

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Гудиева Мадина Куйраевна

Содержание

Цель работы

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.

Теоретические сведения

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный (от англ. discretion — чье-либо усмотрение) — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. [1]

Для каждого файла в Linux задается набор разрешений. Разрешения могут быть следующими:

- `r` — read — возможность открытия и чтения файла. Для директории это возможность просматривать содержимое директории.
- `w` — write — возможность изменения файла. Для директории это возможность добавлять, удалять или переименовывать файлы в директории.
- `x` — execute — возможность выполнения файла (запуска файла). [2]

Набор разрешений состоит из 3 блоков `gwx`:

- Первый блок `gwx` определяет права доступа для владельца-пользователя.
- Второй блок `gwx` определяет права доступа для владельца-группы.
- Третий блок `gwx` определяет права доступа для всех остальных. [2]

Для каждого файла или директории в Linux задаются права доступа. Они задаются тремя атрибутами: набором разрешений, именем владельца, именем группы.

Набор разрешений — это три блока прав доступа: права доступа для владельца файла, права доступа для группы, права доступа для всех остальных.

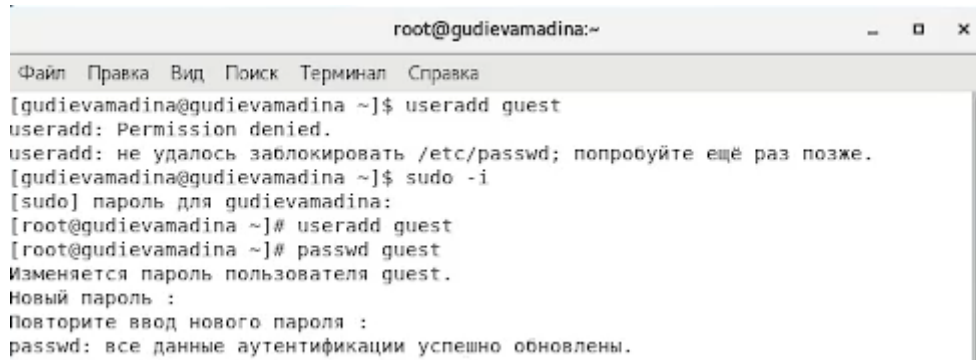
Разрешения записываются символами `r`, `w`, `x`.

Набор разрешений состоит из трех блоков и записывается в виде трех `gwx`, записанных друг за другом в виде одного «слова».

Если какая-либо возможность отключена (запрещена), то вместо соответствующего символа в наборе разрешений ставится прочерк (символ минус).

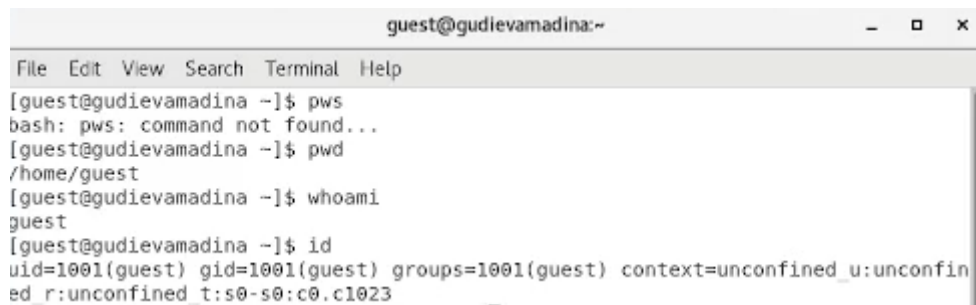
Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя guest, а также задала для этого пользователя пароль.



```
root@gudievamadina:~  
[gudievamadina@gudievamadina ~]$ useradd guest  
useradd: Permission denied.  
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.  
[gudievamadina@gudievamadina ~]$ sudo -i  
[sudo] пароль для gudievamadina:  
[root@gudievamadina ~]# useradd guest  
[root@gudievamadina ~]# passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.
```

2. Вошла в систему от имени пользователя guest.
3. Определите директорию, в которой я нахожусь, командой pwd. С помощью этой команды я убедилась, что нахожусь в домашней директории пользователя.
4. Уточнила имя пользователя командой whoami
5. Уточнила имя пользователя, его группу, а также группы, куда входит пользователь, командой id. Затем воспользовалась командой groups, которая дополнительно обозначила домашнюю директорию.



```
guest@gudievamadina:~  
[guest@gudievamadina ~]$ pws  
bash: pws: command not found...  
[guest@gudievamadina ~]$ pwd  
/home/guest  
[guest@gudievamadina ~]$ whoami  
guest  
[guest@gudievamadina ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

6. Просмотрела файл '/etc/passwd' командой cat '/etc/passwd'. Нашла в нём свою учётную запись, где увидела выведенные ранее значения uid, gid .

