

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Солдатов А. Е.

Содержание

1	Цель работы.....	2
2	Задание	2
3	Теоретическое введение	2
4	Выполнение лабораторной работы.....	2
4.1	Заполнение таблицы 2.1.....	6
4.2	Заполнение таблицы 2.2.....	8
5	Выводы	9
	Список литературы.....	9

Список иллюстраций

Рис. 1:	Создание пользователя.....	3
Рис. 2:	Вход за нового пользователя	3
Рис. 3:	pwd	3
Рис. 4:	whoami.....	3
Рис. 5:	id	4
Рис. 6:	Просмотр файла.....	4
Рис. 7:	Проверка директорий.....	4
Рис. 8:	Проверка атрибутов	5
Рис. 9:	Создание директории.....	5
Рис. 10:	Снятие атрибутов	5
Рис. 11:	Попытка.....	6
Рис. 12:	Выполнение команд	6

Список таблиц

Таблица 1:	Описание некоторых каталогов файловой системы GNU Linux	2
------------	---	---

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

Выполнить пункты лабораторной работы

3 Теоретическое введение

Здесь описываются теоретические аспекты, связанные с выполнением работы.

Например, в табл. 1 приведено краткое описание стандартных каталогов Unix.

Таблица 1: Описание некоторых каталогов файловой системы GNU Linux

Имя каталога	Описание каталога
/	Корневая директория, содержащая всю файловую
/bin	Основные системные утилиты, необходимые как в однопользовательском режиме, так и при обычной работе всем пользователям
/etc	Общесистемные конфигурационные файлы и файлы конфигурации установленных программ
/home	Содержит домашние директории пользователей, которые, в свою очередь, содержат персональные настройки и данные пользователя
/media	Точки монтирования для сменных носителей
/root	Домашняя директория пользователя root
/tmp	Временные файлы
/usr	Вторичная иерархия для данных пользователя

Более подробно про Unix см. в [1–4].

4 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя “guest” (используя учётную запись администратора) и задал для нее пароль (рис. 1).

```
[aesoldatov@aesoldatov ~]$ sudo useradd guest  
[sudo] password for aesoldatov:  
[aesoldatov@aesoldatov ~]$ sudo passwd guest  
Changing password for user guest.
```

Рис. 1: Создание пользователя

Вошел в систему от имени пользователя “guest”. (рис. 2).

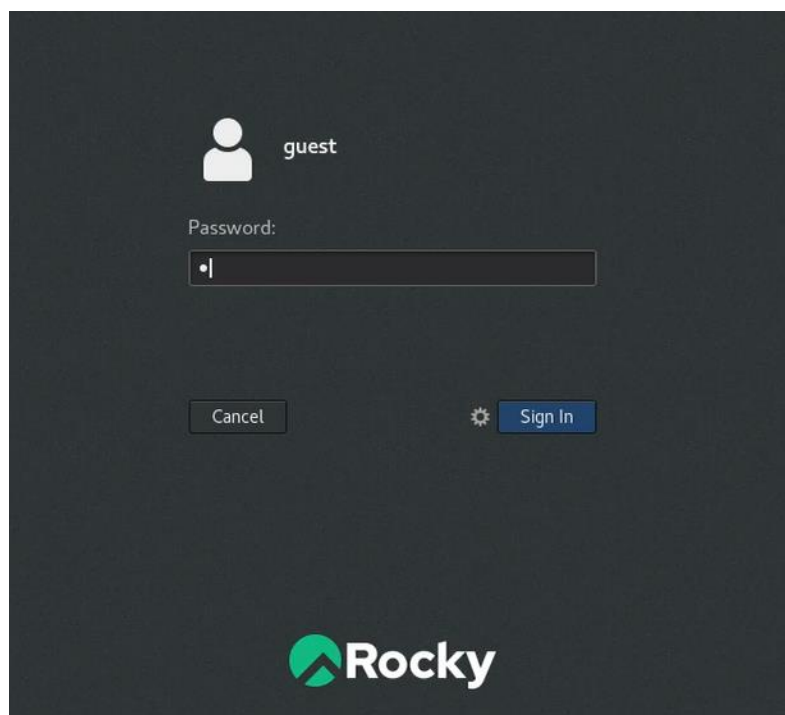


Рис. 2: Вход за нового пользователя

Определил директорию, в которой нахожусь, сравнил ее с приглашением командной строки и определил, является ли она моей домашней директорией. (рис. 3).

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

Рис. 3: pwd

Уточнил имя моего пользователя с помощью команды “whoami”. (рис. 4).

```
[guest@aesoldatov ~]$ whoami  
guest
```

Рис. 4: whoami

Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой “id” и сравнил вывод с командой “groups”. (рис. 5).

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

Рис. 5: id

Просмотрел файл “/etc/passwd” командой “cat /etc/passwd”, нашел в нём свою учётную запись и определил “uid” и “gid” пользователя. Потом сравнил найденные значения с полученными в предыдущих пунктах. (рис. 6).

```
[guest@aesoldatov ~]$ 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
dbus:x:81:81:System message bus:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/sbin/nologin
tss:x:59:59:Account used for TPM access:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
geoclue:x:997:995:User for geoclue:/var/lib/geoclue:/sbin/nologin
unbound:x:996:992:Unbound DNS resolver:/etc/unbound:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:995:991:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
dnsmasq:x:988:988:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
qemu:x:107:107:qemu user:/sbin/nologin
clevis:x:987:987:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/sbin/nologin
gluster:x:986:986:GlusterFS daemons:/run/gluster:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
chrony:x:985:985:/var/lib/chrony:/sbin/nologin
setroubleshoot:x:984:983:/var/lib/setroubleshoot:/sbin/nologin
saslauthd:x:983:76:Saslauthd user:/run/saslauthd:/sbin/nologin
libstoragemgmt:x:982:982:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
sssd:x:981:981:User for sssd:/sbin/nologin
cockpit-ws:x:980:979:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:979:978:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin
colord:x:977:976:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:976:975:/run/gnome-initial-setup:/sbin/nologin
pesign:x:975:974:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
aesoldatov:x:1000:1000:AESoldatov:/home/aesoldatov:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@aesoldatov ~]$
```

