

Дискреционное разграничение прав в Linux. Основные атрибуты

Куденко Максим Русланович¹

6 ноября, 2024, 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

```
[mrkudenko@mrkudenko ~]$ su
Пароль:
[root@mrkudenko mrkudenko]# su guest
[guest@mrkudenko mrkudenko]$ pwd
/home/mrkudenko
[guest@mrkudenko mrkudenko]$ cd
[guest@mrkudenko ~]$ pwd
/home/guest
[guest@mrkudenko ~]$ whoami
guest
[guest@mrkudenko ~]$ id guest
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel)
[guest@mrkudenko ~]$ groups guest
guest : guest wheel
[guest@mrkudenko ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

```
dbus:x:81:81:System message bus:/:sbin/nologin
polkitd:x:998:996:User for polkitd:/:sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/:sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/:usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/:usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/:sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:981:980:/:run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/:sbin/nologin
guest:x:1001:1001:guest:/home/guest:/bin/bash
guest2:x:1002:1002:/:home/guest2:/bin/bash
mrkudenko:x:1003:1003:/:home/mrkudenko:/bin/bash
lavrentyukudenko:x:1004:1004:/:home/lavrentyukudenko:/bin/bash
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@mrkudenko ~]$  
[guest@mrkudenko ~]$ ls -l /home  
итого 8  
drwx-----, 14 guest      guest      4096 сен 10  2023 guest  
drwx-----,  3 guest2     guest2      78 сен 17  2023 guest2  
drwx-----, 14 mrkudenko  mrkudenko 4096 ноя  6 22:22 mrkudenko  
[guest@mrkudenko ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@mrkudenko ~]$  
[guest@mrkudenko ~]$ mkdir dir1  
[guest@mrkudenko ~]$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 ноя  6 22:31 dir1  
[guest@mrkudenko ~]$ chmod 000 dir1/  
[guest@mrkudenko ~]$ ls -l | grep dir1  
d------. 2 guest guest 6 ноя  6 22:31 dir1  
[guest@mrkudenko ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@mrkudenko ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@mrkudenko ~]$
```

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.