

Лабораторная работа №2: Дискреционное разграничение прав в Linux. Основные атрибуты

дисциплина: Информационная безопасность

Швец Сергей Сергеевич

2021, 02 October

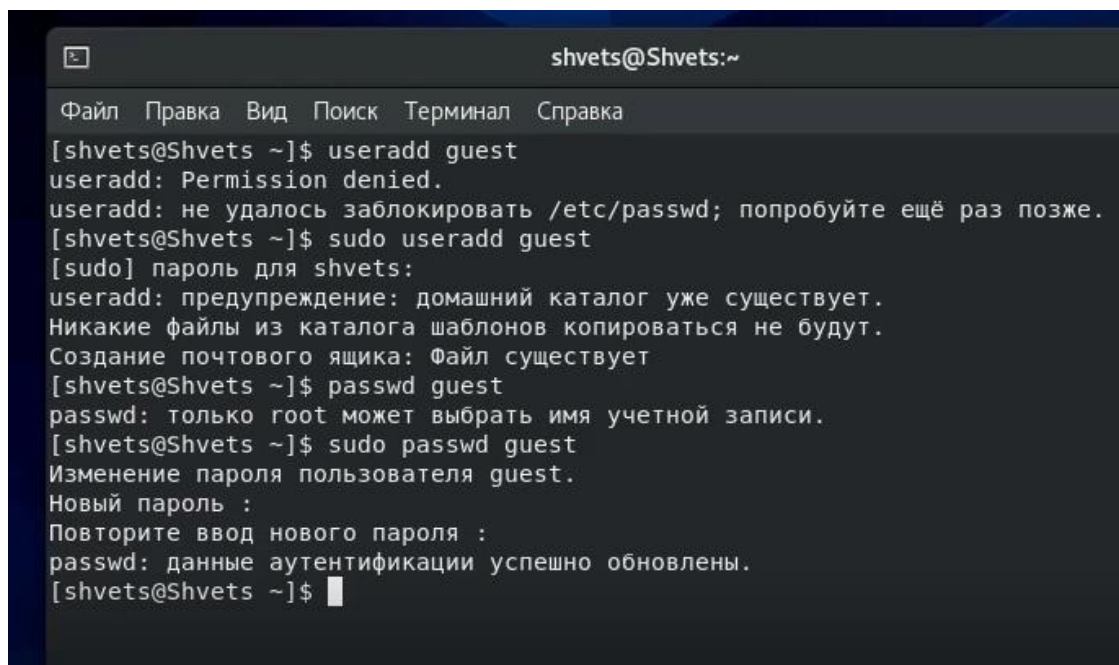
Цель работы

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.

Выполнение работы

Создание учетной записи

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



```
shvets@Shvets:~  
Файл Правка Вид Поиск Терминал Справка  
[shvets@Shvets ~]$ useradd guest  
useradd: Permission denied.  
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.  
[shvets@Shvets ~]$ sudo useradd guest  
[sudo] пароль для shvets:  
useradd: предупреждение: домашний каталог уже существует.  
Никакие файлы из каталога шаблонов копироваться не будут.  
Создание почтового ящика: Файл существует  
[shvets@Shvets ~]$ passwd guest  
passwd: только root может выбрать имя учетной записи.  
[shvets@Shvets ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль :  
Повторите ввод нового пароля :  
passwd: данные аутентификации успешно обновлены.  
[shvets@Shvets ~]$
```

Figure 1: Создание учетной записи

Учетная запись

Вход в систему через пользователя guest.



