

Лабораторная работа №2

Дисциплина: Основы информационной безопасности

Аветисян Давид Артурович

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	19
4	Список литературы	20

List of Figures

2.1	Создание нового пользователя	6
2.2	Вход от имени guest	6
2.3	Вход от имени guest	7
2.4	Команды, которые показывают информацию о пользователе . . .	7
2.5	Просмотр /etc/passwd	8
2.6	Команда grep - поиск по файлу	8
2.7	Директории в системе	9
2.8	Новая директория	10
2.9	Права на файл	10
2.10	Попытка создать файл	11
2.11	Проверка	11

List of Tables

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 Выполнение лабораторной работы

- 1) В прошлой лабораторной работе мы установили операционную систему Rocky Linux. С помощью команды `useradd guest` создаём в этой операционной системе ещё одного пользователя - `guest`. С помощью команды `passwd guest` устанавливаем пароль для пользователя `guest` (fig. 2.1). Перед всеми командами мы прописываем `sudo`, что даёт нам права суперпользователя.

```
[daavetisyan@daavetisyan lab02]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[daavetisyan@daavetisyan lab02]$ sudo useradd guest
[sudo] пароль для daavetisyan:
[daavetisyan@daavetisyan lab02]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[daavetisyan@daavetisyan lab02]$
```

Figure 2.1: Создание нового пользователя

- 2) Выходим из нашего пользователя и входим от имени пользователя `guest` (fig. 2.2, fig. 2.3).

```
[daavetisyan@daavetisyan lab02]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[daavetisyan@daavetisyan lab02]$ sudo useradd guest
[sudo] пароль для daavetisyan:
[daavetisyan@daavetisyan lab02]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[daavetisyan@daavetisyan lab02]$
```

Figure 2.2: Вход от имени guest

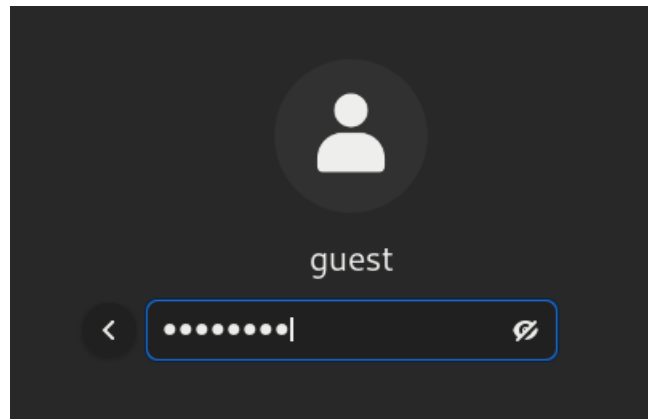


Figure 2.3: Вход от имени guest

- 3) Зашли от имени пользователя guest. Открыли терминал. Пишем команду `pwd`, которая покажет нам директорию, в которой мы находимся. Мы находимся в директории `/home/guest`. С приглашением командной строки совпадает. Мы находимся в домашней директории. С помощью команды `whoami` мы уточняем имя нашего пользователя. Имя - `guest`. Вывод команды `id` покажет нам имя пользователя, его группу, а также группы, куда входит пользователь (`uid`, `gid` и др.). Запомним вывод этой команды. Команда `groups` выводит нам группы, в которых мы состоим (fig. 2.4). Сравниваем полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. Они совпадают.

```
[guest@daavetisyan ~]$ pwd
/home/guest
[guest@daavetisyan ~]$ whoiam
bash: whoiam: command not found...
[guest@daavetisyan ~]$ whoami
guest
[guest@daavetisyan ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@daavetisyan ~]$ groups
guest
[guest@daavetisyan ~]$
```

Figure 2.4: Команды, которые показывают информацию о пользователе

- 4) Просматриваем файл `/etc/passwd` с помощью `cat` (fig. 2.5). Наш пользователь `guest` находится внизу списка. `uid` и `gid` пользователя совпадает с выводом

прошлых команд. Чтобы вывести только нашего пользователя guest, проще применить после команду grep, которая делает поиск по файлу (fig. 2.6).

```
[guest@daavetisyan ~]$ /etc/passwd
bash: /etc/passwd: Отказано в доступе
[guest@daavetisyan ~]$ 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
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:980:979::/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
daavetisyan:x:1000:1000:daavetisyan:/home/daavetisyan:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@daavetisyan ~]$
```

Figure 2.5: Просмотр /etc/passwd

```
[guest@daavetisyan ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
```

Figure 2.6: Команда grep - поиск по файлу

- 5) С помощью команды `ls -l /home/` смотрим директории в нашей системе. Видим две директории: одна гостевая (guest), другая моя (daavetisyan). Мне

