

Лабораторная работа №2

Основы информационной безопасности - Бекауов А.Т

Российский университет дружбы народов, Москва, Россия

Введение

Цель данной лабораторной 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

Выполнение лабораторной работы

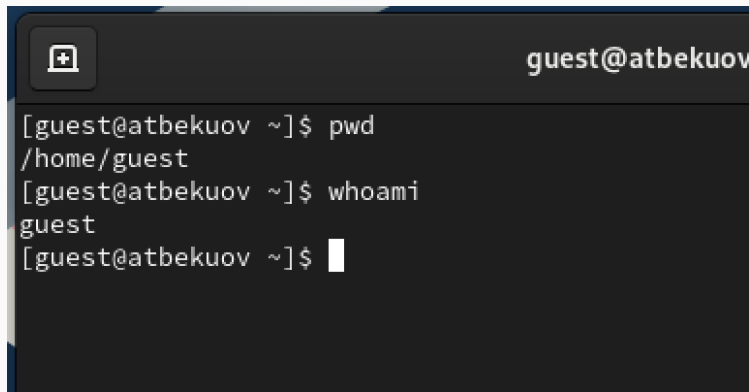
Создание пользователя guest

Первым делом создаю в учётную запись пользователя guest с помощью команды `sudo useradd guest` и введя `passwd guest` задаю пароль, для созданного пользователя

```
[atbekauov@atbekuov ~]$ sudo useradd guest1
[atbekauov@atbekuov ~]$ sudo passwd guest1
Changing password for user guest1.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[atbekauov@atbekuov ~]$
```

Проверка домашней директории и имени пользователя

Захожу под пользователем guest и ввожу в терминале команду pwd, чтобы определить нахожусь в домашней директории, затем ввожу whoami, чтобы убедиться, что я в пользователе guest



```
guest@atbekuov ~$ pwd
/home/guest
guest@atbekuov ~$ whoami
guest
guest@atbekuov ~$
```

Сравнение gid и groups, uid и имени

Далее ввожу команду `id`, получая `gid` (group id) и `uid` (user id). Сравниваю их с выводом команды `groups` и именем пользователя в приглашении командной строки

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

Далее просматриваю файл `/etc/passwd` командой `cat /etc/passwd`.

```
[guest@atbekuov ~]$ 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
```


Нахожу там пользователя guest и сравниваю информацию в нём с полученными uid и gid.

```
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@atbekuov ~]$
```

Поддиректории директории /home

С помощью команды `ls -l /home`, получаю список поддиректорий каталога `/home`. Вижу, что права доступа разрешают пользователю запись, чтение и исполнение, а группе и остальным - всё запрещено.

```
[guest@atbekuov ~]$ ls -l /home
total 8
drwx-----. 14 atbekauov atbekauov 4096 Mar  8 11:40 atbekauov
drwx-----. 14 guest      guest      4096 Mar  8 12:05 guest
[guest@atbekuov ~]$ lsattr /home
```

Вывод команды lsattr /home

С помощью команды `lsattr /home` проверю, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`.

```
crnk ~$ cat /etc/passwd | grep guest | cut -d: -f1,7 | xargs -n1 lsattr -l
[guest@atbekuov ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/atbekauov
----- /home/guest
```

Создание папки dir1

Командой `mkdir` создаю директорию `dir1` в домашнем каталоге `guest`.

```
[guest@atbekuov ~]$ mkdir dir1
[guest@atbekuov ~]$ ls
Desktop  dir1  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[guest@atbekuov ~]$
```

Права доступа к dir1

Введя команды `ls -l` и `lsattr`, определю права доступа к `dir1`.

```
[guest@atbekuov ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest 6 Mar 8 12:05 Desktop
drwxr-xr-x. 2 guest guest 6 Mar 8 12:16 dir1
drwxr-xr-x. 2 guest guest 6 Mar 8 12:05 Documents
drwxr-xr-x. 2 guest guest 6 Mar 8 12:05 Downloads
drwxr-xr-x. 2 guest guest 6 Mar 8 12:05 Music
drwxr-xr-x. 2 guest guest 4096 Mar 8 12:16 Pictures
drwxr-xr-x. 2 guest guest 6 Mar 8 12:05 Public
drwxr-xr-x. 2 guest guest 6 Mar 8 12:05 Templates
drwxr-xr-x. 2 guest guest 6 Mar 8 12:05 Videos
[guest@atbekuov ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@atbekuov ~]$
```

Изменение прав доступа к dir1

Сниму с директории dir1 все атрибуты командой `chmod`. Затем проверю изменения введя `ls -l`

```
[guest@atbekuov ~]$ chmod 000 dir1
[guest@atbekuov ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest    6 Mar  8 12:05 Desktop
d------. 2 guest guest    6 Mar  8 12:16 dir1
drwxr-xr-x. 2 guest guest    6 Mar  8 12:05 Documents
drwxr-xr-x. 2 guest guest    6 Mar  8 12:05 Downloads
drwxr-xr-x. 2 guest guest    6 Mar  8 12:05 Music
drwxr-xr-x. 2 guest guest 4096 Mar  8 12:18 Pictures
drwxr-xr-x. 2 guest guest    6 Mar  8 12:05 Public
drwxr-xr-x. 2 guest guest    6 Mar  8 12:05 Templates
drwxr-xr-x. 2 guest guest    6 Mar  8 12:05 Videos
[guest@atbekuov ~]$
```

Попытаюсь создать в директории dir1 файл file1. Получаю отказ, если заглянуть внутрь папки dir1, вижу что и файл file1 создан не был.

