

Лабораторная работа №2

Дисциплина: Операционные системы

Первойкин Илья Сергеевич

Содержание

Цель работы	5
Теоретические данные	6
Задание	7
Выполнение лабораторной работы	8
Выводы	15
Библиография	16

Список иллюстраций

1	Новый пользователь в Виртуальной машине	8
2	Захожу в систему от имени нового пользователя	9
3	Работа в домашнем каталоге	9
4	Команда id	9
5	Работа в содержимом файле /etc/passwd	10
6	Работа в содержимом файле /etc/passwd	10
7	Работа с каталогом /home	11
8	Новый каталог dir1	11
9	Меняем директорию dir1 атрибуты	12
10	Рассматриваем различные комбинации атрибутов файлов	12
11	Таблица 2.1 «Установленные права и разрешённые действия» . .	13
12	Таблица 2.1 «Установленные права и разрешённые действия» . .	14
13	Таблица 2.2 «Минимальные права для совершения операций» . .	14

Список таблиц

Цель работы

Цель данной лабораторной работы - получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Теоретические данные

Рассмотрим три параметра доступа для каждого файла в ОС Linux:

1.Чтение - разрешить доступ к получению содержимого файла, но записывать нельзя. Для каталога позволяет получить список файлов и каталогов, которые в нём располагаются;

2.Запись - разрешить записывать данные в файл или изменять уже имеющиеся. Также можно создавать и менять файлы и каталоги;

3.Выполнение - нельзя выполнить программу, если у неё нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система понимает, что этот файл нужно запустить как программу.

Атрибуты — это набор основных девяти битов, определяющих какие из пользователей обладают правами на чтение, запись и исполнение. Первые три бита отвечают права доступа владельца, вторые — для группы пользователей, последние — для всех остальных пользователей в системе.

Установка атрибутов производится командой `chmod`. Установка бита чтения (r) позволяет сделать файл доступным для чтения. Наличие бита записи (w) позволяет изменять файл. Установка бита запуска (x) позволяет запускать файл на исполнение.

Задание

1.Создать нового пользователя в Виртуальной машине, установить для него пароль. 2.Заполнить таблицу «Установленные права и разрешённые действия». 3.На основании предыдущей заполненной таблицы определить те или иные минимально необходимые права для выполнения операций внутри директории. Заполнить таблицу «Минимальные права для совершения операций».

Выполнение лабораторной работы

1). Создал нового пользователя guest командой useradd, затем установил для него пароль с помощью команды passwd guest.

```
[ispervoyjkin@localhost ~]$ su
Password:
[root@localhost ispersvoyjkin]# useradd guest
[root@localhost ispersvoyjkin]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ispersvoyjkin]#
```

Рис. 1: Новый пользователь в Виртуальной машине

2). Зашёл в систему от имени пользователя guest, используя только что придуманный пароль.

