

Дискреционное разграничение прав в Linux. Основные атрибуты

Пименов Михаил НБИ-01-19¹

13 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

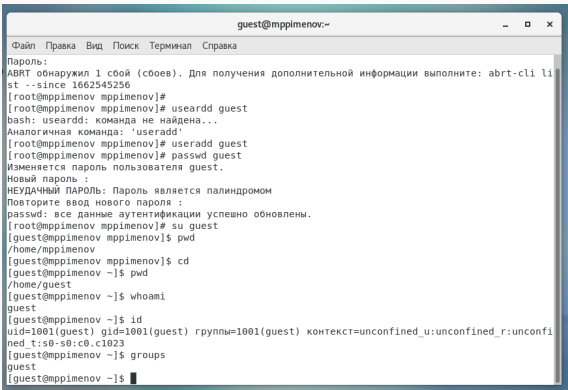
Цели и задачи работы

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

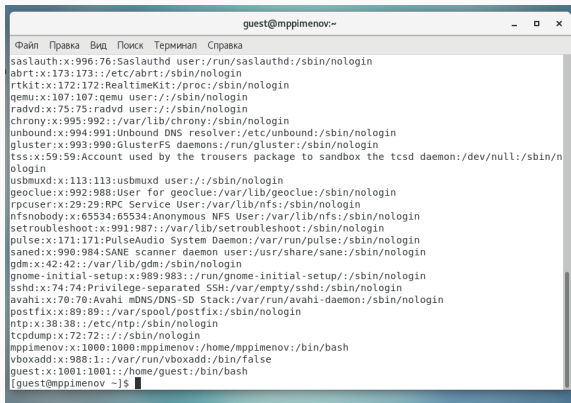
Определяем UID и группу



```
guest@mppimenov:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
Пароль:  
ABRT обнаружил 1 сбой (сбоев). Для получения дополнительной информации выполните: abrt-cli li  
st --since 1662545256  
[root@mppimenov mppimenov]#  
[root@mppimenov mppimenov]# useradd guest  
bash: useradd: команда не найдена...  
Аналогичная команда: 'useradd'  
[root@mppimenov mppimenov]# useradd guest  
[root@mppimenov mppimenov]# passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[root@mppimenov mppimenov]# su guest  
[guest@mppimenov mppimenov]$ pwd  
/home/mppimenov  
[guest@mppimenov mppimenov]$ cd  
[guest@mppimenov ~]$ pwd  
/home/guest  
[guest@mppimenov ~]$ whoami  
guest  
[guest@mppimenov ~]$ id  
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest) контекст=unconfined_u:unconfined_r:unconfi  
ned_t:s0-s0:c0.c1023  
[guest@mppimenov ~]$ groups  
guest  
[guest@mppimenov ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях



The image shows a terminal window titled "guest@mppimenov:~". 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, listing system users and regular users. The output is as follows:

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

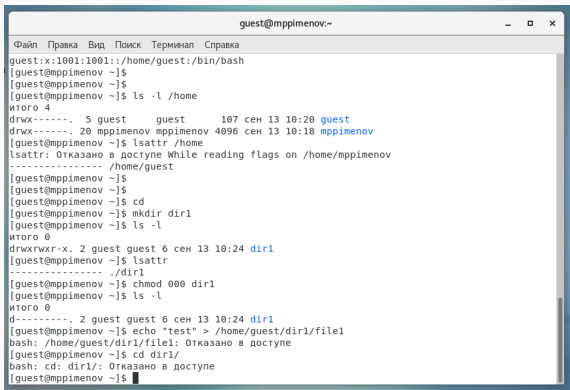
Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@mppimenov ~]$  
[guest@mppimenov ~]$ ls -l /home  
итого 4  
drwx-----. 5 guest      guest      107 сен 13 10:20 guest  
drwx-----. 20 mppimenov mppimenov 4096 сен 13 10:18 mppimenov  
[guest@mppimenov ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/mppimenov  
----- /home/guest  
[guest@mppimenov ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@mppimenov:~' with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal shows a sequence of commands and their outputs. It starts with 'guest:x:1001:1001:~/home/guest:/bin/bash', followed by 'ls -l /home' showing permissions for 'guest' and 'mppimenov'. Then 'lsattr /home' shows 'lsattr: Отказано в доступе While reading flags on /home/mppimenov'. The user then navigates to '/home/guest', creates a directory 'dir1', and attempts to remove its attributes with 'chmod 000 dir1'. The final output shows 'd-----, 2 guest guest 6 сен 13 10:24 dir1', indicating the attributes have been successfully removed.

```
guest@mppimenov:~  
Файл Правка Вид Поиск Терминал Справка  
guest:x:1001:1001:~/home/guest:/bin/bash  
[guest@mppimenov ~]$  
[guest@mppimenov ~]$  
[guest@mppimenov ~]$ ls -l /home  
итого 4  
drwx-----. 5 guest guest 107 сен 13 10:20 guest  
drwx-----. 20 mppimenov mppimenov 4096 сен 13 10:18 mppimenov  
[guest@mppimenov ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/mppimenov  
----- /home/guest  
[guest@mppimenov ~]$  
[guest@mppimenov ~]$  
[guest@mppimenov ~]$ cd  
[guest@mppimenov ~]$ mkdir dir1  
[guest@mppimenov ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 13 10:24 dir1  
[guest@mppimenov ~]$ lsattr  
----- ./dir1  
[guest@mppimenov ~]$ chmod 000 dir1  
[guest@mppimenov ~]$ ls -l  
итого 0  
d-----, 2 guest guest 6 сен 13 10:24 dir1  
[guest@mppimenov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@mppimenov ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@mppimenov ~]$
```

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.