

Л.3. Дискреционное разграничение прав в Linux. Два пользователя

Греков Максим Сергеевич

2021

RUDN University, Moscow, Russian Federation

Цель работы

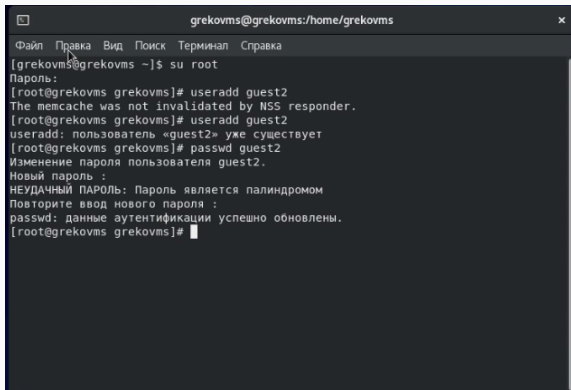
Целью данной лабораторной работы является получение практических навыков работы в консоли с атрибутами файлов для групп пользователей

Ход работы

В установленной операционной системе создали учётную запись пользователя `guest2` (используя учётную запись администратора) с помощью команды `useradd guest`

Задали пароль для пользователя `guest2` (используя учётную запись администратора) с помощью команды `passwd guest`

Новый пользователь

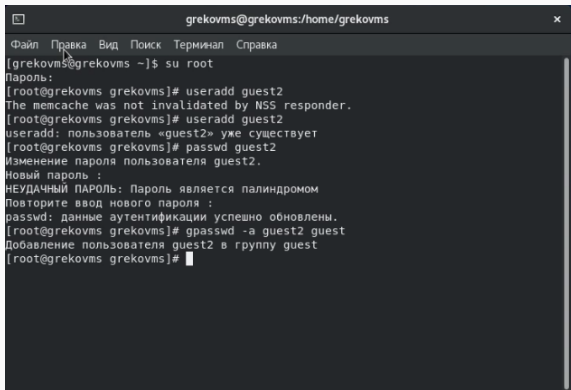


```
grekovms@grekovms:/home/grekovms
Файл Правка Вид Поиск Терминал Справка
[grekovms@grekovms ~]$ su root
Пароль:
[root@grekovms grekovms]# useradd guest2
The memcache was not invalidated by NSS responder.
[root@grekovms grekovms]# useradd guest2
useradd: пользователь «guest2» уже существует
[root@grekovms grekovms]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@grekovms grekovms]#
```

Figure 1: Новый пользователь

Добавление в группу

Добавили пользователя guest2 в группу guest с помощью команды `gpasswd -a guest2 guest`

A terminal window titled 'grekovms@grekovms:/home/grekovms' with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal shows a sequence of commands and their outputs: switching to root, adding user 'guest2' (which fails because it already exists), setting a password for 'guest2' (which fails because it's a palindrome), and finally adding 'guest2' to the 'guest' group using 'gpasswd -a guest2 guest'.

```
grekovms@grekovms:/home/grekovms
Файл Правка Вид Поиск Терминал Справка
[grekovms@grekovms ~]$ su root
Пароль:
[root@grekovms grekovms]# useradd guest2
The memcache was not invalidated by NSS responder.
[root@grekovms grekovms]# useradd guest2
useradd: пользователь «guest2» уже существует
[root@grekovms grekovms]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@grekovms grekovms]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@grekovms grekovms]#
```

Figure 2: Добавление в группу

Два пользователя

Осуществили вход в систему от двух пользователей на двух разных консолях (вкладках): guest на первой консоли и guest2 на второй консоли

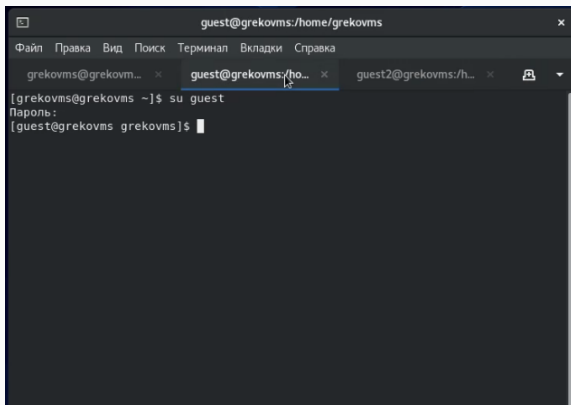
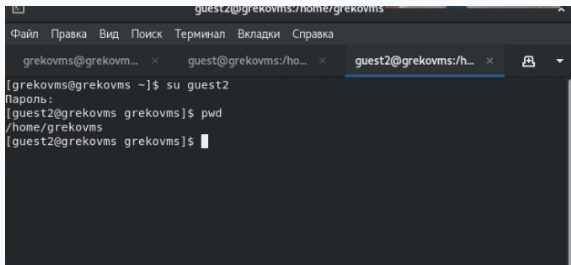