удалось получить список поддиректорий директории /home. На директориях установлены права чтения, записи и выполнения для самого пользователя (для группы и остальных пользователей никаких прав доступа не установлено). С помощью команды `lsattr /home` посмотрим, какие расширенные атрибуты стоят на директориях (fig. 2.7). И мне сразу выдаёт, что у меня, как у гостя, нет таких прав.

```
[guest@daavetisyan ~]$ ls -l /home
итого 8
drwx-----. 16 daavetisyan daavetisyan 4096 сен 17 15:35 daavetisyan
drwx-----. 14 guest      guest      4096 сен 17 17:56 guest
[guest@daavetisyan ~]$ lsattr /home
bash: lsattr: command not found...
[guest@daavetisyan ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/daavetisyan
----- /home/guest
[guest@daavetisyan ~]$
```

Figure 2.7: Директории в системе

- 6) Создаём директорию `dir1` с помощью команды `mkdir`. С помощью команды `ls -l` посмотрим, какие права доступа и расширенные атрибуты были выставлены на директорию (fig. 2.8). Чтение, запись и выполнение доступны для самого пользователя и для группы, для остальных - только чтение и выполнение, расширенных атрибутов не установлено.

```

[guest@daavetisyan ~]$ ls
Видео  Документы  Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол'  Шаблоны
[guest@daavetisyan ~]$ mkdir dir1
[guest@daavetisyan ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 17 18:03 dir1
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Видео
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Документы
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Изображения
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Музыка
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Шаблоны
[guest@daavetisyan ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[guest@daavetisyan ~]$

```

Figure 2.8: Новая директория

- 7) Снимаем с директории dir1 все атрибуты командой `chmod`. И сразу же посмотрим, что изменилось с помощью команды `ls -l` (fig. 2.9). Как мы видим, мы убрали права с файла. А именно: чтение, запись и выполнение.

```

[guest@daavetisyan ~]$ chmod 000 dir1
[guest@daavetisyan ~]$ ls -l
итого 0
d-----. 2 guest guest 6 сен 17 18:03 dir1
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Видео
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Документы
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Загрузки
drwxr-xr-x. 2 guest guest 68 сен 17 18:04 Изображения
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Музыка
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 17 17:56 Шаблоны
[guest@daavetisyan ~]$

```

Figure 2.9: Права на файл

- 8) Пытаемся создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1` (fig. 2.10). Как мы видим, ничего не получается, так как в прошлом пункте мы забрали право на запись в директории.

Стоит отметить, что в саму директорию теперь зайти также нельзя, по той же причине. Чтобы убедиться в том, что файл не был создан, дадим право на чтение директории (fig. 2.11). Просмотрев директорию, мы не обнаруживаем там файла, который мы пытались создать.

```
[guest@daavetisyan ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@daavetisyan ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@daavetisyan ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@daavetisyan ~]$
```

Figure 2.10: Попытка создать файл

```
[guest@daavetisyan ~]$ chmod 700 dir1
[guest@daavetisyan ~]$ ls -l
итого 0
drwx-----. 2 guest guest  6 сен 17 18:03 dir1
drwxr-xr-x.  2 guest guest  6 сен 17 17:56 Видео
drwxr-xr-x.  2 guest guest  6 сен 17 17:56 Документы
drwxr-xr-x.  2 guest guest  6 сен 17 17:56 Загрузки
drwxr-xr-x.  2 guest guest 130 сен 17 18:05 Изображения
drwxr-xr-x.  2 guest guest  6 сен 17 17:56 Музыка
drwxr-xr-x.  2 guest guest  6 сен 17 17:56 Общедоступные
drwxr-xr-x.  2 guest guest  6 сен 17 17:56 'Рабочий стол'
drwxr-xr-x.  2 guest guest  6 сен 17 17:56 Шаблоны
[guest@daavetisyan ~]$ ls -l /home/guest/dir1
итого 0
[guest@daavetisyan ~]$
```

Figure 2.11: Проверка

9) Заполним таблицу “Установленные права и разрешённые действия”. Нужно заполнить 64 ячейки.

Создание файла: `echo "text" > /home/guest/dir1/file2`. Удаление файла: `rm -r /home/guest/dir1/file1`. Запись в файл: `echo "textnew" > /home/guest/dir1/file1`. Чтение файла: `cat /home/guest/dir1/file1`. Смена директории: `cd dir1`. Просмотр файлов в директории: `ls dir1`. Переименование файла: `mv /home/guest/dir1/file1 filenew`. Смена атрибутов файла: `chattr -a /home/guest/dir1/file1`.

Пра-ва		Со-зда-ние	Уда-ле-ние	За-пись	Чте-ние	Сме-на	Просмотр	Пере-имено-вание	Смена атрибу-тов
ди-рек-то-рии	Пра-ва	фай-ла	фай-ла	фай-ла	фай-ла	ди-рек-то-рии	файлов в директо-рии	файла	файла
d (000)	(000)	-	-	-	-	-	-	-	-
d -x (100)	(000)	-	-	-	-	+	-	-	-
d -w- (200)	(000)	-	-	-	-	-	-	-	-
d -wx (300)	(000)	+	+	-	-	+	-	+	-
d r- (400)	(000)	-	-	-	-	-	+	-	-
d r-x (500)	(000)	-	-	-	-	+	+	-	-
d rw- (600)	(000)	-	-	-	-	-	+	-	-
d rwx (700)	(000)	+	+	-	-	+	+	+	-
<hr/>									
d (000)	(100)	-	-	-	-	-	-	-	-
d -x (100)	(100)	-	-	-	-	+	-	-	-
d -w- (200)	(100)	-	-	-	-	-	-	-	-

