

Лабораторная работа №3

Дисциплина: Информационная безопасность

Манаева Варвара Евгеньевна.

20 сентября 2023

Российский университет дружбы народов, Москва, Россия

Цели и задачи 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.

1. Создать двух новых пользователей (гостевых аккаунтов) виртуальной машины;
2. Через гостевые аккаунты выполнить задания лабораторной работы;
3. Заполнить таблицы об уровнях доступа и действиях с файлами/директориями.

Выполнение лабораторной работы

1. В установленной ОС создаю учётную запись пользователя guest

```
[vemanaeva@vemanaeva ~]$ sudo useradd guest  
[sudo] пароль для vemanaeva:
```

Рис. 1: Создание учетной записи пользователя guest

2. Задаём пароль для пользователя guest

```
[vemaanaeva@vemaanaeva ~]$ sudo passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 7 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[vemaanaeva@vemaanaeva ~]$
```

Рис. 2: адание пароля для пользователя guest

3. Аналогично пунктам 1 и 2 создаю пользователя guest2

```
[vemanaeva@vemanaeva ~]$ sudo adduser guest2
[vemanaeva@vemanaeva ~]$ sudo passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 7 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[vemanaeva@vemanaeva ~]$
```

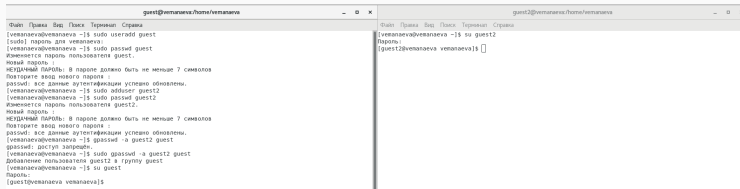
Рис. 3: Создание учетной записи пользователя guest2 и задание пароля

4. С помощью команды `gpasswd -a guest2 guest` добавляю пользователя `guest2` в группу `guest`

```
[vemanaeva@vemanaeva ~]$ gpasswd -a guest2 guest
gpasswd: доступ запрещён.
[vemanaeva@vemanaeva ~]$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
```

Рис. 4: Команда `gpasswd -a guest2 guest`

5. Захожу в две консоли, в каждую от разных пользователей (guest и guest2)

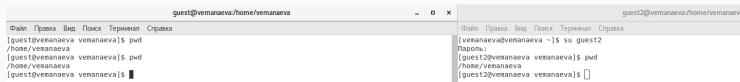


```
guest@venmanova:/home/venmanova
[venmanova@venmanova ~]$ sudo useradd guest
[sudo] пароль для venmanova:
[venmanova@venmanova ~]$ sudo passwd guest
Изменится пароль пользователя guest.
новый пароль :
ПЕРДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 7 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[venmanova@venmanova ~]$ sudo adduser guest2
[venmanova@venmanova ~]$ sudo passwd guest2
Изменится пароль пользователя guest2.
новый пароль :
ПЕРДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 7 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[venmanova@venmanova ~]$ sudo su guest2 guest
Добавление пользователя guest2 в группу guest
[venmanova@venmanova ~]$ su guest2
[guest2@venmanova: ~]$

guest2@venmanova:/home/venmanova
[venmanova@venmanova ~]$
```

Рис. 5: Две консоли

6. С помощью команды `pwd` определить, в какой директории находятся пользователи



The image shows two terminal windows side-by-side. The left window is titled 'guest@venanaeva:/home/venanaeva' and shows the following commands and output:

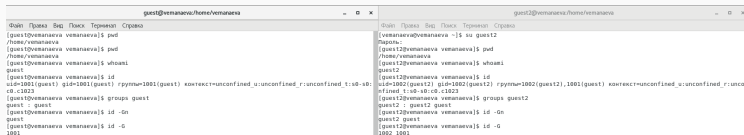
```
guest@venanaeva:/home/venanaeva$ pwd
/home/venanaeva
guest@venanaeva:/home/venanaeva$ pwd
/home/venanaeva
guest@venanaeva:/home/venanaeva$
```

The right window is titled 'guest2@venanaeva:/home/venanaeva' and shows the following commands and output:

```
guest2@venanaeva:/home/venanaeva$ su guest2
[venanaeva@venanaeva ~]$
Пароль:
[guest2@venanaeva venanaeva]$ pwd
/home/venanaeva
[guest2@venanaeva venanaeva]$
```

Рис. 6: В какой директории находятся пользователи?

7. Уточняю информацию о пользователях с помощью команды `id`, определяем группы с помощью команды `groups` для обоих пользователей. Сравнивая выводы команд `groups`, `id -Gn` и `id -G`



The image shows two terminal windows side-by-side. The left window is titled 'quest@vematnaeva/home/vematnaeva' and shows the following commands and output:

```
(quest@vematnaeva vematnaeva)$ pwd
/home/vematnaeva
(quest@vematnaeva vematnaeva)$ pwd
/home/vematnaeva
(quest@vematnaeva vematnaeva)$ whoami
quest
(quest@vematnaeva vematnaeva)$ id
uid=1001(quest) gid=1001(quest) rpytn=1001(quest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-c1023
(quest@vematnaeva vematnaeva)$ groups quest
quest : quest
(quest@vematnaeva vematnaeva)$ id -Gn
quest
(quest@vematnaeva vematnaeva)$ id -G
1001
```

The right window is titled 'quest2@vematnaeva/home/vematnaeva' and shows the following commands and output:

```
(vematnaeva@vematnaeva ~)$ su quest2
Пароль:
(quest2@vematnaeva vematnaeva)$ pwd
/home/vematnaeva
(quest2@vematnaeva vematnaeva)$ whoami
quest2
(quest2@vematnaeva vematnaeva)$ id
uid=1002(quest2) gid=1002(quest2) rpytn=1002(quest2),1001(quest) контекст=unconfined_u:unconfined_r:unco
nfinet_t:s0-s0:c0-c1023
(quest2@vematnaeva vematnaeva)$ groups quest2
quest2 : quest2 quest
(quest2@vematnaeva vematnaeva)$ id -Gn
quest2 quest
(quest2@vematnaeva vematnaeva)$ id -G
1002 1001
```

Рис. 7: Информация о пользователях

По результатам выполнения команд `id -G`, `id -Gn` и `groups` видно, что первая выводит только ID групп, в которых состоит пользователь, вторая — названия групп, в которых состоит пользователь, и третья выводит строку вида

```
<username> : <groupname> <groupname> <groupname> <groupname>
```

8. Сравниваем информацию о пользователях с содержанием файла /etc/group

```
[guest2@vemanaeva vemanaeva]$ cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
men:x:8:
kmem:x:9:
wheel:x:10:vemanaeva
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
stapusr:x:156:
stapusr:x:157:
stapdev:x:158:
input:x:999:
systemd-journal:x:190:
systemd-network:x:192:
dbus:x:81:
polkitd:x:998:
printadmin:x:997:
libstoragemgmt:x:996:
colord:x:995:
rpc:x:32:
sane:x:994:
dip:x:40:
cgred:x:993:
ssh keys:x:992:
saslauth:x:76:
abrt:x:173:
setroubleshoot:x:991:
rtkit:x:172:
```

```
pulse-access:x:990:
pulse-rt:x:989:
pulse:x:171:
radvd:x:75:
chrony:x:988:
unbound:x:987:
kvm:x:36:qemu
qemu:x:107:
tss:x:59:
libvirt:x:986:
usbmuxd:x:113:
geoclue:x:985:
gluster:x:984:
gdm:x:42:
rpcuser:x:29:
nfsnobody:x:65534:
gnome-initial-setup:x:983:
sshd:x:74:
slocate:x:21:
avahi:x:70:
postdrop:x:98:
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
vemanaeva:x:1000:vemanaeva
vboxsf:x:982:
vboxdrmpcs:x:981:
guest:x:1001:guest2
guest2:x:1002:
[guest2@vemanaeva vemanaeva]$
```

Рис. 9: Информация файла /etc/group, часть 2

Рис. 8: Информация файла /etc/group, часть 1

От имени пользователя `guest2` регистрируем этого пользователя в группе `guest` командой `newgrp guest`

```
[guest2@vemanaeva vemanaeva]$ groups guest2
guest2 : guest2 guest
[guest2@vemanaeva vemanaeva]$ id -Gn
guest2 guest
[guest2@vemanaeva vemanaeva]$ id -G
1002 1001
```

Пользователь `guest2` уже находится в группе `guest`!!!

Рис. 10: Регистрируем второго гостевого пользователя в группе `guest`

От имени пользователя `guest` разрешаем все действия для группы в папке `/home/guest`

```
[guest@vemanaeva vemanaeva]$ chmod g+rx /home/guest
```

Рис. 11: Команда `chmod g+rx /home/guest`

От имени пользователя `guest` снимаем все атрибуты с директории `/home/guest/dir1` командой `chmod 000 dir1`

```
[guest@vemanaeva vemanaeva]$ cd ~
[guest@vemanaeva ~]$ pwd
/home/guest
[guest@vemanaeva ~]$ mkdir dir1
[guest@vemanaeva ~]$ chmod 000 dir1
[guest@vemanaeva ~]$ chmod 700 dir1
[guest@vemanaeva ~]$ echo "test" >> dir1/file1
[guest@vemanaeva ~]$ cat dir1/file1
test
[guest@vemanaeva ~]$ chmod 000 dir1/file1
[guest@vemanaeva ~]$ chmod 000 dir1
[guest@vemanaeva ~]$ █
```

Рис. 12: Команда `chmod 000 dir1`

Заполняем таблицу «Установленные права и разрешённые действия»

Таблица 1: Отрывок из таблицы “Установленные права и разрешённые действия” {#tbl:access_1}

Права ди- ректории	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись фай- ла	Чте- ние фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d--wx—	(000)	+	+	-	-	+	-	+	-
d--wx—	(010)	+	+	-	-	+	-	+	-
d--wx—	(020)	+	+	+	-	+	-	+	-
d--wx—	(030)	+	+	+	-	+	-	+	-
d--wx—	(040)	+	+	-	+	+	-	+	+
d--wx—	(050)	+	+	-	+	+	-	+	+
d--wx—	(060)	+	+	+	+	+	-	+	+

На основании заполненной таблицы определяю те или иные минимально необходимые права для выполнения операций внутри директории `dir1`

Таблица 2: Минимальные права для совершения операций {#tbl:access_2}

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

Выводы по проделанной работе

В результате выполнения работы мы получили практические навыки работы в консоли с атрибутами файлов и закрепили теоретические основы дискреционного разграничения доступа в современных системах на базе ОС Linux.

Были записаны скринкасты выполнения и защиты лабораторной работы.