

Дискреционное разграничение прав в Linux. Основные атрибуты

Арутюн Гиндоян 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.

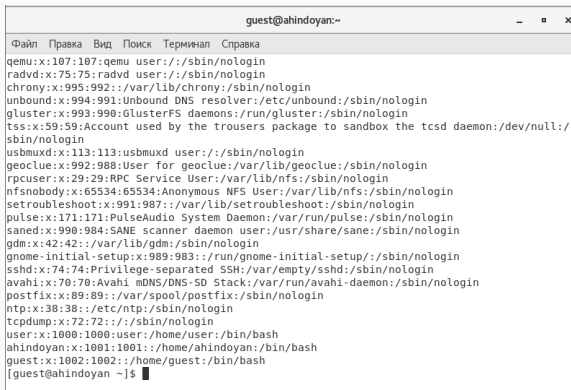
Процесс выполнения лабораторной работы

Определяем UID и группу

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

Figure 1: Информация о пользователе guest

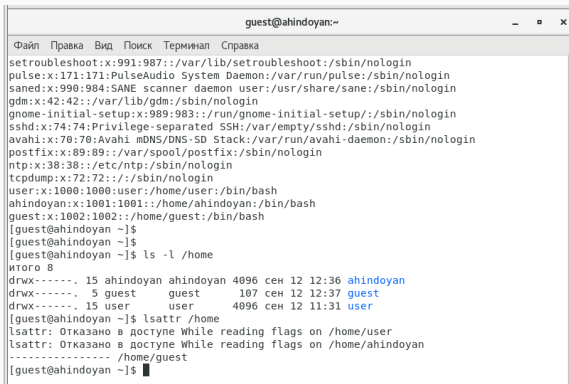
Файл с данными о пользователях



```
guest@ahindoyan:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
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  
ahindoyan:x:1001:1001:./home/ahindoyan:/bin/bash  
guest:x:1002:1002:./home/guest:/bin/bash  
[guest@ahindoyan ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

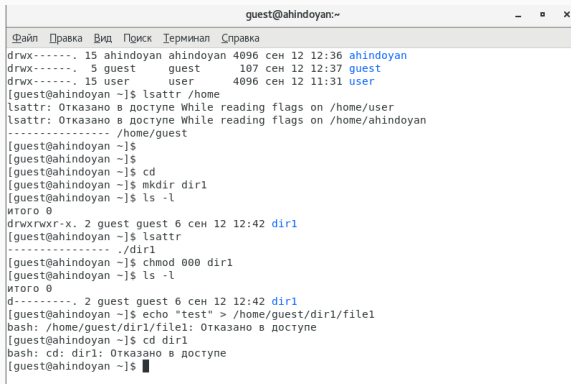


A terminal window titled 'guest@ahindoyan:~' with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal displays the following output:

```
setroubleshoot:x:991:987::/var/lib/setroubleshoot:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
sane: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
ahindoyan:x:1001:1001:/home/ahindoyan:/bin/bash
guest:x:1002:1002:/home/guest:/bin/bash
[guest@ahindoyan ~]$
[guest@ahindoyan ~]$
[guest@ahindoyan ~]$ ls -l /home
итого 8
drwx-----. 15 ahindoyan ahindoyan 4096 сен 12 12:36 ahindoyan
drwx-----.  5 guest      guest    107 сен 12 12:37 guest
drwx-----. 15 user       user     4096 сен 12 11:31 user
[guest@ahindoyan ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/user
lsattr: Отказано в доступе While reading flags on /home/ahindoyan
----- /home/guest
[guest@ahindoyan ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@ahindoyan:~' with standard window controls. It shows a series of commands and their outputs. First, 'lsattr /home' lists attributes for /home, showing 'ahindoyan' (4096), 'guest' (107), and 'user' (4096). Then, 'lsattr /home/guest' shows 'guest' (107). Next, 'cd' and 'mkdir dir1' are executed. Then, 'ls -l' shows 'dir1' with permissions 'drwxrwxr-x'. Finally, 'chmod 000 dir1' is executed, and a subsequent 'ls -l' shows 'dir1' with permissions 'd-----'.

```
guest@ahindoyan:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
drwx----- . 15 ahindoyan ahindoyan 4096 сен 12 12:36 ahindoyan  
drwx----- . 5 guest guest 107 сен 12 12:37 guest  
drwx----- . 15 user user 4096 сен 12 11:31 user  
[guest@ahindoyan ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/user  
lsattr: Отказано в доступе While reading flags on /home/ahindoyan  
----- /home/guest  
[guest@ahindoyan ~]$  
[guest@ahindoyan ~]$  
[guest@ahindoyan ~]$ cd  
[guest@ahindoyan ~]$ mkdir dir1  
[guest@ahindoyan ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 12 12:42 dir1  
[guest@ahindoyan ~]$ lsattr  
----- ./dir1  
[guest@ahindoyan ~]$ chmod 000 dir1  
[guest@ahindoyan ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 сен 12 12:42 dir1  
[guest@ahindoyan ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@ahindoyan ~]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@ahindoyan ~]$ █
```

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.