

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Парфенова Елизавета Евгеньевна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	18
	Список литературы	19

Список иллюстраций

3.1	Создание новой учетной записи guest	8
3.2	Задание пароля для новой учетной записи	8
3.3	Вывод команды pwd	9
3.4	Вывод команды whoami	9
3.5	Вывод команды id и groups	9
3.6	Содержимое файла /etc/passwd	10
3.7	Вывод команды cat /etc/passwd grep guest	10
3.8	Директории домашнего каталога	10
3.9	Расширенные атрибуты поддиректорий	11
3.10	Информация о правах и расширенных атрибутах dir1	11
3.11	Снятие всех атрибутов с команды dir1	12
3.12	Попытка создания файла	12

Список таблиц

2.1	Формат записи прав доступа системы GNU Linux	7
3.1	Установленные права и разрешённые действия	13
3.2	Минимальные права для совершения операций	16

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 Теоретическое введение

Права доступа в операционной системе Linux представляют собой ключевой элемент безопасности, определяющий, какой доступ имеют пользователи и программы к файлам и каталогам. Чтобы посмотреть права пользователя в Linux, необходимо воспользоваться следующей командой [1]:

```
ls -l
```

Изменить права доступа можно с помощью команды *chmod*. Основной синтаксис команды *chmod* выглядит следующим образом [2]:

```
chmod [опции]
```

Есть 3 вида разрешений. Они определяют права пользователя на 3 действия: чтение, запись и выполнение. В Linux эти действия обозначаются вот так:

- r — read (чтение) — право просматривать содержимое файла;
- w — write (запись) — право изменять содержимое файла;
- x — execute (выполнение) — право запускать файл, если это программа или скрипт.

У каждого файла есть 3 группы пользователей, для которых можно устанавливать права доступа.

- owner (владелец) — отдельный человек, который владеет файлом. Обычно это тот, кто создал файл, но владельцем можно сделать и кого-то другого.
- group (группа) — пользователи с общими заданными правами.
- others (другие) — все остальные пользователи, не относящиеся к группе и не являющиеся владельцами [3].

Существуют два основных способа записи прав доступа: символьный и числовой формат. Символьный формат использует читаемые буквы и символы для представления прав доступа, в то время как числовой формат использует числа в восьмеричной системе [1].

В табл. 2.1 приведено краткое описание стандартных каталогов Unix.

Таблица 2.1: Формат записи прав доступа системы GNU Linux

Права доступа	Символьный формат	Числовой формат
Чтение	r	4
Запись	w	2
Выполнение	x	1
Нет доступа	-	0

3 Выполнение лабораторной работы

Заходим в виртуальную машину Rocky Linux и с помощью команды *useradd guest* создаем новую учетную запись пользователя *guest*. Для этого также командой “su” заходим в систему от имени администратора, введя пароль. (рис. 3.1).

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

Рис. 3.1: Создание новой учетной записи *guest*

Далее задаем пароль командой *passwd guest*. Он должен быть не менее 8 символов. (рис. 3.2).

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

Рис. 3.2: Задание пароля для новой учетной записи

Затем выходим из системы с помощью *Log out* и заходим в новую учетную запись, вводя пароль. В консоли определяем директорию, в которой находимся, командой *pwd*. (рис. 3.3) Видим, что эта директория является нашей домашней директорией. Также проверяем это с помощью команды *cd ~* (переход в домашнюю директорию) и видим, что наше местоположение не меняется.


```
[guest@eeparfenova ~]$ pwd
/home/guest
```

Рис. 3.3: Вывод команды pwd

Командой *whoami* уточняем имя пользователя. Видим, что оно guest, как мы и задавали. (рис. 3.4)

```
/home/guest
[guest@eeparfenova ~]$ whoami
guest
```

Рис. 3.4: Вывод команды whoami

В выводе команды *id* видим, что имя нашего пользователя guest, его id = 1001 (uid), а также он входит в группу guest с таким же id (group). Далее введем команду *groups* и увидим наше имя пользователя - значит наш пользователь входит только в 1 группу, как и было указано выше. (рис. 3.5). Также видим, что имя пользователя в выводе *id* совпадает с приглашением командной строки.

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

Рис. 3.5: Вывод команды id и groups

Командой *cat /etc/passwd* посмотрим файл */etc/passwd* и найдем там свою учетную запись самой последней строкой. (рис. 3.6). Видим, что имя пользователя, а также uid и gid, равные 1001, совпадают с нашими прошлыми данными. Проверим, правильно ли мы все нашли, с помощью команды *cat /etc/passwd | grep guest* (рис. 3.7). Все оказалось верно

```
[guest@eeparfenova ~]$ 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:997:994:PipeWire System Daemon:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
design:x:983:982:Group for the design signing daemon:/run/design:/sbin/nologin
gnome-initial-setup:x:982:981:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
eeparfenova:x:1000:1000:eeparfenova:/home/eeparfenova:/bin/bash
vboxadd:x:979:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
```

Рис. 3.6: Содержимое файла /etc/passwd

```
[guest@eeparfenova ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/home/guest:/bin/bash
```

