

Отчёт по лабораторной работе №3

Дискреционное разграничение прав в Linux. Два пользователя

Джафер Идрисов

Содержание

1	Цель работы	5
2	Выполнение работы	6
3	Выводы	16
	Список литературы	17

List of Figures

2.1	Добавление пользователей в группу	6
2.2	Информация о пользователях	7
2.3	Содержимое файла /etc/group и регистрация в группе	8
2.4	Изменение прав у директории	8
2.5	Заполнение таблицы	9

List of Tables

2.1	Установленные права и разрешённые действия для групп	10
2.2	Минимальные права для совершения операций	15

1 Цель работы

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

2 Выполнение работы

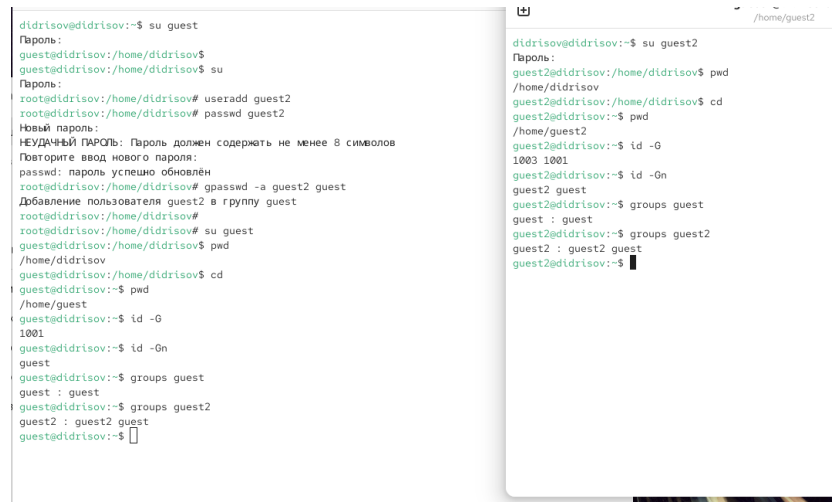
1. В предыдущей работе в установленной операционной системе создали учетную запись пользователя `guest` и задали пароль для пользователя (используя учетную запись администратора) и зашла в эту учетную запись
2. Аналогично создали второго пользователя `guest2` и выполнили вход в эту учетную запись
3. Добавили пользователя `guest2` в группу `guest` используя команду: `Gpasswd -a guest2 guest`

```
didrisov@didrisov:~$ su guest
Пароль:
guest@didrisov:/home/didrisov$
guest@didrisov:/home/didrisov$ su
Пароль:
root@didrisov:/home/didrisov# useradd guest2
root@didrisov:/home/didrisov# passwd guest2
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
root@didrisov:/home/didrisov# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
root@didrisov:/home/didrisov#
```

Figure 2.1: Добавление пользователей в группу

4. Выполнили вход в две учетные записи `guest` `guest2` на разных консолях
5. Для обоих пользователей командой `Pwd` определили директорию, в которой находимся. Сравнили ее с приглашением командой строки.

6. Уточнили имя нашего пользователя, его группу, кто входит в нее и к каким группам принадлежит он сам. Определили командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Сравнили выводы команды `groups` с выводом команд `id -Gn` и `id -G`.



```
didrisov@didrisov:~$ su guest
Пароль:
guest@didrisov:/home/didrisov$
guest@didrisov:/home/didrisov$ su
Пароль:
root@didrisov:/home/didrisov# useradd guest2
root@didrisov:/home/didrisov# passwd guest2
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: пароль успешно обновлен
root@didrisov:/home/didrisov# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
root@didrisov:/home/didrisov#
root@didrisov:/home/didrisov# su guest
guest@didrisov:/home/didrisov$ pwd
/home/didrisov
guest@didrisov:/home/didrisov$ cd
/home/guest
guest@didrisov:~$ id -G
1001
guest@didrisov:~$ id -Gn
guest
guest@didrisov:~$ groups guest
guest : guest
guest@didrisov:~$ groups guest2
guest2 : guest2 guest
guest@didrisov:~$

didrisov@didrisov:~$ su guest2
Пароль:
guest2@didrisov:/home/didrisov$ pwd
/home/didrisov
guest2@didrisov:/home/didrisov$ cd
/home/guest2
guest2@didrisov:~$ id -G
1003 1001
guest2@didrisov:~$ id -Gn
guest2 guest
guest2@didrisov:~$ groups guest
guest : guest
guest2@didrisov:~$ groups guest2
guest2 : guest2 guest
guest2@didrisov:~$
```

