

Лабораторная работа №3. Дискреционное разграничение прав в Linux. Два пользователя.

Евдокимов Иван Андреевич. НФИбд-01-20

11 сентября, 2023, Москва, Россия

Российский Университет Дружбы Народов

Цель лабораторной работы

Цель лабораторной работы

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

Процесс выполнения лабораторной работы

1. В установленной ОС создаю учетную запись пользователя guest. Задаю пароль для созданного пользователя.

```
[eangreevich@iven ~]$ useradd guest
useradd: пользователь «guest» уже существует
[eangreevich@iven ~]$ █
```

Рис. 1: Создаю учетную запись пользователя

```
[eangreevich@iven ~]$ passwd guest
passwd: только root может выбрать имя учетной записи.
```

Рис. 2: Задаю пароль

2. Создаю пользователя guest2.

```
[eangreevich@iven ~]$ sudo useradd guest2
[sudo] пароль для eangreevich:
[eangreevich@iven ~]$ useradd guest2
useradd: пользователь «guest2» уже существует
[eangreevich@iven ~]$ su guest2
Пароль:
su: Сбой при проверке подлинности
[eangreevich@iven ~]$ su guest2
Пароль:
su: Сбой при проверке подлинности
[eangreevich@iven ~]$ su guest2
Пароль:
su: Сбой при проверке подлинности
[eangreevich@iven ~]$ passwd guest2
passwd: только root может выбрать имя учетной записи.
[eangreevich@iven ~]$ sydo passwd guest
bash: sydo: команда не найдена...
[eangreevich@iven ~]$ sudo passwd guest
[sudo] пароль для eangreevich:
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[eangreevich@iven ~]$
```

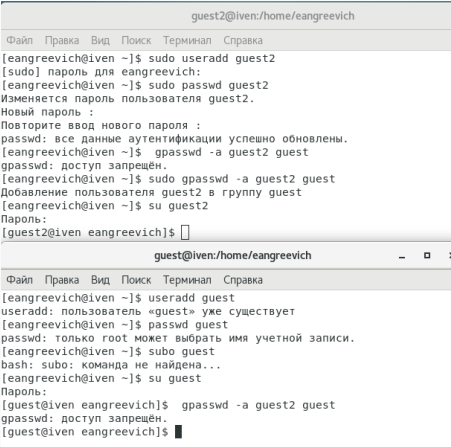
Рис. 3: Создаю пользователя guest2

3. Добавляю пользователя `guest2` в группу `guest`. Вхожу в систему от двух пользователей, в двух разных консолях.

```
[eangreevich@iven ~]$ sudo gpasswd -a guest2 guest  
Добавление пользователя guest2 в группу guest  
[eangreevich@iven ~]$
```

Рис. 4: Вхожу в систему

4. Добавьте пользователя guest2 в группу guest: `gpasswd -a guest2 guest`

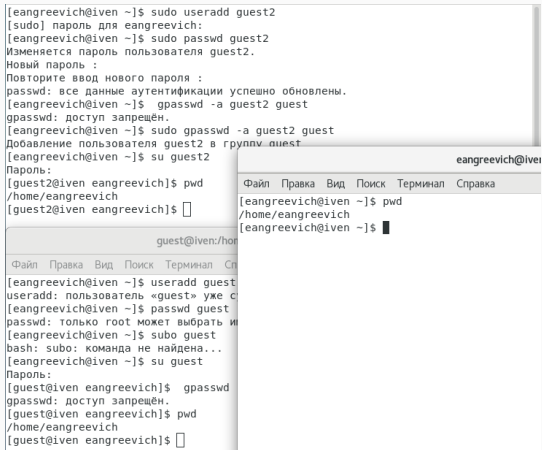


```
guest2@iven:/home/eangreevich
Файл  Правка  Вид  Поиск  Терминал  Справка
[eangreevich@iven ~]$ sudo useradd guest2
[sudo] пароль для eangreevich:
[eangreevich@iven ~]$ sudo passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[eangreevich@iven ~]$ gpasswd -a guest2 guest
gpasswd: доступ запрещен.
[eangreevich@iven ~]$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[eangreevich@iven ~]$ su guest2
Пароль:
[guest2@iven eangreevich]$ █

guest@iven:/home/eangreevich
Файл  Правка  Вид  Поиск  Терминал  Справка
[eangreevich@iven ~]$ useradd guest
useradd: пользователь «guest» уже существует
[eangreevich@iven ~]$ passwd guest
passwd: только root может выбрать имя учетной записи.
[eangreevich@iven ~]$ sudo guest
bash: sudo: команда не найдена...
[eangreevich@iven ~]$ su guest
Пароль:
[guest@iven eangreevich]$ gpasswd -a guest2 guest
gpasswd: доступ запрещен.
[guest@iven eangreevich]$ █
```