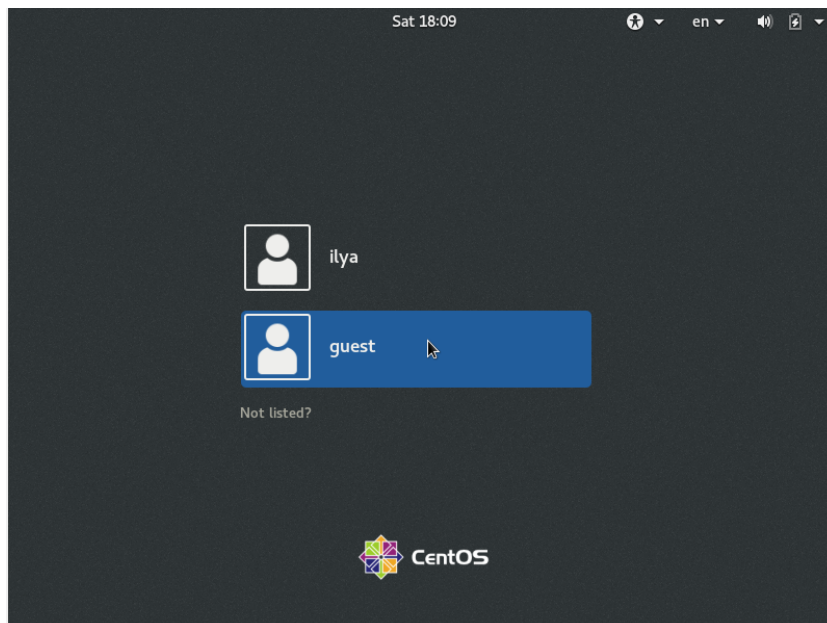


Рис. 2: Захожу в систему от имени нового пользователя

3). Выполнил команду `pwd`, которая показывает, что мы находимся в домашнем каталоге пользователя `guest`. Уточнил имя пользователя командой `whoami`, ожидаемо получаем вывод `guest`.

```
[guest@localhost ~]$ su guest
Password:
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$
```

Рис. 3: Работа в домашнем каталоге

4). С помощью команды `id` узнал, что `uid = 1001`, `gid = 1001` (`guest`), а также ввёл команду `groups` и убедился, что группа состоит из одного пользователя `guest`.

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

Рис. 4: Команда `id`

5). В содержимом файла /etc/passwd нашёл информацию о пользователе, что соответствует данным, полученным с помощью команды id и pwd.

```
[guest@localhost ~]$ 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:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:995:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:994:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sane:x:996:993:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
gluster:x:995:992:GlusterFS daemons:/run/gluster:/sbin/nologin
amandabackup:x:33:6:Amanda user:/var/lib/amanda:/bin/bash
```

Рис. 5: Работа в содержимом файле /etc/passwd

```
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:995:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:994:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sane:x:996:993:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
gluster:x:995:992:GlusterFS daemons:/run/gluster:/sbin/nologin
amandabackup:x:33:6:Amanda user:/var/lib/amanda:/bin/bash
sasauthd:x:994:76:Sasauthd user:/run/sasauthd:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
setroubleshoot:x:993:990:/:var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
chrony:x:992:987:/:var/lib/chrony:/sbin/nologin
unbound:x:991:986:Unbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
sssd:x:990:984:User for sssd:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:989:983:User for geoclue:/var/lib/geoclue:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gnome-initial-setup:x:988:982:/:run/gnome-initial-setup:/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
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
ispervoyjkin:x:1000:1000:ilya:/home/ispervoyjkin:/bin/bash
guest:x:1001:1001:/:home/guest:/bin/bash
[guest@localhost ~]$
```

Рис. 6: Работа в содержимом файле /etc/passwd

6). Определил содержимое каталога /home. С помощью команды ls -l /home/ я

убедился, что у меня есть домашние директории с их атрибутами `gwx` в первом бите для каждой. С помощью команды `lsattr /home` рассмотрел расширенные атрибуты текущего пользователя.

Список поддиректорий директории получить удалось. На директориях установлены права чтения, записи и выполнения для пользователя (для группы и остальных пользователей никаких прав доступа нет). Удалось увидеть расширенные атрибуты только директории того пользователя, от имени которого я нахожусь в системе.

```
[guest@localhost ~]$ ls -l /home/  
total 8  
drwx-----. 16 guest      guest      4096 Sep 16 18:11 guest  
drwx-----. 21 ispervoyjkin ispervoyjkin 4096 Sep 16 18:06 ispervoyjkin  
[guest@localhost ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/ispervoyjkin  
----- /home/guest  
[guest@localhost ~]$
```

