

Дискреционное разграничение прав в Linux. Основные атрибуты

Буянбадрах Тогтохжав¹

24 февраля, 2025, 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

```
btogtozhav@btogtozhav:~$ su guest
Пароль:
guest@btogtozhav:/home/btogtozhav$ pwd
/home/btogtozhav
guest@btogtozhav:/home/btogtozhav$ cd
guest@btogtozhav:~$ pwd
/home/guest
guest@btogtozhav:~$ whoami
guest
guest@btogtozhav:~$ id guest
uid=1001(guest) gid=1001(guest) группы=1001(guest)
guest@btogtozhav:~$ groups guest
guest : guest
guest@btogtozhav:~$ █
```

Рис. 1: Информация о пользователе guest

Файл с данными о пользователях

```
adm:x:3:4:adm:/var/adm:/usr/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/usr/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/usr/sbin/nologin
operator:x:11:0:operator:/root:/usr/sbin/nologin
games:x:12:100:games:/usr/games:/usr/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/usr/sbin/nologin
nobody:x:65534:65534:Kernel OverFlow User:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
dbus:x:81:81:System Message Bus:/usr/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
systemd-oom:x:999:999:systemd Userspace OOM Killer:/sbin/nologin
polkitd:x:114:114>User for polkitd:/sbin/nologin
colord:x:998:997>User for colord:/var/lib/colord:/sbin/nologin
stapunpriv:x:159:159:systemtap unprivileged user:/var/lib/stapunpriv:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/sbin/nologin
geoclue:x:997:996>User for geoclue:/var/lib/geoclue:/sbin/nologin
sssd:x:996:995>User for sssd:/run/sss:/sbin/nologin
libstoragemgmt:x:994:994:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-coredump:x:993:993:systemd Core Dumper:/usr/sbin/nologin
wsdd:x:992:992:Web Services Dynamic Discovery host daemon:/sbin/nologin
clevis:x:991:991:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:990:990:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
pipewire:x:989:989:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
flatpak:x:988:988:Flatpak system helper:/usr/sbin/nologin
gdm:x:42:42:GNOME Display Manager:/var/lib/gdm:/usr/sbin/nologin
gnome-initial-setup:x:987:986:/run/gnome-initial-setup:/sbin/nologin
dnsmasq:x:986:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
pesign:x:985:984:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:984:983:chrony system user:/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:tcpdump:/usr/sbin/nologin
gnome-remote-desktop:x:981:981:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
guest:x:1001:1001:/home/guest:/bin/bash
btogtozhav:x:1002:1002:/home/btogtozhav:/bin/bash
guest@btogtozhav:~$
```

Рис. 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
guest@btogtozhav:~$  
guest@btogtozhav:~$ ls -l /home  
итого 4  
drwx----- 14 btogtozhav btogtozhav 4096 мар  2 10:48 btogtozhav  
drwx-----,  3 guest      guest      78 фев  5 19:27 guest  
guest@btogtozhav:~$ lsattr /home  
----- /home/guest  
lsattr: Отказано в доступе While reading flags on /home/btogtozhav  
guest@btogtozhav:~$
```

Рис. 3: Расширенные атрибуты

Атрибуты директории

```
guest@btogtonzhav:~$  
guest@btogtozhav:~$ cd  
guest@btogtozhav:~$ mkdir dir1  
guest@btogtozhav:~$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 март 2 10:55 dir1  
guest@btogtozhav:~$ chmod 000 dir1/  
guest@btogtozhav:~$ ls -l | grep dir1  
d----- . 2 guest guest 6 март 2 10:55 dir1  
guest@btogtozhav:~$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
guest@btogtozhav:~$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
guest@btogtozhav:~$ █
```

Рис. 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) |

Рис. 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.