

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Чемоданова Ангелина Александровна

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Таблицы прав доступа	9
4	Выводы	14

Список иллюстраций

2.1	Создание учетной записи guest	5
2.2	Пароль учетной записи guest	5
2.3	Вход под учетной записью guest	5
2.4	Команда pwd	6
2.5	Имя пользователя. Команды whoami, id	6
2.6	Файл /etc/passwd	7
2.7	Команда ls -l /home/	7
2.8	Команда lsattr /home	7
2.9	Изменения каталога dir1	8
2.10	Изменения файла test1	8
3.1	Проверка при правах на директорию 000 и действий на файл . . .	12
3.2	Проверка при правах на директорию 300 и разных правах на файл	13

1 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.

2 Выполнение лабораторной работы

1. Создаем учетную запись пользователя guest(используя учетную запись администратора) при помощи команды `useradd guest`. (рис. [2.1]).

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

Рис. 2.1: Создание учетной записи guest

2. Задаю пароль для пользователя guest(используя учетную запись администратора) при помощи команды `passwd guest`. (рис. [2.2]).

```
[root@aachemodanova aachemodanova]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@aachemodanova aachemodanova]#
```

Рис. 2.2: Пароль учетной записи guest

3. Вхожу в систему под от имени пользователя guest. (рис. [2.3]).

```
[root@aachemodanova aachemodanova]# su guest
[guest@aachemodanova aachemodanova]$
```

Рис. 2.3: Вход под учетной записью guest

4. Определяю директорию, в которой нахожусь. Директория не являлась домашней, перехожу в домашнюю директорию.(рис. [2.4]).

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

Рис. 2.4: Команда pwd

5. Уточняю имя пользователя командой whoami. Уточняю имя пользователя, его группу, а также группы, куда входит пользователь, командой id. Запоминаю выведенные значения uid, gid и другие. (рис. [2.5]).

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

Рис. 2.5: Имя пользователя. Команды whoami, id

6. Посмотрели файл /etc/passwd командой cat /etc/passwd. Нашли в нем свою учетную запись. Определили uid пользователя. Определили gid пользователя. (рис. [2.6]).

```
[guest@aachemodanova ~]$ 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
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:997:993:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
sssd:x:996:992:User for sssd:/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:/usr/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:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:980:979:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
aachemodanova:x:1000:1000:aachemodanova:/home/aachemodanova:/bin/bash
vboxadd:x:977:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@aachemodanova ~]$
```

Рис. 2.6: Файл /etc/passwd

7. Определили существующие в системе директории командой `ls -l /home/`. (рис. [2.7]).

```
[guest@aachemodanova ~]$ ls -l /home/
total 4
drwx-----. 17 aachemodanova aachemodanova 4096 Feb 29 23:51 aachemodanova
drwx-----.  3 guest          guest          78 Feb 29 23:58 guest
[guest@aachemodanova ~]$
```

Рис. 2.7: Команда `ls -l /home/`

8. Проверили, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой `lsattr /home`. (рис. [2.8]).

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

Рис. 2.8: Команда `lsattr /home`

9. Создали в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определили командами `ls -l` и `lsattr`, какие права доступа и расширенные

атрибуты были выставлены на директорию dir1. Сняли с директории dir1 все атрибуты командой `chmod 000 dir1` и проверили с ее помощью правильность выполнения команды `ls -l`. (рис. [2.9]).

```
[guest@aachemodanova ~]$ mkdir dir1
[guest@aachemodanova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Mar  1 00:06 dir1
[guest@aachemodanova ~]$ lsattr
----- ./dir1
[guest@aachemodanova ~]$ chmod 000 dir1
[guest@aachemodanova ~]$ ls -l
total 0
d-----. 2 guest guest 6 Mar  1 00:06 dir1
[guest@aachemodanova ~]$
```

Рис. 2.9: Изменения каталога dir1

10. Попытались создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`. Не получилось.(рис. [2.10]).

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

Рис. 2.10: Изменения файла test1

3 Таблицы прав доступа

14. Заполним таблицу «Установленные права и разрешённые действия»