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

Таблица 1(1)

	A	B	C	D	E	F	G	H	I	J
1	Права директории	Права файла	Создание файла	Уда-ление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
2	d(000)	(000)	-	-	-	-	-	-	-	-
3	d(100)	(000)	-	-	-	-	+	-	-	+
4	d(200)	(000)	-	-	-	-	-	-	-	-
5	d(300)	(000)	+	+	-	-	+	-	+	+
6	d(400)	(000)	-	-	-	-	-	+	-	-
7	d(500)	(000)	-	-	-	-	+	+	-	+
8	d(600)	(000)	-	-	-	-	-	+	-	-
9	d(700)	(000)	+	+	-	-	+	+	+	+
10	d(000)	(100)	-	-	-	-	-	-	-	-
11	d(100)	(100)	-	-	-	-	+	-	-	+
12	d(200)	(100)	-	-	-	-	-	-	-	-
13	d(300)	(100)	+	+	-	-	+	-	+	+
14	d(400)	(100)	-	-	-	-	-	+	-	-
15	d(500)	(100)	-	-	-	-	+	+	-	+
16	d(600)	(100)	-	-	-	-	-	+	-	-
17	d(700)	(100)	+	+	-	-	+	+	+	+
18	d(000)	(200)	-	-	-	-	-	-	-	-
19	d(100)	(200)	-	-	+	-	+	-	-	+
20	d(200)	(200)	-	-	-	-	-	-	-	-
21	d(300)	(200)	+	+	+	-	+	-	+	+
22	d(400)	(200)	-	-	-	-	-	+	-	-
23	d(500)	(200)	-	-	+	-	+	+	-	+
24	d(600)	(200)	-	-	-	-	-	-	-	-
25	d(700)	(200)	+	+	+	-	+	+	+	+

Таблица 1(1)

	A	B	C	D	E	F	G	H	I	J
25	d(700)	(200)	+	+	+	-	+	+	+	+
26	d(000)	(300)	-	-	-	-	-	-	-	-
27	d(100)	(300)	-	-	-	-	-	-	-	-
28	d(200)	(300)	-	-	-	-	-	-	-	-
29	d(300)	(300)	+	+	+	-	+	-	+	+
30	d(400)	(300)	-	-	-	-	-	+	-	-
31	d(500)	(300)	-	-	+	-	+	+	-	+
32	d(600)	(300)	-	-	-	-	-	+	-	-
33	d(700)	(300)	+	+	+	-	+	+	+	+
34	d(000)	(400)	-	-	-	-	-	-	-	-
35	d(100)	(400)	-	-	-	+	+	-	-	+
36	d(200)	(400)	-	-	-	-	-	-	-	-
37	d(300)	(400)	+	+	-	+	+	-	+	+
38	d(400)	(400)	-	-	-	-	-	+	-	-
39	d(500)	(400)	-	-	-	+	+	+	-	+
40	d(600)	(400)	-	-	-	-	-	+	-	-
41	d(700)	(400)	+	+	-	+	+	+	+	+
42	d(000)	(500)	-	-	-	-	-	-	-	-
43	d(100)	(500)	-	-	-	+	+	-	-	+
44	d(200)	(500)	-	-	-	-	-	-	-	-
45	d(300)	(500)	+	+	-	+	+	-	+	+
46	d(400)	(500)	-	-	-	-	-	+	-	-
47	d(500)	(500)	-	-	-	+	+	+	-	+
48	d(600)	(500)	-	-	-	-	-	+	-	-
49	d(700)	(500)	+	+	-	+	+	+	+	+

Таблица 1(1)

	A	B	C	D	E	F	G	H	I	J
49	d(700)	(500)	+	+	-	+	+	+	+	+
50	d(000)	(600)	-	-	-	-	-	-	-	-
51	d(100)	(600)	-	-	+	+	+	-	-	+
52	d(200)	(600)	-	-	-	-	-	-	-	-
53	d(300)	(600)	+	+	+	+	+	-	+	+
54	d(400)	(600)	-	-	-	-	-	+	-	-
55	d(500)	(600)	-	-	+	+	+	+	-	+
56	d(600)	(600)	-	-	-	-	-	+	-	-
57	d(700)	(600)	+	+	+	+	+	+	+	+
58	d(000)	(700)	-	-	-	-	-	-	-	-
59	d(100)	(700)	-	-	+	+	+	-	-	+
60	d(200)	(700)	-	-	-	-	-	-	-	-
61	d(300)	(700)	+	+	-	+	+	-	+	+
62	d(400)	(700)	-	-	-	-	-	+	-	-
63	d(500)	(700)	-	-	+	+	+	+	-	+
64	d(600)	(700)	-	-	-	-	-	+	-	-
65	d(700)	(700)	+	+	+	+	+	+	+	+
66										
67										
68										
69										
70										
71										
72										
73										

Таблица 2

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

Заключение

В ходе данной лабораторной работы я получил практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux