

Лабораторная работа №2

Информационная безопасность

Банникова Екатерина Алексеевна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	12
	Список литературы	13

Список иллюстраций

3.1	Создание пользователя и установка пароля	7
3.2	Вход в систему пользователя guest1	7
3.3	Проверка данных пользователя	8
3.4	/etc/password	8
3.5	dir1(1)	9
3.6	dir1(2)	9
3.7	Снятие атрибутов	10
3.8	Права на действия	10
3.9	Права на действия	11
3.10	Минимальные права для совершения операций	11

Список таблиц

1 Цель работы

1. Получение практических навыков работы с атрибутами файлов.
2. Закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Теоретическое введение

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

3 Выполнение лабораторной работы

Создаем нового пользователя guest1 командой useradd, затем устанавливаем для него пароль с помощью команды passwd guest1

```
[eabannikova@eabannikova ~]$ sudo useradd guest1
[eabannikova@eabannikova ~]$ sudo passwd guest1
Изменение пароля пользователя guest1.
Новый пароль :
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
```

Рис. 3.1: Создание пользователя и установка пароля

Заходим в систему от имени пользователя guest1, используя только что установленный пароль.

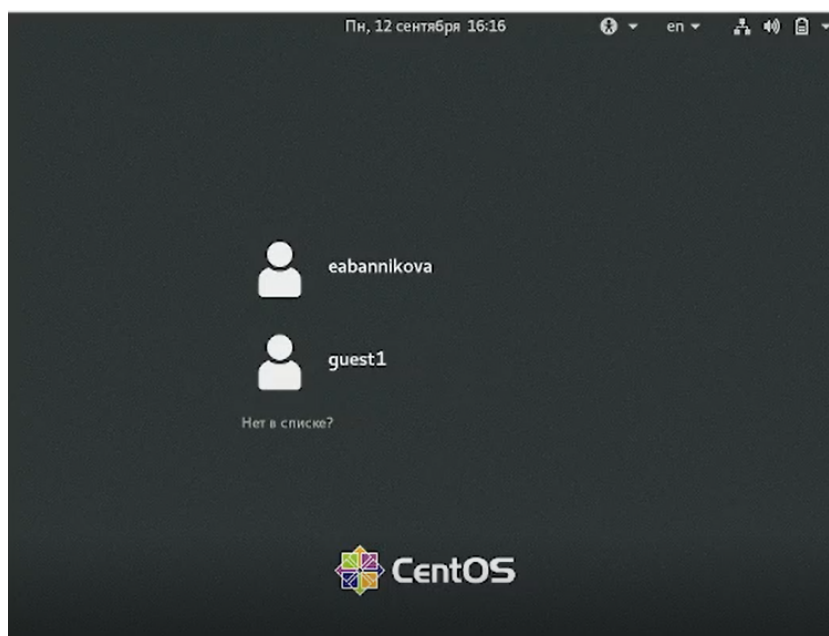


Рис. 3.2: Вход в систему пользователя guest1

Выполняем команду `pwd`, которая показывает, что мы находимся в домашнем каталоге пользователя `guest1`. Уточняем имя пользователя командой `whoami`, получаем вывод `guest1`. Уточняем имя пользователя, его группу, группы, куда входит пользователь, командой `id`. Вводим команду `groups`, видим, что группа состоит из одного пользователя `guest`, данные совпадают с командой `id`.

```
[guest1@eabannikova ~]$ pwd
/home/guest1
[guest1@eabannikova ~]$ whoami
guest1
[guest1@eabannikova ~]$ id
uid=1002(guest1) gid=1002(guest1) группы=1002(guest1) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest1@eabannikova ~]$ groups
bash: groups: команда не найдена...
gr[guest1@eabannikova ~]$
[guest1@eabannikova ~]$ groups
guest1
```

Рис. 3.3: Проверка данных пользователя

Посмотрим файл `/etc/passwd` командой `cat /etc/passwd`. Находим информацию о пользователе, что соответствует данным, полученным с помощью команды `id` и `pwd`.

```
[guest1@eabannikova ~]$ 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 by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
geoclue:x:997:995:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
qemu:x:107:107:qemu user:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/sbin/nologin
unbound:x:996:991:Unbound DNS resolver:/etc/unbound:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
gluster:x:995:990:GlusterFS daemons:/run/gluster:/sbin/nologin
```

