

Лабораторная работа № 3

Дискреционное разграничение прав в Linux. Два пользователя

Абу Сувейлим Мухаммед Мунифович

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	15
	Список литературы	16

Список иллюстраций

4.1	Имя и пароль пользователя guest2	8
4.2	Пользователь guest2; группа guest	8
4.3	Два консоля	8
4.4	Домашняя директория guest	9
4.5	Домашняя директория guest2	9
4.6	Команда groups	9
4.7	Команда grep guest	10
4.8	Команда newgrp	10
4.9	Команда chmod	10

Список таблиц

table1	Установленные права и разрешённые действия для групп	11
table2	Минимальные права для совершения операций от имени пользова- телей входящих в группу	14

1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

2 Задание

Заполнить таблицу «Установленные права и разрешённые действия для групп».

3 Теоретическое введение

В метаданных каждого объекта (в inode файла/директории) содержится список разрешений на доступ к нему для разных категорий субъектов [1].

Атрибуты Minimal ACL поддерживают три базовых класса субъектов доступа к файлу (класс All объединяет все три класса):

User access (u) – доступ для владельца файла; Group access (g) – доступ для группы, владеющей файлом; Other access (o) – доступ для остальных пользователей (кроме пользователя root). All access (a) – доступ для всех субъектов доступа (u, g, o). Для каждого из этих классов определены три типа разрешений:

На чтение содержимого файла (read) – символ «r». На запись внутри файла или изменения его содержимого (write) – символ «w». На исполнение файла (если это бинарный исполняемый файл или файл сценария интерпретатора (execute)) – символ «x» [2].

4 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest2 (используя учётную запись администратора) и зададим пароль для пользователя guest2 (используя учётную запись администратора) (рис. 4.1):

```
[root@smabu smabu]# useradd guest2
[root@smabu smabu]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@smabu smabu]#
```

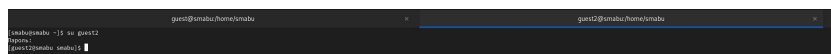
Рис. 4.1: Имя и пароль пользователя guest2

Добавим пользователя guest2 в группу guest (рис. 4.2):

```
[root@smabu smabu]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@smabu smabu]#
```

Рис. 4.2: Пользователь guest2; группа guest

Войдем в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли (рис. 4.3):



```
guest@smabu/home/smabu
smabu@smabu ~$ su guest
guest@smabu ~$

guest2@smabu/home/smabu
```

Рис. 4.3: Два консоля

Определим директорию, в которой мы находимся, командой pwd (рис. 4.4, 4.5):


```
[guest@smabu ~]$ pwd  
/home/guest
```

Рис. 4.4: Домашняя директория guest

```
[guest2@smabu ~]$ pwd  
/home/guest2
```

Рис. 4.5: Домашняя директория guest2

Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др сравнил с выводом командой `groups` рис. 4.6:

```
[guest2@smabu smabu]$ groups guest  
guest : guest  
[guest2@smabu smabu]$ groups guest2  
guest2 : guest2 guest  
[guest2@smabu smabu]$ id -Gn  
guest2 guest  
[guest2@smabu smabu]$ id -G  
1002 1001  
[guest2@smabu smabu]$
```

Рис. 4.6: Команда groups

Находил свою учётную запись. Определил `uid` пользователя. Определил `gid` пользователя и сравнил найденные значения с полученными в предыдущих пунктах (рис. 4.7):

```
[guest@smabu smabu]$ cat /etc/group | grep guest
guest:x:1001:guest2
guest2:x:1002:
```

Рис. 4.7: Команда grep guest

От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой (рис. 4.8)

```
[guest2@smabu smabu]$ newgrp guest
[guest2@smabu smabu]$
```

Рис. 4.8: Команда newgrp

От имени пользователя guest измените права директории /home/guest, разрешив все действия для пользователей группы (рис. 4.9):

```
[guest@smabu smabu]$ chmod g+rx /home/guest
[guest@smabu smabu]$
```

Рис. 4.9: Команда chmod

Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, Заполним таблицу «Установленные права и разрешённые действия для групп», определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-». Сравним табл. 2.1 (из лабораторной работы № 3) и табл. 3.1 (таблица «Установленные права и разрешённые действия для групп»). На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполните табл. 3.2.

