

Лабораторная работа №3

Дисциплина: Основы информационной безопасности

Первойкин Илья Сергеевич

Содержание

Цель работы	5
Теоретические данные	6
Задание	8
Выполнение лабораторной работы	9
Выводы	14
Библиография	15

Список иллюстраций

1	Создание пользователя и установка пароля	9
2	Проверка групп	10
3	Команда <code>/etc/passwd</code>	10
4	Результат команды <code>/etc/passwd</code>	10
5	Регистрация пользователя в группе <code>group</code>	11
6	Смена атрибутов	11
7	Таблица 3.1 «Установленные права и разрешённые действия» . .	12
8	Таблица 3.1 «Установленные права и разрешённые действия» . .	13
9	Таблица 3.2 «Минимальные права для совершения операций» . .	13

Список таблиц

Цель работы

Цель данной лабораторной работы — Получить практические навыки работы в консоли с атрибутами файлов для групп пользователей.

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.

В ОС Linux, группа — это набор пользователей. Основная цель групп — это определить права на чтение, запись и исполнение сразу для нескольких пользователей, состоящих в группе. Так же пользователи могут быть добавлены в уже существующие группы для получения их прав.

Группы бывают двух видов:

- Первичная группа — это группа, приписанная к файлам, созданным пользователем. Обычно имя первичной группы совпадает с именем пользователя. У каждого пользователя может быть только одна первичная группа.
- Вторичная группа — используется для определения прав для набора пользователей. Пользователь может состоять в нескольких вторичных группах или не состоять ни в одной.

Задание

1. Создать нового пользователя в Виртуальной машине, установить для него пароль, чтобы можно было работать с двумя пользователями одновременно.
2. Заполнить таблицу «Установленные права и разрешённые действия» (см. табл. 3.1)
3. На основании заполненной таблицы 3.1 определить те или иные минимально необходимые права для выполнения операций внутри директории. Заполнить таблицу «Минимальные права для совершения операций» 3.2.

Выполнение лабораторной работы

1). Создал нового пользователя guest2 командой useradd, затем установил для него пароль с помощью команды passwd guest2.

```
[ispervoyjkin@localhost ~]$ su
Password:
[root@localhost ispersvoyjkin]# useradd guest2
[root@localhost ispersvoyjkin]# passwd guest2
Changing password for user guest2.
New password:
BAD PASSWORD: The password is shorter than 7 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ispersvoyjkin]# █
```

Рис. 1: Создание пользователя и установка пароля

2). Зашёл в систему от имени пользователей guest и guest2 на двух терминалах, используя команду su - и только что установленный пароль.

Выполнил команду pwd, которая показывает, что мы находимся в соответствующих домашних каталогах пользователей. Уточнил имя пользователя, используя команду whoami, получил вывод guest и guest2 соответственно. Определил группы для каждого пользователя, в которых состоят пользователи командой groups. Пользователь guest состоит только в группе guest, а пользователь guest2 состоит в двух группах — guest и guest2. Эту же информацию можно узнать с помощью команды id -Gn.

guest@localhost:/home/ispervoyjkin	guest2@localhost:/home/i
<pre>File Edit View Search Terminal Help [ispervoyjkin@localhost ~]\$ su Password: [root@localhost ispersvoyjkin]# useradd guest2 [root@localhost ispersvoyjkin]# passwd guest2 Changing password for user guest2. New password: BAD PASSWORD: The password is shorter than 7 characters Retype new password: passwd: all authentication tokens updated successfully. [root@localhost ispersvoyjkin]# su guest [guest@localhost ispersvoyjkin]\$ whoami guest [guest@localhost ispersvoyjkin]\$ groups guest guest : guest [guest@localhost ispersvoyjkin]\$ id -Gn guest guest [guest@localhost ispersvoyjkin]\$ id -G guest 1001 [guest@localhost ispersvoyjkin]\$</pre>	<pre>File Edit View Search Terminal Help [ispervoyjkin@localhost ~]\$ su guest2 Password: [guest2@localhost ispersvoyjkin]\$ whoami guest2 [guest2@localhost ispersvoyjkin]\$ groups guest2 guest2 : guest2 [guest2@localhost ispersvoyjkin]\$ id -Gn guest2 guest2 [guest2@localhost ispersvoyjkin]\$ id -G guest2 1002 [guest2@localhost ispersvoyjkin]\$</pre>

