

Дискреционное разграничение прав в Linux. Основные атрибуты

Мегегхо Меконтчу Надэж НПИбд-02-19 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

```
guest@nadezh:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[nadezh@nadezh ~]$ su  
Пароль:  
[root@nadezh nadezh]# useradd guest  
[root@nadezh nadezh]# passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[root@nadezh nadezh]# su guest  
[guest@nadezh nadezh]$ pwd  
/home/nadezh  
[guest@nadezh nadezh]$ cd  
[guest@nadezh ~]$ pwd  
/home/guest  
[guest@nadezh ~]$ whoami  
guest  
[guest@nadezh ~]$ id guest  
uid=1002(guest) gid=1002(guest) rгруппы=1002(guest)  
[guest@nadezh ~]$ groups  
guest  
[guest@nadezh ~]$ █
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

```
guest@nadezh:-
Файл  Правка  Вид  Поиск  Терминал  Справка
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
saslauth:x:996:76:Saslauthd user:/run/saslauthd:/sbin/nologin
abrt:x:173:173:./etc/abrt:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
qemu:x:107:107:qemu user:./:/sbin/nologin
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
sane: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
user:x:1000:1000:user:/home/user:/bin/bash
nadezh:x:1001:1001:./home/nadezh:/bin/bash
guest:x:1002:1002:./home/guest:/bin/bash
[guest@nadezh ~]$
[guest@nadezh ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@nadezh ~]$  
[guest@nadezh ~]$  
[guest@nadezh ~]$ ls -l /home  
итого 8  
drwx-----. 5 guest  guest  107 сен 12 13:26 guest  
drwx-----. 15 nadezh nadezh 4096 сен 12 13:19 nadezh  
drwx-----. 15 user   user   4096 сен 12 11:31 user  
[guest@nadezh ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/user  
lsattr: Отказано в доступе While reading flags on /home/nadezh  
----- /home/guest  
[guest@nadezh ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@nadezh ~]$  
[guest@nadezh ~]$ cd  
[guest@nadezh ~]$ mkdir dir1  
[guest@nadezh ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 12 13:27 dir1  
[guest@nadezh ~]$ lsattr  
----- ./dir1  
[guest@nadezh ~]$ chmod 000 dir1  
[guest@nadezh ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 сен 12 13:27 dir1  
[guest@nadezh ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@nadezh ~]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@nadezh ~]$
```

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.