Установленные права и разрешённые действия для групп

Права директории	Права файла	<div> <div>Про- Пе- Сме-</div> <div>смотр ре- на</div> <div>Сме- фай- име- ат-</div> <div>на лов но- ри-</div> <div>зда- ле- За- Чте- ди- в ди- ва- бу-</div> <div>ние ние пись ние рек- рек- ние тов</div> <div>фай- фай- в фай- то- то- фай- фай-</div> <div>ла ла файл ла рии рии ла ла</div> </div>							
		Со-	Уда-						
d(000)	(000)	-	-	-	-	-	-	-	-
d(010)	(000)	-	-	-	-	+	-	-	-
d(020)	(000)	-	-	-	-	-	-	-	-
d(030)	(000)	+	+	-	-	+	-	+	-
d(040)	(000)	-	-	-	-	-	+	-	-
d(050)	(000)	-	-	-	-	+	+	-	-
d(060)	(000)	-	-	-	-	-	+	-	-
d(070)	(000)	+	+	-	-	+	+	+	-
d(000)	(010)	-	-	-	-	-	-	-	-
d(010)	(010)	-	-	-	-	+	-	-	-
d(020)	(010)	-	-	-	-	-	-	-	-
d(030)	(010)	+	+	-	-	+	-	+	-
d(040)	(010)	-	-	-	-	-	+	-	-
d(050)	(010)	-	-	-	-	+	+	-	-
d(060)	(010)	-	-	-	-	-	+	-	-
d(070)	(010)	+	+	-	-	+	+	+	-
d(000)	(020)	-	-	-	-	-	-	-	-
d(010)	(020)	-	-	+	-	+	-	-	-
d(020)	(020)	-	-	-	-	-	-	-	-

Права директории	Права файла								
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Про- смотр фай- лов в ди- рек- то- рии	Пе- ре- име- но- ва- ние фай- ла	Сме- на ат- ри- бу- тов фай- ла
d(030)	(020)	+	+	+	-	+	-	+	-
d(040)	(020)	-	-	-	-	-	+	-	-
d(050)	(020)	-	-	+	-	+	+	-	-
d(060)	(020)	-	-	-	-	-	+	-	-
d(070)	(020)	+	+	+	-	+	+	+	-
d(000)	(030)	-	-	-	-	-	-	-	-
d(010)	(030)	-	-	+	-	+	-	-	-
d(020)	(030)	-	-	-	-	-	-	-	-
d(030)	(030)	+	+	+	-	+	-	+	-
d(040)	(030)	-	-	-	-	-	+	-	-
d(050)	(030)	-	-	+	-	+	+	-	-
d(060)	(030)	-	-	-	-	-	+	-	-
d(070)	(030)	+	+	+	-	+	+	+	-
d(000)	(040)	-	-	-	-	-	-	-	-
d(010)	(040)	-	-	-	+	+	-	-	-
d(020)	(040)	-	-	-	-	-	-	-	-
d(030)	(040)	+	+	-	+	+	-	+	-
d(040)	(040)	-	-	-	-	-	+	-	-
d(050)	(040)	-	-	-	+	+	+	-	-
d(060)	(040)	-	-	-	-	-	+	-	-
d(070)	(040)	+	+	-	+	+	+	+	-

							Про- смотр	Пе- ре-	Сме- на	
							Сме- на	фай- лов	име- но-	ат- ри-
							ди- рек-	в ди- рек-	ва- ние	бу- тов
Права директории	Права файла	Со- зда- ние	Уда- ле- ние	За- пись	Чте- ние	фай- ла	то- рии	то- рии	фай- ла	фай- ла
d(000)	(050)	-	-	-	-	-	-	-	-	-
d(010)	(050)	-	-	-	+	+	-	-	-	-
d(020)	(050)	-	-	-	-	-	-	-	-	-
d(030)	(050)	+	+	-	+	+	-	+	-	-
d(040)	(050)	-	-	-	-	-	+	-	-	-
d(050)	(050)	-	-	-	+	+	+	-	-	-
d(060)	(050)	-	-	-	-	-	+	-	-	-
d(070)	(050)	+	+	-	+	+	+	+	-	-
d(000)	(060)	-	-	-	-	-	-	-	-	-
d(010)	(060)	-	-	+	+	+	-	-	-	-
d(020)	(060)	-	-	-	-	-	-	-	-	-
d(030)	(060)	+	+	+	+	+	-	+	-	-
d(040)	(060)	-	-	-	-	-	+	-	-	-
d(050)	(060)	-	-	+	+	+	+	-	-	-
d(060)	(060)	-	-	-	-	-	+	-	-	-
d(070)	(060)	+	+	+	+	+	+	+	-	-
d(000)	(070)	-	-	-	-	-	-	-	-	-
d(010)	(070)	-	-	+	+	+	-	-	-	-
d(020)	(070)	-	-	-	-	-	-	-	-	-
d(030)	(070)	+	+	+	+	+	-	+	-	-
d(040)	(070)	-	-	-	-	-	+	-	-	-

Права директории	Права файла	Сме- на Сме- на Сме- на				Про- смотр фай- лов в ди- рек- то- рии			
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	фай- лов в ди- рек- то- рии	име- но- ва- ние фай- ла	Сме- на ат- ри- бу- тов фай- ла
d(050)	(070)	-	-	+	+	+	+	-	-
d(060)	(070)	-	-	-	-	-	+	-	-
d(070)	(070)	+	+	+	+	+	+	+	-

На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1.

Минимальные права для совершения операций от имени пользователей входящих в группу

Операция	Минимальные права на	
	директорию	Минимальные права на файл
Создание файла	d(030)	(000)
Удаление файла	d(030)	(000)
Чтение файла	d(010)	(040)
Запись в файл	d(010)	(020)
Переименование файла	d(030)	(000)
Создание поддиректории	d(030)	(000)
Удаление поддиректории	d(030)	(000)

5 Выводы

Получил практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. // skillbox.ru.
2. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.