

Дискреционное разграничение прав в Linux. Основные атрибуты.

¹ Булаев Максим Александрович НПИбд-01-19

16 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

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@mabulaev ~]$ pwd
/home/guest
[guest@mabulaev ~]$ whoami
guest
[guest@mabulaev ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@mabulaev ~]$ groups
guest
[guest@mabulaev ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

```
polkitd:x:998:996:User for polkitd:/:sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/:sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:994:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:993:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:992:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
setroubleshoot:x:991:986:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:990:985:User for flatpak system helper:/sbin/nologin
colord:x:989:984:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:988:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
systemd-oom:x:981:981:systemd Userspace OOM Killer:/usr/sbin/nologin
pesign:x:980:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:979:979:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:978:978:/var/lib/chrony:/sbin/nologin
dnsmasq:x:977:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
mabulaev:x:1000:1000:mabulaev:/home/mabulaev:/bin/bash
vboxadd:x:976:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@mabulaev ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@mabulaev ~]$ ls -l /home/  
total 8  
drwx-----. 14 guest      guest      4096 Sep 17 15:47 guest  
drwx-----. 14 mabulaev  mabulaev  4096 Sep 17 15:43 mabulaev  
[guest@mabulaev ~]$ lsattr /home  
lsattr: Permission denied while reading flags on /home/mabulaev  
----- /home/guest  
[guest@mabulaev ~]$ █
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Videos
[guest@mabulaev ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@mabulaev ~]$ chmod 000 dir1
[guest@mabulaev ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Desktop
d----- . 2 guest guest 6 Sep 17 16:00 dir1
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Documents
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Music
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Public
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Templates
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Videos
[guest@mabulaev ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@mabulaev ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@mabulaev ~]$
```

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

Таким образом, я получил навыки работы с атрибутами файлов и сведения о разграничении доступа.