Рис. 3.4: `/etc/passwd`

Определим содержимое каталога `/home`. С помощью команды `ls -l /home/` нам удалось получить список поддиректорий. У каждой из них установлены права на чтение, запись и выполнение только для самого пользователя. Проверяем

какие расширенные атрибуты уставновлены на поддиректориях, находящихся в директории /home, командоц lsattr /home. Нам удалось увидеть расширенные атрибуты директории, но не удалось увидеть расширенные атрибуты директорий других пользователей. Создадим в домашней директории поддиректорию dir1 командой mkdir dir1. Определим командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию.

```
[guest1@eabannikova ~]$ ls -l /home/
итого 8
drwx-----. 31 eabannikova eabannikova 4096 сен 12 15:47 eabannikova
drwx-----. 3 guest      guest      92 сен 12 16:12 guest
drwx-----. 15 guest1    guest1    4096 сен 12 16:17 guest1
[guest1@eabannikova ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/eabannikova
lsattr: Отказано в доступе While reading flags on /home/guest
----- /home/guest1
[guest1@eabannikova ~]$ mkdir dir1
[guest1@eabannikova ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest1 guest1 6 сен 12 16:28 dir1
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Видео
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Документы
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Загрузки
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Изображения
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Музыка
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Общедоступные
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 'Рабочий стол'
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Шаблоны
```

Рис. 3.5: dir1(1)

```
[guest1@eabannikova ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
```

Рис. 3.6: dir1(2)

Снимем с директории dir1 все атрибуты командой chmod 000 dir1 и проверим с ее помощью правильность выполненич командой ls -l. Попытаемся создать в директории dir1 файл file, но получим отказ от выполнения, так как шагом ранее сняли все атрибуты с директории. Проверим, действительно ли файл не создан.

```
[guest1@eabannikova ~]$ chmod 000 dir1
[guest1@eabannikova ~]$ ls -l
итого 0
d----- 2 guest1 guest1 6 сен 12 16:28 dir1
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Видео
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Документы
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Загрузки
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Изображения
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Музыка
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Общедоступные
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 'Рабочий стол'
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 Шаблоны
[guest1@eabannikova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest1@eabannikova ~]$ ls -l /home/guest/dir1
ls: невозможно получить доступ к '/home/guest/dir1': Отказано в доступе
[guest1@eabannikova ~]$
```

Рис. 3.7: Снятие атрибутов

Заполним таблицу “Установленные права и разрешенные действия”.

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименовывание файла	Смена атрибутов файла
d----- (000)	0	-	-	-	-	-	-	-	-
d--x----- (100)	0	-	-	-	-	+	-	-	+
d-w----- (200)	0	-	-	-	-	-	-	-	-
d-wx----- (300)	0	+	+	-	-	+	-	+	+
dr----- (400)	0	-	-	-	-	-	+	-	-
dr-x----- (500)	0	-	-	-	-	+	+	-	+
drw----- (600)	0	-	-	-	-	-	+	-	-
drwx----- (700)	0	+	+	-	-	+	+	+	+
d----- (000)	--x----- (100)	-	-	-	-	-	-	-	-
d--x----- (100)	--x----- (100)	-	-	-	-	+	-	-	+
d-w----- (200)	--x----- (100)	-	-	-	-	-	-	-	-
d-wx----- (300)	--x----- (100)	+	+	-	-	+	-	+	+
dr----- (400)	--x----- (100)	-	-	-	-	-	+	-	-
dr-x----- (500)	--x----- (100)	-	-	-	-	+	+	-	+
drw----- (600)	--x----- (100)	-	-	-	-	-	+	-	-
drwx----- (700)	--x----- (100)	+	+	-	-	+	+	+	+
d----- (000)	-w----- (200)	-	-	-	-	-	-	-	-
d--x----- (100)	-w----- (200)	-	-	+	-	+	-	-	+
d-w----- (200)	-w----- (200)	-	-	-	-	-	-	-	-
d-wx----- (300)	-w----- (200)	+	+	+	-	+	-	+	+
dr----- (400)	-w----- (200)	-	-	-	-	-	+	-	-
dr-x----- (500)	-w----- (200)	-	-	+	-	+	+	-	+
drw----- (600)	-w----- (200)	-	-	-	-	-	+	-	-
drwx----- (700)	-w----- (200)	+	+	+	-	+	+	+	+
d----- (000)	-wx----- (300)	-	-	-	-	-	-	-	-
d--x----- (100)	-wx----- (300)	-	-	+	-	+	-	-	+
d-w----- (200)	-wx----- (300)	-	-	-	-	-	-	-	-
d-wx----- (300)	-wx----- (300)	+	+	+	-	+	-	+	+
dr----- (400)	-wx----- (300)	-	-	-	-	-	+	-	-
dr-x----- (500)	-wx----- (300)	-	-	+	-	+	+	-	+
drw----- (600)	-wx----- (300)	-	-	-	-	-	+	-	-
drwx----- (700)	-wx----- (300)	+	+	+	-	+	+	+	+

