

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Чемоданова А.А.

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.

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

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

Рис. 1: Создание учетной записи guest

2. Задаю пароль для пользователя guest(использую учетную запись администратора) при помощи команды `passwd guest`.

```
[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: Пароль учетной записи guest

3. Вхожу в систему под от имени пользователя guest.

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

Рис. 3: Вход под учетной записью guest

4. Определяю директорию, в которой нахожусь. Директория не являлась домашней, перехожу в домашнюю директорию.

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

Рис. 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.

```
[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. 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.

```
guest@achemodanova:~$ 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:996:996: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:998:998:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-sos:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:50:50:Account used for Tls 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/none/missing:/sbin/nologin
cockpit-ws-instance:x:985:985:User for cockpit-ws instances/none/missing:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/usr/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevvis:x:983:982:Clevvis Decryption Framework unprivileged user:/var/cache/clevvis:/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
sddm:x:14:14:private:separated sbin:/usr/share/empty.sddm:/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
achemodanova:x:1000:1000:achemodanova:/home/achemodanova:/bin/bash
vboxadd:x:977:1:/var/run/vboxadd:/home/False
guest:x:1001:1001:/home/guest:/bin/bash
guest@achemodanova:~$
```

Рис. 6: Файл `/etc/passwd`

7. Определили существующие в системе директории командой `ls -l /home/`.

```
[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. 7: Команда `ls -l /home/`

8. Проверили, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой lsattr /home.

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

Рис. 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`.

```
[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. 9: Изменения каталога `dir1`

10. Попытались создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`. Не получилось.

```
[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. 10: Изменения файла test1

14. Заполним таблицу «Установленные права и разрешённые действия»

Права дирек- тории	Права файла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние файла	Смена дирек- тории	Про- смотр фай- лов в дирек- тории	Пере- имено- вание файла	Смена атри- бутов файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-

```
[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. 11: 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	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 поддиректории	d(300)	(000)

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

Рис. 12: Проверка при правах на директорию 300 и разных правах на файл

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.