

Дискреционное разграничение прав в Linux. Основные атрибуты

Шаян Фаисал НФИбд-02-19¹

15 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

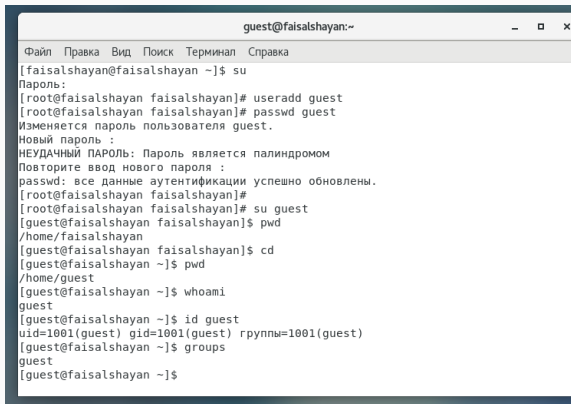
Цели и задачи работы

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

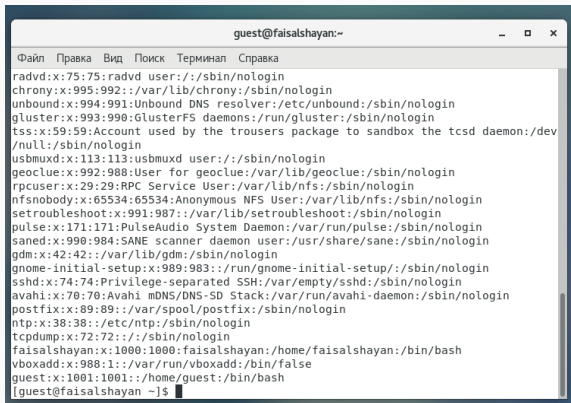
Определяем UID и группу



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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях



The image shows a terminal window titled "guest@faisalshayan:~". The terminal displays the output of a command that lists the contents of the /etc/passwd file. The output shows a list of system users and regular users, each with their username, UID, GID, and shell path. The users listed are: radvd, chrony, unbound, gluster, tss, usbmuxd, geoclue, rpcuser, nfsnobody, setroubleshoot, pulse, saned, gdm, gnome-initial-setup, sshd, avahi, postfix, ntp, tcpdump, faisalshayan, vboxadd, and guest. The terminal window has a menu bar with options: Файл, Правка, Вид, Поиск, Терминал, Справка.

```
guest@faisalshayan:~  
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  
saned: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  
faisalshayan:x:1000:1000:faisalshayan:/home/faisalshayan:/bin/bash  
vboxadd:x:988:1:./var/run/vboxadd:/bin/false  
guest:x:1001:1001:./home/guest:/bin/bash  
[guest@faisalshayan ~]$
```

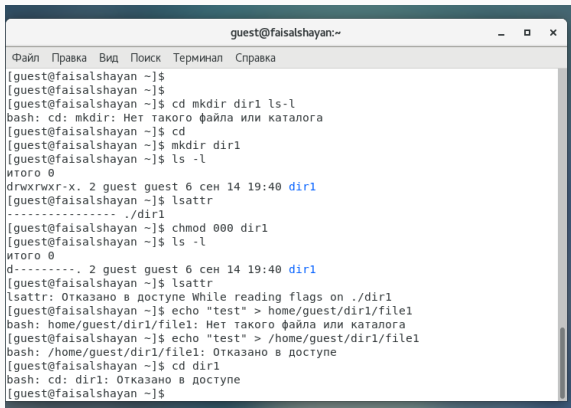
Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@faisalshayan ~]$  
[guest@faisalshayan ~]$  
[guest@faisalshayan ~]$ ls -l /home  
итого 4  
drwx-----. 20 faisalshayan faisalshayan 4096 сен 14 19:38 faisalshayan  
drwx-----. 5 guest guest 107 сен 14 19:39 guest  
[guest@faisalshayan ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/faisalshayan  
----- /home/guest  
[guest@faisalshayan ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@faisalshayan:~' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows a sequence of commands to create a directory, set permissions, and remove its attributes. The output shows the directory 'dir1' with permissions 'drwxrwxr-x' and ownership '2 guest guest 6 сен 14 19:40'. After running 'lsattr', it shows '----- ./dir1'. After 'chmod 000 dir1', it shows 'd----- 2 guest guest 6 сен 14 19:40 dir1'. Finally, after 'lsattr', it shows 'lsattr: Отказано в доступе While reading flags on ./dir1'. Subsequent attempts to create files in 'dir1' fail with 'bash: /home/guest/dir1/file1: Нет такого файла или каталога' and 'bash: /home/guest/dir1/file1: Отказано в доступе'.

```
guest@faisalshayan ~]$  
[guest@faisalshayan ~]$  
[guest@faisalshayan ~]$ cd mkdir dir1 ls-l  
bash: cd: mkdir: Нет такого файла или каталога  
[guest@faisalshayan ~]$ cd  
[guest@faisalshayan ~]$ mkdir dir1  
[guest@faisalshayan ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 14 19:40 dir1  
[guest@faisalshayan ~]$ lsattr  
----- ./dir1  
[guest@faisalshayan ~]$ chmod 000 dir1  
[guest@faisalshayan ~]$ ls -l  
итого 0  
d----- 2 guest guest 6 сен 14 19:40 dir1  
[guest@faisalshayan ~]$ lsattr  
lsattr: Отказано в доступе While reading flags on ./dir1  
[guest@faisalshayan ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Нет такого файла или каталога  
[guest@faisalshayan ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@faisalshayan ~]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@faisalshayan ~]$
```

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.