Рис. 6: Просмотр файла

Определил существующие в системе директории. (рис. 7).

```
[guest@aesoldatov ~]$ ls -l /home/
total 8
drwx-----. 17 aesoldatov aesoldatov 4096 map 7 12:51 aesoldatov
drwx-----. 15 guest      guest      4096 map 7 13:20 guest
[guest@aesoldatov ~]$
```

Рис. 7: Проверка директорий

Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории “/home”. (рис. 8).

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

Рис. 8: Проверка атрибутов

Создал в домашней директории поддиректорию “dir1” командой “mkdir dir1” и определил командами “ls -l” и “lsattr”, какие права доступа и расширенные атрибуты были выставлены на директорию “dir1”. (рис. 9).

```
[guest@aesoldatov ~]$ mkdir dir1
[guest@aesoldatov ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Desktop
drwxrwxr-x. 2 guest guest    6 map  7 13:36 dir1
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Documents
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Downloads
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Music
drwxr-xr-x. 2 guest guest 4096 map  7 13:36 Pictures
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Public
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Templates
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Videos
[guest@aesoldatov ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@aesoldatov ~]$
```

Рис. 9: Создание директории

Снял с директории “dir1” все атрибуты командой “chmod 000 dir1” и проверил с её помощью правильность выполнения команды “ls -l”. (рис. 10).

```
[guest@aesoldatov ~]$ chmod 000 dir1
[guest@aesoldatov ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Desktop
d----- . 2 guest guest    6 map  7 13:36 dir1
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Documents
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Downloads
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Music
drwxr-xr-x. 2 guest guest 4096 map  7 13:37 Pictures
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Public
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Templates
drwxr-xr-x. 2 guest guest    6 map  7 13:18 Videos
[guest@aesoldatov ~]$
```

Рис. 10: Снятие атрибутов

Попытался создать в директории “dir1” файл “file1” командой ‘echo “test” > /home/guest/dir1/file1’ и проверил командой “ls -l /home/guest/dir1” получилось ли создать файл. (рис. 11).

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

[guest@aesoldatov ~]$ chmod 700 dir1
[guest@aesoldatov ~]$ ls -l /home/guest/dir1
total 0
[guest@aesoldatov ~]$ █
```

Рис. 11: Попытка

Заполнил таблицу «Установленные права и разрешённые действия» выполняя разные действия с разными разрешениями системы. (рис. 12).

```
[guest@aesoldatov ~]$ touch dir1/file
[guest@aesoldatov ~]$ chmod 000 dir1
[guest@aesoldatov ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest 6 map 7 13:18 Desktop
d----- . 2 guest guest 18 map 7 14:05 dir1
drwxr-xr-x. 2 guest guest 6 map 7 13:18 Documents
drwxr-xr-x. 2 guest guest 6 map 7 13:18 Downloads
drwxr-xr-x. 2 guest guest 6 map 7 13:18 Music
drwxr-xr-x. 2 guest guest 4096 map 7 14:02 Pictures
drwxr-xr-x. 2 guest guest 6 map 7 13:18 Public
drwxr-xr-x. 2 guest guest 6 map 7 13:18 Templates
drwxr-xr-x. 2 guest guest 6 map 7 13:18 Videos
[guest@aesoldatov ~]$ rm dir1/file
rm: cannot remove 'dir1/file': Permission denied
[guest@aesoldatov ~]$ echo "file" > dir1/file
bash: dir1/file: Permission denied
[guest@aesoldatov ~]$ cat dir1/file
cat: dir1/file: Permission denied
[guest@aesoldatov ~]$ mv dir1/file
mv: missing destination file operand after 'dir1/file'
Try 'mv --help' for more information.
[guest@aesoldatov ~]$ mv dir1/file ~
mv: cannot stat 'dir1/file': Permission denied
[guest@aesoldatov ~]$ ls -l dir1
ls: cannot open directory 'dir1': Permission denied
[guest@aesoldatov ~]$ chmod 300 dir1/file
chmod: cannot access 'dir1/file': Permission denied
[guest@aesoldatov ~]$ █
```

Рис. 12: Выполнение команд

4.1 Заполнение таблицы 2.1

Права дирек тории	Права файла	Созда ние файла	Удале ние файла	Запис ь в файл	Чтени е файла	Смена дирек тории	Просм отр файло в в	Переи мено- вание файла	Смена атриб утов файла
-------------------------	----------------	-----------------------	-----------------------	----------------------	---------------------	-------------------------	------------------------------	----------------------------------	---------------------------------

							дирек тории		
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)	+	+	+	+	+	+	+	+

4.2 Заполнение таблицы 2.2

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)	-

5 Выводы

Получил практические навыки работы в консоли с атрибутами файлов и акрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.
2. Robbins A. Bash Pocket Reference. O'Reilly Media, 2016. 156 с.
3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
4. Newham C. [Learning the bash Shell: Unix Shell Programming](#). O'Reilly Media, 2005. 354 с.