Рис. 2: Проверка групп

3). В содержимом файла /etc/passwd находим информацию о группах, в которых состоят пользователи, что соответствует данным, полученным с помощью команды id и groups. От имени пользователя guest2 выполнил регистрацию пользователя в группе командой newgrp.

```
[guest@localhost ispersvoyjkin]$ cat /etc/group
```

Рис. 3: Команда /etc/passwd

```
chrony:x:987:
unbound:x:986:
kvm:x:36:qemu
qemu:x:107:
tss:x:59:
libvirt:x:985:
sssd:x:984:
usbmuxd:x:113:
geoclue:x:983:
ntp:x:38:
gdm:x:42:
rpcuser:x:29:
nfsnobody:x:65534:
gnome-initial-setup:x:982:
sshd:x:74:
slocate:x:21:
avahi:x:70:
postdrop:x:90:
postfix:x:89:
tcpdump:x:72:
ispervoyjkin:x:1000:ispervoyjkin
guest:x:1001:
guest2:x:1002:
```

Рис. 4: Результат команды /etc/passwd

```

iservoyjkin:x:1000:iservoyjkin
guest:x:1001:
guest2:x:1002:
[guest@localhost iservoyjkin]$ chmod g+rw /home/guest
[guest@localhost iservoyjkin]$ chmod 000 /home/guest
[guest@localhost iservoyjkin]$ ls -l
ls: cannot open directory .: Permission denied
[guest@localhost iservoyjkin]$ pwd
/home/iservoyjkin
[guest@localhost iservoyjkin]$ cd ../guest
[guest@localhost ~]$ chmod g+rw /home/guest
[guest@localhost ~]$ chmod 000 /home/guest/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 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 ~]$

[iservoyjkin@localhost ~]$ su guest2
Password:
[guest2@localhost iservoyjkin]$ whoami
guest2
[guest2@localhost iservoyjkin]$ groups guest2
guest2 : guest2
[guest2@localhost iservoyjkin]$ id -Gn guest2
guest2
[guest2@localhost iservoyjkin]$ id -G guest2
1002
[guest2@localhost iservoyjkin]$ cd ../guest2
[guest2@localhost ~]$ su guest2
Password:
[guest2@localhost ~]$

```

Рис. 5: Регистрация пользователя в группе group

4). От имени пользователя guest изменил права на директорию /home/guest, чтобы пользователи в группе получили доступ к файлам в домашнем каталоге. Также меняю директорию dir1 атрибуты с помощью команды chmod 000. Далее проверяем изменения командой ls -l (рис. [-@fig:006]).

```

[guest2@localhost ~]$ newgrp guest
Password:

```

Рис. 6: Смена атрибутов

5). Далее решил изучить, как влияют различные комбинации атрибутов файлов и директории на различные действия. Для этого менял атрибуты файлов от имени пользователя guest командой chmod. А от имени пользователя guest2 пытался создать файл командой touch, удалить его командой rm, записать в файл командой echo >, прочитать файл командой cat, сменить директорию командой cd, просмотреть директорию командой ls, переименовать файл командой rename и сменить атрибуты командой chattr .

Все приведённые исследования отмечал в таблице (шаблон представлен в описании выполнения лабораторной работы №3). Успех отмечал +, в случае ошибки доступа записывал -

