

Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя.

Пономарева Лилия Михайловна

Содержание

Цель работы	5
Теоретическое введение	6
Выполнение лабораторной работы	8
Выводы	16
Список литературы	17

Список иллюстраций

1	Создание нового пользователя	8
2	Добавления пользователя в группу	8
3	Пользователь guest	9
4	Пользователь guest2	9
5	Имя, группа пользователя	9
6	Имя, группа пользователя	10
7	Команда id -Gn и id -G	10
8	Файл /etc/group	10
9	Регистрация пользователя в группе	11
10	Изменение прав директории /home/guest	11
11	Снятие атрибутов с директории /home/guest/dir1	11
12	Проверка значений атрибутов	11

Список таблиц

1	Установленные права и разрешённые действия для групп	12
2	Минимальные права для совершения операций от имени пользователей входящих в группу	15

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей[1].

Теоретическое введение

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов к объектам, которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ, которые работают от лица псевдопользовательских учетных записей.

В рамках дискреционного разграничения доступа каждому файлу назначен пользователь-владелец и группа-владелец файла.

В метаданных каждого объекта содержится список разрешений на доступ к нему для разных категорий субъектов.

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».

Для директорий трактовка типов разрешений иная:

r – разрешение на «открытие» директории, то есть на чтение списка файлов, которые содержит эта директория.

w – разрешение на модификацию этого списка файлов (создание/удаление/переименование/и файлов этой директории.

x – разрешение на «исполнение» директории, то есть на возможность перейти в нее.

Чтобы изменить расширения для определенного файла используется команда `chmod` с соответствующими аргументами.

Выполнение лабораторной работы

1. Создала учётную запись пользователя guest2, используя учётную запись администратора(рис. 1)

useradd guest2

passwd guest

```
[root@lmponomareva lmponomareva]# useradd guest2
[root@lmponomareva lmponomareva]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@lmponomareva lmponomareva]#
```

Рис. 1: Создание нового пользователя

2. Добавила пользователя guest2 в группу guest(рис. 2)

gpasswd -a guest2 guest

```
[root@lmponomareva lmponomareva]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@lmponomareva lmponomareva]#
```

Рис. 2: Добавления пользователя в группу

3. Вошла в систему от двух пользователей на двух разных консолях и командой pwd определила директорию, в которой нахожусь(рис. 3 и рис. 4)

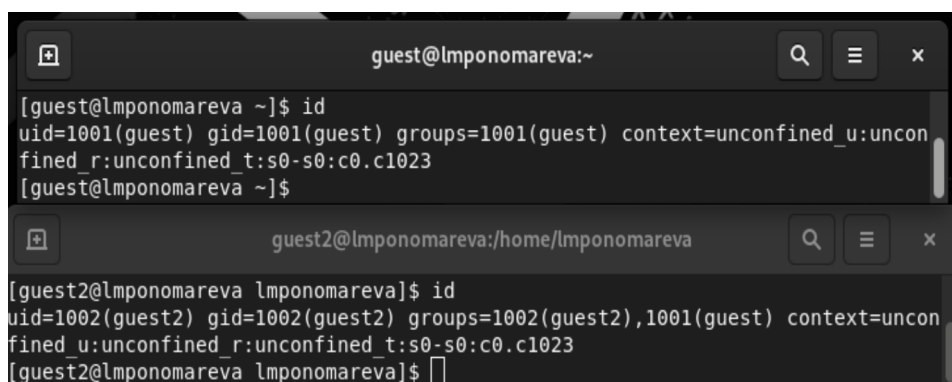

```
[root@lmponomareva lmponomareva]# su guest
[guest@lmponomareva lmponomareva]$ pwd
/home/lmponomareva
```

Рис. 3: Пользователь guest

```
[lmponomareva@lmponomareva ~]$ su guest2
Password:
[guest2@lmponomareva lmponomareva]$ pwd
/home/lmponomareva
```

Рис. 4: Пользователь guest2

5. Уточнила имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам(рис. 5)

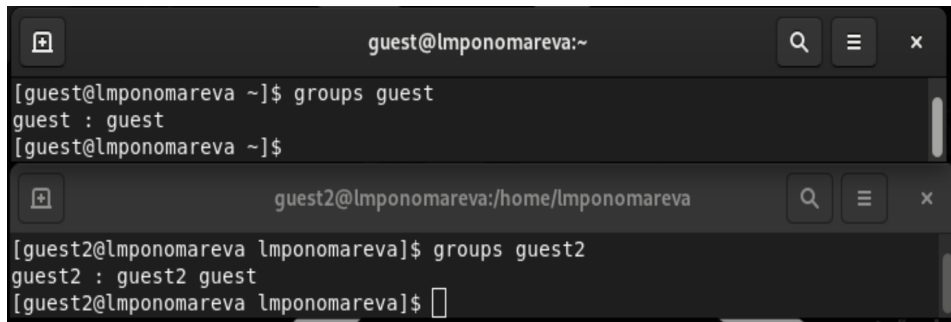


```
guest@lmponomareva:~
[guest@lmponomareva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@lmponomareva ~]$

guest2@lmponomareva:/home/lmponomareva
[guest2@lmponomareva lmponomareva]$ id
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@lmponomareva lmponomareva]$
```