Figure 2.2: Информация о пользователях

7. Сравнили полученную информацию с содержимым файла `/etc/group`. Посмотрели файл командой `cat /etc/group`.
8. От имени пользователя `guest2` выполнили регистрацию пользователя `guest2` в группе `guest` командой `newgrp guest`

```
1.1.1.x:~#.172.17.0.2.net:::/sbin/nologin
geoclue:x:997:996:User for geoclue:/var/lib/geoclue:/sbin/nologin
sssd:x:996:995:User for sssd:/run/sss/:/sbin/nologin
libstoragemgmt:x:994:994:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-coredump:x:993:993:systemd Core Dumper:/usr/sbin/nologin
wssd:x:992:992:Web Services Dynamic Discovery host daemon:/sbin/nologin
clevis:x:991:991:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sb
in/nologin
setroubleshoot:x:990:990:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/
nologin
pipewire:x:989:989:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
flatpak:x:988:988:Flatpak system helper:/usr/sbin/nologin
gdm:x:42:42:GNOME Display Manager:/var/lib/gdm:/usr/sbin/nologin
gnome-initial-setup:x:987:986:/run/gnome-initial-setup:/sbin/nologin
dnsmasq:x:986:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
psign:x:985:984:Group for the pesign signing daemon:/run/psign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:984:983:chrony system user:/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:tcpdump:/usr/sbin/nologin
gnome-remote-desktop:x:981:981:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/s
bin/nologin
guest:x:1001:1001:/home/guest:/bin/bash
didrisov:x:1002:1002:/home/didrisov:/bin/bash
guest2:x:1003:1003:/home/guest2:/bin/bash
quest2@didrisov:~$ newgrp guest
quest2@didrisov:~$
```

Figure 2.3: Содержимое файла /etc/group и регистрация в группе

9. От имени пользователя `guest` изменили права директории `/home/guest`, разрешив все действия для пользователей группы: `chmod g+rx /home/guest`. И также от имени пользователя `guest` сняли с директории `/home/guest/dir1` все атрибуты командой `chmod 000 dir1` и проверили правильность снятия атрибутов

```

guest@didrisov:~$ cd
guest@didrisov:~$ chmod g+rxw /home/guest
guest@didrisov:~$ ls -l /home
итого 8
drwx-----, 14 didrisov didrisov 4096 мар 7 16:21 didrisov
drwxrwx---, 3 guest guest 78 фев 5 19:27 guest
drwx-----, 3 guest2 guest2 78 мар 7 16:23 guest2
drwx-----, 14 1000 1000 4096 фев 5 17:57 user
guest@didrisov:~$ cd
guest@didrisov:~$ mkdir dir1
guest@didrisov:~$ chmod 000 dir1/
guest@didrisov:~$ ls -l | grep dir1/
guest@didrisov:~$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
guest@didrisov:~$ cd dir1/
bash: cd: dir1/: Отказано в доступе
guest@didrisov:~$

```

Figure 2.4: Изменение прав у директории

Меняя атрибуты у директории `dir1` и файла `file1` от имени пользователя `guest` и