Рис. 3.7: Вывод команды cat /etc/passwd | grep guest

Командой `ls -l /home/` определим все существующие в домашнем каталоге директории. Поддиректориями являются guest и eeparfenova (рис. 3.8). Владелец директорий имеет право на чтение, запись и выполнение (изменение), остальные не могут ничего.

```
[guest@eeparfenova ~]$ ls -l /home
total 8
drwx-----. 14 eeparfenova eeparfenova 4096 Sep 12 12:19 eeparfenova
drwx-----. 14 guest guest 4096 Sep 12 12:26 guest
```

Рис. 3.8: Директории домашнего каталога

Командой `lsattr /home` проверим расширенные атрибуты, установленные на поддиректориях /home. Видим, что на поддиректории guest не установлено никаких расширенных атрибутов, а информацию об этом на директории других пользователей (eeparfenova) мы увидеть не можем (рис. 3.9).

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

Рис. 3.9: Расширенные атрибуты поддиректорий

Командой *mkdir dir1* создаем новую директорию *dir1*. Командами *ls -l* и *lsattr* видим, что владелец имеет право на чтение, запись и изменения (то есть все права), а для остальных доступно только чтение и не доступно внесение изменений. А по выводу второй команды видим, что никаких расширенных атрибутов не установлено (рис. 3.10).

```
[guest@eeparfenova ~]$ mkdir dir1
[guest@eeparfenova ~]$ ls
Desktop dir1 Documents Downloads Music Pictures Public Templates Videos
[guest@eeparfenova ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest 6 Sep 12 12:20 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 12 12:35 dir1
drwxr-xr-x. 2 guest guest 6 Sep 12 12:20 Documents
drwxr-xr-x. 2 guest guest 38 Sep 12 12:24 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 12 12:20 Music
drwxr-xr-x. 2 guest guest 4096 Sep 12 12:33 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 12 12:20 Public
drwxr-xr-x. 2 guest guest 6 Sep 12 12:20 Templates
drwxr-xr-x. 2 guest guest 6 Sep 12 12:20 Videos
[guest@eeparfenova ~]$ lsattr /dir1
lsattr: No such file or directory while trying to stat /dir1
[guest@eeparfenova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
```

Рис. 3.10: Информация о правах и расширенных атрибутах *dir1*

Командой *chmod 000 dir1* снимаем все атрибуты с директории *dir1* и проверяем, получилось ли это командой *ls -l* (рис. 3.11). Все прошло корректно

```
[guest@eeparfenova ~]$ chmod 000 dir1
[guest@eeparfenova ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest    6 Sep 12 12:20 Desktop
d------. 2 guest guest    6 Sep 12 12:35 dir1
drwxr-xr-x. 2 guest guest    6 Sep 12 12:20 Documents
drwxr-xr-x. 2 guest guest   38 Sep 12 12:24 Downloads
drwxr-xr-x. 2 guest guest    6 Sep 12 12:20 Music
drwxr-xr-x. 2 guest guest 4096 Sep 12 12:38 Pictures
drwxr-xr-x. 2 guest guest    6 Sep 12 12:20 Public
drwxr-xr-x. 2 guest guest    6 Sep 12 12:20 Templates
drwxr-xr-x. 2 guest guest    6 Sep 12 12:20 Videos
```

Рис. 3.11: Снятие всех атрибутов с команды dir1

Командой `echo "test" > /home/guest/dir1/file1` создаем в директории dir1 файл file1, однако получаем отказ в операции, так как с директории dir1 сняты абсолютно все атрибуты и мы не имеем никаких прав в ней. Отказ в операции не создал файл внутри директории (так как и на это у нас нет парва), однако проверить это с помощью `ls -l /home/guest/dir1` мы также не можем, так как атрибут на просмотр директории также снят (у нас нет на это прав) (рис. 3.12)

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

Рис. 3.12: Попытка создания файла

Далее заполним таблицу «Установленные права и разрешённые действия» опытным путем. Получившаяся таблица 3.1

Таблица 3.1: Установленные права и разрешённые действия

Права директории	Права файла	Про-							
		Сме-	смотр	Пе-	Сме-	фай-	ре-	на	Сме-
		на	лов в	име-	на	лов в	име-	на	на
		ди-	ди-	нова-	ди-	ди-	нова-	атри-	бу-
		рек-	рек-	ние	рек-	рек-	ние	тов	тов
фай-	фай-	то-	то-	фай-	то-	то-	фай-	фай-	фай-
ла	ла	рии	рии	ла	рии	рии	ла	ла	ла
d(000)	(000)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(000)	(100)	-	-	-	-	-	-	-	-
d(100)	(100)	-	-	-	-	+	-	-	+
d(200)	(100)	-	-	-	-	-	-	-	-
d(300)	(100)	+	+	-	-	+	-	+	+
d(400)	(100)	-	-	-	-	-	+	-	-
d(500)	(100)	-	-	-	-	+	+	-	+
d(600)	(100)	-	-	-	-	-	+	-	-
d(700)	(100)	+	+	-	-	+	+	+	+
d(000)	(200)	-	-	-	-	-	-	-	-
d(100)	(200)	-	-	+	-	+	-	-	+
d(200)	(200)	-	-	-	-	-	-	-	-