Figure 2: Guest

Учетная запись

Определение директории и уточнение имени пользователя

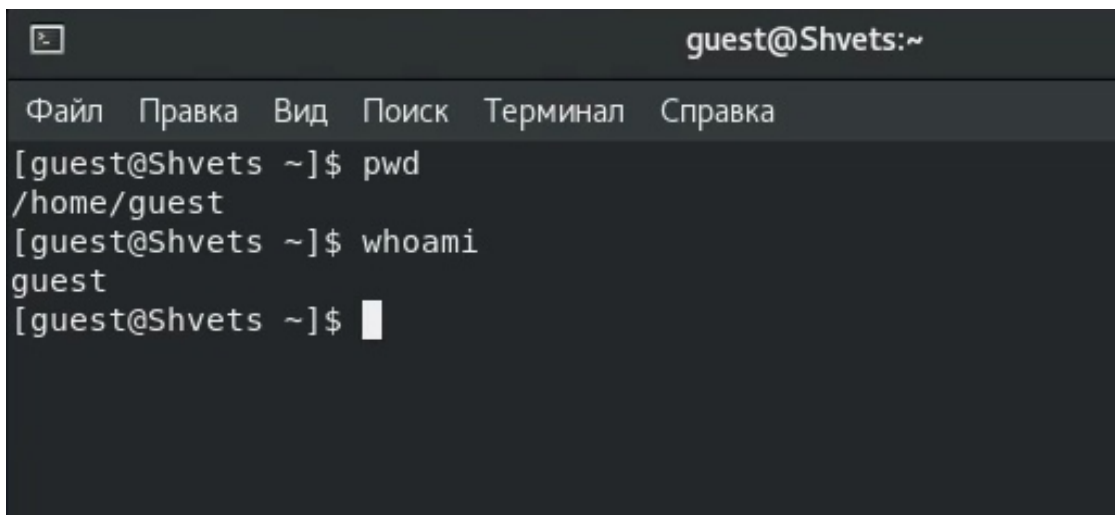
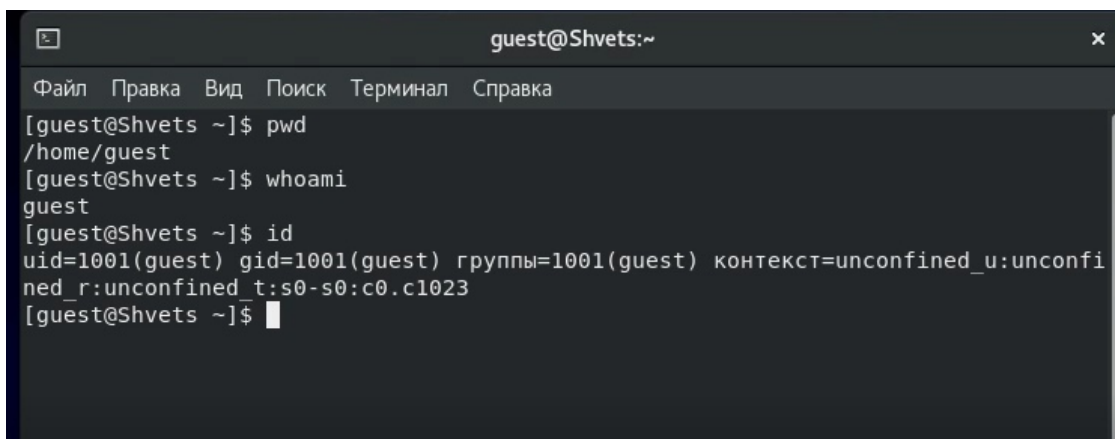


Figure 3: директория и пользователь

Учетная запись

Уточняем имя пользователя, группу, а также группы, куда входит пользователь, посредством команды `id`.

