

Отчет по лабораторной работе №2

Информационная безопасность

Астафьева Анна Андреевна НПИбд-01-18

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	16

List of Figures

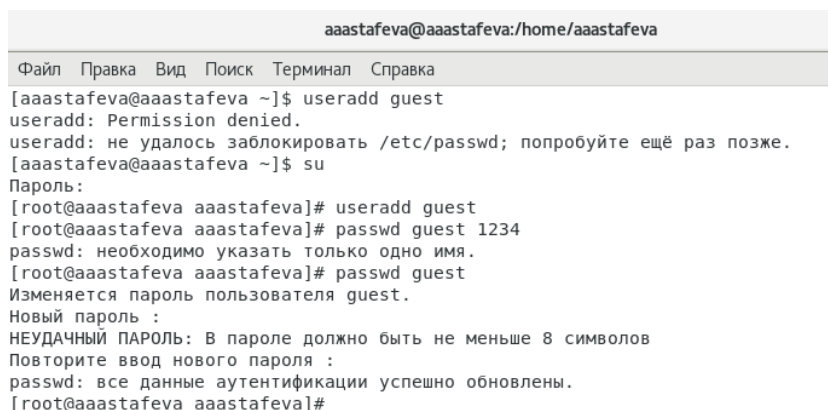
2.1	Создание учетной записи пользователя guest, создание пароля . .	5
2.2	Смена пользователя	5
2.3	Определение директории, уточнение имени	6
2.4	Уточнение информации о пользователе	6
2.5	Просмотр файла /etc/passwd	7
2.6	Определение существующих директорий	7
2.7	Проверка расширенных атрибутов	7
2.8	Домашняя поддиректория	8
2.9	Снятие атрибутов	8
2.10	Попытка создания файла	8
2.11	Папка dir1	8

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 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создала учетную запись пользователя guest (используя учетную запись администратора): `useradd guest`. Задала пароль для пользователя guest: `passwd guest` (рис. 2.1).



```
aaastafeva@aaastafeva:/home/aaastafeva
Файл Правка Вид Поиск Терминал Справка
[aaastafeva@aaastafeva ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[aaastafeva@aaastafeva ~]$ su
Пароль:
[root@aaastafeva aaastafeva]# useradd guest
[root@aaastafeva aaastafeva]# passwd guest 1234
passwd: необходимо указать только одно имя.
[root@aaastafeva aaastafeva]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@aaastafeva aaastafeva]#
```

Figure 2.1: Создание учетной записи пользователя guest, создание пароля

2. Вошла в систему от имени пользователя guest. (рис. 2.2).



```
[root@aaastafeva aaastafeva]# su - guest
```

Figure 2.2: Смена пользователя

3. Определила директорию, в которой нахожусь, командой `pwd`. Она является домашней директорией. Уточнила имя своего пользователя командой `whoami`. (рис. 2.3).

```
[guest@aaastafeva ~]$ pwd
/home/guest
[guest@aaastafeva ~]$ whoami
guest
[guest@aaastafeva ~]$ █
```

Figure 2.3: Определение директории, уточнение имени

4. Уточнила имя своего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомнила. Сравнила вывод `id` с выводом команды `groups`. (рис. 2.4).

```
[guest@aaastafeva ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:uncc
nconfined_t:s0-s0:c0.c1023
[guest@aaastafeva ~]$ groups
guest
[guest@aaastafeva ~]$ █
```

Figure 2.4: Уточнение информации о пользователе

Команда `groups` выводит имя пользователя.

5. Просмотрела файл `/etc/passwd` командой: `cat /etc/passwd` Нашла в нем свою учетную запись. Определила `uid` пользователя. Определила `gid` пользователя. Сравнила найденные значения с полученными в предыдущих пунктах. (Одинаковы). (рис. 2.5).

```

guest@aaastafeva:~
Файл Правка Вид Поиск Терминал Справка
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
chrony:x:993:988:./var/lib/chrony:/sbin/nologin
unbound:x:992:987: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:/d
sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
gluster:x:990:984:GlusterFS daemons:/run/gluster:/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:989:983:./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
ntp:x:38:38:./etc/ntp:/sbin/nologin
tcpdump:x:72:72:./:/sbin/nologin
aaastafeva:x:1000:1000:aaastafeva:/home/aaastafeva:/bin/bash
vboxadd:x:988:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
[guest@aaastafeva ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:./home/guest:/bin/bash
[guest@aaastafeva ~]$ █

```

Figure 2.5: Просмотр файла /etc/passwd

6. Определила существующие в системе директории командой: `ls -l /home/`. Список поддиректорий получить не удалось, на директориях для владельца установлены права на чтение, исполнение и запись, у пользователей групп и остальных пользователей прав нет. (рис. 2.6).

```

guest:x:1001:1001:./home/guest:/bin/bash
[guest@aaastafeva ~]$ ls -l /home/
итого 4
drwx-----. 15 aaastafeva aaastafeva 4096 окт  2 16:10 aaastafeva
drwx-----.  5 guest      guest      107 окт  2 16:25 guest
[guest@aaastafeva ~]$