```
[guest@gudievamadina ~]$ 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:6:0: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
```

```

guest@gudievamadina:~
File Edit View Search Terminal Help
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
ibus: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/
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sane:x:996:994:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
sasauth:x:995:76:Sasauthd user:/run/sasauthd:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
setroubleshoot:x:994:991:/:var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
chrony:x:993:988:/:var/lib/chrony:/sbin/nologin
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/d
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/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
gnome-initial-setup:x:989:983:/:run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/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
cpdump:x:72:72:/:/sbin/nologin
gudievamadina:x:1000:1000:gudievamadina:/home/gudievamadina:/bin/bash
vboxadd:x:988:1:/:var/run/vboxadd:/bin/false
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
guest:x:1001:1001:/:home/guest:/bin/bash

```

7. Определила существующие в системе директории. Увидела директории моих пользователей, в них пользователь имеет права на чтение, запись и исполнение файлов .

```

[guest@gudievamadina ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/:home/guest:/bin/bash
[guest@gudievamadina ~]$

```

8. Просмотрела, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории '/home'. Увидела, что расширенных атрибутов на поддиректориях моего пользователя нет. Второго пользователя просмотреть не могу .

```

[guest@gudievamadina ~]$ ls -l /home/
total 8
drwx-----. 20 gudievamadina gudievamadina 4096 Sep 16 18:03 gudievamadina
drwx-----. 15 guest          guest          4096 Sep 16 21:20 guest
[guest@gudievamadina ~]$

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

```

9. Создала в домашней директории поддиректорию dir1. Определила, что она получила права 775, а также не получила расширенных атрибутов.

```

[guest@gudievamadina ~]$ mkdir dir1
[guest@gudievamadina ~]$ ls -l
Desktop
dir1
Documents
Downloads
Music
Pictures
Public
Templates
Videos
[guest@gudievamadina ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1

```

10. Сняла с директории dir1 все атрибуты и проверила это.

```

[guest@gudievamadina ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 21:20 Desktop
d----- . 2 guest guest 6 Sep 16 21:29 dir1
drwxr-xr-x. 2 guest guest 6 Sep 16 21:20 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 21:20 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 16 21:20 Music
drwxr-xr-x. 2 guest guest 6 Sep 16 21:20 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 21:20 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 21:20 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 21:20 Videos
[guest@gudievamadina ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
lsattr: Permission denied While reading flags on ./dir1

```

11. Попыталась создать в директории dir1 файл file1, т.к. прав на создание файла у меня не было, я получила отказ.

