

Дискреционное разграничение прав в Linux. Основные атрибуты

Николай Рыбалко¹

8 марта, 2025, Москва, Россия

¹Российский Университет Дружбы Народов

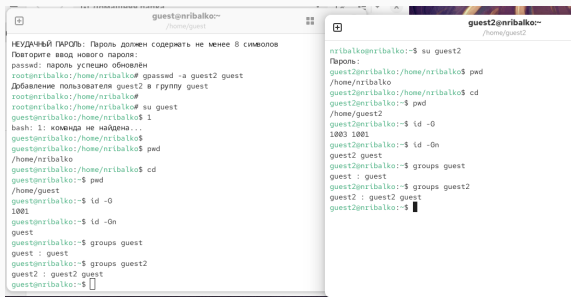
Цели и задачи работы

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@nribalko:~ /home/guest' and shows the process of creating a user 'guest' with a password '1001'. The right window is titled 'guest2@nribalko:~ /home/guest2' and shows the process of creating a user 'guest2' with a password '1002' and setting its group to 'guest'.

```
guest@nribalko:~  
/home/guest  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов  
Повторите ввод нового пароля:  
passwd: пароль успешно обновлён  
root@nribalko:/home/nribalko# gpaswd -a guest2 guest  
Добавление пользователя guest2 в группу guest  
root@nribalko:/home/nribalko#  
root@nribalko:/home/nribalko# su guest  
guest@nribalko:/home/nribalko$ 1  
bash: 1: команда не найдена...  
guest@nribalko:/home/nribalko$  
guest@nribalko:/home/nribalko$ pwd  
/home/nribalko  
guest@nribalko:/home/nribalko$ cd  
/home/guest  
guest@nribalko:~$ pwd  
/home/guest  
guest@nribalko:~$ id -G  
1001  
guest@nribalko:~$ id -Gn  
guest  
guest@nribalko:~$ groups guest  
guest : guest  
guest@nribalko:~$ groups guest2  
guest2 : guest2 guest  
guest@nribalko:~$
```

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

Рис. 1: Информация о пользователях

Файл с данными о пользователях



A terminal window titled "guest2@nribalko:~" with the path "/home/guest2" below it. The window displays the output of the command "cat /etc/group", which lists system and regular users in a colon-separated format. The users listed are geoclue, sssd, libstorage, systemd-core, wsdd, clevis, setroubleshoot, pipewire, flatpak, brlapi, gdm, gnome-initial-setup, dnsmasq, pesign, sshd, chrony, tcpdump, plocate, gnome-remote-desktop, guest, nribalko, and another guest user. The terminal shows the prompt "guest2@nribalko:~\$ newgrp guest" and the subsequent prompt "guest2@nribalko:~\$".

```
geoclue:x:996:
sssd:x:995:
libstorage:x:994:
systemd-core:x:993:
wsdd:x:992:
clevis:x:991:
setroubleshoot:x:990:
pipewire:x:989:
flatpak:x:988:
brlapi:x:987:
gdm:x:42:
gnome-initial-setup:x:986:
dnsmasq:x:985:
pesign:x:984:
sshd:x:74:
chrony:x:983:
tcpdump:x:72:
plocate:x:982:
gnome-remote-desktop:x:981:
guest:x:1001:guest
nribalko:x:1002:
guest2:x:1003:
guest2@nribalko:~$ newgrp guest
guest2@nribalko:~$
```