		Про-							
		смотр Пе- Сме-							
		на лов в име- на							
		Сме- фай- ре- на							
		на ди- рек- ди- нова- атри-							
		зд- ле- За- Чте- ди- ди- рек- рек- ние- бу-							
		ние ние пись ние рек- рек- ние тов							
Права	Права	См-	Уда-	За-	Чте-	Сме-	фай-	ре-	Сме-
директории	файла	фай-	фай-	в	фай-	то-	то-	фай-	фай-
		ла	ла	файл	ла	рии	рии	ла	ла
d(300)	(200)	+	+	+	-	+	-	+	+
d(400)	(200)	-	-	-	-	-	+	-	-
d(500)	(200)	-	-	+	-	+	+	-	+
d(600)	(200)	-	-	-	-	-	+	-	-
d(700)	(200)	+	+	+	-	+	+	+	+
d(000)	(300)	-	-	-	-	-	-	-	-
d(100)	(300)	-	-	-	-	+	-	-	+
d(200)	(300)	-	-	-	-	-	-	-	-
d(300)	(300)	+	+	+	-	+	-	+	+
d(400)	(300)	-	-	-	-	-	+	-	-
d(500)	(300)	-	-	-	-	+	+	-	+
d(600)	(300)	-	-	-	-	-	+	-	-
d(700)	(300)	+	+	+	-	+	+	+	+
d(000)	(400)	-	-	-	-	-	-	-	-
d(100)	(400)	-	-	-	+	+	-	-	+
d(200)	(400)	-	-	-	-	-	-	-	-
d(300)	(400)	+	+	-	+	+	-	+	+
d(400)	(400)	-	-	-	-	-	+	-	-
d(500)	(400)	-	-	-	-	+	+	-	+
d(600)	(400)	-	-	-	-	-	+	-	-
d(700)	(400)	+	+	-	+	+	+	+	+

		Про-							
		смотр							
		Пе-							
		Сме-							
		на							
		лов в							
		име-							
		атри-							
		бу-							
		тов							
Права	Права	Со-	Уда-			Сме-	фай-	ре-	на
директории	файла	зда-	ле-	За-	Чте-	ди-	ди-	нова-	бу-
		ние	ние	пись	ние	рек-	рек-	ние	тов
		фай-	фай-	в	фай-	то-	то-	фай-	фай-
		ла	ла	файл	ла	рии	рии	ла	ла
d(000)	(500)	-	-	-	-	-	-	-	-
d(100)	(500)	-	-	-	-	+	-	-	+
d(200)	(500)	-	-	-	-	-	-	-	-
d(300)	(500)	+	+	-	+	+	-	+	+
d(400)	(500)	-	-	-	-	-	+	-	-
d(500)	(500)	-	-	-	-	+	+	-	+
d(600)	(500)	-	-	-	-	-	+	-	-
d(700)	(500)	+	+	-	+	+	+	+	+
d(000)	(600)	-	-	-	-	-	-	-	-
d(100)	(600)	-	-	-	-	+	-	-	+
d(200)	(600)	-	-	-	-	-	-	-	-
d(300)	(600)	+	+	+	+	+	-	+	+
d(400)	(600)	-	-	-	-	-	+	-	-
d(500)	(600)	-	-	-	-	+	+	-	+
d(600)	(600)	-	-	-	-	-	+	-	-
d(700)	(600)	+	+	+	+	+	+	+	+
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(700)	-	-	-	-	+	-	-	+
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(700)	-	-	-	-	-	+	-	-

							Про-		
							смотр	Пе-	Сме-
							Сме-	фай-	на
		Со-	Уда-				на	лов в	атри-
		зда-	ле-	За-	Чте-	ди-	ди-	нове-	бу-
		ние	ние	пись	ние	рек-	рек-	ние	тов
Права	Права	фай-	фай-	в	фай-	то-	то-	фай-	фай-
директории	файла	ла	ла	файл	ла	рии	рии	ла	ла
d(500)	(700)	-	-	-	-	+	+	-	+
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(700)	+	+	+	+	+	+	+	+

На основе анализа уже заполненной таблицы заполним следующую таблицу, которая указывает на минимальные права для файла и директории для того или иного действия. Получившаяся таблица 3.2

Таблица 3.2: Минимальные права для совершения операций

	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)

Операция	Минимальные права на	
	директорию	Минимальные права на файл
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

4 Выводы

Мы 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.

Список литературы

1. Как дать права пользователю Linux: инструкция [Электронный ресурс]. ООО «ТАЙМВЭБ.КЛАУД», 2024. URL: <https://timeweb.cloud/tutorials/linux/kak-dat-prava-polzovatelyu-linux>.
2. Что делает команда chmod и как ее использовать в Linux [Электронный ресурс]. ООО «Селектел», 2024. URL: <https://selectel.ru/blog/tutorials/what-the-chmod-command-does-and-how-to-use-it-in-linux/>.
3. Права доступа в Linux [Электронный ресурс]. CodeChick.io, 2024. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.