

Дискреционное разграничение прав в Linux. Основные атрибуты

Солодовников Игорь НБИ-01-19¹

13 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

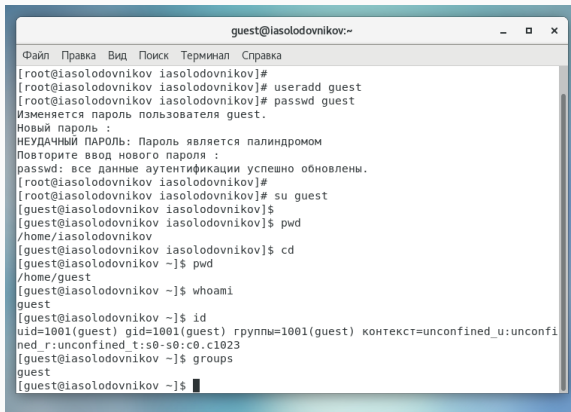
Цели и задачи работы

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

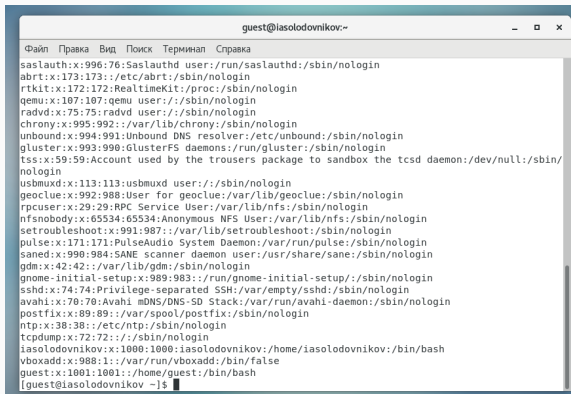
Определяем UID и группу



```
guest@iasolodovnikov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iasolodovnikov iasolodovnikov]#  
[root@iasolodovnikov iasolodovnikov]# useradd guest  
[root@iasolodovnikov iasolodovnikov]# passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[root@iasolodovnikov iasolodovnikov]#  
[root@iasolodovnikov iasolodovnikov]# su guest  
[guest@iasolodovnikov iasolodovnikov]$  
[guest@iasolodovnikov iasolodovnikov]$ pwd  
/home/iasolodovnikov  
[guest@iasolodovnikov iasolodovnikov]$ cd  
[guest@iasolodovnikov ~]$ pwd  
/home/guest  
[guest@iasolodovnikov ~]$ whoami  
guest  
[guest@iasolodovnikov ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@iasolodovnikov ~]$ groups  
guest  
[guest@iasolodovnikov ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях



```
guest@iasolodovnikov:~  
Файл Правка Вид Поиск Терминал Справка  
saslauthd:x:996:76:Saslauthd user:/run/saslauthd:/sbin/nologin  
abrt:x:173:173:./etc/abrt:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
qemu:x:107:107:qemu user:/:/sbin/nologin  
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  
iasolodovnikov:x:1000:1000:iasolodovnikov:/home/iasolodovnikov:/bin/bash  
vboxadd:x:988:1:./var/run/vboxadd:/bin/false  
guest:x:1001:1001:./home/guest:/bin/bash  
[guest@iasolodovnikov ~]$
```

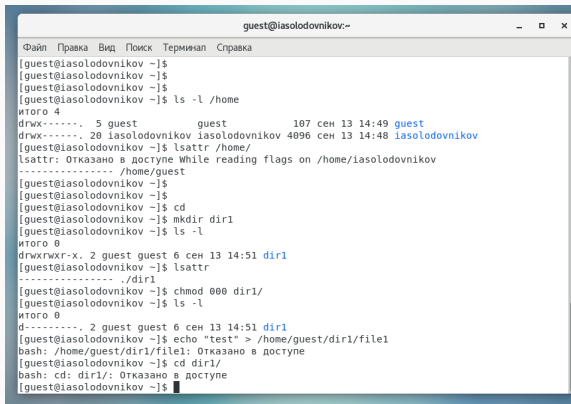
Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@iasolodovnikov ~]$  
[guest@iasolodovnikov ~]$  
[guest@iasolodovnikov ~]$  
[guest@iasolodovnikov ~]$ ls -l /home  
итого 4  
drwx-----. 5 guest      guest      107 сен 13 14:49 guest  
drwx-----. 20 iasolodovnikov iasolodovnikov 4096 сен 13 14:48 iasolodovnikov  
[guest@iasolodovnikov ~]$ lsattr /home/  
lsattr: Отказано в доступе While reading flags on /home/iasolodovnikov  
----- /home/guest  
[guest@iasolodovnikov ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@iasolodovnikov:~' with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal shows a sequence of commands and outputs to remove attributes from the /home directory. It starts with 'ls -l /home' showing permissions 'drwx-----' for guest. Then 'lsattr /home/' shows 'lsattr: Отказано в доступе While reading flags on /home/iasolodovnikov'. Then 'cd /home/guest' and 'ls -l' shows 'drwxrwxr-x' for guest. Then 'chmod 000 dir1/' and 'ls -l' shows 'd-----' for guest. Finally, 'echo "test" > /home/guest/dir1/file1' results in 'bash: /home/guest/dir1/file1: Отказано в доступе'.

```
guest@iasolodovnikov:~  
[guest@iasolodovnikov ~]$  
[guest@iasolodovnikov ~]$  
[guest@iasolodovnikov ~]$  
[guest@iasolodovnikov ~]$ ls -l /home  
итого 4  
drwx-----. 5 guest          guest          107 сен 13 14:49 guest  
drwx-----. 20 iasolodovnikov iasolodovnikov 4096 сен 13 14:48 iasolodovnikov  
[guest@iasolodovnikov ~]$ lsattr /home/  
lsattr: Отказано в доступе While reading flags on /home/iasolodovnikov  
----- /home/guest  
[guest@iasolodovnikov ~]$  
[guest@iasolodovnikov ~]$  
[guest@iasolodovnikov ~]$ cd  
[guest@iasolodovnikov ~]$ mkdir dir1  
[guest@iasolodovnikov ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 13 14:51 dir1  
[guest@iasolodovnikov ~]$ lsattr  
----- ./dir1  
[guest@iasolodovnikov ~]$ chmod 000 dir1/  
[guest@iasolodovnikov ~]$ ls -l  
итого 0  
d-----. 2 guest guest 6 сен 13 14:51 dir1  
[guest@iasolodovnikov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@iasolodovnikov ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@iasolodovnikov ~]$
```

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.