

Дискреционное разграничение прав в Linux. Основные атрибуты

Карпоев Михаил Артемович НФИбд-01-18¹

29 сентября, 2021, Москва, Россия

¹Российский Университет Дружбы Народов

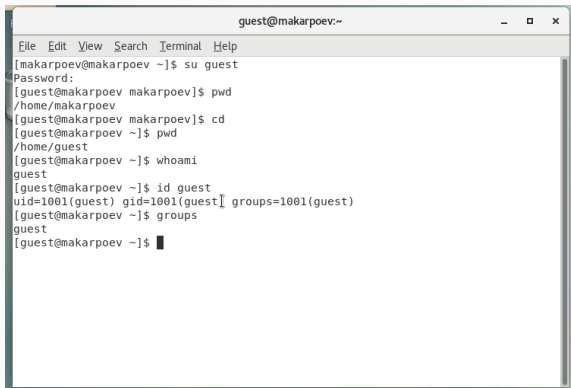
Цели и задачи работы

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

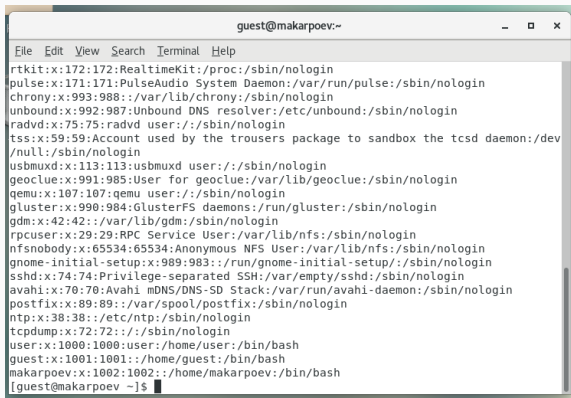
Определяем UID и группу



```
guest@makarpoev:~  
File Edit View Search Terminal Help  
[makarpoev@makarpoev ~]$ su guest  
Password:  
[guest@makarpoev makarpoev]$ pwd  
/home/makarpoev  
[guest@makarpoev makarpoev]$ cd  
[guest@makarpoev ~]$ pwd  
/home/guest  
[guest@makarpoev ~]$ whoami  
guest  
[guest@makarpoev ~]$ id guest  
uid=1001(guest) gid=1001(guest) groups=1001(guest)  
[guest@makarpoev ~]$ groups  
guest  
[guest@makarpoev ~]$
```

Figure 1: Информация о пользователе guest

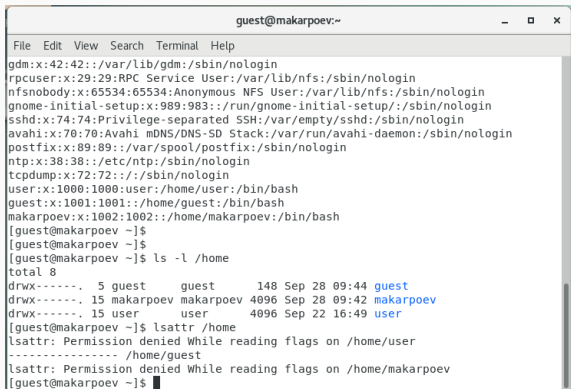
Файл с данными о пользователях

A terminal window titled 'guest@makarpoev:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal displays the output of the 'cat /etc/passwd' command, listing system users and regular users. The output is as follows:

```
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
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/null:/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
user:x:1000:1000:user:/home/user:/bin/bash
guest:x:1001:1001:./home/guest:/bin/bash
makarpoev:x:1002:1002:./home/makarpoev:/bin/bash
[guest@makarpoev ~]$
```

Figure 2: Содержимое файла /etc/passwd

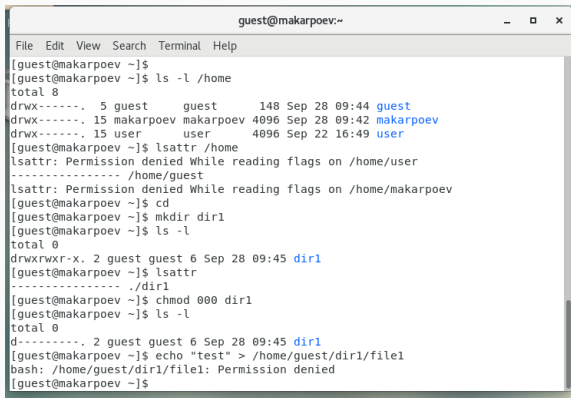
Доступ к домашним директориям



```
guest@makarpoev:~  
File Edit View Search Terminal Help  
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  
user:x:1000:1000:user:/home/user:/bin/bash  
guest:x:1001:1001:./home/guest:/bin/bash  
makarpoev:x:1002:1002:./home/makarpoev:/bin/bash  
[guest@makarpoev ~]$  
[guest@makarpoev ~]$  
[guest@makarpoev ~]$ ls -l /home  
total 8  
drwx-----, 5 guest      guest      148 Sep 28 09:44 guest  
drwx-----, 15 makarpoev makarpoev 4096 Sep 28 09:42 makarpoev  
drwx-----, 15 user       user       4096 Sep 22 16:49 user  
[guest@makarpoev ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/user  
----- /home/guest  
lsattr: Permission denied While reading flags on /home/makarpoev  
[guest@makarpoev ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@makarpoev:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows a series of commands and outputs to remove attributes from the /home directory. It starts with 'ls -l /home' showing three entries: 'guest', 'makarpoev', and 'user'. Then 'lsattr /home' is run, resulting in 'Permission denied' for /home/user and /home/guest, and 'Permission denied While reading flags on /home/makarpoev'. Next, 'cd' is used to move to /home, followed by 'mkdir dir1'. Then 'ls -l' shows 'dir1' with attributes 'drwxrwxr-x'. 'lsattr' shows '----- ./dir1'. Finally, 'chmod 000 dir1' is run, and a second 'ls -l' shows 'dir1' with attributes 'd-----'. An attempt to create a file in the directory with 'echo "test" > /home/guest/dir1/file1' fails with 'Permission denied'.

```
guest@makarpoev:~  
File Edit View Search Terminal Help  
[guest@makarpoev ~]$  
[guest@makarpoev ~]$ ls -l /home  
total 8  
drwx-----. 5 guest      guest      148 Sep 28 09:44 guest  
drwx-----. 15 makarpoev makarpoev 4096 Sep 28 09:42 makarpoev  
drwx-----. 15 user       user       4096 Sep 22 16:49 user  
[guest@makarpoev ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/user  
----- /home/guest  
lsattr: Permission denied While reading flags on /home/makarpoev  
[guest@makarpoev ~]$ cd  
[guest@makarpoev ~]$ mkdir dir1  
[guest@makarpoev ~]$ ls -l  
total 0  
drwxrwxr-x. 2 guest guest 6 Sep 28 09:45 dir1  
[guest@makarpoev ~]$ lsattr  
----- ./dir1  
[guest@makarpoev ~]$ chmod 000 dir1  
[guest@makarpoev ~]$ ls -l  
total 0  
d-----. 2 guest guest 6 Sep 28 09:45 dir1  
[guest@makarpoev ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@makarpoev ~]$
```

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.