Рис. 7: Работа с каталогом `/home`

7). Далее создал новый каталог `dir1` и увидел, что у него больше атрибутов по сравнению со стандартными директориями.

```
[guest@localhost ~]$ mkdir dir1  
[guest@localhost ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Desktop  
drwxrwxr-x. 2 guest guest 6 Sep 16 18:15 dir1  
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Music  
drwxr-xr-x. 2 guest guest 100 Sep 16 18:13 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Public  
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Videos  
[guest@localhost ~]$ lsattr  
----- ./Desktop  
----- ./Downloads  
----- ./Templates  
----- ./Public  
----- ./Documents  
----- ./Music  
----- ./Pictures  
----- ./Videos  
----- ./dir1  
[guest@localhost ~]$ █
```

Рис. 8: Новый каталог `dir1`

8). Поменял директории `dir1` атрибуты с помощью команды `chmod 000`. Далее, при попытке создать файл, выводится сообщение об ошибке, т.к. забрали права на всё у всех пользователей. Файл, соответственно, также не создаётся.

```
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Desktop
d------. 2 guest guest 6 Sep 16 18:15 dir1
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Music
drwxr-xr-x. 2 guest guest 147 Sep 16 18:15 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Videos
[guest@localhost ~]$
```

Рис. 9: Меняем директории dir1 атрибуты

9). Рассмотрим, как влияют различные комбинации атрибутов файлов и директории на различные действия. Для этого будем создавать файл “test”, запишем в него командой echo >, прочитаем файл командой cat, поменяем директорию командой cd, посмотрим директорию командой ls, а также переименуем файл командой rename и поменяем атрибуты командой chattr.

```
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@localhost ~]$ ls -l /home/guest/dir1/
ls: cannot open directory /home/guest/dir1/: Permission denied
[guest@localhost ~]$ chmod 700 dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Desktop
drwx-----. 2 guest guest 6 Sep 16 18:15 dir1
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Music
drwxr-xr-x. 2 guest guest 194 Sep 16 18:16 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 18:09 Videos
[guest@localhost ~]$ ls -l /home/guest/dir1/
total 0
[guest@localhost ~]$ cd dir1
[guest@localhost dir1]$ ls
[guest@localhost dir1]$ cd ../
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$
```

Рис. 10: Рассматриваем различные комбинации атрибутов файлов

Таблица «Установленные права и разрешённые действия».

Установленные права и разрешённые действия (таб. 2.1)

Права директори и	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директор ии	Просмот р файлов в директор ии	Переиме нование файла	Смена атрибуто в
d (000)	(000)	-	-	-	-	-	-	-	-
d -x (100)	(000)	-	-	-	-	+	-	-	-
d -w- (200)	(000)	-	-	-	-	-	-	-	-
d -wx (300)	(000)	+	+	-	-	+	-	+	-
dr- (400)	(000)	-	-	-	-	-	+	-	-
d r-x (500)	(000)	-	-	-	-	+	+	-	-
d rw- (600)	(000)	-	-	-	-	-	+	-	-
d rwx (700)	(000)	+	+	-	-	+	+	+	-
d (000)	(100)	-	-	-	-	-	-	-	-
d -x (100)	(100)	-	-	-	-	+	-	-	-
d -w- (200)	(100)	-	-	-	-	-	-	-	-
d -wx (300)	(100)	+	+	-	-	+	-	+	-
dr- (400)	(100)	-	-	-	-	-	+	-	-
d r-x (500)	(100)	-	-	-	-	+	+	-	-
d rw- (600)	(100)	-	-	-	-	-	+	-	-
d rwx (700)	(100)	+	+	-	-	+	+	+	-
d (000)	(200)	-	-	-	-	-	-	-	-
d -x (100)	(200)	-	-	+	-	+	-	-	-
d -w- (200)	(200)	-	-	-	-	-	-	-	-
d -wx (300)	(200)	+	+	+	-	+	-	+	-
dr- (400)	(200)	-	-	-	-	-	+	-	-
d r-x (500)	(200)	-	-	+	-	+	+	-	-
d rw- (600)	(200)	-	-	-	-	-	+	-	-
d rwx (700)	(200)	+	+	+	-	+	+	+	-
d (000)	(300)	-	-	-	-	-	-	-	-
d -x (100)	(300)	-	-	+	-	+	-	-	-
d -w- (200)	(300)	-	-	-	-	-	-	-	-
d -wx (300)	(300)	+	+	-	+	+	-	+	-
dr- (400)	(300)	-	-	-	-	-	+	-	-
d r-x (500)	(300)	-	-	+	-	+	+	-	-
d rw- (600)	(300)	-	-	-	-	-	+	-	-
d rwx (700)	(300)	+	+	+	-	+	+	+	-
d (000)	(400)	-	-	-	-	-	-	-	-
d -x (100)	(400)	-	-	-	+	+	-	-	+
d -w- (200)	(400)	-	-	-	-	-	-	-	-
d -wx (300)	(400)	+	+	-	+	+	-	+	+
dr- (400)	(400)	-	-	-	-	-	+	-	-
d r-x (500)	(400)	-	-	-	+	+	+	-	+
d rw- (600)	(400)	-	-	-	-	-	+	-	-
d rwx (700)	(400)	+	+	-	+	+	+	+	+
d (000)	(500)	-	-	-	-	-	-	-	-

