

Дискреционное разграничение прав в Linux. Основные атрибуты

Романов Дмитрий Романович НБИ-01-19¹

13 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

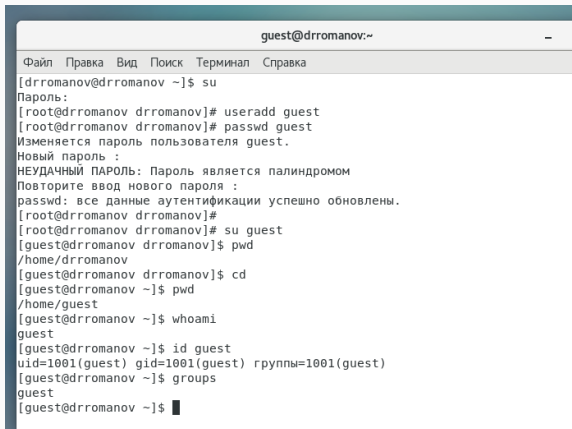
Цели и задачи работы

Цель лабораторной работы

Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Процесс выполнения лабораторной работы

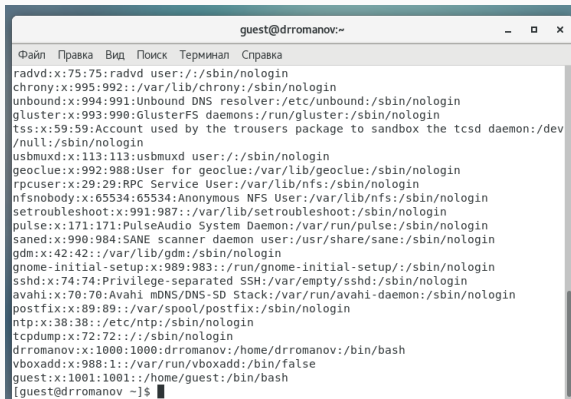
Определяем UID и группу



```
guest@drromanov:~  
Файл Правка Вид Поиск Терминал Справка  
[drromanov@drromanov ~]$ su  
Пароль:  
[root@drromanov drromanov]# useradd guest  
[root@drromanov drromanov]# passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[root@drromanov drromanov]#  
[root@drromanov drromanov]# su guest  
[guest@drromanov drromanov]$ pwd  
/home/drromanov  
[guest@drromanov drromanov]$ cd  
[guest@drromanov ~]$ pwd  
/home/guest  
[guest@drromanov ~]$ whoami  
guest  
[guest@drromanov ~]$ id guest  
uid=1001(guest) gid=1001(guest) группы=1001(guest)  
[guest@drromanov ~]$ groups  
guest  
[guest@drromanov ~]$ █
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях



A terminal window titled 'guest@drromanov:~' displays the contents of the /etc/passwd file. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The output shows a list of system and regular users, each with their username, UID, GID, and shell path. The regular users listed are drromanov and guest.

```
guest@drromanov:~  
Файл Правка Вид Поиск Терминал Справка  
radvd:x:75:75:radvd user:/:/sbin/nologin  
chrony:x:995:992::/var/lib/chrony:/sbin/nologin  
unbound:x:994:991:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
gluster:x:993:990:GlusterFS daemons:/run/gluster:/sbin/nologin  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin  
geoclue:x:992:988:User for geoclue:/var/lib/geoclue:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
setroubleshoot:x:991:987::/var/lib/setroubleshoot:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
sane:x:990:984:SANE scanner daemon user:/usr/share/sane:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:989:983::/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
postfix:x:89:89::/var/spool/postfix:/sbin/nologin  
ntp:x:38:38::/etc/ntp:/sbin/nologin  
tcpdump:x:72:72::/sbin/nologin  
drromanov:x:1000:1000:drromanov:/home/drromanov:/bin/bash  
vboxadd:x:988:1::/var/run/vboxadd:/bin/false  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@drromanov ~]$
```

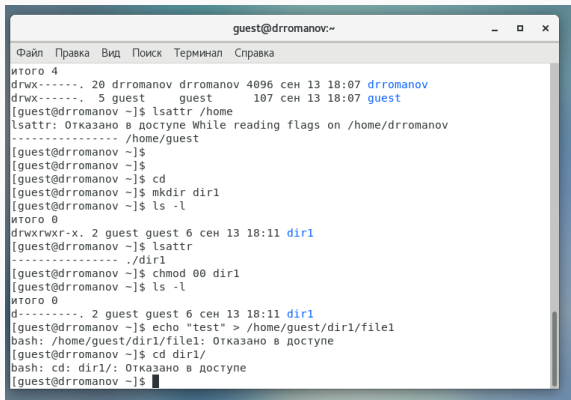
Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@drromanov ~]$  
[guest@drromanov ~]$  
[guest@drromanov ~]$ ls -l /home  
итого 4  
drwx-----. 20 drromanov drromanov 4096 сен 13 18:07 drromanov  
drwx-----.  5 guest      guest    107 сен 13 18:07 guest  
[guest@drromanov ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/drromanov  
----- /home/guest  
[guest@drromanov ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@drromanov:~' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal output shows the process of removing permissions from the '/home/guest' directory. It starts with a 'lsattr' command that fails with 'Отказано в доступе'. Then, 'cd' is used to move into the directory, 'mkdir dir1' is used to create a subdirectory, and 'chmod 00 dir1' is used to remove permissions from 'dir1'. The process is repeated for the 'dir1' directory. The window has standard Linux window controls (minimize, maximize, close) in the top right corner.

```
guest@drromanov:~  
Файл Правка Вид Поиск Терминал Справка  
итого 4  
drwx-----, 20 drromanov drromanov 4096 сен 13 18:07 drromanov  
drwx-----, 5 guest guest 107 сен 13 18:07 guest  
[guest@drromanov ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/drromanov  
----- /home/guest  
[guest@drromanov ~]$  
[guest@drromanov ~]$  
[guest@drromanov ~]$ cd  
[guest@drromanov ~]$ mkdir dir1  
[guest@drromanov ~]$ ls -l  
итого 0  
drwxrwxr-x, 2 guest guest 6 сен 13 18:11 dir1  
[guest@drromanov ~]$ lsattr  
----- ./dir1  
[guest@drromanov ~]$ chmod 00 dir1  
[guest@drromanov ~]$ ls -l  
итого 0  
d-----, 2 guest guest 6 сен 13 18:11 dir1  
[guest@drromanov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@drromanov ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@drromanov ~]$
```

Figure 4: Снятие атрибутов с директории

Права и разрешённые действия

Операция	Права на директорию	Права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	-r----- (400)
Запись в файл	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

Figure 5: Минимальные права для совершения операций

Выводы по проделанной работе

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.