

Дискреционное разграничение прав в Linux. Основные атрибуты

Владислав Пузырёв¹

20 сентября, 2023, Москва, Россия

¹Российский Университет Дружбы Народов

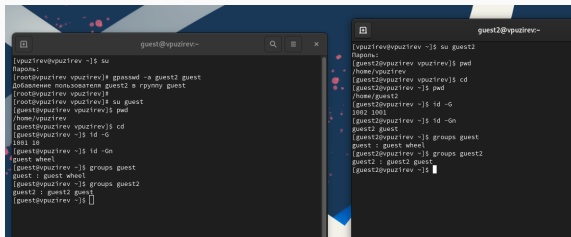
Цели и задачи работы

Цель лабораторной работы

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

Процесс выполнения лабораторной работы

Определяем UID и группу двух пользователей



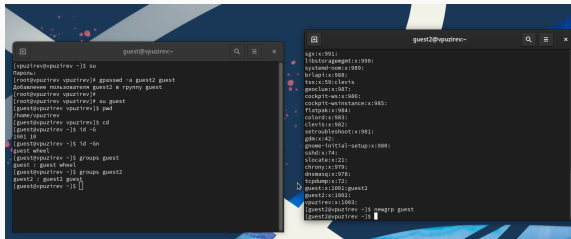
The image shows two terminal windows side-by-side. The left window is titled 'guest@vpuzirev-' and shows the process of creating a user named 'guest' using 'passwd', adding a shell with 'rsh', and setting a home directory. The right window is titled 'guest2@vpuzirev-' and shows the process of creating a user named 'guest2' using 'passwd', adding a shell with 'rsh', and setting a home directory. Both windows show the output of 'id' and 'groups' commands to verify the user creation.

```
guest@vpuzirev-  
[vpuzirev@vpuzirev ~]$ su  
Пароль:  
[root@vpuzirev vpuzirev]# passwd -s guest  
Добавление пользователя guest s rshmy guest  
[root@vpuzirev vpuzirev]#  
[root@vpuzirev vpuzirev]# su guest  
[guest@vpuzirev vpuzirev]$ pwd  
/home/vpuzirev  
[guest@vpuzirev vpuzirev]$ cd  
[guest@vpuzirev ~]$ id -G  
1001 10  
[guest@vpuzirev ~]$ id -Gn  
guest wheel  
[guest@vpuzirev ~]$ groups guest  
guest : guest wheel  
[guest@vpuzirev ~]$ groups guest2  
guest2 : guest2 guest  
[guest@vpuzirev ~]$
```

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

Figure 1: Информация о пользователях

Файл с данными о пользователях



The image displays two terminal windows side-by-side. The left window, titled 'guest@vputrev-', shows the process of creating a user group named 'guest' using the 'su' command, adding members 'guest1' and 'guest2', and setting permissions. The right window, titled 'guest2@vputrev-', shows the contents of the '/etc/group' file, which lists the 'guest' group and its members.

```
guest@vputrev- ~$ su
Password:
[root@vputrev vputrev]# groupadd -s guest2 guest
Addgroup: newgroup: guest2: s: rpyou: guest
[root@vputrev vputrev]#
[root@vputrev vputrev]# su guest
[guest@vputrev vputrev]# pwd
/home/vputrev
[guest@vputrev vputrev]# cd
[guest@vputrev ~]$ id -G
1001 10
[guest@vputrev ~]$ id -Gn
guest wheel
[guest@vputrev ~]$ groups guest
guest : guest wheel
[guest@vputrev ~]$ groups guest2
guest2 : guest2 guest
[guest@vputrev ~]$
```

```
guest2@vputrev- ~$ cat /etc/group
sgix:1001:
libstoragegmt:1000:
systemd-cored:1000:
br:1001:1000:
taux:50:clevis
pencil:1000:1000:
cockpit-ws:1000:
cockpit-ws-instance:1000:
flatpak:1000:
colord:1000:
clevis:1000:
setrouselinux:1001:
gdm:1002:
gnome-initial-setup:1000:
sshd:1001:
slocate:1001:
chromium:1000:
dramax:1000:
kcpdump:1000:
guests:1000:guest2
guest2:1002:
vputrev:1000:
[guest2@vputrev ~]$ newgrp guest
[guest2@vputrev ~]$
```

