

Дискреционное разграничение прав в Linux. Основные атрибуты

Маргарита Фомичёва¹

16 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

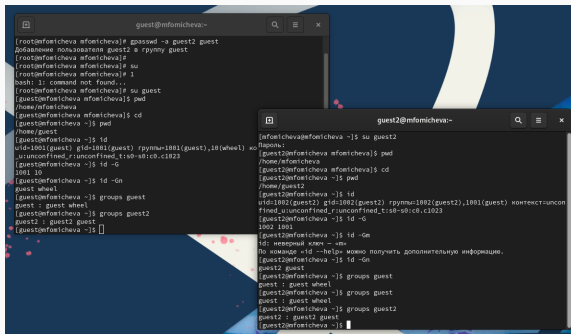
Цели и задачи работы

Цель лабораторной работы

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

Процесс выполнения лабораторной работы

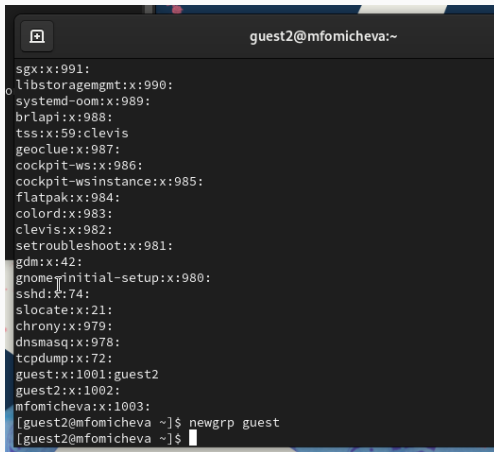
Определяем UID и группу двух пользователей



```
guest@mfonicheva:~  
[root@mfonicheva mfonicheva]# passwd -s guest2 guest  
Добавление пользователя guest2 в rpymy guest  
[root@mfonicheva mfonicheva]#  
[root@mfonicheva mfonicheva]# su  
[root@mfonicheva mfonicheva]# 1  
bash: 1: command not found...  
[root@mfonicheva mfonicheva]# su guest  
[guest@mfonicheva mfonicheva]$ pwd  
/home/mfonicheva  
[guest@mfonicheva mfonicheva]$ cd  
[guest@mfonicheva ~]$ pwd  
/home/guest  
[guest@mfonicheva ~]$ id  
uid=1001(guest) gid=1001(guest) rpymy=1001(guest),10(wheel) ко  
_u:unconfined_r:unconfined_t:s0-s0:c0,c1023  
[guest@mfonicheva ~]$ id -G  
1001 10  
[guest@mfonicheva ~]$ id -Gn  
guest wheel  
[guest@mfonicheva ~]$ groups guest  
guest : guest wheel  
[guest@mfonicheva ~]$ groups guest2  
guest2 : guest2 guest  
[guest@mfonicheva ~]$  
  
guest2@mfonicheva:~  
[mfonicheva@mfonicheva ~]$ su guest2  
Пароль:  
[guest2@mfonicheva mfonicheva]$ pwd  
/home/mfonicheva  
[guest2@mfonicheva mfonicheva]$ cd  
[guest2@mfonicheva ~]$ pwd  
/home/guest2  
[guest2@mfonicheva ~]$ id  
uid=1002(guest2) gid=1002(guest2) rpymy=1002(guest2),1001(guest) контекст:uncon  
fined_u:unconfined_r:unconfined_t:s0-s0:c0,c1023  
[guest2@mfonicheva ~]$ id -G  
1002 1001  
[guest2@mfonicheva ~]$ id -Gn  
id: неверный xmem - sm-  
10 кода: id --help можно получить дополнительную информацию.  
[guest2@mfonicheva ~]$ id -Gn  
guest2 guest  
[guest2@mfonicheva ~]$ groups guest  
guest : guest wheel  
[guest2@mfonicheva ~]$ groups guest  
guest : guest wheel  
[guest2@mfonicheva ~]$ groups guest2  
guest2 : guest2 guest  
[guest2@mfonicheva ~]$
```