Figure 3: Два пользователя

Текущая директория

Для обоих пользователей командой `pwd` определили директорию, в которой находились. Сравнили её с приглашениями командной строки и получили идентичные значения



```
guest2@grekovms:/home/grekovms
Файл Правка Вид Поиск Терминал Вкладки Справка
grekovms@grekovm... x guest@grekovms:/ho... x guest2@grekovms:/h... x
[grekovms@grekovms ~]$ su guest2
Пароль:
[guest2@grekovms grekovms]$ pwd
/home/grekovms
[guest2@grekovms grekovms]$
```

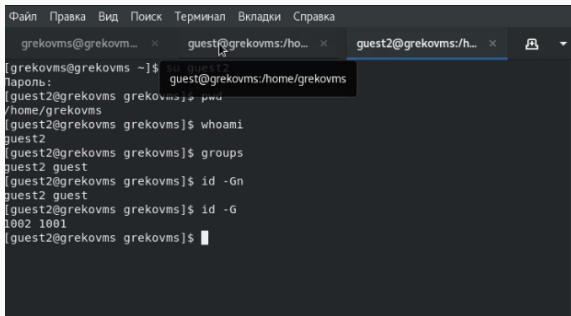
Figure 4: Текущая директория

Уточнили имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам.

Определили командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`.

Сравнили вывод команды `groups` с выводом команд `id -Gn` и `id -G`.

Группы пользователей



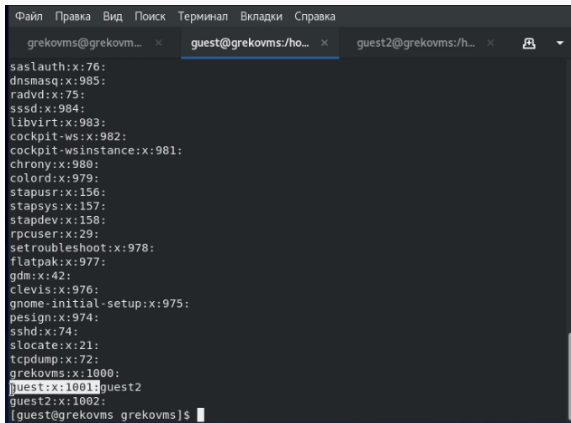
A terminal window with three tabs: 'grekovms@grekovm...', 'guest1@grekovms:/ho...', and 'guest2@grekovms:/h...'. The active tab is 'guest2@grekovms:/h...'. The terminal shows the following commands and output:

```
[grekovms@grekovms ~]$ su guest2
Пароль:
[guest2@grekovms grekovms]$ pwd
/home/grekovms
[guest2@grekovms grekovms]$ whoami
guest2
[guest2@grekovms grekovms]$ groups
guest2 guest
[guest2@grekovms grekovms]$ id -Gn
guest2 guest
[guest2@grekovms grekovms]$ id -G
1002 1001
[guest2@grekovms grekovms]$
```

Figure 5: Группы пользователей

Файл /etc/group

Сравнили полученную информацию с содержимым файла /etc/group, посмотрели файл командой `cat /etc/group`



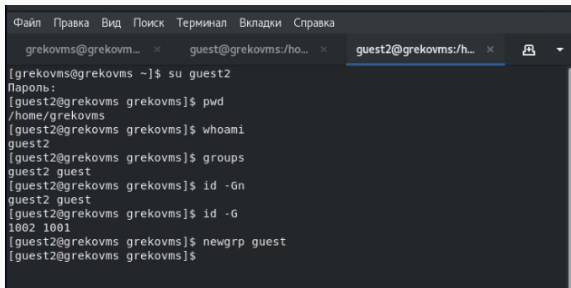
The image shows a terminal window with a dark background. At the top, there is a menu bar with options: 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', 'Вкладки', and 'Справка'. Below the menu bar, there are three tabs: 'grekovms@grekovm...', 'guest@grekovms/ho...', and 'guest2@grekovms/h...'. The active tab is 'guest@grekovms/ho...'. The terminal displays the output of the command `cat /etc/group`, which lists system users and their group memberships. The output is as follows:

```
saslauth:x:76:
dnsmasq:x:985:
radvd:x:75:
sssd:x:984:
libvirt:x:983:
cockpit-ws:x:982:
cockpit-wsinstance:x:981:
chrony:x:980:
colord:x:979:
stapusr:x:156:
stapsys:x:157:
stapdev:x:158:
rpcuser:x:29:
setroubleshoot:x:978:
flatpak:x:977:
gdm:x:42:
clevi:x:976:
gnome-initial-setup:x:975:
pesign:x:974:
sshd:x:74:
slocate:x:21:
tcpdump:x:72:
grekovms:x:1000:
guest:x:1001:guest2
guest2:x:1002:
[guest@grekovms grekovms]$
```

Figure 6: Файл /etc/group

Регистрация в группе

От имени пользователя guest2 выполнили регистрацию пользователя guest2 в группе guest командой `newgrp guest`



```
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка
grekovms@grekovm...  x  guest@grekovms:/ho...  x  guest2@grekovms:/h...  x  [?]  ▾

[grekovms@grekovms ~]$ su guest2
Пароль:
[guest2@grekovms grekovms]$ pwd
/home/grekovms
[guest2@grekovms grekovms]$ whoami
guest2
[guest2@grekovms grekovms]$ groups
guest2 guest
[guest2@grekovms grekovms]$ id -Gn
guest2 guest
[guest2@grekovms grekovms]$ id -G
1002 1001
[guest2@grekovms grekovms]$ newgrp guest
[guest2@grekovms grekovms]$
```