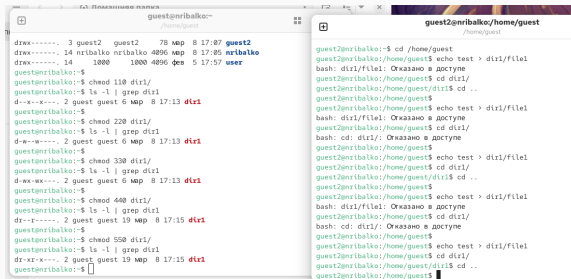
Рис. 2: Содержимое файла /etc/group

Атрибуты директории

```
guest@nribalko:~$  
guest@nribalko:~$ cd  
guest@nribalko:~$ chmod g+rxw /home/guest  
guest@nribalko:~$ mkdir dir1  
guest@nribalko:~$ chmod 000 dir1/  
guest@nribalko:~$ ls -l | grep dir1  
d----- . 2 guest guest 6 мар 8 17:13 dir1  
guest@nribalko:~$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
guest@nribalko:~$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
guest@nribalko:~$ ls -l /home/  
итого 8  
drwxrwx---. 4 guest guest 90 мар 8 17:13 guest  
drwx-----. 3 guest2 guest2 78 мар 8 17:07 guest2  
drwx-----. 14 nribalko nribalko 4096 мар 8 17:05 nribalko  
drwx-----. 14 1000 1000 4096 фев 5 17:57 user  
guest@nribalko:~$ █
```

Рис. 3: Снятие атрибутов с директории

Заполнение таблицы



The image shows two terminal windows. The left window, titled 'guest@nribalko:~/home/guest', displays a table with columns for permissions, user count, user names, and timestamps. The table is being populated with data for 'guest2' and 'nribalko'. The right window, titled 'guest2@nribalko:/home/guest', shows the commands used to generate the data, including 'cd /home/guest', 'echo test > dir1/file1', and 'ls -l | grep dir1'.

```
guest@nribalko:~/home/guest
drwx-----, 3 guest2 guest2 78 map 8 17:07 guest2
drwx-----, 14 nribalko nribalko 4896 map 8 17:05 nribalko
drwx-----, 14 1000 1000 4896 qes 5 17:57 user
guest@nribalko:~$
guest@nribalko:~$ chmod 110 dir1/
guest@nribalko:~$ ls -l | grep dir1
d-x-x-----, 2 guest guest 6 map 8 17:13 dir1
guest@nribalko:~$
guest@nribalko:~$ chmod 220 dir1/
guest@nribalko:~$ ls -l | grep dir1
d-w--w-----, 2 guest guest 6 map 8 17:13 dir1
guest@nribalko:~$
guest@nribalko:~$ chmod 330 dir1/
guest@nribalko:~$ ls -l | grep dir1
d-xx-w-----, 2 guest guest 6 map 8 17:13 dir1
guest@nribalko:~$
guest@nribalko:~$ chmod 440 dir1/
guest@nribalko:~$ ls -l | grep dir1
dr--r-----, 2 guest guest 19 map 8 17:15 dir1
guest@nribalko:~$
guest@nribalko:~$ chmod 550 dir1/
guest@nribalko:~$ ls -l | grep dir1
dr-xr-x-----, 2 guest guest 19 map 8 17:15 dir1
guest@nribalko:~$

guest2@nribalko:/home/guest
guest2@nribalko:~$ cd /home/guest
guest2@nribalko:/home/guest$ echo test > dir1/file1
bash: dir1/file1: Оказано в доп.т.не
guest2@nribalko:/home/guest$ cd dir1/
guest2@nribalko:/home/guest/dir1$ cd ..
guest2@nribalko:/home/guest$
guest2@nribalko:/home/guest$ echo test > dir1/file1
bash: dir1/file1: Оказано в доп.т.не
guest2@nribalko:/home/guest$ cd dir1/
bash: cd: dir1/: Оказано в доп.т.не
guest2@nribalko:/home/guest$
guest2@nribalko:/home/guest$ echo test > dir1/file1
guest2@nribalko:/home/guest$ cd dir1/
guest2@nribalko:/home/guest/dir1$ cd ..
guest2@nribalko:/home/guest$
guest2@nribalko:/home/guest$ echo test > dir1/file1
bash: dir1/file1: Оказано в доп.т.не
guest2@nribalko:/home/guest$ cd dir1/
bash: cd: dir1/: Оказано в доп.т.не
guest2@nribalko:/home/guest$ cd dir1/
guest2@nribalko:/home/guest/dir1$ cd ..
guest2@nribalko:/home/guest$
```

Рис. 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)	----- (040)
Запись в файл	d----x--- (010)	----- (020)
Переименование файла	d---wx--- (030)	----- (000)
Создание поддиректории	d---wx--- (030)	----- (000)
Удаление поддиректории	d---wx--- (030)	----- (000)

Рис. 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.