Рис. 5: Имя, группа пользователя

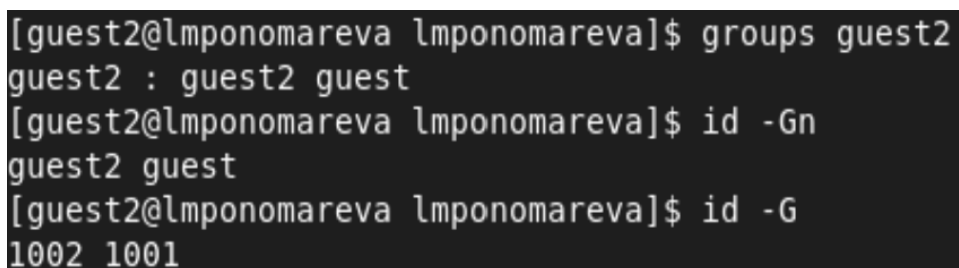
Определила командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`(рис. 6)



```
guest@lmponomareva:~  
[guest@lmponomareva ~]$ groups guest  
guest : guest  
[guest@lmponomareva ~]$  
guest2@lmponomareva:/home/lmponomareva  
[guest2@lmponomareva lmponomareva]$ groups guest2  
guest2 : guest2 guest  
[guest2@lmponomareva lmponomareva]$
```

Рис. 6: Имя, группа пользователя

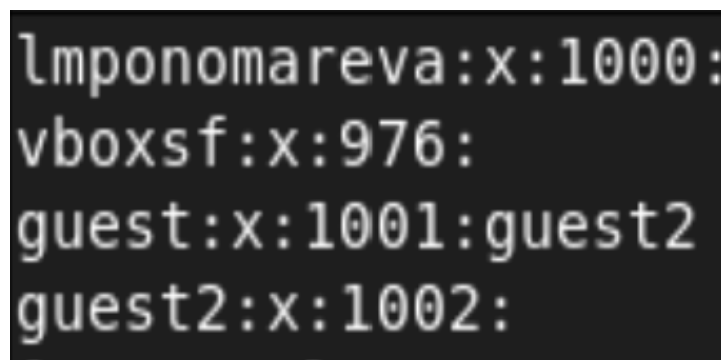
Сравнила вывод команды groups с выводом команд id -Gn и id -G(рис. 7)



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

Рис. 7: Команда id -Gn и id -G

6. Сравнила полученную информацию с содержимым файла /etc/group(рис. 8)



```
lmponomareva:x:1000:  
vboxsf:x:976:  
guest:x:1001:guest2  
guest2:x:1002:
```

Рис. 8: Файл /etc/group

7. От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest командой newgrp guest(рис. 9)

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

Рис. 9: Регистрация пользователя в группе

8. От имени пользователя guest изменила права директории /home/guest, разрешив все действия для пользователей группы: chmod g+rxw /home/guest(рис. 10)

```
[guest@lmponomareva ~]$ chmod g+rxw /home/guest
```

Рис. 10: Изменение прав директории /home/guest

9. От имени пользователя guest сняла с директории /home/guest/dir1 все атрибуты командой chmod 000 dir1(рис. 11), и проверила правильность снятия атрибутов(рис. 12)

```
[guest@lmponomareva ~]$ chmod 000 dir1
```

Рис. 11: Снятие атрибутов с директории /home/guest/dir1

```
[guest@lmponomareva ~]$ ls -l /home  
total 4  
drwxrwx---. 5 guest      guest      125 Sep 17 21:48 guest  
drwx-----. 3 guest2     guest2     98 Sep 24 18:35 guest2  
drwx-----. 14 lmponomareva lmponomareva 4096 Sep 24 18:08 lmponomareva  
[guest@lmponomareva ~]$ ls -l  
total 0  
d------. 2 guest guest 17 Sep 17 19:35 dir1
```

Рис. 12: Проверка значений атрибутов

Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнила табл. 1, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».

Таблица 1: Установленные права и разрешённые действия для групп

Права	Просмотр								
	фай-				Смена		лов в		
ди-	Чтение				ди-	ди-	Смена		
рек-	Права	Создание	Удаление	Запись	из	рек-	рек-	Переименование	бу-вание
то-	фай-	фай-	фай-	в	фай-	то-	то-	фай-	фай-
рии	ла	ла	ла	файл	ла	рии	рии	ла	ла
d---	----	-	-	-	-	-	-	-	-
d--x	----	-	-	-	-	+	-	-	-
d-w-	----	-	-	-	-	-	-	-	-
d-wx	----	+	+	-	-	+	-	+	-
dr--	----	-	-	-	-	-	+	-	-
dr-x	----	-	-	-	-	+	+	-	-
drw-	----	-	-	-	-	-	+	-	-
drwx	----	+	+	-	-	+	+	+	-
d---x	----x	-	-	-	-	-	-	-	-
d--x	----x	-	-	-	-	+	-	-	-
d-w-	----x	-	-	-	-	-	-	-	-
d-wx	----x	+	+	-	-	+	-	+	-
dr--	----x	-	-	-	-	-	+	-	-
dr-x	----x	-	-	-	-	+	+	-	-
drw-	----x	-	-	-	-	-	+	-	-
drwx	----x	+	+	-	-	+	+	+	-

