

Лабораторная работа 2

Основы информационной безопасности

Тимофеева Екатерина Николаевна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Заполнение таблицы 2.1	12
5	Заполнение таблицы 2.2	15
6	Выводы	16
	Список литературы	17

Список иллюстраций

3.1	Выполнение 1-3 заданий	7
3.2	Выполнение 4-7 заданий	8
3.3	Выполнение 8 задания	9
3.4	Выполнение 9-11 заданий	10
3.5	Выполнение 12-13 заданий	11

Список таблиц

1 Цель 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

2 Теоретическое введение

Операционная система — то комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы.

3 Выполнение лабораторной работы

Атрибуты файлов

В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора): `useradd guest`

Задайте пароль для пользователя guest (используя учётную запись администратора): `passwd guest` Войдите в систему от имени пользователя guest. (рис. [3.1]).

```
[entimofeeva@entimofeeva ~]$ su
Password:
[root@entimofeeva entimofeeva]# useradd guest
useradd: user 'guest' already exists
[root@entimofeeva entimofeeva]# passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@entimofeeva entimofeeva]#
```

Рис. 3.1: Выполнение 1-3 заданий

Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию.

Уточните имя вашего пользователя командой `whoami`.

Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравните вывод `id` с выводом команды `groups`.

Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. (рис. [3.2]).

```
[guest@entimofeeva ~]$ pwd
/home/guest
[guest@entimofeeva ~]$ cd ~
[guest@entimofeeva ~]$ whoami
guest
[guest@entimofeeva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined
_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@entimofeeva ~]$ groups
guest
[guest@entimofeeva ~]$
```

Рис. 3.2: Выполнение 4-7 заданий

Просмотрите файл `/etc/passwd` командой `cat /etc/passwd`. Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах. (рис. [3.3]).


```
File Edit View Search Terminal Help
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
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/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/libsm:/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/sshd:/sbin/nologin
tcpdump:x:72:72:./:/sbin/nologin
entimofeeva:x:1000:1000:entimofeeva:/home/entimofeeva:/bin/bash
guest:x:1001:1001:./home/guest:/bin/bash
[guest@entimofeeva ~]$
```

Рис. 3.3: Выполнение 8 задания

Определите существующие в системе директории командой `ls -l /home/` Удалось ли вам получить список поддиректорий директории `/home`? Какие права установлены на директориях?

Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home` Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей?

Создайте в домашней директории поддиректорию `dir1` командой `mkdir dir1` Определите командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`. (рис. [3.4]).

```

[guest@entimofeeva ~]$ ls -l /home/
total 8
drwx-----. 15 entimofeeva entimofeeva 4096 Feb 24 16:43 entimofeeva
drwx-----. 15 guest      guest      4096 Feb 24 17:05 guest
[guest@entimofeeva ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/entimofeeva
----- /home/guest
[guest@entimofeeva ~]$ mkdir dir1
[guest@entimofeeva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Desktop
drwxrwxr-x. 2 guest guest 6 Feb 24 17:26 dir1
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Documents
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Music
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Public
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Templates
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Videos
[guest@entimofeeva ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@entimofeeva ~]$ chmod 000 dir1

```

Рис. 3.4: Выполнение 9-11 заданий

Снимите с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l`

Попытайтесь создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1` Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой `ls -l /home/guest/dir1` действительно ли файл `file1` не находится внутри директории `dir1`. (рис. [3.5]).

```
./dir1
[guest@entimofeeva ~]$ chmod 000 dir1
[guest@entimofeeva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Desktop
d------. 2 guest guest 6 Feb 24 17:26 dir1
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Documents
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Music
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Public
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Templates
drwxr-xr-x. 2 guest guest 6 Feb 24 16:55 Videos
[guest@entimofeeva ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@entimofeeva ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@entimofeeva ~]$
```

Рис. 3.5: Выполнение 12-13 заданий

Заполните таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

4 Заполнение таблицы 2.1

Права ди- ректо- рии	Права файла	Со- зда- ние файла	Уда- ление файла	За- пись в файл	Чте- ние файла	Сме- на ди- ректо- рии	Про- смотр фай- лов в ди- ректо- рии	Переиме- нование файла	Сме- на атри- бутов файла
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)	+	+	+	+	+	+	+	+

Таблица 2.1 «Установленные права и разрешённые действия»

5 Заполнение таблицы 2.2

На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполните табл. 2.2.

Операция	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)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

Таблица 2.2 “Минимальные права для совершения операций”

6 Выводы

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

Список литературы

Операционные системы: <https://blog.skillfactory.ru/glossary/operaczionnaya-sistema/>

Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>