

Дискреционное разграничение прав в Linux. Основные атрибуты

Радойичич Милица НФИбд-03-18¹

28 сентября, 2021, Москва, Россия

¹Российский Университет Дружбы Народов

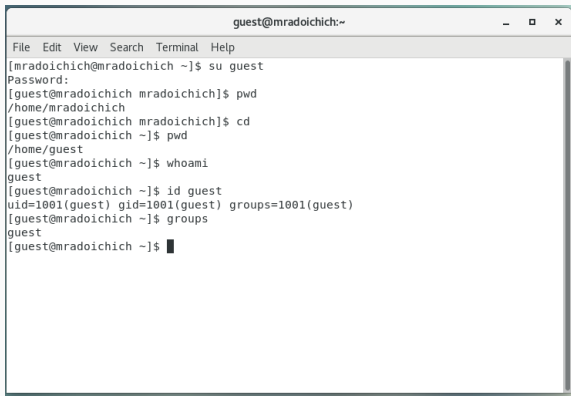
Цели и задачи работы

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

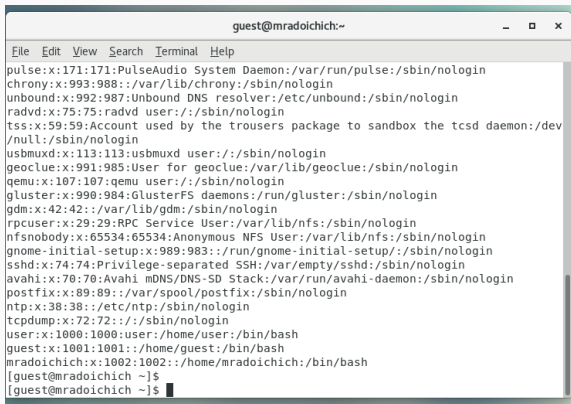
Определяем UID и группу

A terminal window titled 'guest@mradoichich:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows a sequence of commands and their outputs: 'su guest' prompts for a password; 'pwd' shows '/home/mradoichich'; 'cd' changes to '/home/guest'; 'whoami' returns 'guest'; 'id guest' returns 'uid=1001(guest) gid=1001(guest) groups=1001(guest)'; and 'groups' returns 'guest'.

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

Figure 1: Информация о пользователе guest

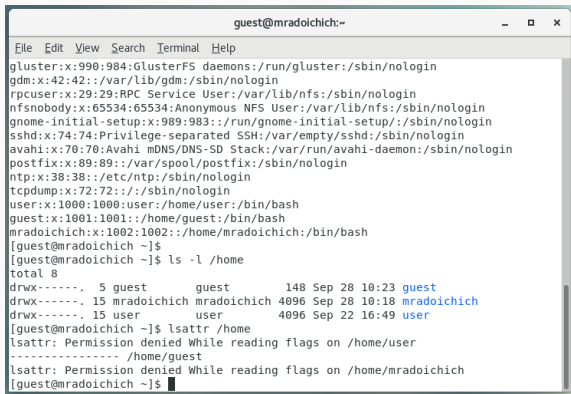
Файл с данными о пользователях

A terminal window titled 'guest@mradoichich:~' with standard window controls. The terminal displays the output of a command that lists the contents of the /etc/passwd file. The output shows system users like pulse, chrony, unbound, radvd, tss, usbmuxd, geoclue, qemu, gluster, gdm, rpcuser, nfsnobody, gnome-initial-setup, sshd, avahi, postfix, ntp, tcpdump, and regular users like user, guest, mradoichich, and their respective home directories and shells. The prompt changes from [guest@mradoichich ~]\$ to [guest@mradoichich ~]\$ after the command is executed.

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

Figure 2: Содержимое файла /etc/passwd

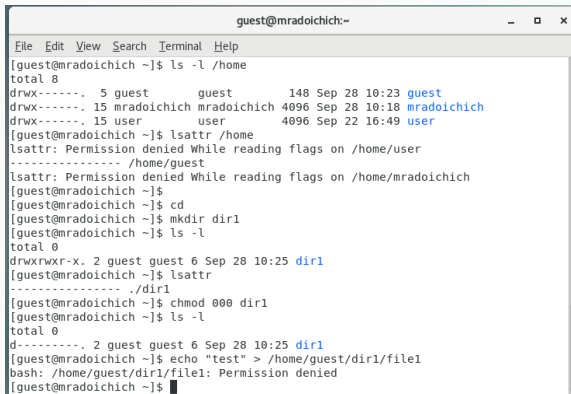
Доступ к домашним директориям



```
guest@mradoichich:~  
File Edit View Search Terminal Help  
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  
mradoichich:x:1002:1002::/home/mradoichich:/bin/bash  
[guest@mradoichich ~]$  
[guest@mradoichich ~]$ ls -l /home  
total 8  
drwx-----. 5 guest      guest      148 Sep 28 10:23 guest  
drwx-----. 15 mradoichich mradoichich 4096 Sep 28 10:18 mradoichich  
drwx-----. 15 user       user       4096 Sep 22 16:49 user  
[guest@mradoichich ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/user  
-----  
/home/guest  
lsattr: Permission denied While reading flags on /home/mradoichich  
[guest@mradoichich ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@mradoichich:~' with standard window controls. The terminal shows a series of commands and their outputs. It starts with 'ls -l /home' showing permissions for 'guest', 'mradoichich', and 'user' directories. Then 'lsattr /home' is run, showing 'Permission denied' for both '/home/user' and '/home/mradoichich'. Next, a directory 'dir1' is created with 'mkdir dir1'. Then 'ls -l' shows 'dir1' with permissions 'drwxrwxr-x'. Finally, 'lsattr' is run on 'dir1', showing 'Permission denied' for 'dir1'. The prompt returns to the user.

```
guest@mradoichich:~  
File Edit View Search Terminal Help  
[guest@mradoichich ~]$ ls -l /home  
total 8  
drwx-----. 5 guest      guest      148 Sep 28 10:23 guest  
drwx-----. 15 mradoichich mradoichich 4096 Sep 28 10:18 mradoichich  
drwx-----. 15 user        user        4096 Sep 22 16:49 user  
[guest@mradoichich ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/user  
----- /home/guest  
lsattr: Permission denied While reading flags on /home/mradoichich  
[guest@mradoichich ~]$  
[guest@mradoichich ~]$ cd  
[guest@mradoichich ~]$ mkdir dir1  
[guest@mradoichich ~]$ ls -l  
total 0  
drwxrwxr-x. 2 guest guest 6 Sep 28 10:25 dir1  
[guest@mradoichich ~]$ lsattr  
----- ./dir1  
[guest@mradoichich ~]$ chmod 000 dir1  
[guest@mradoichich ~]$ ls -l  
total 0  
d-----.. 2 guest guest 6 Sep 28 10:25 dir1  
[guest@mradoichich ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@mradoichich ~]$
```

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.