

Дискреционное разграничение прав в Linux. Основные атрибуты

Даутов С.А. НПИ-01-19¹

12 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

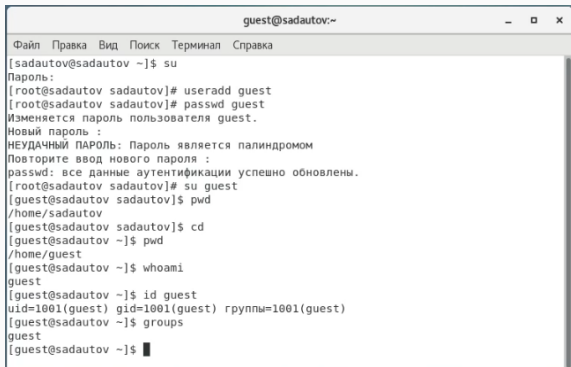
Цели и задачи работы

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

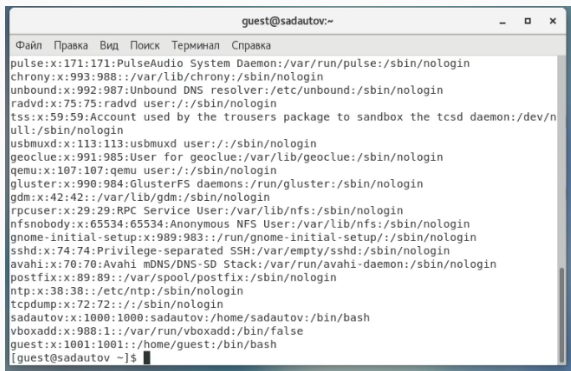
Определяем UID и группу



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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

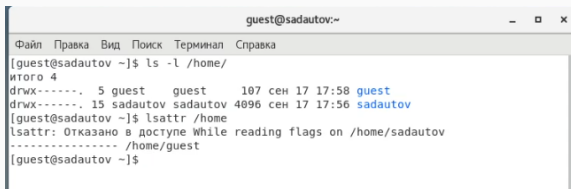


The image shows a terminal window titled 'guest@sadautov:~'. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal displays the output of the 'cat /etc/passwd' command, listing system and regular users. The output is as follows:

```
guest@sadautov:~  
Файл Правка Вид Поиск Терминал Справка  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
chrony:x:993:988::/var/lib/chrony:/sbin/nologin  
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
radvd:x:75:75:radvd user:/:/sbin/nologin  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/n  
ull:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin  
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin  
qemu:x:107:107:qemu user:/:/sbin/nologin  
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/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  
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  
sadautov:x:1000:1000:sadautov:/home/sadautov:/bin/bash  
vboxadd:x:988:1::/var/run/vboxadd:/bin/false  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@sadautov ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям



```
guest@sadautov:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@sadautov ~]$ ls -l /home/  
итого 4  
drwx-----. 5 guest      guest      107 сен 17 17:58 guest  
drwx-----. 15 sadautov sadautov 4096 сен 17 17:56 sadautov  
[guest@sadautov ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/sadautov  
----- /home/guest  
[guest@sadautov ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
guest@sadaufov ~$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/sadaufov
-----
/home/guest
guest@sadaufov ~$
```

```
guest@sadaufov~
Файл Права Бит Ресурсы Типовая Свойства
-----
guest@sadaufov ~$ cd
guest@sadaufov ~$ mkdir dir1
guest@sadaufov ~$ ls -l
иторо 0
drwxr-xr-x. 2 guest guest 6 сен 17 18:02 dir1
guest@sadaufov ~$ lsattr
-----
./dir1
guest@sadaufov ~$ chmod 000 dir1
guest@sadaufov ~$ ls -l
иторо 0
d----- . 2 guest guest 6 сен 17 18:02 dir1
guest@sadaufov ~$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
guest@sadaufov ~$
guest@sadaufov ~$ chmod 300 dir1
guest@sadaufov ~$
```

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.