Figure 7: Регистрация в группе

От имени пользователя guest изменили права директории /home/guest, разрешив все действия для пользователей группы, применили команду `chmod g+rxw /home/guest`

```
clevis:x:976:  
gnome-initial-setup:x:975:  
pesign:x:974:  
sshd:x:74:  
slocate:x:21:  
tcpdump:x:72:  
grekovms:x:1000:  
guest:x:1001:guest2  
guest2:x:1002:  
[guest@grekovms grekovms]$ ls  
ls: невозможно открыть каталог '.': Отказано в доступе  
[guest@grekovms grekovms]$ chmod g+rxw /home/guest  
[guest@grekovms grekovms]$
```

Figure 8: Права для группы

От имени пользователя guest сняли с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1`, проверили правильность снятия атрибутов

```
chmod: невозможно получить доступ к 'dir1': Отказано в досту  
[guest@grekovms grekovms]$ chmod 000 /home/guest/dir1  
[guest@grekovms grekovms]$ ls  
ls: невозможно открыть каталог '.': Отказано в доступе  
[guest@grekovms grekovms]$
```

Figure 9: Снятие атрибутов

Меняя атрибуты у директории `dir1` и файла `file1` от имени пользователя `guest` и делая проверку от пользователя `guest2`, заполнили таблицу, определив опытным путём, какие операции разрешены, а какие нет.

На основании заполненной таблицы определили те или иные минимально необходимые права для выполнения пользователем `guest2` операций внутри директории `dir1` и заполнили вторую таблицу.

1	Установленные права и разрешённые действия									
2	Права директо рии	Права файла	Создани е файла	Удалени е файла	Запись в файл	Чтение файла	Смена директо рии	Просмотр файлов в директор ии	Переиме нование файла	Смена атрибутов файла
3	--- (000)	--- (000)	-	-	-	-	-	-	-	-
4	-- x (010)	--- (000)	-	-	-	-	+	-	-	+
5	- w - (020)	--- (000)	-	-	-	-	-	-	-	-
6	- w x (030)	--- (000)	+	+	-	-	+	-	+	+
7	r - - (040)	--- (000)	-	-	-	-	-	+	-	-
8	r - x (050)	--- (000)	-	-	-	-	+	+	-	+
9	r w - (060)	--- (000)	-	-	-	-	-	+	-	-
10	r w x (070)	--- (000)	+	+	-	-	+	+	+	+
11	--- (000)	-- x (010)	-	-	-	-	-	-	-	-
12	-- x (010)	-- x (010)	-	-	-	-	+	-	-	+
13	- w - (020)	-- x (010)	-	-	-	-	-	-	-	-
14	- w x (030)	-- x (010)	+	+	-	-	+	-	+	+
15	r - - (040)	-- x (010)	-	-	-	-	-	+	-	-
16	r - x (050)	-- x (010)	-	-	-	-	+	+	-	+
17	r w - (060)	-- x (010)	-	-	-	-	-	+	-	-
18	r w x (070)	-- x (010)	+	+	-	-	+	+	+	+
19	--- (000)	- w - (020)	-	-	-	-	-	-	-	-
20	-- x (010)	- w - (020)	-	+	-	-	+	-	-	+
21	- w - (020)	- w - (020)	-	-	-	-	-	-	-	-
22	- w x (030)	- w - (020)	+	+	-	-	+	-	+	+
23	r - - (040)	- w - (020)	-	-	-	-	-	+	-	-
24	r - x (050)	- w - (020)	-	+	-	-	+	+	-	+
25	r w - (060)	- w - (020)	-	-	-	-	-	+	-	-
26	r w x (070)	- w - (020)	+	+	-	-	+	+	+	+
27	--- (000)	- w x (030)	-	-	-	-	-	-	-	-
28	-- x (010)	- w x (030)	-	+	-	-	+	-	-	+
29	- w - (020)	- w x (030)	-	-	-	-	-	-	-	-
30	- w x (030)	- w x (030)	+	+	-	-	+	-	+	+

Figure 10: Фрагмент заполнения таблицы 1

1	<u>Минимальные права для совершения операций</u>		
2	Операция	Минимальные права на директорию	Минимальные права на файл
3	Создание файла	- w x (030)	--- (000)
4	Удаление файла	- w x (030)	--- (000)
5	Чтение файла	- - x (010)	r - - (040)
6	Запись в файл	- - x (010)	- w - (020)
7	Переименование файла	- w x (030)	--- (000)
8	Создание поддиректории	- w x (030)	--- (000)
9	Удаление поддиректории	- w x (030)	--- (000)

Figure 11: Фрагмент заполнения таблицы 2

Вывод

В ходе лабораторной работы получили практические навыки работы в консоли с атрибутами файлов для групп пользователей

