

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Кадров Виктор Максимович

Содержание

1	Цель работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	7
4.1	Создание нового пользователя	7
4.2	Авторизация и проверка начальных значений	7
4.3	Просмотр файла /etc/passwd	8
4.4	Атрибуты /home	9
4.5	Эксперименты с атрибутами	10
5	Выводы	13

Список иллюстраций

4.1	Создание пользователя	7
4.2	Проверка начальных значений	8
4.3	Проверка начальных значений	8
4.4	/etc/passwd	9
4.5	/home и атрибуты	9
4.6	Изменение атрибутов	10
4.7	Эксперименты	11

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 Задание

1. Создание нового пользователя
2. Авторизация и проверка начальных значений
3. Просмотр файла `/etc/passwd`
4. Атрибуты `/home`
5. Эксперименты с атрибутами

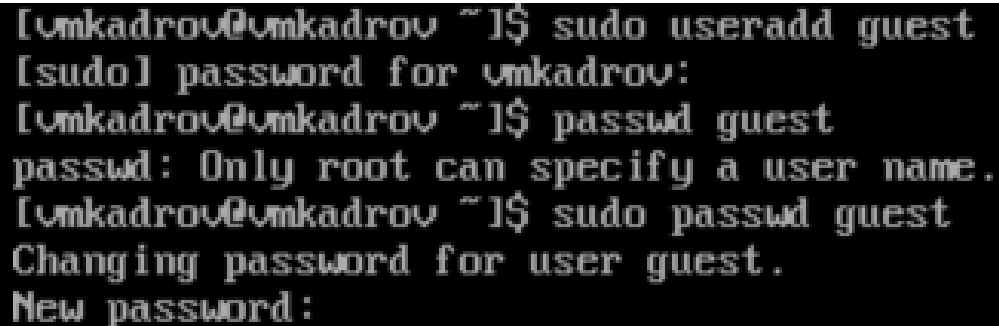
3 Теоретическое введение

Дискреционное (избирательное, контролируемое) разграничение доступа — управление доступом субъектов к объектам базируется на том, что пользователи в том или ином объеме могут управлять настройками политик безопасности. Наиболее популярной реализацией дискреционной модели является модель, которая реализует ограничение доступа к файлам и объектам межпроцессной коммуникации в обычных пользовательских представителях семейств операционных систем Unix и Windows. В этих реализациях пользователь может произвольно изменить права доступа к файлу, который он создал, например, сделать его общедоступным.

4 Выполнение лабораторной работы

4.1 Создание нового пользователя

Создадим пользователя *guest* при помощи команды **useadd** (рис. 4.1).

A terminal window with a black background and white text. The commands and their outputs are as follows:

```
[vmkadro@vmkadro ~]$ sudo useradd guest
[sudo] password for vmkadro:
[vmkadro@vmkadro ~]$ passwd guest
passwd: Only root can specify a user name.
[vmkadro@vmkadro ~]$ sudo passwd guest
Changing password for user guest.
New password:
```

Рис. 4.1: Создание пользователя

4.2 Авторизация и проверка начальных значений

Проверим директорию, в которой находимся и домашнюю директорию нового пользователя через *\$HOME* (рис. 4.2).

```
[vmkadrov@vmkadrov ~]$ su guest
Password:
[guest@vmkadrov vmkadrov]$ pwd
/home/vmkadrov
[guest@vmkadrov vmkadrov]$ echo $HOME
/home/guest
[guest@vmkadrov vmkadrov]$ _
```

Рис. 4.2: Проверка начальных значений

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

Рис. 4.3: Проверка начальных значений

4.3 Просмотр файла `/etc/passwd`

Прочитаем файл `/etc/passwd` и найдем там нового пользователя.


```

[guest@vmkadrov ~]$ whoami
guest
[guest@vmkadrov ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vmkadrov ~]$ groups
guest
[guest@vmkadrov ~]$ 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
tss:x:59:59:Account used for TPM access:/:usr/sbin/nologin
sssd:x:997:994:User for sssd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:996:993:chrony system user:/var/lib/chrony:/sbin/nologin
systemd-oom:x:991:991:systemd Userspace OOM Killer:/:usr/sbin/nologin
vmkadrov:x:1000:1000:vmkadrov:/home/vmkadrov:/bin/bash
guest:x:1001:1001:~/home/guest:/bin/bash
[guest@vmkadrov ~]$ _

```

Рис. 4.4: /etc/passwd

4.4 Атрибуты /home

Используем **lsattr** для проверки атрибутов доступа и расширенных атрибутов в /home (рис. 4.5).

```

[guest@vmkadrov ~]$ ls -l /home/
total 0
drwx-----. 2 guest    guest    62 Feb 19 18:43 guest
drwx-----. 2 vmkadrov vmkadrov 83 Feb 19 18:21 vmkadrov
[guest@vmkadrov ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/vmkadrov
----- /home/guest
[guest@vmkadrov ~]$

```

Рис. 4.5: /home и атрибуты

4.5 Эксперименты с атрибутами

Попробуем различные значения атрибутов доступа и запишем результаты в таблицу. Например, установим *000* на *./dir1* (рис. 4.6) и произведем различные действия (рис. 4.7).