Рис. 11: Таблица 2.1 «Установленные права и разрешённые действия»

d -x (100) (500)	-	-	-	+	+	-	-	+
d -w (200) (500)	-	-	-	-	-	-	-	-
d -wx (300) (500)	+	+	-	+	+	-	+	+
dr- (400) (500)	-	-	-	-	-	+	-	-
d r-x (500) (500)	-	-	-	+	+	+	-	+
d rw- (600) (500)	-	-	-	-	-	+	-	-
d rwx (700) (500)	+	+	-	+	+	+	+	+
d (000) (600)	-	-	-	-	-	-	-	-
d -x (100) (600)	-	-	+	+	+	-	-	+
d -w (200) (600)	-	-	-	-	-	-	-	-
d -wx (300) (600)	+	+	+	+	+	-	+	+
dr- (400) (600)	-	-	-	-	-	+	-	-
d r-x (500) (600)	-	-	+	+	+	+	-	+
d rw- (600) (600)	-	-	-	-	-	+	-	-
d rwx (700) (600)	+	+	+	+	+	+	+	+
d (000) (700)	-	-	-	-	-	-	-	-
d -x (100) (700)	-	-	+	+	+	-	-	+
d -w (200) (700)	-	-	-	-	-	-	-	-
d -wx (300) (700)	+	+	+	+	+	-	+	+
dr- (400) (700)	-	-	-	-	-	+	-	-
d r-x (500) (700)	-	-	+	+	+	+	-	+
d rw- (600) (700)	-	-	-	-	-	+	-	-
d rwx (700) (700)	+	+	+	+	+	+	+	+

Рис. 12: Таблица 2.1 «Установленные права и разрешённые действия»

10). Таблица «Минимальные права для совершения операций».

Минимальные права для совершения операция (таб. 2.2)		
Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d -wx (300)	(000)
Удаление файла	d -wx (300)	(000)
Чтение файла	d -x (100)	(400)
Запись в файл	d -x (100)	(200)
Переименование файла	d -wx (300)	(000)
Создание поддиректории	d -wx (300)	(000)
Удаление поддиректории	d -wx (300)	(000)

Рис. 13: Таблица 2.2 «Минимальные права для совершения операций»

Выводы

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.

Библиография

СПИСОК ЛИТЕРАТУРЫ

- 1.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>
- 2.Теоретические знания, приведённые в Лабораторной работе №2 - https://esystem.rudn.ru/pluginfile.php/2090123/mod_resource/content/6/002-lab_discret_attr.pdf
- 3.Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

- 1.[Электронный ресурс] - доступ: <https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux>
- 2.[Электронный ресурс] - доступ: <https://debianinstall.ru/diskretnoe-razgranichenie-dostupa-linux/>