

Дискреционное разграничение прав в Linux. Основные атрибуты

Максим Платонов¹

19 февраля, 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

```
[mplatonov@mplatonov ~]$ su
Пароль:
[root@mplatonov mplatonov]# useradd guest
Создание почтового ящика: Файл существует
[root@mplatonov mplatonov]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@mplatonov mplatonov]# su guest
[guest@mplatonov mplatonov]$ 1
bash: 1: command not found...
[guest@mplatonov mplatonov]$
[guest@mplatonov mplatonov]$
[guest@mplatonov mplatonov]$ pwd
/home/mplatonov
[guest@mplatonov mplatonov]$ cd
[guest@mplatonov ~]$ pwd
/home/guest
[guest@mplatonov ~]$ whoami
guest
[guest@mplatonov ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:guest_t:s0-s0:c0.c1023
[guest@mplatonov ~]$ groups
guest
[guest@mplatonov ~]$ █
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

```
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
mplatonov:x:1000:1000::/home/mplatonov:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@mplatonov ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
tcpdump:x:72:72::/sbin/nologin
mplatonov:x:1000:1000::/home/mplatonov:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@mplatonov ~]$
[guest@mplatonov ~]$
[guest@mplatonov ~]$ ls -l /home
итого 4
drwx-----. 3 guest      guest      78 фев 19 17:22 guest
drwx-----. 14 mplatonov mplatonov 4096 фев 19 17:21 mplatonov
[guest@mplatonov ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@emplatonov ~]$ cd
[guest@emplatonov ~]$ mkdir dir1
[guest@emplatonov ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 фев 19 17:29 dir1
[guest@emplatonov ~]$ chmod 000 dir1
[guest@emplatonov ~]$ ls -l
итого 0
d------. 2 guest guest 6 фев 19 17:29 dir1
[guest@emplatonov ~]$ echo "test" > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@emplatonov ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@emplatonov ~]$
```

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.