Рис. 5: Добавляю в группу

5. С помощью команды `pwd` определяю директорию.
Определяю, что она является домашней.



```
[eangreevich@iven ~]$ sudo useradd guest2
[sudo] пароль для eangreevich:
[eangreevich@iven ~]$ sudo passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[eangreevich@iven ~]$ gpasswd -a guest2 guest
gpasswd: доступ запрещён.
[eangreevich@iven ~]$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest.
[eangreevich@iven ~]$ su guest2
Пароль:
[guest2@iven eangreevich]$ pwd
/home/eangreevich
[guest2@iven eangreevich]$ █
```

```
guest@iven:/home/eangreevich
Файл  Правка  Вид  Поиск  Терминал  Справка
[eangreevich@iven ~]$ pwd
/home/eangreevich
[eangreevich@iven ~]$ █
```

```
guest@iven:/home/eangreevich
Файл  Правка  Вид  Поиск  Терминал  Справка
[eangreevich@iven ~]$ useradd guest
useradd: пользователь «guest» уже существует
[eangreevich@iven ~]$ passwd guest
passwd: только root может выбрать имя пользователя
[eangreevich@iven ~]$ sudo useradd guest
bash: sudo: команда не найдена...
[eangreevich@iven ~]$ su guest
Пароль:
[guest@iven eangreevich]$ gpasswd
gpasswd: доступ запрещён.
[guest@iven eangreevich]$ pwd
/home/eangreevich
[guest@iven eangreevich]$ █
```

Рис. 6: Определяю директорию

6. Уточняю имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определяю командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Сравниваю вывод команды `groups` с выводом команд `id -Gn` и `id -G..`

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



```
guest@iven:/home/eangreevich
[еangreevich@iven ~]$ useradd guest
useradd: пользователь «guest» уже существует
[еangreevich@iven ~]$ passwd guest
passwd: только root может выбрать имя учетной записи.
[еangreevich@iven ~]$ sudo guest
bash: sudo: команда не найдена...
[еangreevich@iven ~]$ su guest
Пароль:
[guest@iven eangreevich]$ gpasswd -a guest2 guest
gpasswd: доступ запрещен.
[guest@iven eangreevich]$ pwd
/home/eangreevich
[guest@iven eangreevich]$ groups guest
guest : guest
[guest@iven eangreevich]$ id -Gn
guest
[guest@iven eangreevich]$ id -G
1001
[guest@iven eangreevich]$
```

7. Сравниваю полученные данные с содержимым файла /etc/group.

```
pulse-rt:x:989:
pulse:x:171:
radvd:x:75:
chrony:x:988:
unbound:x:987:
kvm:x:36:qemu
qemu:x:107:
tss:x:59:
libvirt:x:986:
usbmuxd:x:113:
geoclue:x:985:
gluster:x:984:
gdm:x:42:
rpcuser:x:29:
nfsnobody:x:65534:
gnome-initial-setup:x:983:
sshd:x:74:
slocate:x:21:
avahi:x:70:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
eangreevich:x:1000:eangreevich
vboxsf:x:982:
vboxdrmpc:x:981:
guest:x:1001:guest2
guest2:x:1002:
[guest2@iven eangreevich]$ █
nfsnobody:x:65534:
gnome-initial-setup:x:983:
sshd:x:74:
slocate:x:21:
avahi:x:70:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
eangreevich:x:1000:eangreevich
vboxsf:x:982:
vboxdrmpc:x:981:
guest:x:1001:guest2
guest2:x:1002:
[guest@iven eangreevich]$ █
```

Рис. 8: Уточняю имя пользователя, группу, и группы

8. Сравниваю полученные данные с данными в приглашении командной строке.

```
[guest2@iven eangreevich]$ newgrp guest  
[guest2@iven eangreevich]$ █
```

Рис. 9: Сравнение данных

9. От имени пользователя guest измените права директории /home/guest, разрешив все действия для пользователей группы:

