

Дискреционное разграничение прав в Linux. Основные атрибуты

Кондратьева Анастасия Алексеевна НФИбд-01-18¹

28 сентября, 2021, Москва, Россия

¹Российский Университет Дружбы Народов

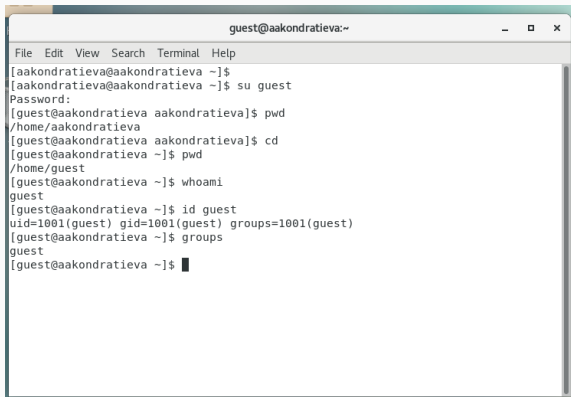
Цели и задачи работы

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

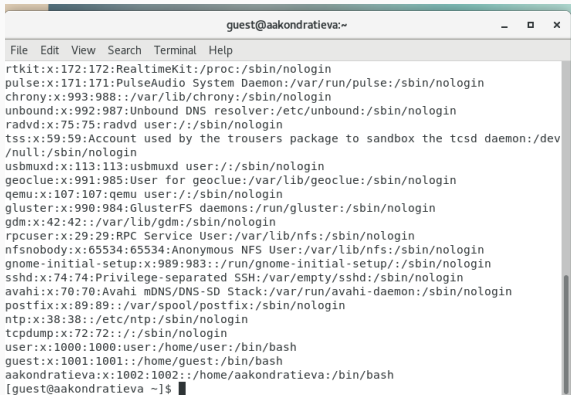
Определяем UID и группу

A terminal window titled 'guest@aakondratieva:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows a sequence of commands and their outputs: switching to the 'guest' user, displaying the password, changing to the '/home/guest' directory, and running 'id guest' and 'groups' to show user details.

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

Figure 1: Информация о пользователе guest

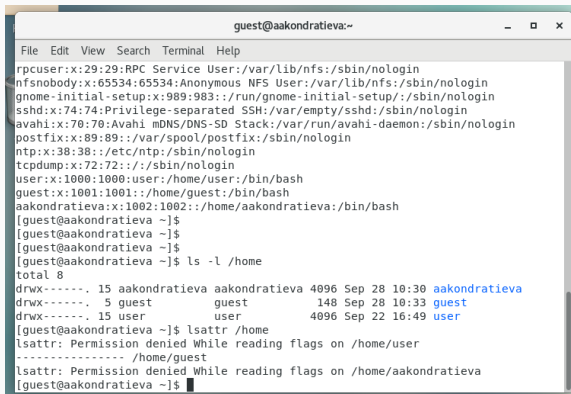
Файл с данными о пользователях

A screenshot of a terminal window titled 'guest@aakondratieva:~'. The terminal displays the output of a command that lists the contents of the /etc/passwd file. The output shows system users like rtkit, pulse, chrony, unbound, radvd, tss, usbmuxd, geoclue, qemu, gluster, gdm, rpcuser, nfsnobody, and regular users like gnome-initial-setup, sshd, avahi, postfix, ntp, tcpdump, user, guest, and aakondratieva, each with their respective UID, GID, name, and shell path.

```
guest@aakondratieva:~  
File Edit View Search Terminal Help  
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  
aakondratieva:x:1002:1002:./home/aakondratieva:/bin/bash  
[guest@aakondratieva ~]$
```

Figure 2: Содержимое файла /etc/passwd

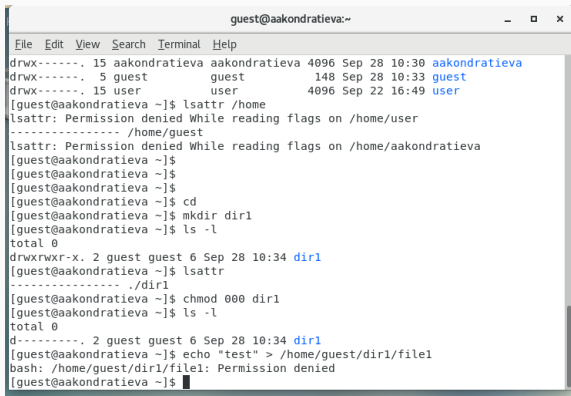
Доступ к домашним директориям



```
guest@aakondratieva:~  
File Edit View Search Terminal Help  
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  
aakondratieva:x:1002:1002:./home/aakondratieva:/bin/bash  
[guest@aakondratieva ~]$  
[guest@aakondratieva ~]$  
[guest@aakondratieva ~]$  
[guest@aakondratieva ~]$ ls -l /home  
total 8  
drwx-----. 15 aakondratieva aakondratieva 4096 Sep 28 10:30 aakondratieva  
drwx-----. 5 guest guest 148 Sep 28 10:33 guest  
drwx-----. 15 user user 4096 Sep 22 16:49 user  
[guest@aakondratieva ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/user  
----- /home/guest  
lsattr: Permission denied While reading flags on /home/aakondratieva  
[guest@aakondratieva ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@aakondratieva:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the execution of 'lsattr' on '/home' and '/home/guest', both resulting in 'Permission denied'. Then, a directory 'dir1' is created and its attributes are removed with 'chmod 000 dir1'. Finally, an attempt to create a file in 'dir1' is shown, also resulting in 'Permission denied'.

```
guest@aakondratieva:~  
File Edit View Search Terminal Help  
drwx-----, 15 aakondratieva aakondratieva 4096 Sep 28 10:30 aakondratieva  
drwx-----, 5 guest guest 148 Sep 28 10:33 guest  
drwx-----, 15 user user 4096 Sep 22 16:49 user  
[guest@aakondratieva ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/user  
----- /home/guest  
lsattr: Permission denied While reading flags on /home/aakondratieva  
[guest@aakondratieva ~]$  
[guest@aakondratieva ~]$  
[guest@aakondratieva ~]$  
[guest@aakondratieva ~]$ cd  
[guest@aakondratieva ~]$ mkdir dir1  
[guest@aakondratieva ~]$ ls -l  
total 0  
drwxrwxr-x. 2 guest guest 6 Sep 28 10:34 dir1  
[guest@aakondratieva ~]$ lsattr  
----- ./dir1  
[guest@aakondratieva ~]$ chmod 000 dir1  
[guest@aakondratieva ~]$ ls -l  
total 0  
d-----, 2 guest guest 6 Sep 28 10:34 dir1  
[guest@aakondratieva ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@aakondratieva ~]$
```

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.