

Дискреционное разграничение прав в Linux. Основные атрибуты

Ласурия Данли НПИбд-01-19 ¹

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

```
[root@localhost lasuriyadr]# useradd guest
[root@localhost lasuriyadr]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost lasuriyadr]# su guest
[guest@localhost lasuriyadr]$ pwd
/home/lasuriyadr
[guest@localhost lasuriyadr]$ cd
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$ id guest
uid=1001(guest) gid=1001(guest) groups=1001(guest)
[guest@localhost ~]$ groups
guest
[guest@localhost ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

```
login
sssd:x:984:985:User for sssd:/sbin/nologin
qemu:x:107:107:qemu user:/sbin/nologin
cockpit-ws:x:983:983:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:982:982:User for cockpit-ws instances:/nonexisting:/sbin/nologin
login
colord:x:981:981:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
setroubleshoot:x:980:977::/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:979:976:User for flatpak system helper:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:978:975::/run/gnome-initial-setup:/sbin/nologin
pesign:x:977:974:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
lasuriyadr:x:1000:1000:/home/lasuriyadr:/bin/bash
vboxadd:x:976:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@localhost ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/home/guest:/bin/bash
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@localhost ~]$ ls -l /home/  
total 4  
drwx-----, 3 guest      guest      78 Sep 17 18:23 guest  
drwx-----, 15 lasuriyadr lasuriyadr 4096 Sep 17 18:21 lasuriyadr  
[guest@localhost ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/lasuriyadr  
----- /home/guest
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls
dir1
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@localhost ~]$ echo "hello" /home/guest/dir1/file1
hello /home/guest/dir1/file1
[guest@localhost ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@localhost ~]$ chmod 300 dir1
[guest@localhost ~]$ cd dir1
[guest@localhost dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest@localhost dir1]$ chmod 000 file1
chmod: cannot access 'file1': No such file or directory
[guest@localhost dir1]$ chmod 300 dir1
chmod: cannot access 'dir1': No such file or directory
[guest@localhost dir1]$ cd ..
[guest@localhost ~]$ ls
dir1
[guest@localhost ~]$ chmod 300 dir1
```

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.