

Дискреционное разграничение прав в Linux. Основные атрибуты

Волков Фрол Сергеевич НПИбд-01-19¹

16 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

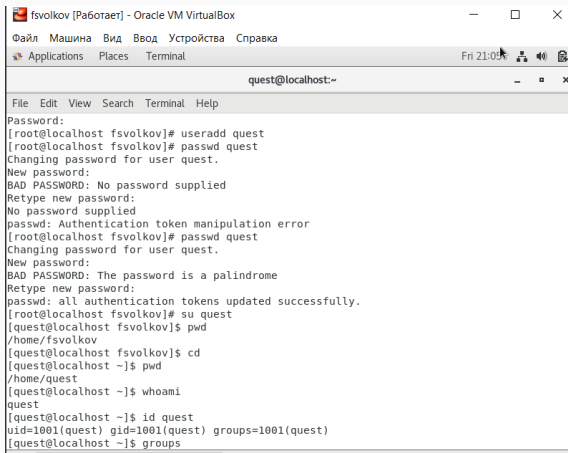
Цели и задачи работы

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

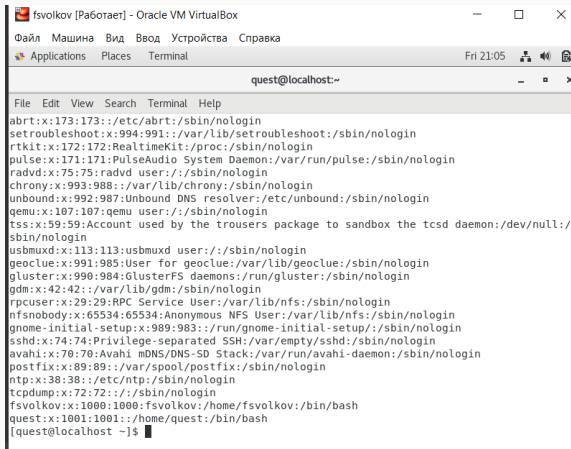
Определяем UID и группу



```
fsvolkov [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Places Terminal
quest@localhost:~
File Edit View Search Terminal Help
Password:
[root@localhost fsvolkov]# useradd quest
[root@localhost fsvolkov]# passwd quest
Changing password for user quest.
New password:
BAD PASSWORD: No password supplied
Retype new password:
No password supplied
passwd: Authentication token manipulation error
[root@localhost fsvolkov]# passwd quest
Changing password for user quest.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost fsvolkov]# su quest
[quest@localhost fsvolkov]$ pwd
/home/fsvolkov
[quest@localhost fsvolkov]$ cd
[quest@localhost ~]$ pwd
/home/quest
[quest@localhost ~]$ whoami
quest
[quest@localhost ~]$ id quest
uid=1001(quest) gid=1001(quest) groups=1001(quest)
[quest@localhost ~]$ groups
```

Figure 1: Информация о пользователе quest

Файл с данными о пользователях



The screenshot shows a terminal window titled "fsvolkov [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar is a toolbar with icons for "Applications", "Places", and "Terminal". The terminal prompt is "quest@localhost:~". The terminal content displays the output of the "cat /etc/passwd" command, listing system users and regular users with their home directories and shells.

```
File Edit View Search Terminal Help
abrt:x:173:173::/etc/abrt:/sbin/nologin
setroubleshoot:x:994:991::/var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
chrony:x:993:988::/var/lib/chrony:/sbin/nologin
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:107:107:qemu 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
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
fsvolkov:x:1000:1000:fsvolkov:/home/fsvolkov:/bin/bash
quest:x:1001:1001:/home/quest:/bin/bash
[quest@localhost ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[quest@localhost ~]$ ls -l /home/
total 4
drwx-----. 15 fsvolkov fsvolkov 4096 Sep 16 21:01 fsvolkov
drwx-----.  5 quest    quest   107 Sep 16 21:03 quest
[quest@localhost ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/fsvolkov
----- /home/quest
[quest@localhost ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[quest@localhost ~]$ cd
[quest@localhost ~]$ mkdir dir1
[quest@localhost ~]$ ls -l
total 0
drwxrwxr-x. 2 quest quest 6 Sep 16 21:08 dir1
[quest@localhost ~]$ lsattr
----- ./dir1
[quest@localhost ~]$ chmod 000 dir1
[quest@localhost ~]$ ls -l
total 0
d----- . 2 quest quest 6 Sep 16 21:08 dir1
[quest@localhost ~]$ echo "test" > /home/quest/dir1/file1
bash: /home/quest/dir1/file1: Permission denied
[quest@localhost ~]$ ls -l /home/quest/dir1
ls: invalid option -- '/'
Try 'ls --help' for more information.
[quest@localhost ~]$ ls -l /home/quest/dir1
ls: cannot open directory /home/quest/dir1: Permission denied
[quest@localhost ~]$ chmod 300 dir1
[quest@localhost ~]$
```

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.