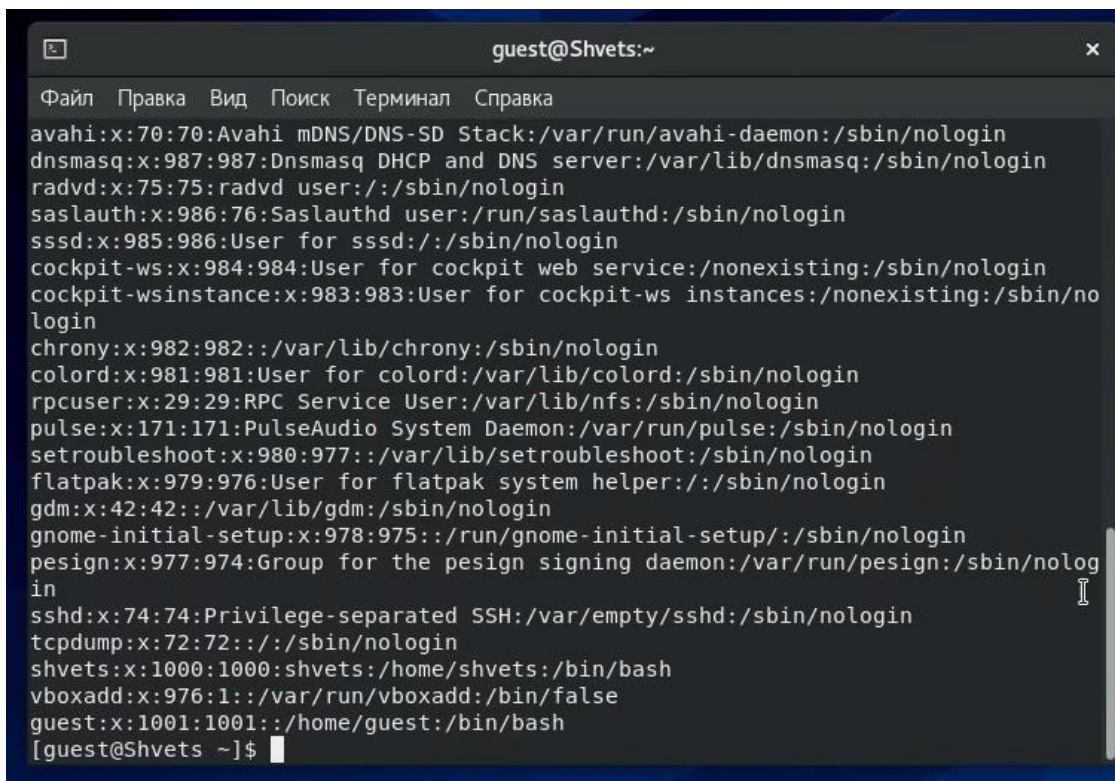


```
guest@Shvets:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@Shvets ~]$ pwd  
/home/guest  
[guest@Shvets ~]$ whoami  
guest  
[guest@Shvets ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@Shvets ~]$
```

Figure 4: имя группа

Учетная запись

Просмотр файла командой `cat /etc/passwd`, поиск учетной записи, определение `uid`, `gid` пользователя.



```
guest@Shvets:~  
Файл Правка Вид Поиск Терминал Справка  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
dnsmasq:x:987:987:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin  
radvd:x:75:75:radvd user:/:/sbin/nologin  
saslauthd:x:986:76:Saslauthd user:/run/saslauthd:/sbin/nologin  
sssd:x:985:986:User for sssd:/:/sbin/nologin  
cockpit-ws:x:984:984:User for cockpit web service:/nonexisting:/sbin/nologin  
cockpit-wsinstance:x:983:983:User for cockpit-ws instances:/nonexisting:/sbin/no  
login  
chrony:x:982:982:/var/lib/chrony:/sbin/nologin  
colord:x:981:981:User for colord:/var/lib/colord:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
setroubleshoot:x:980:977:/var/lib/setroubleshoot:/sbin/nologin  
flatpak:x:979:976:User for flatpak system helper:/:/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:978:975:/run/gnome-initial-setup:/sbin/nologin  
design:x:977:974:Group for the design signing daemon:/var/run/design:/sbin/nolog  
in  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72:/:/sbin/nologin  
shvets:x:1000:1000:shvets:/home/shvets:/bin/bash  
vboxadd:x:976:1:/var/run/vboxadd:/bin/false  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@Shvets ~]$
```

Figure 5: Значения `uid` и `gid`

Учетная запись

Определение существующих в системе директорий командой `ls -l /home/`.

```
[guest@Shvets ~]$ ls -l /home/
итого 8
drwx-----. 15 guest  guest  4096 окт  2 22:02 guest
drwx-----. 15 shvets shvets 4096 окт  2 21:31 shvets
[guest@Shvets ~]$
```