```

[guest@gudievamadina ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@gudievamadina ~]$

```

12. Заполнила таблицу «Установленные права и разрешённые действия». Для этого я создала в директории 8 файлов с разными правами на каждом. После этого я меняла права dir1 и пробовала взаимодействовать с каждым из этих файлов, также пыталась зайти внутрь папки. Таким образом я проделала необходимые действия с каждым вариантов прав директории и прав файла .

Права директории	Права файла	Создание файла	Удаление файла	Запись файла	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов
d (000)	(000)	-	-	-	-	-	-	-	-
d-x-----(100)	(000)	-	-	-	-	+	-	-	-
d-w-----(200)	(000)	-	-	-	-	-	-	-	-
d-wx-----(300)	(000)	+	+	-	-	+	-	+	-
dr-----(400)	(000)	-	-	-	-	-	+	-	-
dr-x-----(500)	(000)	-	-	-	-	+	+	-	-
drw-----(600)	(000)	-	-	-	-	-	+	-	-
drwx-----(700)	(000)	+	+	-	-	+	+	+	-
d (000)	---x---(100)	-	-	-	-	-	-	-	-
d-x---(100)	---x---(100)	-	-	-	-	+	-	-	-
d-w---(200)	---x---(100)	-	-	-	-	-	-	-	-
d-wx---(300)	---x---(100)	+	+	-	-	+	-	+	-
dr---(400)	---x---(100)	-	-	-	-	-	+	-	-
dr-x---(500)	---x---(100)	-	-	-	-	+	+	-	-
drw---(600)	---x---(100)	-	-	-	-	-	+	-	-
drwx---(700)	---x---(100)	+	+	-	-	+	+	+	-
d (000)	---w---(200)	-	-	-	-	-	-	-	-
d-x---(100)	---w---(200)	-	-	+	-	+	-	-	-
d-w---(200)	---w---(200)	-	-	-	-	-	-	-	-
d-wx---(300)	---w---(200)	+	+	+	-	+	-	+	-
dr---(400)	---w---(200)	-	-	-	-	-	+	-	-
dr-x---(500)	---w---(200)	-	-	+	-	+	+	-	-
drw---(600)	---w---(200)	-	-	-	-	-	+	-	-
drwx---(700)	---w---(200)	+	+	+	-	+	+	+	-
d (000)	---wx---(300)	-	-	-	-	-	-	-	-
d-x---(100)	---wx---(300)	-	-	+	-	+	-	-	-
d-w---(200)	---wx---(300)	-	-	-	-	-	-	-	-
d-wx---(300)	---wx---(300)	+	+	+	-	+	-	+	-
dr---(400)	---wx---(300)	-	-	-	-	-	+	-	-
dr-x---(500)	---wx---(300)	-	-	+	-	+	+	-	-
drw---(600)	---wx---(300)	-	-	-	-	-	+	-	-
drwx---(700)	---wx---(300)	+	+	+	-	+	+	+	-
d (000)	-f---(400)	-	-	-	-	-	-	-	-
d-x---(100)	-f---(400)	-	-	-	+	+	-	-	+
d-w---(200)	-f---(400)	-	-	-	-	-	-	-	-
d-wx---(300)	-f---(400)	+	+	-	+	+	-	+	+
dr---(400)	-f---(400)	-	-	-	-	-	+	-	-
dr-x---(500)	-f---(400)	-	-	-	+	+	+	-	+
drw---(600)	-f---(400)	-	-	-	-	-	+	-	-
drwx---(700)	-f---(400)	+	+	-	+	+	+	+	+
d (000)	-f-x---(500)	-	-	-	-	-	-	-	-
d-x---(100)	-f-x---(500)	-	-	-	+	+	-	-	+
d-w---(200)	-f-x---(500)	-	-	-	-	-	-	-	-
d-wx---(300)	-f-x---(500)	+	+	-	+	+	-	+	+
dr---(400)	-f-x---(500)	-	-	-	-	-	+	-	-
dr-x---(500)	-f-x---(500)	-	-	-	+	+	+	-	+
drw---(600)	-f-x---(500)	-	-	-	-	-	+	-	-
drwx---(700)	-f-x---(500)	+	+	-	+	+	+	+	+
d (000)	-rw---(600)	-	-	-	-	-	-	-	-
d-x---(100)	-rw---(600)	-	-	+	+	+	-	-	+
d-w---(200)	-rw---(600)	-	-	-	-	-	-	-	-
d-wx---(300)	-rw---(600)	+	+	+	+	+	-	+	+
dr---(400)	-rw---(600)	-	-	-	-	-	+	-	-
dr-x---(500)	-rw---(600)	-	-	+	+	+	+	-	+
drw---(600)	-rw---(600)	-	-	-	-	-	+	-	-
drwx---(700)	-rw---(600)	+	+	+	+	+	+	+	+
d (000)	-rwx---(700)	-	-	-	-	-	-	-	-
d-x---(100)	-rwx---(700)	-	-	+	+	+	-	-	+
d-w---(200)	-rwx---(700)	-	-	-	-	-	-	-	-
d-wx---(300)	-rwx---(700)	+	+	+	+	+	-	+	+
dr---(400)	-rwx---(700)	-	-	-	-	-	+	-	-
dr-x---(500)	-rwx---(700)	-	-	+	+	+	+	-	+
drw---(600)	-rwx---(700)	-	-	-	-	-	+	-	-
drwx---(700)	-rwx---(700)	+	+	+	+	+	+	+	+

13. На основе полученной информации из таблицы прошлого пункта, я смогла определить те или иные минимально необходимые права для выполнения операций внутри директории dir1. Так как в предыдущем пункте не требовалось создавать подкаталог, я дополнительно попробовала создать dir2 внутри dir1 (меняя права dir1) и удалить её.

Операция	Минимальные права на директорию	Минимальные 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)	-
Удаление поддиректории	d-wx-----(300)	-

Выводы

Таким образом я успешно приобрела практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Дискреционное разграничение доступа Linux. // Debianinstall. 2018. URL: <https://debianinstall.ru/diskretionnoe-razgranichenie-dostupa-linux/> (дата обращения 02.10.2021).
2. Права доступа к файлам в Linux. // Pingvinus. 2018. URL: <https://pingvinus.ru/note/file-permissions> (дата обращения 02.10.2021).
3. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-математических и естественных наук. М.: РУДН, 2015. 64 с..