

Дискреционное разграничение прав в Linux. Основные атрибуты

Рябцева Маргарита Михайловна НБИ-01-19¹

12 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

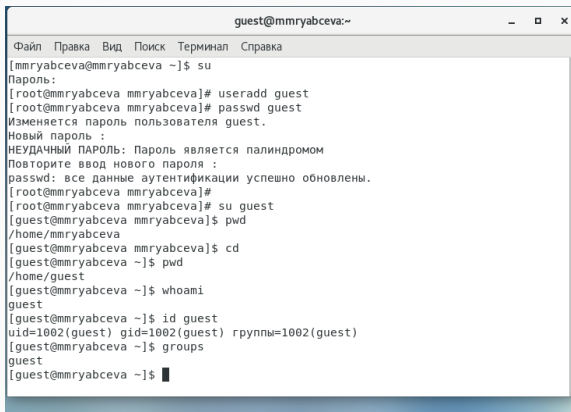
Цели и задачи работы

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

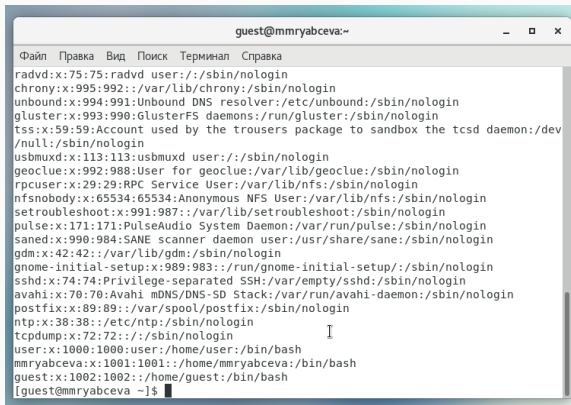
Определяем UID и группу



```
guest@mmryabceva:~  
Файл Правка Вид Поиск Терминал Справка  
[mmryabceva@mmryabceva ~]$ su  
Пароль:  
[root@mmryabceva mmryabceva]# useradd guest  
[root@mmryabceva mmryabceva]# passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[root@mmryabceva mmryabceva]#  
[root@mmryabceva mmryabceva]# su guest  
[guest@mmryabceva mmryabceva]$ pwd  
/home/mmryabceva  
[guest@mmryabceva mmryabceva]$ cd  
[guest@mmryabceva ~]$ pwd  
/home/guest  
[guest@mmryabceva ~]$ whoami  
guest  
[guest@mmryabceva ~]$ id guest  
uid=1002(guest) gid=1002(guest) группы=1002(guest)  
[guest@mmryabceva ~]$ groups  
guest  
[guest@mmryabceva ~]$ █
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях



```
guest@mmryabceva:~  
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  
user:x:1000:1000:user:/home/user:/bin/bash  
mmryabceva:x:1001:1001::/home/mmryabceva:/bin/bash  
guest:x:1002:1002::/home/guest:/bin/bash  
[guest@mmryabceva ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@mmryabceva ~]$  
[guest@mmryabceva ~]$ ls -l /home  
итого 8  
drwx-----.  5 guest      guest      107 сен 12 14:01 guest  
drwx-----. 15 mmryabceva mmryabceva 4096 сен 12 14:01 mmryabceva  
drwx-----. 15 user       user       4096 сен 12 11:31 user  
[guest@mmryabceva ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/user  
lsattr: Отказано в доступе While reading flags on /home/mmryabceva  
----- /home/guest  
[guest@mmryabceva ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@mmryabceva ~]$  
[guest@mmryabceva ~]$  
[guest@mmryabceva ~]$ cd  
[guest@mmryabceva ~]$ mkdir dir1  
[guest@mmryabceva ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 12 14:02 dir1  
[guest@mmryabceva ~]$ lsattr  
----- ./dir1  
[guest@mmryabceva ~]$ chmod 000 dir1  
[guest@mmryabceva ~]$ ls -l  
итого 0  
d-----. 2 guest guest 6 сен 12 14:02 dir1  
[guest@mmryabceva ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@mmryabceva ~]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@mmryabceva ~]$
```

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.