						Просмотр			
						фай-			
Права					Смена	лов в		Смена	
ди-					Чтение	ди-	ди-	атри-	
рек-	Права	Создание	Удаление	Запись	из	рек-	рек-	Переименование	
то-	фай-	фай-	фай-	в	фай-	то-	то-	фай-	фай-
рии	ла	ла	ла	файл	ла	рии	рии	ла	ла
d---	--w-	-	-	-	-	-	-	-	-
d--x	--w-	-	-	+	-	+	-	-	-
d-w-	--w-	-	-	-	-	-	-	-	-
d-wx	--w-	+	+	+	-	+	-	+	-
dr--	--w-	-	-	-	-	-	+	-	-
dr-x	--w-	-	-	+	-	+	+	-	-
drw-	--w-	-	-	-	-	-	+	-	-
drwx	--w-	+	+	+	-	+	+	+	-
d---	--wx	-	-	-	-	-	-	-	-
d--x	--wx	-	-	+	-	+	-	-	-
d-w-	--wx	-	-	-	-	-	-	-	-
d-wx	--wx	+	+	+	-	+	-	+	-
dr--	--wx	-	-	-	-	-	+	-	-
dr-x	--wx	-	-	+	-	+	+	-	-
drw-	--wx	-	-	-	-	-	+	-	-
drwx	--wx	+	+	+	-	+	+	+	-
d---	-r--	-	-	-	-	-	-	-	-
d--x	-r--	-	-	-	+	+	-	-	-
d-w-	-r--	-	-	-	-	-	-	-	-
d-wx	-r--	+	+	-	+	+	-	+	-
dr--	-r--	-	-	-	-	-	+	-	-
dr-x	-r--	-	-	-	+	+	+	-	-

						Просмотр			
						фай-			
Права						Смена	лов в	Смена	
ди-					Чтение	ди-	ди-	атри-	
рек-	Права	Создание	Удаление	Запись	из	рек-	рек-	Переименование	
то-	фай-	фай-	фай-	в	фай-	то-	то-	фай-	фай-
рии	ла	ла	ла	файл	ла	рии	рии	ла	ла
drw-	-r--	-	-	-	-	-	+	-	-
drwx	-r--	+	+	-	+	+	+	+	-
d---	-r-x	-	-	-	-	-	-	-	-
d--x	-r-x	-	-	-	+	+	-	-	-
d-w-	-r-x	-	-	-	-	-	-	-	-
d-wx	-r-x	+	+	-	+	+	-	+	-
dr--	-r-x	-	-	-	-	-	+	-	-
dr-x	-r-x	-	-	-	+	+	+	-	-
drw-	-r-x	-	-	-	-	-	+	-	-
drwx	-r-x	+	+	-	+	+	+	+	-
d---	-rw-	-	-	-	-	-	-	-	-
d--x	-rw-	-	-	+	+	+	-	-	-
d-w-	-rw-	-	-	-	-	-	-	-	-
d-wx	-rw-	+	+	+	+	+	-	+	-
dr--	-rw-	-	-	-	-	-	+	-	-
dr-x	-rw-	-	-	+	+	+	+	-	-
drw-	-rw-	-	-	-	-	-	+	-	-
drwx	-rw-	+	+	+	+	+	+	+	-
d---	-rwx	-	-	-	-	-	-	-	-
d--x	-rwx	-	-	+	+	+	-	-	-
d-w-	-rwx	-	-	-	-	-	-	-	-
d-wx	-rwx	+	+	+	+	+	-	+	-

						Просмотр фай-			
						Смена	лов в	Смена	
Права					Чтение	ди-	ди-	атри-	
рек-	Права	Создание	Удаление	Запись	из	рек-	рек-	Переименование	
то-	фай-	фай-	фай-	в	фай-	то-	то-	фай-	фай-
рии	ла	ла	ла	файл	ла	рии	рии	ла	ла
dr--	-rwx	-	-	-	-	-	+	-	-
dr-x	-rwx	-	-	+	+	+	+	-	-
drw-	-rwx	-	-	-	-	-	+	-	-
drwx	-rwx	+	+	+	+	+	+	+	-

15. На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнила табл. 2

Таблица 2: Минимальные права для совершения операций от имени пользователей входящих в группу

Операция	Права на директорию	Права на файл
Создание файла	d-wx	---
Удаление файла	d-wx	---
Чтение файла	d--x	r--
Запись в файл	d--x	-w-
Переименование файла	d-wx	---
Создание поддиректории	d-wx	---
Удаление поддиректории	d-wx	---

Выводы

Получили навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3.