

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Парфенова Е. Е.

12 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Парфенова Елизавета Евгеньевна
- студент
- Российский университет дружбы народов
- 1032216437@pfur.ru
- <https://github.com/parfenovae>



Вводная часть

Важность знания атрибутов файлов и директорий для дальнейшей корректной работы с ОС Linux, а также умения практически применять эти знания

Цели: получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Задачи :

- практическое применение команды `chmod` для изменения атрибутов директорий и файлов
- заполнение и анализ приведенных таблиц

Теоретическое введение

Права доступа в операционной системе Linux представляют собой ключевой элемент безопасности, определяющий, какой доступ имеют пользователи и программы к файлам и каталогам. Чтобы посмотреть права пользователя в Linux, необходимо воспользоваться следующей командой:

```
ls -l
```

Изменить права доступа можно с помощью команды *chmod*.

3 вида разрешений:

- r — read (чтение) — право просматривать содержимое файла
- w — write (запись) — право изменять содержимое файла
- x — execute (выполнение) — право запускать файл, если это программа или скрипт

3 группы пользователей:

- owner (владелец) — отдельный человек, который владеет файлом
- group (группа) — пользователи с общими заданными правами
- others (другие) — все остальные пользователи, не относящиеся к группе и не являющиеся владельцами

Существуют два основных способа записи прав доступа: символьный и числовой формат.

Таблица 1: Формат записи прав доступа системы GNU Linux

Права доступа	Символьный формат	Числовой формат
Чтение	r	4
Запись	w	2
Выполнение	x	1
Нет доступа	-	0

Выполнение лабораторной работы

Создадим новой учетной записи пользователя guest

```
[eeparfenova@eeparfenova ~]$ su
Password:
[root@eeparfenova eeeparfenova]# useradd guest
[root@eeparfenova eeeparfenova]#
```

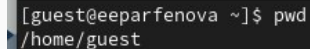
Рис. 1: Создание новой учетной записи guest

Создадим пароля новой учетной записи

```
[root@eeparfenova eeeparfenova]# passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@eeparfenova eeeparfenova]#
```

Рис. 2: Задание пароля для новой учетной записи

Определим директорию командой *pwd*

A terminal window with a dark background. The prompt is [guest@eeparfenova ~]\$ and the command pwd has been entered. The output is /home/guest.

```
[guest@eeparfenova ~]$ pwd  
/home/guest
```

Рис. 3: Вывод команды *pwd*

Итог: мы находимся в домашней директории

Уточнением имени пользователя с помощью *whoami*



```
/home/guest  
[guest@eeparfenova ~]$ whoami  
guest
```

A terminal window with a dark background. The first line shows the prompt and the user's location: `/home/guest`. The second line shows the command `[guest@eeparfenova ~]$ whoami` being entered. The third line shows the output `guest`.

Рис. 4: Вывод команды *whoami*

Сравним выходы команд *id* и *groups*

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

Рис. 5: Вывод команды `id` и `groups`

Итог: информация при выводе обеих команд совпадает

Посмотрим содержимое файла /etc/passwd и сравним данные нашей учетной записи с прошлыми. Итог: все данные одинаковые

```
[guest@eepafenova ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:6:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
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
pipewire:x:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexistent:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexistent:/sbin/nologin
flatpak:x:987:986:User for Flatpak system helper:/:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:Clevis Encryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981:/run/gnome-initial-setup:/sbin/nologin
sshd:x:14:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chromy:x:981:980:chromy system user:/var/lib/chromy:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
eepafenova:x:1000:1000:eepafenova:/home/eepafenova:/bin/bash
vboxadd:x:979:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
```

Рис. 6: Содержимое файла /etc/passwd

Определим все директории в нашем домашнем каталоге и проверим расширенные атрибуты, установленные на поддиректориях

```
[guest@eeparfenova ~]$ ls -l /home
total 8
drwx-----, 14 eeparfenova eeparfenova 4096 Sep 12 12:19 eeparfenova
drwx-----, 14 guest      guest      4096 Sep 12 12:26 guest
```

Рис. 7: Директории домашнего каталога

```
[guest@eeparfenova ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/eeparfenova
----- /home/guest
```

Рис. 8: Расширенные атрибуты поддиректорий

Директория dir1

Создадим новую директорию и выведем информацию об атрибутах

```
[guest@eeparfenova ~]$ mkdir dir1
[guest@eeparfenova ~]$ ls
Desktop dir1 Documents Downloads Music Pictures Public Templates Videos
[guest@eeparfenova ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Desktop
drwxr-xr-x. 2 guest guest  6 Sep 12 12:35 dir1
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Documents
drwxr-xr-x. 2 guest guest 38 Sep 12 12:24 Downloads
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Music
drwxr-xr-x. 2 guest guest 4096 Sep 12 12:33 Pictures
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Public
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Templates
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Videos
[guest@eeparfenova ~]$ lsattr /dir1
lsattr: No such file or directory while trying to stat /dir1
[guest@eeparfenova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
```

Рис. 9: Информация о правах и расширенных атрибутах dir1

Снимем все атрибуты с директории dir1 и проверим это

```
[guest@eeparfenova ~]$ chmod 000 dir1
[guest@eeparfenova ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Desktop
d------. 2 guest guest  6 Sep 12 12:35 dir1
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Documents
drwxr-xr-x. 2 guest guest 38 Sep 12 12:24 Downloads
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Music
drwxr-xr-x. 2 guest guest 4096 Sep 12 12:38 Pictures
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Public
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Templates
drwxr-xr-x. 2 guest guest  6 Sep 12 12:20 Videos
```

Рис. 10: Снятие всех атрибутов с команды dir1

Создадим файл и проверим его создание

```
[guest@eeparfenova ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@eeparfenova ~]$ ls -l /home/guest/dir1  
ls: cannot open directory '/home/guest/dir1': Permission denied  
[guest@eeparfenova ~]$
```

Рис. 11: Попытка создания файла

Итог: файл не был создан и просмотреть директорию нельзя

Минимальные права для совершения операций на директорию

Таблица 2: Минимальные права для совершения операций на директорию

Операция	Минимальные права на директорию
Создание файла	d(300)
Удаление файла	d(300)
Чтение файла	d(100)
Запись в файл	d(100)
Переименование файла	d(300)
Создание поддиректории	d(300)
Удаление поддиректории	d(300)

Минимальные права для совершения операций на файл

Таблица 3: Минимальные права для совершения операций на файл

Операция	Минимальные права на файл
Создание файла	(000)
Удаление файла	(000)
Чтение файла	(400)
Запись в файл	(200)
Переименование файла	(000)
Создание поддиректории	(000)
Удаление поддиректории	(000)

Вывод

Мы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux. Мы практически применили команду `chmod` для изменения атрибутов директорий и файлов, а также заполнили и проанализировали таблицы