

Дискреционное разграничение прав в Linux. Основные атрибуты

Никулин Максим НПИбд-01-19 ¹

17 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

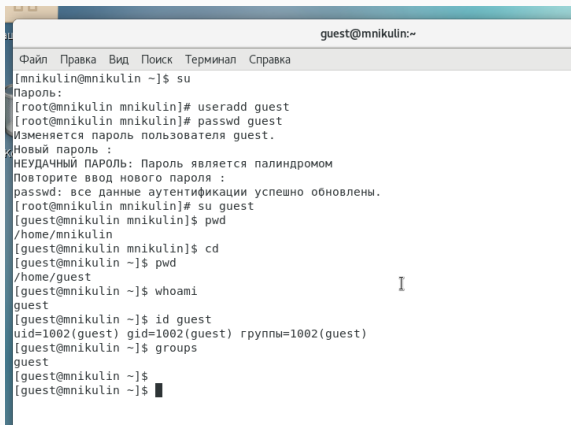
Цели и задачи работы

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

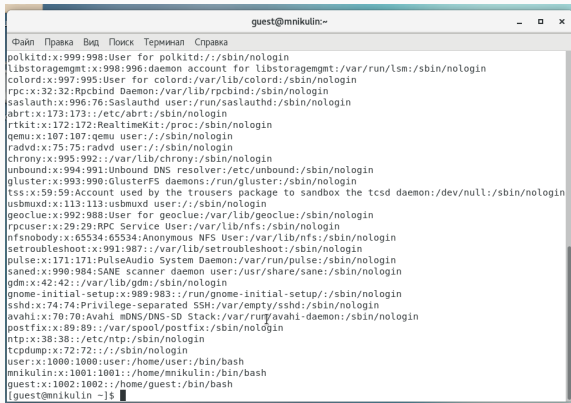
Определяем UID и группу



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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A screenshot of a terminal window titled 'guest@mnikulin:~'. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal displays the output of the 'cat /etc/passwd' command, showing a list of system and regular users. Each line represents a user entry in the format 'username:x:uid:gid:gecos:home:shell'. The users listed include polkitd, libstoragemgmt, colord, rpcbind, saslauthd, abrt, rtkit, qemu, radvd, chrony, unbound, gluster, tss, usbmuxd, geoclue, rpcuser, nfsnobody, setroubleshoot, pulse, saned, gdm, gnome-initial-setup, sshd, avahi, postfix, ntp, tcpdump, user, mnikulin, and guest. The prompt '[guest@mnikulin ~]\$' is visible at the bottom.

```
guest@mnikulin:~  
Файл Правка Вид Поиск Терминал Справка  
polkitd:x:999:998:User for polkitd:/:sbin/nologin  
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin  
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin  
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin  
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  
user:x:1000:1000:user:/home/user:/bin/bash  
mnikulin:x:1001:1001:./home/mnikulin:/bin/bash  
guest:x:1002:1002:./home/guest:/bin/bash  
[guest@mnikulin ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
guest:x:1002:1002::/home/guest:/bin/bash
[guest@mnikulin ~]$ ls -l /home
итого 8
drwx-----.  5 guest      guest      107 сен 17 12:25 guest
drwx-----. 15 mnikulin  mnikulin 4096 сен 17 12:23 mnikulin
drwx-----. 15 user      user      4096 сен 12 11:31 user
[guest@mnikulin ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/user
lsattr: Отказано в доступе While reading flags on /home/mnikulin
----- /home/guest
[guest@mnikulin ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@mnikulin ~]$  
[guest@mnikulin ~]$ cd  
[guest@mnikulin ~]$ mkdir dir1  
[guest@mnikulin ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 17 12:26 dir1  
[guest@mnikulin ~]$ lsattr  
----- ./dir1  
[guest@mnikulin ~]$ chmod 000 dir1  
[guest@mnikulin ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 сен 17 12:26 dir1  
[guest@mnikulin ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@mnikulin ~]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@mnikulin ~]$
```

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.