

Дискреционное разграничение прав в Linux. Основные атрибуты

Угбокхон Джошуа Озиегбе НКНКБД-01-18¹

28 сентября, 2021, Москва, Россия

¹Российский Университет Дружбы Народов

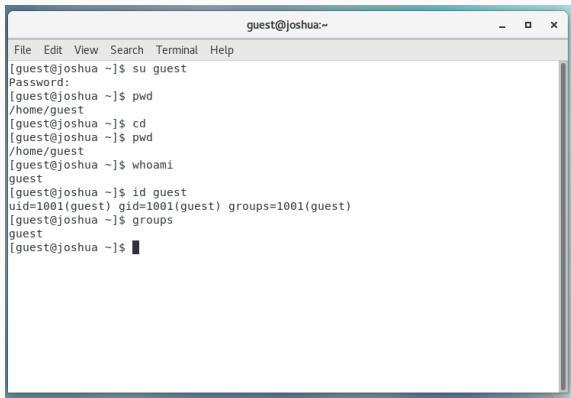
Цели и задачи работы

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

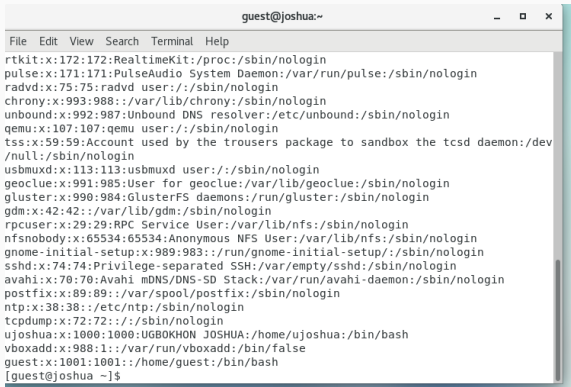
Определяем UID и группу

A terminal window titled 'guest@joshua:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows a sequence of commands and their outputs: 'su guest' (password prompt), 'pwd' (returns /home/guest), 'cd' (returns /home/guest), 'whoami' (returns guest), 'id guest' (returns uid=1001(guest) gid=1001(guest) groups=1001(guest)), and 'groups' (returns guest).

```
guest@joshua:~  
File Edit View Search Terminal Help  
[guest@joshua ~]$ su guest  
Password:  
[guest@joshua ~]$ pwd  
/home/guest  
[guest@joshua ~]$ cd  
[guest@joshua ~]$ pwd  
/home/guest  
[guest@joshua ~]$ whoami  
guest  
[guest@joshua ~]$ id guest  
uid=1001(guest) gid=1001(guest) groups=1001(guest)  
[guest@joshua ~]$ groups  
guest  
[guest@joshua ~]$
```

Figure 1: Информация о пользователе guest

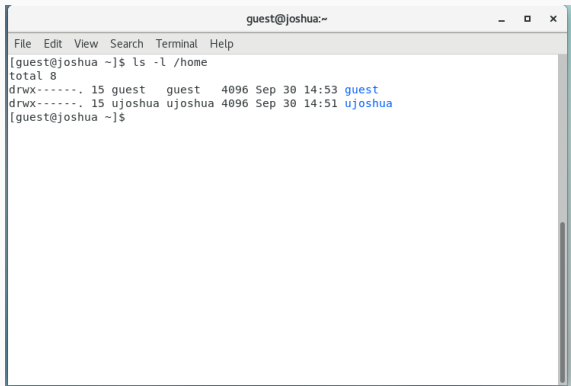
Файл с данными о пользователях

A screenshot of a terminal window titled 'guest@joshua:~'. The terminal displays the output of the 'cat /etc/passwd' command, showing a list of system and user accounts. The accounts listed are: rtkit, pulse, radvd, chrony, unbound, qemu, tss, usbmuxd, geoclue, gluster, gdm, rpcuser, nfsnobody, gnome-initial-setup, sshd, avahi, postfix, ntp, tcpdump, ujoshua, vboxadd, and guest. Each entry follows the format 'username:x:UID:GID:Full Name:Home Directory:Shell'.

```
guest@joshua:~  
File Edit View Search Terminal Help  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
radvd:x:75:75:radvd user:/:/sbin/nologin  
chrony:x:993:988:./var/lib/chrony:/sbin/nologin  
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
qemu:x:107:107:qemu user:/:/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:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin  
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin  
gdm:x:42:42:./var/lib/gdm:/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  
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  
ujoshua:x:1000:1000:UGBOKHON JOSHUA:/home/ujoshua:/bin/bash  
vboxadd:x:988:1:./var/run/vboxadd:/bin/false  
guest:x:1001:1001:./home/guest:/bin/bash  
[guest@joshua ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

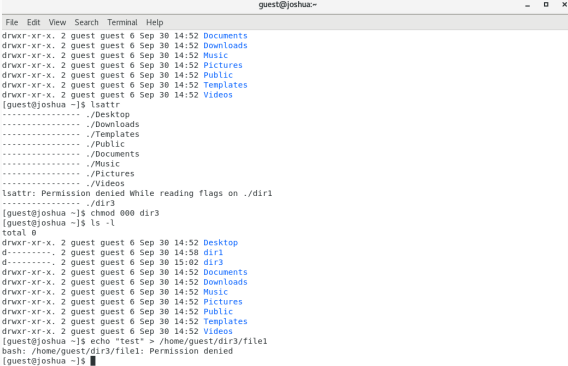


A terminal window titled 'guest@joshua:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command '[guest@joshua ~]\$ ls -l /home' has been executed, resulting in the following output:

```
total 8
drwx-----, 15 guest    guest    4096 Sep 30 14:53 guest
drwx-----, 15 uJoshua uJoshua 4096 Sep 30 14:51 uJoshua
[guest@joshua ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

A terminal window titled 'guest@joshua:~' showing a series of commands and their outputs. The user first runs 'lsattr' to list attributes of the current directory, showing standard system directories like Desktop, Downloads, Templates, Public, Documents, Music, Pictures, and Videos. Then, they create a directory 'dir3' and run 'lsattr' on it, which shows it has no attributes. Finally, they attempt to remove attributes from 'dir3' using 'chmod 000 dir3' followed by 'ls -l', but the command 'chmod' results in a 'Permission denied' error.

```
guest@joshua:~  
File Edit View Search Terminal Help  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Music  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Public  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Videos  
[guest@joshua ~]$ lsattr  
----- ./Desktop  
----- ./Downloads  
----- ./Templates  
----- ./Public  
----- ./Documents  
----- ./Music  
----- ./Pictures  
----- ./Videos  
lsattr: Permission denied While reading flags on ./dir1  
----- ./dir3  
[guest@joshua ~]$ chmod 000 dir3  
[guest@joshua ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Desktop  
d----- 2 guest guest 6 Sep 30 14:58 dir1  
d----- 2 guest guest 6 Sep 30 15:02 dir3  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Music  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Public  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 30 14:52 Videos  
[guest@joshua ~]$ echo "test" > /home/guest/dir3/file1  
bash: /home/guest/dir3/file1: Permission denied  
[guest@joshua ~]$
```

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.