]$ uid  
bash: uid: command not found...  
[guest@akhalfina ~]$ gid  
bash: gid: command not found...  
[guest@akhalfina ~]$ groups  
guest  
[guest@akhalfina ~]$
```

Теперь посмотрим запись о нашем пользователе в файле **passwd**. Для удобства выведем только интересующую нас строку при помощи команды **cat /etc/passwd | grep guest** (Рис. 4)

```
[guest@akhalfina ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001:./home/guest:/bin/bash
```

Посмотрим существующие в системе директории при помощи команды **ls -l /home/**. Видим две директории, соответствующие нашим пользователям. На каждую выставлены права на чтение, запись и исполнение. (Рис. 5)

```
[guest@akhalfina ~]$ ls -l /home/  
total 8  
drwx-----. 15 akhalfina akhalfina 4096 Sep 15 22:54 akhalfina  
drwx-----. 15 guest      guest      4096 Sep 15 22:55 guest  
[guest@akhalfina ~]$
```

Теперь посмотрим расширенные атрибуты, установленные на поддиректориях. (Рис. 6)

```
[guest@akhalfina ~]$ lsattr /home  
lsattr: Permission denied while reading flags on /home/akhalfina  
----- /home/guest  
[guest@akhalfina ~]$
```

Далее создадим директорию **dir1** и проверим выставленные на неё права доступа (Рис. 7)

```
[guest@akhalfina ~]$ mkdir dir1
[guest@akhalfina ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Desktop
drwxrwxr-x. 2 guest guest 6 Sep 15 23:00 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Videos
[guest@akhalfina ~]$
```

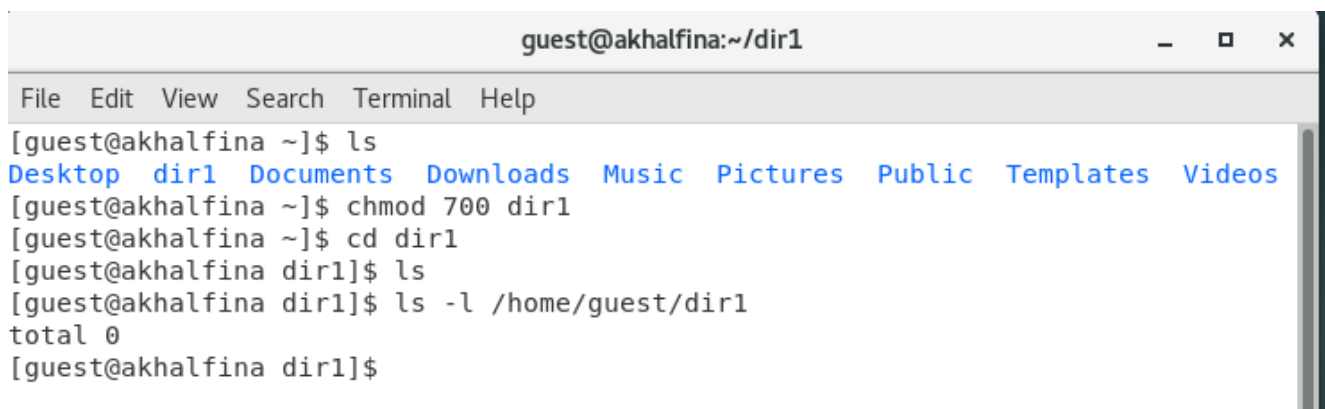
Снимем с директории все атрибуты и проверим результат. (Рис. 8)

```
[guest@akhalfina ~]$ chmod 000 dir1
[guest@akhalfina ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Desktop
d------. 2 guest guest 6 Sep 15 23:00 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 22:54 Videos
[guest@akhalfina ~]$
```

Попробуем создать файл. Видим что файл не создался из-за нехватки прав доступа (Рис. 9)

```
[guest@akhalfina ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
```

Проверим действительно ли файл не создался. Для этого нам необходимо добавить права на папку. Видим что в папке пусто и файл действительно не создавался. (Рис. 10)



Разный набор прав позволяет совершать разные действия с директориями и файлами. В таблице 1 приведены примеры действий, доступных при наличии тех или иных прав.

Таблица 1. Установленные права и разрешённые действия

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Пф ди
d (000)	-(000)	—	—	—	—	—	—
d--x----- (100)	----- -(000)	—	—	—	—	+	—
d-w----- (200)	----- -(000)	+	—	—	—	—	—
dr----- (400)	----- -(000)	—	—	—	—	—	+
drwx----- (700)	----- -(000)	+	—	—	—	+	+
d--x----- (100)	---x----- - (100)	—	—	—	—	+	—
d--x----- (100)	--w----- -- (200)	—	+	+	+	+	—
d--x----- (100)	-r----- - (400)	—	—	—	+	+	—
d--x----- (100)	-rwx----- -- (700)	—	+	+	+	+	—
d-w----- (200)	---x----- - (100)	+	—	—	—	—	—
d-w----- (200)	--w----- -- (200)	+	+	+	+	—	—
d-w----- (200)	-r----- - (400)	+	—	—	+	—	—
d-w----- (200)	-rwx----- -- (700)	+	+	+	+	—	—
dr----- (400)	---x----- - (100)	—	—	—	—	—	+

Права директории (400)	Права файла (200)	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Д ф + ди
dr----- (400)	-r----- - (400)	—	—	—	+	—	+
dr----- (400)	-rwx---- -- (700)	—	+	+	+	—	+
drwx----- (700)	---x----- - (100)	+	—	—	—	+	+
drwx----- (700)	--w----- -- (200)	+	+	+	+	+	+
drwx----- (700)	-r----- - (400)	+	—	—	+	+	+
drwx----- (700)	-rwx---- -- (700)	+	+	+	+	+	+

В таблице 2 представлены минимальные наборы прав, для совершения тех или иных действий.

Таблица 2. Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-w-----	-----
Удаление файла	d-----	--w-----
Чтение файла	d-----	-r-----
Запись в файл	d-----	--w-----
Переименование файла	d-w-----	-----
Создание поддиректории	d-w-----	-----
Удаление поддиректории	d-w-----	-----

Выводы

В ходе выполнения работы была получены практические навыки работы с правами доступа файлов и папок.