```

Figure 2.6: Определение существующих директорий

7. Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home` Нам не удалось увидеть расширенные атрибуты директории и также расширенные атрибуты директорий других пользователей. (рис. 2.7).

```

[guest@aaastafeva ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/aaastafeva
----- /home/guest
[guest@aaastafeva ~]$ █

```

Figure 2.7: Проверка расширенных атрибутов

8. Создала в домашней директории поддиректорию `dir1` командой: `mkdir dir1`.
Определила командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1` (рис. 2.8).

```
[guest@aaastafeva ~]$ mkdir dir1
[guest@aaastafeva ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 окт  2 16:30 dir1
[guest@aaastafeva ~]$ lsattr
----- ./dir1
[guest@aaastafeva ~]$
```

Figure 2.8: Домашняя поддиректория

9. Сняла с директории `dir1` все атрибуты командой: `chmod 000 dir1` и проверила с ее помощью правильность выполнения команды `ls -l` (рис. 2.9).

```
----- ./dir1
[guest@aaastafeva ~]$ chmod 000 dir1
[guest@aaastafeva ~]$ ls -l
итого 0
d-----. 2 guest guest 6 окт  2 16:30 dir1
[guest@aaastafeva ~]$
```

Figure 2.9: Снятие атрибутов

10. Попыталась создать в директории `dir1` файл `file1` командой: `echo "test" > /home/guest/dir1/file1`. Мы получили отказ, так как сняли все атрибуты и не имеем никаких прав в директории `dir1`. Файл не создался. Проверила командой: `ls -l /home/guest/dir1` действительно ли файл `file1` не находится внутри директории `dir1` (рис. 2.10), (рис. 2.11).

```
[guest@aaastafeva ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Отказано в доступе
[guest@aaastafeva ~]$
```

Figure 2.10: Попытка создания файла

```
[guest@aaastafeva ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@aaastafeva ~]$
```

Figure 2.11: Папка `dir1`

11. Заполнила таблицу «Установленные права и разрешенные действия», выполняя действия от имени владельца директории (файлов), определив опытным путем, какие операции разрешены, а какие нет. Если операция разрешена, занесла в таблицу знак «+», если не разрешена, знак «-». (табл. 2.1)

Table 2.1: Установленные права и разрешённые действия

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

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

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d-w- (200)	r- (400)	-	-	-	-	-	-	-	-
d-w- (200)	r-x (500)	-	-	-	-	-	-	-	-
d-w- (200)	rw- (600)	-	-	-	-	-	-	-	-
d-w- (200)	rwX (700)	-	-	-	-	-	-	-	-
d-wX (300)	— (000)	+	+	-	-	+	-	+	+
d-wX (300)	-x (100)	+	+	-	-	+	-	+	+
d-wX (300)	-w- (200)	+	+	+	-	+	-	+	+
d-wX (300)	-wX (300)	+	+	+	-	+	-	+	+
d-wX (300)	r- (400)	+	+	-	+	+	-	+	+
d-wX (300)	r-x (500)	+	+	-	+	+	-	+	+
d-wX (300)	rw- (600)	+	+	+	+	+	-	+	+

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d-wx (300)	rwX (700)	+	+	+	+	+	-	+	+
dr- (400)	— (000)	-	-	-	-	-	+	-	-
dr- (400)	-X (100)	-	-	-	-	-	+	-	-
dr- (400)	-w- (200)	-	-	-	-	-	+	-	-
dr- (400)	-wx (300)	-	-	-	-	-	+	-	-
dr- (400)	r- (400)	-	-	-	-	-	+	-	-
dr- (400)	r-X (500)	-	-	-	-	-	+	-	-
dr- (400)	rw- (600)	-	-	-	-	-	+	-	-
dr- (400)	rwX (700)	-	-	-	-	-	+	-	-
dr-X (500)	— (000)	-	-	-	-	+	+	-	+
dr-X (500)	-X (100)	-	-	-	-	+	+	-	+

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
dr-x (500)	-w- (200)	-	-	+	-	+	+	-	+
dr-x (500)	-wx (300)	-	-	+	-	+	+	-	+
dr-x (500)	r- (400)	-	-	-	+	+	+	-	+
dr-x (500)	r-x (500)	-	-	-	+	+	+	-	+
dr-x (500)	rw- (600)	-	-	+	+	+	+	-	+
dr-x (500)	rwX (700)	-	-	+	+	+	+	-	+
drw- (600)	— (000)	-	-	-	-	-	+	-	-
drw- (600)	-x (100)	-	-	-	-	-	+	-	-
drw- (600)	-w- (200)	-	-	-	-	-	+	-	-
drw- (600)	-wx (300)	-	-	-	-	-	+	-	-
drw- (600)	r- (400)	-	-	-	-	-	+	-	-

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

12. На основании заполненной таблицы определила те или иные минимально

необходимые права для выполнения операций внутри директории dir1. (см. табл. 2.2).

Table 2.2: Минимальные права для совершения операций

Операция	Мин права на директорию	Мин права на файл
Создание файла	-wx (300)	— (000)
Удаление файла	-wx (300)	— (000)
Чтение файла	-x (100)	r- (400)
Запись в файл	-x (100)	-w- (200)
Переименование файла	-wx (300)	— (000)
Создание поддиректории	-wx (300)	— (000)
Удаление поддиректории	-wx (300)	— (000)

3 Выводы

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