Рис. 3.8: Права на действия

d----- (000)	r----- (400)	-	-	-	-	-	-	-	-
d-x----- (100)	r----- (400)	-	-	-	+	+	-	-	+
d-w----- (200)	r----- (400)	-	-	-	-	-	-	-	+
d-wx----- (300)	r----- (400)	+	+	-	+	+	-	+	+
d-r----- (400)	r----- (400)	-	-	-	-	-	+	-	-
d-rx----- (500)	r----- (400)	-	-	-	+	+	+	-	+
d-wr----- (600)	r----- (400)	-	-	-	-	-	+	-	-
d-wrx----- (700)	r----- (400)	+	+	-	+	+	+	+	+
d----- (000)	r-x----- (500)	-	-	-	-	-	-	-	-
d-x----- (100)	r-x----- (500)	-	-	-	+	+	-	-	+
d-w----- (200)	r-x----- (500)	-	-	-	-	-	-	-	-
d-wx----- (300)	r-x----- (500)	+	+	-	+	+	-	+	+
d-r----- (400)	r-x----- (500)	-	-	-	-	-	+	-	-
d-rx----- (500)	r-x----- (500)	-	-	-	+	+	+	-	+
d-wr----- (600)	r-x----- (500)	-	-	-	-	-	+	-	-
d-wrx----- (700)	r-x----- (500)	+	+	-	+	+	+	+	+
d----- (000)	rw----- (600)	-	-	-	-	-	-	-	-
d-x----- (100)	rw----- (600)	-	-	-	+	+	+	-	+
d-w----- (200)	rw----- (600)	-	-	-	-	-	-	-	-
d-wx----- (300)	rw----- (600)	+	+	+	+	+	-	+	+
d-r----- (400)	rw----- (600)	-	-	-	-	-	+	-	-
d-rx----- (500)	rw----- (600)	-	-	+	+	+	+	-	+
d-wr----- (600)	rw----- (600)	-	-	-	-	-	+	-	-
d-wrx----- (700)	rw----- (600)	+	+	+	+	+	+	+	+
d----- (000)	rx----- (700)	-	-	-	-	-	-	-	-
d-x----- (100)	rx----- (700)	-	-	-	+	+	-	-	+
d-w----- (200)	rx----- (700)	-	-	-	-	-	-	-	-
d-wx----- (300)	rx----- (700)	+	+	+	+	+	-	+	+
d-r----- (400)	rx----- (700)	-	-	-	-	-	+	-	-
d-rx----- (500)	rx----- (700)	-	-	-	+	+	+	-	+
d-wr----- (600)	rx----- (700)	-	-	-	-	-	+	-	-
d-wrx----- (700)	rx----- (700)	+	+	+	+	+	+	+	+

Рис. 3.9: Права на действия

Заполним таблицу “Минимальные права для совершения операций”.

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)	r----- (400)
Запись в файл	d--x----- (100)	-w----- (200)
Переименовывание файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

Рис. 3.10: Минимальные права для совершения операций

4 Выводы

Получила практические навыки работы в консоли атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы