

Дискреционное разграничение прав в Linux. Основные атрибуты

Назарьева Алена НФИбд-03-18

2021, 1 october

inst{1}RUDN University, Moscow, Russian Federation

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

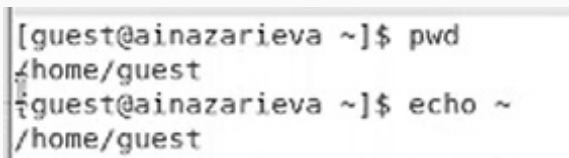
Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя guest, задала пароль для пользователя guest (рис. -fig. 1)

```
[ainazarieva@ainazarieva ~]$ su
Пароль:
[root@ainazarieva ainazarieva]# useradd guest
[root@ainazarieva ainazarieva]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
```

Figure 1: учетная запись guest

Вошла в систему от имени пользователя guest. Определила директорию, в которой вы находитесь, командой `pwd`. Сравнила её с приглашением командной строки. Она является моей домашней директорией. (рис. -fig. 2)



```
[guest@ainazarieva ~]$ pwd
/home/guest
[guest@ainazarieva ~]$ echo ~
/home/guest
```

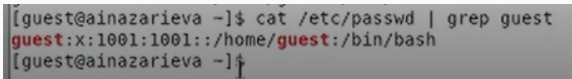
Figure 2: домашняя директория

Уточнила имя моего пользователя командой `whoami:guest`.
Уточнила имя моего пользователя, его группу, а также группы, куда входит пользователь, командой `id`.
Выведенные значения `uid`, `gid` и др. запомнила. Сравнила вывод `id` с выводом команды `groups`. Сравнила полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. (рис. -fig. 3)

```
root@kali:~/guest
[guest@ainazarieva ~]$ whoami
guest
[guest@ainazarieva ~]$ id
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:unconfined_r:u
nconfined_t:s0-s0:c0.c1023
[guest@ainazarieva ~]$ groups
guest
[guest@ainazarieva ~]$ █
```

Figure 3: пункты 5-7

Просмотрела файл `/etc/passwd` командой `cat /etc/passwd | grep guest`. Нашла в нём свою учётную запись. Определила `uid` пользователя. Определила `gid` пользователя. Сравнила найденные значения с полученными в предыдущих пунктах: они совпадают. (рис. -fig. 4)



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

Figure 4: сравнение значений

Определила существующие в системе директории командой `ls -l /home/` Мне удалось получить список поддиректорий директории `/home`. Установленные права-`drwx`— (рис. -fig. 5)

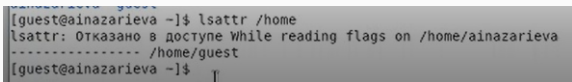
```
[guest@ainazarieva ~]$ ls -l /home/
итого 8
drwx-----. 15 ainazarieva ainazarieva 4096 сен 27 22:12 ainazarieva
drwx-----. 15 guest      guest      4096 сен 27 22:15 guest
[guest@ainazarieva ~]$
```

Figure 5: существующие директория

Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой:

`lsattr /home`

Мне не удалось увидеть расширенные атрибуты директории.
(рис. -fig. 6)



```
[guest@ainazarieva ~]$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/ainazarieva
----- /home/guest
[guest@ainazarieva ~]$
```

Figure 6: расширенные атрибуты

Создала в домашней директории поддиректорию dir1 командой

```
mkdir dir1
```

Определила командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1: 000 000.

Сняла с директории dir1 все атрибуты командой `chmod 000 dir1` и проверила с её помощью правильность выполнения команды

`ls -l` (рис. -fig. 7)

```
[guest@ainazarieva ~]$ mkdir dir1
mkdir: невозможно создать каталог «dir1»: Файл существует
[guest@ainazarieva ~]$ ls -l dir1
ls: невозможно открыть каталог dir1: Отказано в доступе
[guest@ainazarieva ~]$ lsattr dir1
[guest@ainazarieva ~]$ chmod 000 dir1
```

Попыталась создать в директории dir1 файл file1 командой

```
echo "test" > /home/guest/dir1/file1
```

Я получила отказ в выполнении операции по созданию файла, т.к. права на директорию не соответствуют

Проверьте командой

```
ls -l /home/guest/dir1
```

, что действительно файл file1 не находится внутри директории dir1.

Заполнила таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесла в таблицу знак «+», если не разрешена, знак «-». (рис. -fig. 8)

