

Дискреционное разграничение прав в Linux. Основные атрибуты

Ярметов Камран НФИбд-01-18¹

15 февраля, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

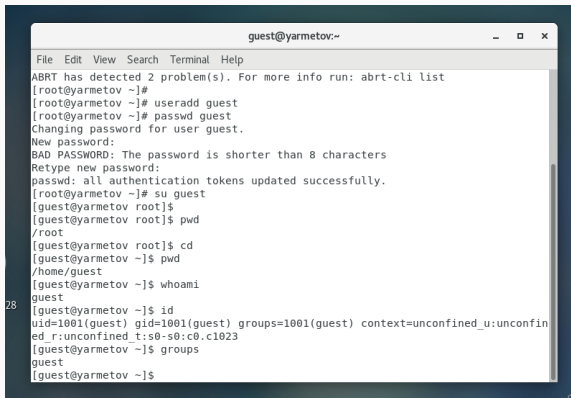
Цели и задачи работы

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

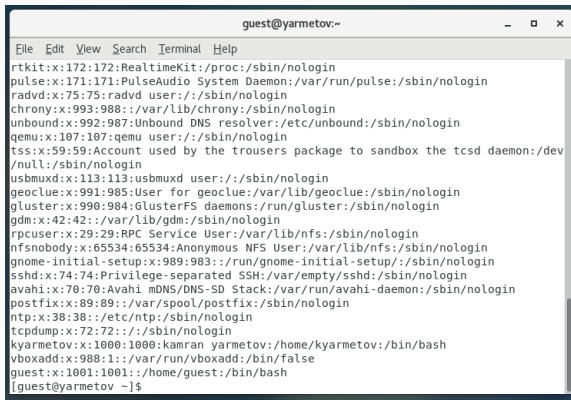


A terminal window titled 'guest@yarmetov:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
ABRT has detected 2 problem(s). For more info run: abrt-cli list
[root@yarmetov ~]#
[root@yarmetov ~]# useradd guest
[root@yarmetov ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@yarmetov ~]# su guest
[guest@yarmetov root]$
[guest@yarmetov root]$ pwd
/root
[guest@yarmetov root]$ cd
[guest@yarmetov ~]$ pwd
/home/guest
[guest@yarmetov ~]$ whoami
guest
[guest@yarmetov ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@yarmetov ~]$ groups
guest
[guest@yarmetov ~]$
```

Figure 1: Информация о пользователе guest

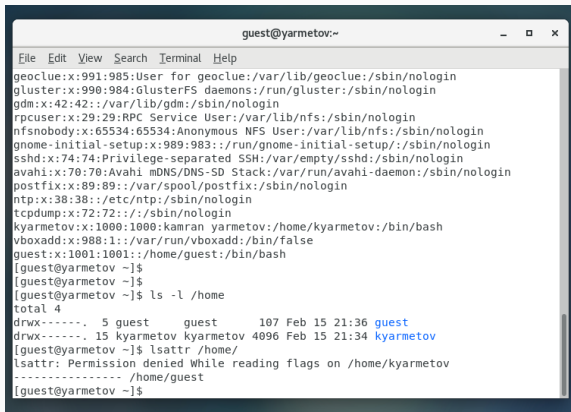
Файл с данными о пользователях



```
guest@yarmetov:~  
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  
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  
kyarmetov:x:1000:1000:kamran yarmetov:/home/kyarmetov:/bin/bash  
vboxadd:x:988:1:/var/run/vboxadd:/bin/false  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@yarmetov ~]$
```

Figure 2: Содержимое файла /etc/passwd

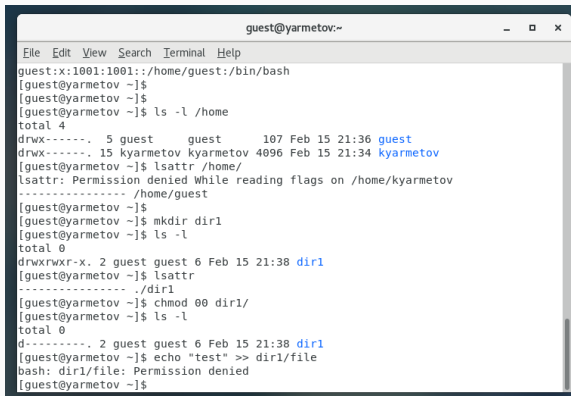
Доступ к домашним директориям



```
guest@yarmetov:~  
File Edit View Search Terminal Help  
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  
kyarmetov:x:1000:1000:kamran yarmetov:/home/kyarmetov:/bin/bash  
vboxadd:x:988:1::/var/run/vboxadd:/bin/false  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@yarmetov ~]$  
[guest@yarmetov ~]$  
[guest@yarmetov ~]$ ls -l /home  
total 4  
drwx-----. 5 guest guest 107 Feb 15 21:36 guest  
drwx-----. 15 kyarmetov kyarmetov 4096 Feb 15 21:34 kyarmetov  
[guest@yarmetov ~]$ lsattr /home/  
lsattr: Permission denied While reading flags on /home/kyarmetov  
----- /home/guest  
[guest@yarmetov ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@yarmetov:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows a user 'guest' with ID 'x:1001:1001' in the '/home/guest' directory. The user runs 'ls -l /home', showing a directory 'guest' with permissions 'drwx-----'. Then, the user runs 'lsattr /home/' and receives a 'Permission denied' message. Next, the user runs 'mkdir dir1' and 'ls -l', showing the new directory 'dir1' with permissions 'drwxrwxr-x'. Finally, the user runs 'chmod 000 dir1/' and 'ls -l', showing 'dir1' with permissions 'd-----'. The last command shown is 'echo "test" >> dir1/file', which also results in a 'Permission denied' message.

```
guest@yarmetov:~  
File Edit View Search Terminal Help  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@yarmetov ~]$  
[guest@yarmetov ~]$  
[guest@yarmetov ~]$ ls -l /home  
total 4  
drwx-----. 5 guest      guest      107 Feb 15 21:36 guest  
drwx-----. 15 kyarmetov kyarmetov 4096 Feb 15 21:34 kyarmetov  
[guest@yarmetov ~]$ lsattr /home/  
lsattr: Permission denied While reading flags on /home/kyarmetov  
----- /home/guest  
[guest@yarmetov ~]$  
[guest@yarmetov ~]$ mkdir dir1  
[guest@yarmetov ~]$ ls -l  
total 0  
drwxrwxr-x. 2 guest guest 6 Feb 15 21:38 dir1  
[guest@yarmetov ~]$ lsattr  
----- ./dir1  
[guest@yarmetov ~]$ chmod 000 dir1/  
[guest@yarmetov ~]$ ls -l  
total 0  
d-----.. 2 guest guest 6 Feb 15 21:38 dir1  
[guest@yarmetov ~]$ echo "test" >> dir1/file  
bash: dir1/file: Permission denied  
[guest@yarmetov ~]$
```

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.