делая проверку от пользователя guest2, заполнили табл. 2, определили опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесли в таблицу знак «+», если не разрешена, знак «-». На основании заполненной таблицы определили те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнили табл. 1.

```
guest2@ddirisoV:~$ sudo su - guest
guest@ddirisoV:~$ cd /home/guest
drwx-----, 14      1000       1000 4096 feb  5 17:57 user
guest@ddirisoV:~$ ls -ldir1
guest@ddirisoV:~$ chmod 000 dir1/
guest@ddirisoV:~$ ls -l | grep dir1
guest@ddirisoV:~$ echo test > dir1/file1
bash: dir1/file1: Ошибка: не существует файла или каталога
guest@ddirisoV:~$ cd dir1/
bash: cd: dir1/: Ошибка: не существует файла или каталога
guest@ddirisoV:~$ ls -ldir1
guest@ddirisoV:~$ chmod 110 dir1/
guest@ddirisoV:~$ ls -l | grep dir1/
guest@ddirisoV:~$ ls -l | grep dir1
d-x--x---, 2 guest guest 6 map  7 16:29 dir1
guest@ddirisoV:~$ ls -ldir1
guest@ddirisoV:~$ chmod 220 dir1/
guest@ddirisoV:~$ ls -l | grep dir1
d-w-m-----, 2 guest guest 6 map  7 16:29 dir1
guest@ddirisoV:~$ ls -ldir1
guest@ddirisoV:~$ chmod 330 dir1/
guest@ddirisoV:~$ ls -l | grep dir1
d-wx--x---, 2 guest guest 6 map  7 16:29 dir1
guest@ddirisoV:~$ ls -ldir1
guest@ddirisoV:~$ chmod 440 dir1/
guest@ddirisoV:~$ ls -l | grep dir1
dr--r-----, 2 guest guest 19 map  7 16:31 dir1
guest@ddirisoV:~$ ls -ldir1
guest@ddirisoV:~$ chmod 550 dir1/
guest@ddirisoV:~$ ls -l | grep dir1
dr-xr-x---, 2 guest guest 19 map  7 16:31 dir1
guest@ddirisoV:~$ ls -ldir1
guest@ddirisoV:~$ chmod 660 dir1/
guest@ddirisoV:~$ ls -l | grep dir1
drw-rw----, 2 guest guest 19 map  7 16:31 dir1
guest@ddirisoV:~$
```

Figure 2.5: Заполнение таблицы

Обозначения в таблице:

- (1) Создание файла
- (2) Удаление файла
- (3) Запись в файл
- (4) Чтение файла
- (5) Смена директории
- (6) Просмотр файлов в директории
- (7) Переименование файл
- (8) Смена атрибутов файла

Table 2.1: Установленные права и разрешённые действия для групп

Права		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
директории	Права файла								
d-----	-----	-	-	-	-	-	-	-	-
(000)	(000)								
d-----x---	-----	-	-	-	-	+	-	-	+
(010)	(000)								
d----w----	-----	-	-	-	-	-	-	-	-
(020)	(000)								
d----wx---	-----	+	+	-	-	+	-	+	+
(030)	(000)								
d---r-----	-----	-	-	-	-	-	+	-	-
(040)	(000)								
d---r-x---	-----	-	-	-	-	+	+	-	+
(050)	(000)								
d---rw----	-----	-	-	-	-	-	+	-	-
(060)	(000)								
d---rwx---	-----	+	+	-	-	+	+	+	+
(070)	(000)								
d-----x---	-----x---	-	-	-	-	-	-	-	-
(000)	(010)								
d-----x---	-----x---	-	-	-	-	+	-	-	+
(010)	(010)								
d----w----	-----x---	-	-	-	-	-	-	-	-
(020)	(010)								
d----wx---	-----x---	+	+	-	-	+	-	+	+
(030)	(010)								

Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d---r-----	-----x---	-	-	-	-	-	+	-	-
(040)	(010)								
d---r-x---	-----x---	-	-	-	-	+	+	-	+
(050)	(010)								
d---rw----	-----x---	-	-	-	-	-	+	-	-
(060)	(010)								
d---rwx---	-----x---	+	+	-	-	+	+	+	+
(070)	(010)								
d-----	-----w----	-	-	-	-	-	-	-	-
(000)	(020)								
d-----x---	-----w----	-	-	+	-	+	-	-	+
(010)	(020)								
d----w----	-----w----	-	-	-	-	-	-	-	-
(020)	(020)								
d----wx---	-----w----	+	+	+	-	+	-	+	+
(030)	(020)								
d---r-----	-----w----	-	-	-	-	-	+	-	-
(040)	(020)								
d---r-x---	-----w----	-	-	+	-	+	+	-	+
(050)	(020)								
d---rw----	-----w----	-	-	-	-	-	+	-	-
(060)	(020)								
d---rwx---	-----w----	+	+	+	-	+	+	+	+
(070)	(020)								
d-----	-----wx---	-	-	-	-	-	-	-	-
(000)	(030)								

Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d-----x---	-----wx---	-	-	+	-	+	-	-	+
(010)	(030)								
d----w----	-----wx---	-	-	-	-	-	-	-	-
(020)	(030)								
d----wx---	-----wx---	+	+	+	-	+	-	+	+
(030)	(030)								
d---r-----	-----wx---	-	-	-	-	-	+	-	-
(040)	(030)								
d---r-x---	-----wx---	-	-	+	-	+	+	-	+
(050)	(030)								
d---rw----	-----wx---	-	-	-	-	-	+	-	-
(060)	(030)								
d---rwx---	-----wx---	+	+	+	-	+	+	+	+
(070)	(030)								
d-----	----r-----	-	-	-	-	-	-	-	-
(000)	(040)								
d-----x---	----r-----	-	-	-	+	+	-	-	+
(010)	(040)								
d----w----	----r-----	-	-	-	-	-	-	-	-
(020)	(040)								
d----wx---	----r-----	+	+	-	+	+	-	+	+
(030)	(040)								
d---r-----	----r-----	-	-	-	-	-	+	-	-
(040)	(040)								
d---r-x---	----r-----	-	-	-	+	+	+	-	+
(050)	(040)								

Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d---rw----	----r-----	-	-	-	-	-	+	-	-
(060)	(040)								
d---rwx---	----r-----	+	+	-	+	+	+	+	+
(070)	(040)								
d-----	----r-x---	-	-	-	-	-	-	-	-
(000)	(050)								
d-----x---	----r-x---	-	-	-	+	+	-	-	+
(010)	(050)								
d----w----	----r-x---	-	-	-	-	-	-	-	-
(020)	(050)								
d----wx---	----r-x---	+	+	-	+	+	-	+	+
(030)	(050)								
d---r-----	----r-x---	-	-	-	-	-	+	-	-
(040)	(050)								
d---r-x---	----r-x---	-	-	-	+	+	+	-	+
(050)	(050)								
d---rw----	----r-x---	-	-	-	-	-	+	-	-
(060)	(050)								
d---rwx---	----r-x---	+	+	-	+	+	+	+	+
(070)	(050)								
d-----	----rw----	-	-	-	-	-	-	-	-
(000)	(060)								
d-----x---	----rw----	-	-	+	+	+	-	-	+
(010)	(060)								
d----w----	----rw----	-	-	-	-	-	-	-	-
(020)	(060)								

Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d----wx---	----rw----	+	+	+	+	+	-	+	+
(030)	(060)								
d---r-----	----rw----	-	-	-	-	-	+	-	-
(040)	(060)								
d---r-x---	----rw----	-	-	+	+	+	+	-	+
(050)	(060)								
d---rw----	----rw----	-	-	-	-	-	+	-	-
(060)	(060)								
d---rwx---	----rw----	+	+	+	+	+	+	+	+
(070)	(060)								
d-----	----rwx---	-	-	-	-	-	-	-	-
(000)	(070)								
d-----x---	----rwx---	-	-	+	+	+	-	-	+
(010)	(070)								
d----w----	----rwx---	-	-	-	-	-	-	-	-
(020)	(070)								
d----wx---	----rwx---	+	+	+	+	+	-	+	+
(030)	(070)								
d---r-----	----rwx---	-	-	-	-	-	+	-	-
(040)	(070)								
d---r-x---	----rwx---	-	-	+	+	+	+	-	+
(050)	(070)								
d---rw----	----rwx---	-	-	-	-	-	+	-	-
(060)	(070)								
d---rwx---	----rwx---	+	+	+	+	+	+	+	+
(070)	(070)								

На основании заполненной таблицы я определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнила таблицу 2.2. Для заполнения последних двух строк опытным путем проверила минимальные права для создания и удаления поддиректории.

Table 2.2: Минимальные права для совершения операций

Операция	Права на директорию	Права на файл
Создание файла	d----wx--- (030)	----- (000)
Удаление файла	d----wx--- (030)	----- (000)
Чтение файла	d-----x--- (010)	----r----- (040)
Запись в файл	d-----x--- (010)	-----w---- (020)
Переименование файла	d----wx--- (030)	----- (000)
Создание поддиректории	d----wx--- (030)	----- (000)
Удаление поддиректории	d----wx--- (030)	----- (000)

Сравнивая таблицу 3.1. с такой же таблицей из предыдущей лабораторной работы, могу сказать, что они одинаковы. Единственное различие только в том, что в предыдущий раз я присваивала права владельцу, а в этот раз группе.

3 Выводы

В ходе выполнения работы, мы смогли приобрести практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Теория разграничения прав пользователей
2. Разрешения доступа к файлам