Пра-ва		Со-зда-ние	Уда-ление	За-пись	Чте-ние	Сме-на	Просмотр	Пере-имено-вание	Смена атрибу-тов
ди-рек-то-рии	Пра-ва	фай-ла	фай-ла	фай-ла	в файл	фай-ла	то-рии	файлов в директо-рии	файла
d -wx (300)	(100)	+	+	-	-	+	-	+	-
d r- (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)	+	+	+	-	+	-	+	-
d r- (400)	(200)	-	-	-	-	-	+	-	-
d r-x (500)	(200)	-	-	+	-	+	+	-	-

Пра- ва	Пра-	Со- зда-	Уда- ле-	За- пись	Чте- ние	Сме- на	Просмотр	Пере-	Смена
ди- рек- то- рии	ва фай- ла	ние фай- ла	ние фай- ла	в файл	фай- ла	ди- рек- то- рии	файлов в директо- рии	имено- вание файла	атрибу- тов файла

d rw-	(200)	-	-	-	-	-	+	-	-
(600)									

d rwx	(200)	+	+	+	-	+	+	+	-
(700)									

d	(300)	-	-	-	-	-	-	-	-
(000)									

d -x	(300)	-	-	+	-	+	-	-	-
(100)									

d -w-	(300)	-	-	-	-	-	-	-	-
(200)									

d -wx	(300)	+	+	-	+	+	-	+	-
(300)									

d r-	(300)	-	-	-	-	-	+	-	-
(400)									

d r-x	(300)	-	-	+	-	+	+	-	-
(500)									

d rw-	(300)	-	-	-	-	-	+	-	-
(600)									

d rwx	(300)	+	+	+	-	+	+	+	-
(700)									

Пра- ва	Со- зда- ние	Уда- ние	За- пись	Чте- ние	Сме- на	Просмотр	Пере- имено- вание	Смена атрибу- тов
Пра- ва	Пра- ва	Пра- ва	Пра- ва	Пра- ва	Пра- ва	Пра- ва	Пра- ва	Пра- ва
ди- рек- то- рии	ди- рек- то- рии	ди- рек- то- рии	ди- рек- то- рии	ди- рек- то- рии	ди- рек- то- рии	ди- рек- то- рии	ди- рек- то- рии	ди- рек- то- рии
ла	ла	ла	ла	ла	ла	ла	ла	ла
d (000)	(400)	-	-	-	-	-	-	-
d -x (100)	(400)	-	-	-	+	+	-	+
d -w- (200)	(400)	-	-	-	-	-	-	-
d -wx (300)	(400)	+	+	-	+	+	-	+
d r- (400)	(400)	-	-	-	-	-	+	-
d r-x (500)	(400)	-	-	-	+	+	+	+
d rw- (600)	(400)	-	-	-	-	-	+	-
d rwx (700)	(400)	+	+	-	+	+	+	+
d (000)	(500)	-	-	-	-	-	-	-
d -x (100)	(500)	-	-	-	+	+	-	+
d -w- (200)	(500)	-	-	-	-	-	-	-

Пра- ва	Со- зда- ние	Уда- ние	За- пись	Чте- ние	Сме- на	Просмотр	Пере- имено- вание	Смена атрибу- тов
ди- рек- то- рии	Пра- ва фай- ла	зда- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	файлов в директо- рии	Смена атрибу- тов файла
d -wx (300)	(500)	+	+	-	+	+	-	+
d r- (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)	+	+	+	+	+	-	+
d r- (400)	(600)	-	-	-	-	-	+	-
d r-x (500)	(600)	-	-	+	+	+	+	+

Пра- ва	Пра-	Со- зда-	Уда- ле-	За- пись	Чте- ние	Сме- на	Просмотр	Пере-	Смена
ди- рек- то- рии	ва фай- ла	ние фай- ла	ние фай- ла	в файл	фай- ла	ди- рек- то- рии	файлов в директо- рии	имено- вание файла	атрибу- тов файла
d rw- (600)	(600)	-	-	-	-	-	+	-	-
d rwx (700)	(600)	+	+	+	+	+	+	+	+
d (000)	(700)	-	-	-	-	-	-	-	-
d -x (100)	(700)	-	-	+	+	+	-	-	+
d -w- (200)	(700)	-	-	-	-	-	-	-	-
d -wx (300)	(700)	+	+	+	+	+	-	+	+
d r- (400)	(700)	-	-	-	-	-	+	-	-
d r-x (500)	(700)	-	-	+	+	+	+	-	+
d rw- (600)	(700)	-	-	-	-	-	+	-	-
d rwx (700)	(700)	+	+	+	+	+	+	+	+

10) 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)	(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)

3 Выводы

Я 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.

4 Список литературы

- Права доступа к файлам в Linux [Электронный ресурс]. 2019. URL: <https://losst.ru/prava-dostupa-k-fajlam-v-linux>.