Права ди- ректо- рии	Права файла	Со- зда- ние файла	Уда- ление файла	За- пись в файл	Чте- ние файла	Сме- на ди- ректо- рии	Про- смотр фай- лов в ди- ректо- рии	Пере- име- нова- ние файла	Сме- на атри- бутов файла
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)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	+	-	-	+
d(100)	(300)	-	-	+	-	+	-	-	+
d(100)	(400)	-	-	-	+	+	-	-	+

d(100)	(500)	-	-	-	+	+	-	-	+
d(100)	(600)	-	-	+	+	+	-	-	+
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	+
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+

d(500)	(100)	-	-	-	-	+	+	-	+
d(500)	(200)	-	-	+	-	+	+	-	+
d(500)	(300)	-	-	+	-	+	+	-	+
d(500)	(400)	-	-	-	+	+	+	-	+
d(500)	(500)	-	-	-	+	+	+	-	+
d(500)	(600)	-	-	+	+	+	+	-	+
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-
d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(700)	(100)	+	+	-	-	+	+	+	+
d(700)	(200)	+	+	+	-	+	+	+	+
d(700)	(300)	+	+	+	-	+	+	+	+
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

Таблица 2.1 «Установленные права и разрешённые действия»
(рис. [3.1]).

```

[guest@aachemodanova ~]$ chmod 000 dir1
[guest@aachemodanova ~]$ ls -l
total 0
d----- . 2 guest guest 6 Mar 1 00:06 dir1
[guest@aachemodanova ~]$ touch /home/guest/dir1/test
touch: cannot touch '/home/guest/dir1/test': Permission denied
[guest@aachemodanova ~]$ chmod 100 dir1
[guest@aachemodanova ~]$ chmod 300 dir1
[guest@aachemodanova ~]$ touch /home/guest/dir1/test
[guest@aachemodanova ~]$ chmod 100 dir1
[guest@aachemodanova ~]$ touch /home/guest/dir1/test1
touch: cannot touch '/home/guest/dir1/test1': Permission denied
[guest@aachemodanova ~]$ rm /home/guest/dir1/test
rm: cannot remove '/home/guest/dir1/test': Permission denied

```

Рис. 3.1: Проверка при правах на директорию 000 и действий на файл

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

Операция	Минималь- ные права на директорию	Минималь- ные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименова- ние файла	d(300)	(000)
Создание под- директории	d(300)	(000)
Удаление под- директории	d(300)	(000)

Таблица 2.2 “Минимальные права для совершения операций”

(рис. [3.2]).

```
[guest@aachemodanova dir1]$ cat test
cat: test: Permission denied
[guest@aachemodanova dir1]$ mv test test1
mv: cannot move 'test' to 'test1': Permission denied
[guest@aachemodanova dir1]$ echo "this is a line" > test.txt
bash: test.txt: Permission denied
[guest@aachemodanova dir1]$ chmod 200 test
[guest@aachemodanova dir1]$ cat test
cat: test: Permission denied
[guest@aachemodanova dir1]$ chmod 200 test
[guest@aachemodanova dir1]$ mv test test1
mv: cannot move 'test' to 'test1': Permission denied
[guest@aachemodanova dir1]$ echo "this is a line" > test.txt
bash: test.txt: Permission denied
[guest@aachemodanova dir1]$ chmod 300 test
[guest@aachemodanova dir1]$ cat test
cat: test: Permission denied
[guest@aachemodanova dir1]$ mv test test1
mv: cannot move 'test' to 'test1': Permission denied
[guest@aachemodanova dir1]$ echo "this is a line" > test.txt
bash: test.txt: Permission denied
[guest@aachemodanova dir1]$ chmod 400 test
[guest@aachemodanova dir1]$ cat test
[guest@aachemodanova dir1]$ mv test test1
mv: cannot move 'test' to 'test1': Permission denied
[guest@aachemodanova dir1]$ echo "this is a line" > test.txt
bash: test.txt: Permission denied
[guest@aachemodanova dir1]$ chmod 500 test
[guest@aachemodanova dir1]$ cat test
[guest@aachemodanova dir1]$ mv test test1
mv: cannot move 'test' to 'test1': Permission denied
[guest@aachemodanova dir1]$ echo "this is a line" > test.txt
bash: test.txt: Permission denied
[guest@aachemodanova dir1]$ chmod 600 test
[guest@aachemodanova dir1]$ cat test
[guest@aachemodanova dir1]$ mv test test1
mv: cannot move 'test' to 'test1': Permission denied
[guest@aachemodanova dir1]$ echo "this is a line" > test.txt
bash: test.txt: Permission denied
[guest@aachemodanova dir1]$ chmod 700 test
[guest@aachemodanova dir1]$ cat test
[guest@aachemodanova dir1]$ mv test test1
mv: cannot move 'test' to 'test1': Permission denied
[guest@aachemodanova dir1]$ echo "this is a line" > test.txt
bash: test.txt: Permission denied
[guest@aachemodanova dir1]$ rm test
rm: cannot remove 'test': Permission denied
[guest@aachemodanova dir1]$
```

Рис. 3.2: Проверка при правах на директорию 300 и разных правах на файл

4 Выводы

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.