`chmod g+rx /home/guest`



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

Рис. 10: Измените права директории

10. От имени пользователя `guest` снимите с директории `/home/guest/dir1` все атрибуты командой `chmod 000 dir1` и проверьте правильность снятия атрибутов

```
[guest@iven eangreevich]$ chmod 000 dir1  
chmod: невозможно получить доступ к «dir1»: Отказано в доступе
```

Рис. 11: Команда `chmod 000 dir1`

11. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполните табл. 3.1, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

Права директории	Права файла	Создание файла	Удаление файла	Запись файла	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибута в файле
d----- (000)	----- (000)	-	-	-	-	-	-	-	-
d-x----- (100)	----- (000)	-	-	-	-	*	-	-	*
d-x----- (100)	--x----- (100)	-	-	-	-	*	-	-	*
d-x----- (100)	--w----- (200)	-	-	*	-	*	-	-	*
d-x----- (100)	--wx----- (300)	-	-	*	-	*	-	-	*
d-x----- (100)	-f----- (400)	-	-	-	*	*	-	-	*
d-x----- (100)	-fx----- (500)	-	-	-	*	*	-	-	*
d-x----- (100)	-fw----- (600)	-	-	*	*	*	-	-	*
d-x----- (100)	-fwx----- (700)	-	-	*	*	*	-	-	*
d-w----- (200)	----- (000)	-	-	-	-	-	-	-	-
d-wx----- (300)	----- (000)	*	*	-	-	*	-	*	*
d-wx----- (300)	--x----- (100)	*	*	-	-	*	-	*	*
d-wx----- (300)	--w----- (200)	*	*	*	-	*	-	*	*
d-wx----- (300)	--wx----- (300)	*	*	*	-	*	-	*	*
d-wx----- (300)	-f----- (400)	*	*	-	*	*	-	*	*
d-wx----- (300)	-fx----- (500)	*	*	-	*	*	-	*	*
d-wx----- (300)	-fw----- (600)	*	*	*	*	*	-	*	*

Рис. 12: табл. 3.1 часть 1

d-wx----- (300)	-rwX----- (700)	+	+	+	+	+	-	+	+
dr----- (400)	----- (000)	-	-	-	-	-	+	-	-
dr-x----- (500)	----- (000)	-	-	-	-	+	+	-	+
dr-x----- (500)	---x----- (100)	-	-	-	-	+	+	-	+
dr-x----- (500)	---w----- (200)	-	-	+	-	+	+	-	+
dr-x----- (500)	---wx----- (300)	-	-	+	-	+	+	-	+
dr-x----- (500)	-f----- (400)	-	-	-	+	+	+	-	+
dr-x----- (500)	-f-x----- (500)	-	-	-	+	+	+	-	+
dr-x----- (500)	-rw----- (600)	-	-	+	+	+	+	-	+
dr-x----- (500)	-rwX----- (700)	-	-	+	+	+	+	-	+
drwx----- (600)	----- (000)	-	-	-	-	-	+	-	-
drwx----- (700)	----- (000)	+	+	-	-	+	+	+	+
drwx----- (700)	---x----- (100)	+	+	-	-	+	+	+	+
drwx----- (700)	---w----- (200)	+	+	+	-	+	+	+	+
drwx----- (700)	---wx----- (300)	+	+	+	-	+	+	+	+
drwx----- (700)	-f----- (400)	+	+	-	+	+	+	+	+
drwx----- (700)	-f-x----- (500)	+	+	-	+	+	+	+	+
drwx----- (700)	-fx----- (600)	+	+	+	+	+	+	+	+
drwx----- (700)	-rwX----- (700)	+	+	+	+	+	+	+	+

Рис. 13: табл. 3.1 часть 2

12. Сравниваю табл. 2.1 (из лабораторной работы № 2) и табл. 3.1. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполните табл. 3.2.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-w----	(200)
Удаление файла	d-w-----	(200)
Чтение файла	dr-----	(400)
Запись файла	d-w-----	(200)
Переименование файла	d-w-----	(200)
Создание поддиректории	d-x-----	(100)
Удаление поддиректории	d-x-----	(100)

Рис. 14: табл. 2.1

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	-r----- (400)
Запись файла	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

Рис. 15: табл. 3.2

Выводы:

Выводы:

Получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах на базе ОС Linux с двумя пользователями.