1	Права	Права фай-	Создание	Удаление	Запись	Чтение	Смена	Просмотр	Переименование	Смена	
2	директории	ла	файла	файла	в файл	файла	директории	файлов в	файла	атрибутов	
3								директории		файла	
4	d (000)	d (000)	-	-	-	-	-	-	-	-	
5	d-x(100)	d (000)	-	-	-	-	+	-	-	+	
6	d-w(200)	d (000)	+	+	-	-	-	-	-	-	
7	d-wx(300)	d (000)	+	+	-	-	+	-	-	+	
8	dr-(400)	d (000)	-	-	-	-	-	+	-	-	
9	dr-x(500)	d (000)	-	-	-	-	+	+	-	+	
10	drw-(600)	d (000)	+	+	-	-	-	+	-	-	
11	drwx(700)	d (000)	+	+	-	-	+	+	-	+	
12	d (000)	d-x(100)	-	-	-	-	-	-	-	-	
13	d-x(100)	d-x(100)	-	-	-	-	+	-	-	+	
14	d-w(200)	d-x(100)	+	+	-	-	-	-	-	-	
15	d-wx(300)	d-x(100)	+	+	-	-	+	-	-	+	
16	dr-(400)	d-x(100)	-	-	-	-	-	+	-	-	
17	dr-x(500)	d-x(100)	-	-	-	-	+	+	-	+	
18	drw-(600)	d-x(100)	+	+	-	-	-	+	-	-	
19	drwx(700)	d-x(100)	+	+	-	-	+	+	+	+	
20	d (000)	d-w-(200)	-	-	+	-	-	-	+	-	
21	d-x(100)	d-w-(200)	-	-	+	-	+	-	+	+	
22	d-w(200)	d-w-(200)	+	+	+	-	-	-	+	-	

Figure 8: пункт 14-1

(рис. -fig. 9)

23	d-wx(300)	d-w-(200)	+	+	+	-	+	-	+	+	
24	dr-(400)	d-w-(200)	-	-	+	-	-	+	+	-	
25	dr-x(500)	d-w-(200)	-	-	+	-	+	+	+	+	
26	drw-(600)	d-w-(200)	+	+	+	-	-	+	+	-	
27	drwx(700)	d-w-(200)	+	+	+	-	+	+	+	+	
28	d (000)	d-wx(300)	-	-	+	-	-	-	+	-	
29	d-x(100)	d-wx(300)	-	-	+	-	+	-	+	+	
30	d-w-(200)	d-wx(300)	+	+	+	-	-	-	+	-	
31	d-wx(300)	d-wx(300)	+	+	+	-	+	-	+	+	
32	dr-(400)	d-wx(300)	-	-	+	-	-	+	+	-	
33	dr-x(500)	d-wx(300)	-	-	+	-	+	+	+	+	
34	drw-(600)	d-wx(300)	+	+	+	-	-	+	+	-	
35	drwx(700)	d-wx(300)	+	+	+	-	+	+	+	+	
36	d (000)	dr-(400)	-	-	-	+	-	-	-	-	
37	d-x(100)	dr-(400)	-	-	-	+	+	-	-	+	
38	d-w-(200)	dr-(400)	+	+	-	+	-	-	-	-	
39	d-wx(300)	dr-(400)	+	+	-	+	+	-	-	+	
40	dr-(400)	dr-(400)	-	-	-	+	-	+	-	-	
41	dr-x(500)	dr-(400)	-	-	-	+	+	+	-	+	
42	drw-(600)	dr-(400)	+	+	-	+	-	+	-	-	
43	drwx(700)	dr-(400)	+	+	-	+	+	+	-	+	
44	d (000)	dr-x(500)	-	-	-	+	-	-	-	-	

Figure 9: пункт 14-2

(рис. -fig. 10)

45	d-x(100)	dr-x(500)	-	-	-	+	+	-	-	+	
46	d-w-(200)	dr-x(500)	+	+	-	+	-	-	-	-	
47	d-wx(300)	dr-x(500)	+	+	-	+	+	-	-	+	
48	dr--(400)	dr-x(500)	-	-	-	+	-	+	-	-	
49	dr-x(500)	dr-x(500)	-	-	-	+	+	+	-	+	
50	drw-(600)	dr-x(500)	+	+	-	+	-	+	-	-	
51	drwx(700)	dr-x(500)	+	+	-	+	+	+	-	+	
52	d (000)	drw-(600)	-	-	+	+	-	-	+	-	
53	d--x(100)	drw-(600)	-	-	+	+	+	-	+	+	
54	d-w-(200)	drw-(600)	+	+	+	+	-	-	+	-	
55	d-wx(300)	drw-(600)	+	+	+	+	+	-	+	+	
56	dr--(400)	drw-(600)	-	-	+	+	-	+	+	-	
57	dr-x(500)	drw-(600)	-	-	+	+	+	+	+	+	
58	drw-(600)	drw-(600)	+	+	+	+	-	+	+	-	
59	drwx(700)	drw-(600)	+	+	+	+	+	+	+	+	
60	d (000)	drwx(700)	-	-	+	+	-	-	+	-	
61	d--x(100)	drwx(700)	-	-	+	+	+	-	+	+	
62	d-w-(200)	drwx(700)	+	+	+	+	-	-	+	-	
63	d-wx(300)	drwx(700)	+	+	+	+	+	-	+	+	
64	dr--(400)	drwx(700)	-	-	+	+	-	+	+	-	
65	dr-x(500)	drwx(700)	-	-	+	+	+	+	+	+	
66	drw-(600)	drwx(700)	+	+	+	+	-	+	+	-	
67	drwx(700)	drwx(700)	+	+	+	+	+	+	+	+	

Figure 10: пункт 14-3

На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнила таблицу. (рис. -fig. 11)

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

Figure 11: пункт 15

Выводы

В результате проделанной работы я Получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.