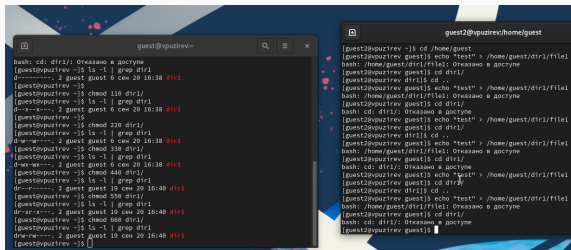
Figure 2: Содержимое файла /etc/group

Атрибуты директории

```
[guest@vpuzirev ~]$  
[guest@vpuzirev ~]$ chmod g+rx  
chmod: пропущен операнд после «g+rx»  
По команде «chmod --help» можно получить дополнительную информацию.  
[guest@vpuzirev ~]$ chmod g+rx /home/guest  
[guest@vpuzirev ~]$ cd  
[guest@vpuzirev ~]$ mkdir dir1  
[guest@vpuzirev ~]$ chmod 000 dir1  
[guest@vpuzirev ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@vpuzirev ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@vpuzirev ~]$ ls -l | grep dir1  
d-----, 2 guest guest 6 сен 20 16:38 dir1  
[guest@vpuzirev ~]$
```

Figure 3: Снятие атрибутов с директории

Заполнение таблицы



```
guest@vpuzirev~  
bash: cd: dir1/: Ошибка: не существует  
[guest@vpuzirev ~]$ ls -l | grep dir1  
d----- 2 guest guest 6 cew 20 16:38 dir1  
[guest@vpuzirev ~]$  
[guest@vpuzirev ~]$ chroot 110 dir1/  
[guest@vpuzirev ~]$ ls -l | grep dir1  
d-x-x-x-- 2 guest guest 6 cew 20 16:38 dir1  
[guest@vpuzirev ~]$  
[guest@vpuzirev ~]$ chroot 220 dir1/  
[guest@vpuzirev ~]$ ls -l | grep dir1  
drwxr-x-- 2 guest guest 8 cew 20 16:38 dir1  
[guest@vpuzirev ~]$ chroot 330 dir1/  
[guest@vpuzirev ~]$ ls -l | grep dir1  
drwxr-x-- 2 guest guest 16 cew 20 16:40 dir1  
[guest@vpuzirev ~]$ chroot 440 dir1/  
[guest@vpuzirev ~]$ ls -l | grep dir1  
drwxr-x-- 2 guest guest 19 cew 20 16:40 dir1  
[guest@vpuzirev ~]$
```

```
guest2@vpuzirev/home/guest  
[guest2@vpuzirev ~]$ cd /home/guest  
[guest2@vpuzirev guest]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Ошибка: не существует  
[guest2@vpuzirev guest]$ cd dir1/  
[guest2@vpuzirev dir1]$ cd ..  
[guest2@vpuzirev guest]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Ошибка: не существует  
[guest2@vpuzirev guest]$ cd dir1/  
[guest2@vpuzirev dir1]$ cd ..  
[guest2@vpuzirev guest]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Ошибка: не существует  
[guest2@vpuzirev dir1]$ cd ..  
[guest2@vpuzirev guest]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Ошибка: не существует  
[guest2@vpuzirev guest]$ cd dir1/  
[guest2@vpuzirev dir1]$ cd ..  
[guest2@vpuzirev guest]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Ошибка: не существует  
[guest2@vpuzirev dir1]$ cd ..  
[guest2@vpuzirev guest]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Ошибка: не существует  
[guest2@vpuzirev guest]$ cd dir1/  
[guest2@vpuzirev dir1]$ cd ..  
[guest2@vpuzirev guest]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Ошибка: не существует  
[guest2@vpuzirev dir1]$ cd ..  
[guest2@vpuzirev guest]$
```

Figure 4: Заполнение таблицы

Права и разрешённые действия

Операция	Минимальные права на директорию	Минимальные 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)

Figure 5: Минимальные права для совершения операций

Выводы по проделанной работе

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