

Дискреционное разграничение прав в Linux. Основные атрибуты

Думингуш Маурисиу Жозе Себаштияу НБИ-01-19¹

14 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

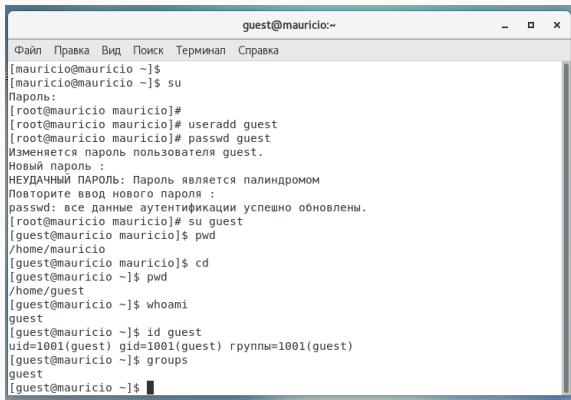
Цели и задачи работы

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

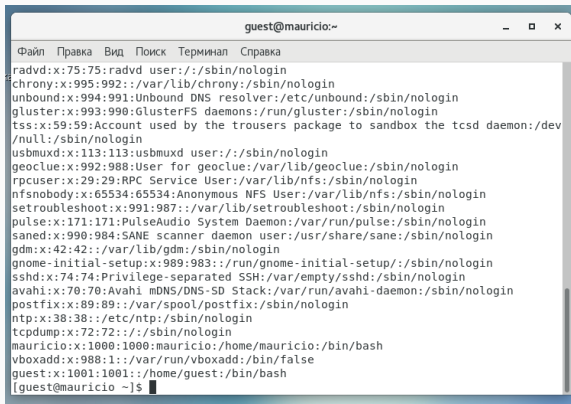
Определяем UID и группу



```
guest@mauricio:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[mauricio@mauricio ~]$  
[mauricio@mauricio ~]$ su  
Пароль:  
[root@mauricio mauricio]#  
[root@mauricio mauricio]# useradd guest  
[root@mauricio mauricio]# passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[root@mauricio mauricio]# su guest  
[guest@mauricio mauricio]$ pwd  
/home/mauricio  
[guest@mauricio mauricio]$ cd  
[guest@mauricio ~]$ pwd  
/home/guest  
[guest@mauricio ~]$ whoami  
guest  
[guest@mauricio ~]$ id guest  
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest)  
[guest@mauricio ~]$ groups  
guest  
[guest@mauricio ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях



The image shows a terminal window titled "guest@mauricio:~". The window contains the output of the command "cat /etc/passwd". The output lists system users and regular users, each with their username, UID, GID, and shell path. The system users listed are radvd, chrony, unbound, gluster, tss, usbmuxd, geoclue, rpcuser, nfsnobody, setroubleshoot, pulse, saned, gdm, gnome-initial-setup, sshd, avahi, postfix, ntp, and tcpdump. The regular users listed are mauricio, vboxadd, and guest.

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

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@mauricio ~]$  
[guest@mauricio ~]$  
[guest@mauricio ~]$ ls -l /home  
итого 4  
drwx-----. 5 guest    guest    107 сен 14 13:38 guest  
drwx-----. 20 mauricio mauricio 4096 сен 14 13:37 mauricio  
[guest@mauricio ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/mauricio  
----- /home/guest  
[guest@mauricio ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

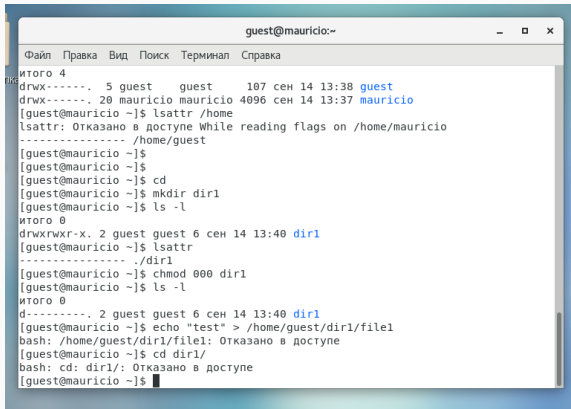
A terminal window titled 'guest@mauricio:~' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows a sequence of commands and outputs for removing directory attributes. It starts with a summary of 4 attributes, then lists them with details like permissions, user, group, and timestamps. The user 'guest' runs 'lsattr /home' and receives an error. Then, they run 'cd /home/guest', 'lsattr', and 'cd'. Next, they create a directory 'dir1' with 'mkdir', list it with 'ls -l', and remove its attributes with 'lsattr'. Another summary shows 0 attributes. Then, they set permissions 'chmod 000 dir1', list it, and remove its attributes with 'lsattr'. A third summary shows 0 attributes. Finally, they attempt to create a file 'file1' with 'echo "test" > /home/guest/dir1/file1', which fails with a permission error. They then attempt to change directory with 'cd dir1/' and fail with another permission error. The session ends with the prompt '[guest@mauricio ~]\$'.

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.