Figure 1: Информация о пользователях

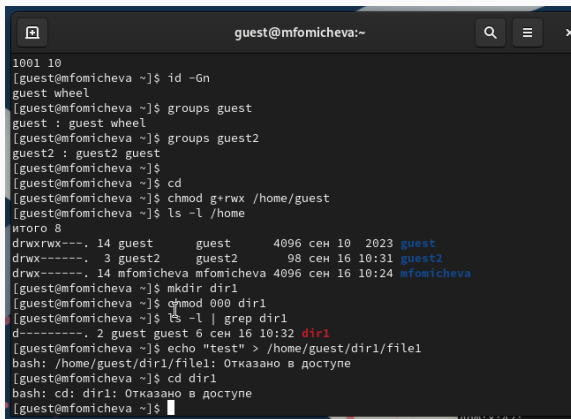
Файл с данными о пользователях

A terminal window with a dark background and light text. The title bar at the top reads "guest2@mfomicheva:~". The terminal displays the contents of the /etc/group file, listing system users and regular users. The users listed are: sgx, libstorageemgmt, systemd-oom, brlapi, tss, geoclue, cockpit-ws, cockpit-wsinstance, flatpak, colord, clevis, setroubleshoot, gdm, gnome-initial-setup, sshd, slocate, chrony, dnsmasq, tcpdump, guest, guest2, mfomicheva, and a new group named "guest" created by the command "newgrp guest".

```
sgx:x:991:
libstorageemgmt:x:990:
systemd-oom:x:989:
brlapi:x:988:
tss:x:59:clevis
geoclue:x:987:
cockpit-ws:x:986:
cockpit-wsinstance:x:985:
flatpak:x:984:
colord:x:983:
clevis:x:982:
setroubleshoot:x:981:
gdm:x:42:
gnome-initial-setup:x:980:
sshd:x:74:
slocate:x:21:
chrony:x:979:
dnsmasq:x:978:
tcpdump:x:72:
guest:x:1001:guest2
guest2:x:1002:
mfomicheva:x:1003:
[guest2@mfomicheva ~]$ newgrp guest
[guest2@mfomicheva ~]$
```

Figure 2: Содержимое файла /etc/group

Атрибуты директории



A terminal window titled 'guest@mfomicheva:~' showing a series of commands and their outputs. The user 'guest' is in the 'wheel' group. They create a directory 'dir1' and attempt to remove its permissions using 'chmod 000 dir1'. The output of 'ls -l | grep dir1' shows the directory with permissions 'd-----' and ownership 'guest guest', indicating that permissions have been removed. Subsequent attempts to enter the directory or create a file fail with 'Отказано в доступе' (Access denied).

```
1001 10
[guest@mfomicheva ~]$ id -Gn
guest wheel
[guest@mfomicheva ~]$ groups guest
guest : guest wheel
[guest@mfomicheva ~]$ groups guest2
guest2 : guest2 guest
[guest@mfomicheva ~]$ cd
[guest@mfomicheva ~]$ chmod g+rxw /home/guest
[guest@mfomicheva ~]$ ls -l /home
итого 8
drwxrwx---. 14 guest      guest      4096 сен 10  2023 guest
drwx-----.  3 guest2     guest2     98 сен 16 10:31 guest2
drwx-----. 14 mfomicheva mfomicheva 4096 сен 16 10:24 mfomicheva
[guest@mfomicheva ~]$ mkdir dir1
[guest@mfomicheva ~]$ chmod 000 dir1
[guest@mfomicheva ~]$ ls -l | grep dir1
d------.  2 guest guest 6 сен 16 10:32 dir1
[guest@mfomicheva ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@mfomicheva ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest@mfomicheva ~]$
```

Figure 3: Снятие атрибутов с директории

Заполнение таблицы

The image displays two terminal windows side-by-side, illustrating the configuration of a Docker container named 'nfoalcheva'.

Left Terminal Window:

```

guest@mfonicheva:~$
draw-----, 14 mfonicheva mfonicheva 4096 cew 16 10:24 nfoalcheva
[guest@mfonicheva ~]$ mkdir dir1
[guest@mfonicheva ~]$ chmod 660 dir1
[guest@mfonicheva ~]$ ls -l | grep dir1
d-----, 2 guest guest 6 cew 16 10:32 dir1
[guest@mfonicheva ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@mfonicheva ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest@mfonicheva ~]$ chmod 770 dir1
[guest@mfonicheva ~]$ ls -l | grep dir1
d--x--x--x, 2 guest guest 6 cew 16 10:32 dir1
[guest@mfonicheva ~]$ cd dir1
[guest@mfonicheva dir1]$ cd ..
[guest@mfonicheva ~]$ chmod 720 dir1
[guest@mfonicheva ~]$ ls -l | grep dir1
d-w-----, 2 guest guest 6 cew 16 10:32 dir1
[guest@mfonicheva ~]$ chmod 330 dir1/
[guest@mfonicheva ~]$ ls -l | grep dir1
d-w-a-----, 2 guest guest 6 cew 16 10:32 dir1
[guest@mfonicheva ~]$ chmod 440 dir1/
[guest@mfonicheva ~]$ ls -l | grep dir1
dr-r-----, 2 guest guest 19 cew 16 10:33 dir1
[guest@mfonicheva ~]$

```

Right Terminal Window:

```

guest2@mfonicheva:/home/guest$
dnsmasq:x:978:
tcpdump:x:72:
guest1:x:1001:guest2
guest2:x:1002:
nfonicheva:x:1003:
[guest2@mfonicheva ~]$ newgrp guest
[guest2@mfonicheva ~]$
[guest2@mfonicheva ~]$ cd /home/guest
[guest2@mfonicheva guest]$ who test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest2@mfonicheva guest]$ cd dir1/
[guest2@mfonicheva dir1]$ cd ..
[guest2@mfonicheva dir1]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest2@mfonicheva dir1]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest2@mfonicheva dir1]$ echo test > dir1/file1
[guest2@mfonicheva dir1]$ cd dir1/
[guest2@mfonicheva dir1]$ cd ..
[guest2@mfonicheva dir1]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest2@mfonicheva dir1]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest2@mfonicheva dir1]$

```

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.