Все данные я внёс в таблицу 3.1 «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 (010)	(000)	-	-	-	-	+	-	-	-
d -w- (020)	(000)	-	-	-	-	-	-	-	-
d -wx (030)	(000)	+	+	-	-	+	-	+	-
dr- (040)	(000)	-	-	-	-	-	+	-	-
d r-x (050)	(000)	-	-	-	-	+	+	-	-
d rw- (060)	(000)	-	-	-	-	-	+	-	-
d rwx (070)	(000)	+	+	-	-	+	+	+	-
d (000)	(010)	-	-	-	-	-	-	-	-
d -x (010)	(010)	-	-	-	-	+	-	-	-
d -w- (020)	(010)	-	-	-	-	-	-	-	-
d -wx (030)	(010)	+	+	-	-	+	-	+	-
dr- (040)	(010)	-	-	-	-	-	+	-	-
d r-x (050)	(010)	-	-	-	-	+	+	-	-
d rw- (060)	(010)	-	-	-	-	-	+	-	-
d rwx (070)	(010)	+	+	-	-	+	+	+	-
d (000)	(020)	-	-	-	-	-	-	-	-
d -x (010)	(020)	-	-	+	-	+	-	-	-
d -w- (020)	(020)	-	-	-	-	-	-	-	-
d -wx (030)	(020)	+	+	+	-	+	-	+	-
dr- (040)	(020)	-	-	-	-	-	+	-	-
d r-x (050)	(020)	-	-	+	-	+	+	-	-
d rw- (060)	(020)	-	-	-	-	-	+	-	-
d rwx (070)	(020)	+	+	+	-	+	+	+	-
d (000)	(030)	-	-	-	-	-	-	-	-
d -x (010)	(030)	-	-	+	-	+	-	-	-
d -w- (020)	(030)	-	-	-	-	-	-	-	-
d -wx (030)	(030)	+	+	-	+	+	-	+	-
dr- (040)	(030)	-	-	-	-	-	+	-	-
d r-x (050)	(030)	-	-	+	-	+	+	-	-
d rw- (060)	(030)	-	-	-	-	-	+	-	-
d rwx (070)	(030)	+	+	+	-	+	+	+	-
d (000)	(040)	-	-	-	-	-	-	-	-
d -x (010)	(040)	-	-	-	+	+	-	-	-
d -w- (020)	(040)	-	-	-	-	-	-	-	-
d -wx (030)	(040)	+	+	-	+	+	-	+	-
dr- (040)	(040)	-	-	-	-	-	+	-	-
d r-x (050)	(040)	-	-	-	+	+	+	-	-
d rw- (060)	(040)	-	-	-	-	-	+	-	-
d rwx (070)	(040)	+	+	-	+	+	+	+	-
d (000)	(050)	-	-	-	-	-	-	-	-

Рис. 7: Таблица 3.1 «Установленные права и разрешённые действия»

d-x (010) (050)	-	-	-	+	+	-	-	-
d-w- (020) (050)	-	-	-	-	-	-	-	-
d-wx (030) (050)	+	+	-	+	+	-	+	-
dr- (040) (050)	-	-	-	-	-	+	-	-
d r-x (050) (050)	-	-	-	+	+	+	-	-
d rw- (060) (050)	-	-	-	-	-	+	-	-
d rwx (070) (050)	+	+	-	+	+	+	+	-
d (000) (060)	-	-	-	-	-	-	-	-
d-x (010) (060)	-	-	+	+	+	-	-	-
d-w- (020) (060)	-	-	-	-	-	-	-	-
d-wx (030) (060)	+	+	+	+	+	-	+	-
dr- (040) (060)	-	-	-	-	-	+	-	-
d r-x (050) (060)	-	-	+	+	+	+	-	-
d rw- (060) (060)	-	-	-	-	-	+	-	-
d rwx (070) (060)	+	+	+	+	+	+	+	-
d (000) (070)	-	-	-	-	-	-	-	-
d-x (010) (070)	-	-	+	+	+	-	-	-
d-w- (020) (070)	-	-	-	-	-	-	-	-
d-wx (030) (070)	+	+	+	+	+	-	+	-
dr- (040) (070)	-	-	-	-	-	+	-	-
d r-x (050) (070)	-	-	+	+	+	+	-	-
d rw- (060) (070)	-	-	-	-	-	+	-	-
d rwx (070) (070)	+	+	+	+	+	+	+	-

Рис. 8: Таблица 3.1 «Установленные права и разрешённые действия»

В сравнении с таблицей из Лабораторной работы №2 мы можем наблюдать, что изменилась только возможность изменять атрибуты файлов. Это связано с тем, что во всех комбинациях стоит 0 в начале, что означает отсутствие прав у владельца файла и директории. Остальные же действия доступны как владельцу, так и членам группы, в равной степени при должной конфигурации прав.

6). На основании этой таблицы я заполнил вторую таблицу (3.2) «Минимальные права для совершения операций». В данной таблице указал минимальные требования на права и директорию для выполнения тех или иных действий. Все данные я внёс в таблицу.

Минимальные права для совершения операция (таб. 2.2)

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx (030)	(000)
Удаление файла	d-wx (030)	(000)
Чтение файла	d-x (010)	(040)
Запись в файл	d-x (010)	(020)
Переименование файла	d-wx (030)	(000)
Создание поддиректории	d-wx (030)	(000)
Удаление поддиректории	d-wx (030)	(000)

Рис. 9: Таблица 3.2 «Минимальные права для совершения операций»

Выводы

Приобрёл практические навыки работы с атрибутами директорий и файлов в группе пользователей через консоль, выяснил минимальные требования и права для совершения различных действий над файлами и директориями.

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 №3 - https://esystem.rudn.ru/pluginfile.php/2090125/mod_resource/content/4/003-lab_discret_2users.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/>