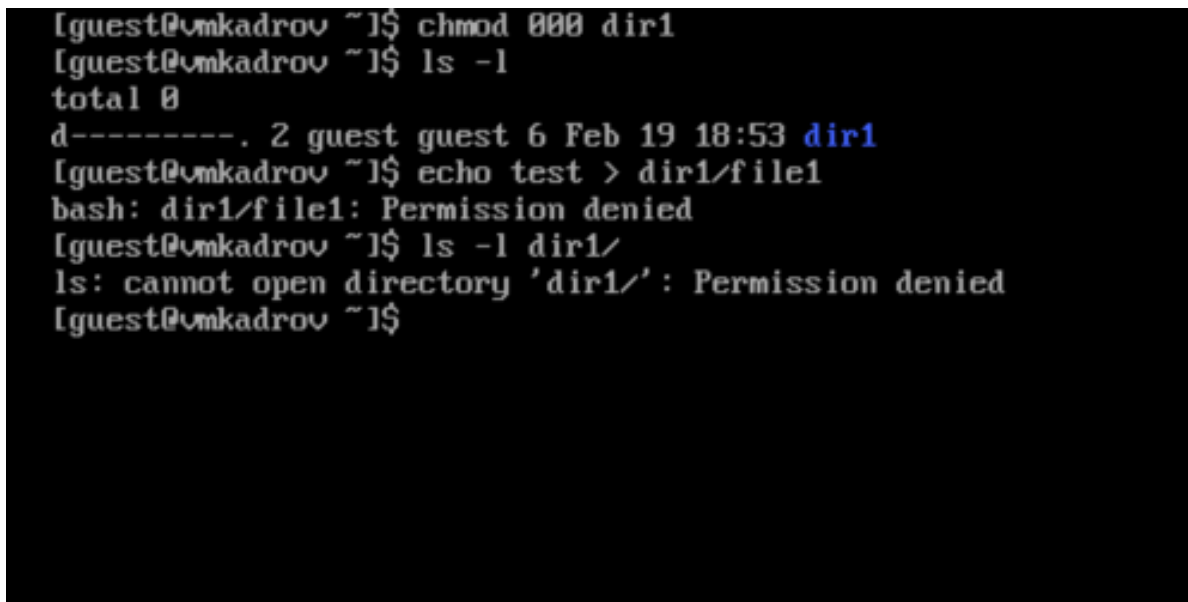
A terminal window with a black background and white text. The text shows a series of commands and their outputs. The first command is 'chmod 000 dir1'. The second is 'ls -l', which shows a directory listing for 'dir1' with permissions 'd-----'. The third command is 'echo test > dir1/file1', which results in a 'Permission denied' error. The fourth command is 'ls -l dir1/', which also results in a 'Permission denied' error. The prompt is '[guest@vmkadrov ~]\$'.

Рис. 4.6: Изменение атрибутов

```
[guest@vnmkadrov ~]$ echo test > dir1/file1
bash: dir1/file1: Permission denied
[guest@vnmkadrov ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@vnmkadrov ~]$ su root
Password:
[root@vnmkadrov guest]# cd dir1/
> ^C
[root@vnmkadrov guest]# cd dir1
[root@vnmkadrov dir1]# touch test_file
[root@vnmkadrov dir1]#
exit
[guest@vnmkadrov ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@vnmkadrov ~]$ rm dir1/test_file
rm: cannot remove 'dir1/test_file': Permission denied
[guest@vnmkadrov ~]$ echo "add" >> dir1/test_file
bash: dir1/test_file: Permission denied
[guest@vnmkadrov ~]$ cat dir1/test_file
cat: dir1/test_file: Permission denied
[guest@vnmkadrov ~]$ touch
.bash_logout .bash_profile .bashrc      dir1/
[guest@vnmkadrov ~]$ touch file
[guest@vnmkadrov ~]$ chmod 000 file
[guest@vnmkadrov ~]$ cat file
cat: file: Permission denied
[guest@vnmkadrov ~]$ cat file
cat: file: Permission denied
[guest@vnmkadrov ~]$ ls dir1/
ls: cannot open directory 'dir1/': Permission denied
[guest@vnmkadrov ~]$ mv file file_1
[guest@vnmkadrov ~]$ ls
dir1 file_1
[guest@vnmkadrov ~]$ ls -l
total 0
d-----, 2 guest guest 23 Feb 19 19:01 dir1
-----, 1 guest guest  8 Feb 19 19:03 file_1
[guest@vnmkadrov ~]$ chmod 100 dir1
[guest@vnmkadrov ~]$ chmod 100 file1
chmod: cannot access 'file1': No such file or directory
[guest@vnmkadrov ~]$ chmod 100 file_1
[guest@vnmkadrov ~]$
```

Рис. 4.7: Эксперименты

						Просмотр			
						фай-			
Права						Смена	лов в	Смена	
ди-						ди-	ди-	атри-	
рек-	Права	Создание	Удаление	Запись	Чтение	рек-	рек-	Переименование	блочно
то-	фай-	фай-	фай-	в	фай-	то-	то-	фай-	фай-
рии	ла	ла	ла	файл	ла	рии	рии	ла	ла
000	000	-	+	-	-	-	-	+	+
100	100	-	+	-	-	-	+	+	+
200	200	-	+	+	-	-	-	+	+

						Просмотр			
						фай-			
Права						Смена	лов в	Смена	
ди-						ди-	ди-	атри-	
рек-	Права	Создание	Удаление	Запись	Чтение	рек-	рек-	Переименование	создание
то-	фай-	фай-	фай-	в	фай-	то-	то-	фай-	фай-
рии	ла	ла	ла	файл	ла	рии	рии	ла	ла
300	300	-	+	+	-	+	-	+	+
400	400	-	+	-	+	-	+	+	+
500	500	-	+	-	+	+	+	+	+
600	600	-	+	+	+	-	+	+	+
700	700	+	+	+	+	+	+	+	+

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	200	200
Удаление файла	000	000
Чтение файла	400	400
Запись в файл	200	200
Переименование файла	000	000
Создание поддиректории	700	700
Удаление поддиректории	700	700

5 Выводы

В ходе лабораторной работы 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.