

Лабораторная работа №2

Дисциплина: Информационная безопасность

Манаева Варвара Евгеньевна.

16 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 нового пользователя (гостевой аккаунт) виртуальной машины;
2. Через гостевой аккаунт выполнить задания лабораторной работы;
3. Заполнить таблицы об уровнях доступа и действиях с файлами/директориями.

Выполнение лабораторной работы

В установленной ОС создаю учетную запись пользователя guest.

```
[vemanaeva@vemanaeva ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[vemanaeva@vemanaeva ~]$ sudo useradd guest
[sudo] пароль для vemanaeva:
```

Рис. 1: Создание учетной записи пользователя

Задаю пароль для созданного пользователя.

```
[vemanaeva@vemanaeva ~]$ sudo passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль содержит имя пользователя в какой либо форме
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
```

Рис. 2: Пароль

Вхожу в систему от имени созданного пользователя.

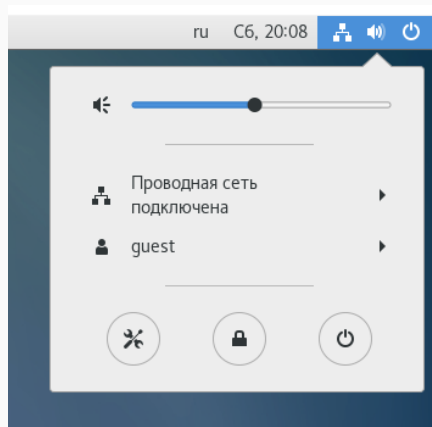


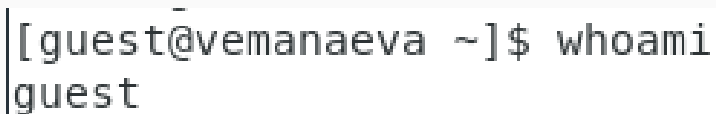
Рис. 3: Вход в систему

С помощью команды pwd определяю директорию.

```
[guest@vemanaeva ~]$ pwd  
/home/guest
```

Рис. 4: pwd

Уточняю имя пользователя командой `whoami`.

A terminal window with a light gray background. The prompt is [guest@vemanaeva ~]\$ and the command whoami has been entered. The output is guest. A vertical line is on the left, and a horizontal line is at the end of the command line.

```
[guest@vemanaeva ~]$ whoami  
guest
```

Рис. 5: `whoami`

Уточняю имя пользователя, группу, и группы, куда входит пользователь.

```
[guest@vemanaeva ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@vemanaeva ~]$ groups  
guest
```

Рис. 6: Уточняю имя пользователя, группу, и группы

Сравниваю полученные данные с данными в приглашении командной строки.

```
[guest@vemanaeva ~]$ id  
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@vemanaeva ~]$ groups  
guest
```

Рис. 7: Сравнение данных

Просматриваю файл /etc/passwd командой cat /etc/passwd.

```
[guest@vemanaeva ~]$ 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:99:99:Nobody:./:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:./:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
polkitd:x:999:998:User for polkitd:./:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sane:x:996:994:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
saslauthd:x:995:76:Saslauthd user:/run/saslauthd:/sbin/nologin
abrt:x:173:173:./etc/abrt:/sbin/nologin
setroubleshoot:x:994:991:./var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
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:/dev/null:/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
vemanaeva:x:1000:1000:vemanaeva:/home/vemanaeva:/bin/bash
vboxadd:x:988:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
```

```
[guest@vemanaeva ~]$ ls -l /home/
итого 8
drwx-----. 15 guest      guest      4096 сен 16 20:08 guest
drwx-----. 15 vemanaeva vemanaeva 4096 сен 16 19:56 vemanaeva
```

Рис. 9: Команда `ls -l /home/`

Проверяю, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой

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

Рис. 10: Проверяю, какие расширенные атрибуты установлены

Создаю в домашней директории поддиректорию dir1 командой mkdir dir1

Определяю командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

```
[guest@vemanaeva ~]$ mkdir dir1
[guest@vemanaeva ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 сен 16 20:17 dir1
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Видео
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Докум
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Загру
drwxr-xr-x. 2 guest guest 68 сен 16 20:15 Изобр
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Музык
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Общед
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Рабоч
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Шабло
[guest@vemanaeva ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
```

Рис. 11: Создаю поддиректорию dir1

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

```
[guest@vemanaeva ~]$ chmod 000 dir1
[guest@vemanaeva ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 16 20:17 dir1
```

Рис. 12: Снимаю с директории `dir1` все атрибуты

Совершаю попытку создания в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1

Проверяю командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1.

```
[guest@vema-naeva ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@vema-naeva ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@vema-naeva ~]$ chmod 700 dir1
[guest@vema-naeva ~]$ ls -l /home/guest/dir1
итого 0
```

Рис. 13: попытка создания в директории dir1 файл file1

Заполняю 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-	Уда-	За- пись фай- ла	Чте- ние фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
		зда- ние фай- ла	ле- ние фай- ла						
d-wx---	(000)	+	+	-	-	+	-	+	-
d-wx---	(100)	+	+	-	-	+	-	+	-
d-wx---	(200)	+	+	+	-	+	-	+	-
d-wx---	(300)	+	+	+	-	+	-	+	-
d-wx---	(400)	+	+	-	+	+	-	+	+
d-wx---	(500)	+	+	-	+	+	-	+	+
d-wx---	(600)	+	+	+	+	+	-	+	+

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---	(400)
Запись в файл	d-x---	(200)
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.