

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Коняева Марина Александровна

НФИбд-01-21

Студ. билет: 1032217044

2024

RUDN

- Коняева Марина Александровна
- Студентка группы НФИбд-01-21
- Студ. билет 1032217044
- Российский университет дружбы народов

- 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

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [2].

1. Создайте учётную запись пользователя guest

```
[makonyaeva@user ~]$ su  
Password:  
[root@user makonyaeva]# useradd guest
```

Рис. 1: (рис. 1. useradd guest)

2. Задайте пароль для пользователя guest

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

Рис. 2: (рис. 2. passwd guest)

3. Войдите в систему от имени пользователя guest

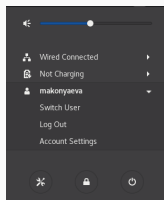


Рис. 3: (рис. 3. log out)

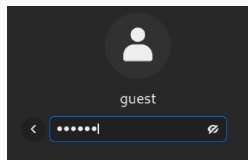
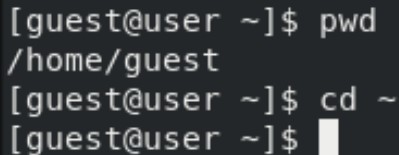


Рис. 4: (рис. 4. log in)

4. Определите директорию, в которой вы находитесь

A terminal window with a dark background and light gray text. It shows three lines of command execution: the first line is '[guest@user ~]\$ pwd' followed by the output '/home/guest' on the next line; the second line is '[guest@user ~]\$ cd ~'; and the third line is '[guest@user ~]\$' followed by a white cursor block.

```
[guest@user ~]$ pwd  
/home/guest  
[guest@user ~]$ cd ~  
[guest@user ~]$
```

Рис. 5: (рис. 6. pwd)

5. Уточните имя вашего пользователя командой

```
[guest@user ~]$ whoami  
guest
```

Рис. 6: (рис. 7. whoami)

6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь

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

Рис. 7: (рис. 8. id и groups)

Ход выполнения лабораторной работы

7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки

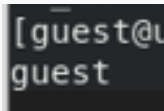


Рис. 8: (рис. 9. Совпадение)

8. Просмотрите файл /etc/passwd. Найдите в нём свою учётную запись.

```
[quest@quest ~]$ 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
dbus:x:81:81:system message bus:/:/sbin/nologin
systemd-coredump:x:999:999:systemd Core Daemon:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/sbin/nologin
cockpit:x:980:980:User for cockpit:/:/sbin/nologin
geoclue:x:997:995:User for geoclue:/var/lib/geoclue:/sbin/nologin
unbound:x:996:992:unbound DNS resolver:/etc/unbound:/sbin/nologin
rftt:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:995:991:Pipewire System Daemon:/var/run/pipewire:/sbin/nologin
dnsmasq:x:996:990:dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
clevis:x:989:989:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
gluster:x:988:988:GlusterFS daemon:/run/gluster:/sbin/nologin
pcr:x:2:2:PCrdns Daemon:/var/lib/pcrdns:/sbin/nologin
chrom:x:907:907:/var/lib/chrom:/sbin/nologin
saslauthd:x:986:76:Saslauthd user:/run/saslauthd:/sbin/nologin
libstoragemgmt:x:985:986:dnsmasq account for libstoragemgmt:/var/run/lsn:/sbin/nologin
sssd:x:984:983:User for sssd:/:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
cockpit-ws:x:983:983:User for cockpit web service:/nonexistent:/sbin/nologin
cockpit-ws-ns:x:982:982:User for cockpit-ws instances:/nonexistent:/sbin/nologin
colord:x:981:981:User for colord:/var/lib/colord:/sbin/nologin
pcre:x:2:2:PCrdns Daemon:/var/lib/pcrdns:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
setroubleshoot:x:980:977:/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:979:978:User for flatpak system helper:/:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:978:975:/run/gnome-initial-setup:/sbin/nologin
design:x:977:974:Group for the design shipping daemon:/run/design:/sbin/nologin
```

9. Определите существующие в системе директории. Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на них?

```
[guest@user ~]$ ls -l /home/  
total 8  
drwx----- 15 guest      guest      4096 Sep 10 05:48 guest  
drwx----- 15 makonyaeva makonyaeva 4096 Sep 10 05:37 makonyaeva
```

Рис. 11: (рис. 12. ls -l /home/)

10. Проверьте, какие расширенные атрибуты установлены на поддиректориях. Удалось ли вам увидеть расширенные атрибуты директории, директорий других пользователей?

```
[guest@user ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/makonyaeva  
----- /home/guest
```

Рис. 12: (рис. 13. lsattr /home)

11. Создайте в домашней директории поддиректорию `dir1` командой. Определите, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`

```
[guest@user ~]$ mkdir dir1
[guest@user ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Desktop
drwxrwxr-x. 2 guest guest 6 Sep 10 05:56 dir1
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Documents
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Music
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Public
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Templates
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Videos
[guest@user ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
```

Рис. 13: (рис. 14. mkdir dir1)

12. Снимите с директории dir1 все атрибуты и проверьте с её помощью правильность выполнения команды ls -l

```
[guest@user ~]$ chmod 000 dir1
[guest@user ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Desktop
d------. 2 guest guest 6 Sep 10 05:56 dir1
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Documents
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Music
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Public
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Templates
drwxr-xr-x. 2 guest guest 6 Sep 10 05:37 Videos
```

Рис. 14: (рис. 15. chmod 000 dir1)

13. Попробуйте создать в директории `dir1` файл `file1`. Почему вы получили отказ? Проверьте, действительно ли файл не находится внутри директории

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

Рис. 15: (рис. 16. `"test" > /home/guest/dir1/file1`)

Ход выполнения лабораторной работы

14. Заполните таблицу «Установленные права и разрешённые действия» (см. табл. 2.1)

Пра- ва ди- рек- то- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Про- смотр фай- лов в ди- рек- то- рии	Переим- ова- ние фай- ла	Сме- на ат- ри- бу- тов фай- ла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+

Ход выполнения лабораторной работы

15. На основании заполненной таблицы определите минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.2.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание	d(300)	(000)

- Были получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

[1] Операционные системы:

<https://blog.skillfactory.ru/glossary/operaczionnaya-sistema/>

[2] Права доступа:

<https://codechick.io/tutorials/unix-linux/unix-linux-permissions>