Figure 6: Директории

Учетная запись

Проверка расширенных атрибутов поддиректорий, находящихся в `/home` расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`.

```
[root@Shvets guest]# lsattr /home
----- /home/shvets
----- /home/guest
[root@Shvets guest]#
```

Figure 7: Расширенные атрибуты

Учетная запись

Создание в домашней директории поддиректорию `dir1` командой `mkdir dir1`.
Определение командами `ls -l` и `lsattr` прав доступа и расширенных атрибутов.

```

[root@Shvets guest]# mkdir dir1
[root@Shvets guest]# ls -l
итого 0
drwxr-xr-x. 2 root  root  6 окт  2 22:14  dir1
drwxr-xr-x. 2 guest guest 6 окт  2 22:02  Видео
drwxr-xr-x. 2 guest guest 6 окт  2 22:02  Документы
drwxr-xr-x. 2 guest guest 6 окт  2 22:02  Загрузки
drwxr-xr-x. 2 guest guest 6 окт  2 22:02  Изображения
drwxr-xr-x. 2 guest guest 6 окт  2 22:02  Музыка
drwxr-xr-x. 2 guest guest 6 окт  2 22:02  Общедоступные
drwxr-xr-x. 2 guest guest 6 окт  2 22:02  'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт  2 22:02  Шаблоны
[root@Shvets guest]# lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[root@Shvets guest]# █

```

Figure 8: Поддиректория

Учетная запись

Снятие с директории dir1 всех атрибутов командой `chmod 000 dir1`.


```

[root@Shvets guest]# lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[root@Shvets guest]# chmod 000 dir1
[root@Shvets guest]# ls -l
итого 0
d----- . 2 root root 6 окт 2 22:14 dir1
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Видео
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Документы
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Загрузки
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Изображения
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Музыка
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Общедоступные
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Шаблоны
[root@Shvets guest]#

```

Figure 9: Снятие атрибутов

Учетная запись

Попытка создания в директории dir1 файла file1 командой `echo "test" > /home/guest/dir1/file1`.

```

d----- . 2 root root 6 окт 2 22:14 dir1
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Видео
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Документы
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Загрузки
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Изображения
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Музыка
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Общедоступные
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт 2 22:02 Шаблоны
[root@Shvets guest]# echo "test" > /home/guest/dir1/file1
[root@Shvets guest]#

```

Figure 10: Создание файла

Таблица

Таблица с установленными правами и разрешенными действиями.

Процесс выполнения

Заполнили таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет

Прото деректәре	Прото файлы	Создание файлы	Удаление файлы	Запись в файлы	Чтение файлы	Смена деректәре	Перемещение файлы в деректәре	Перемещение файлы	Смена атрибутов файлы
d<000	d<0000	+	+	+	+	+	+	+	+
d w (200)	d<0000	+	+	+	+	+	+	+	+
d w<000	d<0000	+	+	+	+	+	+	+	+
d w (400)	d<0000	+	+	+	+	+	+	+	+
d w<000	d<0000	+	+	+	+	+	+	+	+
d w (800)	d<0000	+	+	+	+	+	+	+	+
d w<000	d<0000	+	+	+	+	+	+	+	+
d<000	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (200)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (400)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (800)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d<000	d w (200)	+	+	+	+	+	+	+	+
d w<000	d w (200)	+	+	+	+	+	+	+	+
d w (200)	d w (200)	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (400)	d w (200)	+	+	+	+	+	+	+	+
d w<000	d w (200)	+	+	+	+	+	+	+	+
d w (800)	d w (200)	+	+	+	+	+	+	+	+
d w<000	d w (200)	+	+	+	+	+	+	+	+
d<000	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (200)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (400)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (800)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d<000	d w (400)	+	+	+	+	+	+	+	+
d w<000	d w (400)	+	+	+	+	+	+	+	+
d w (200)	d w (400)	+	+	+	+	+	+	+	+
d w<000	d w (400)	+	+	+	+	+	+	+	+
d w (400)	d w (400)	+	+	+	+	+	+	+	+
d w<000	d w (400)	+	+	+	+	+	+	+	+
d w (800)	d w (400)	+	+	+	+	+	+	+	+
d w<000	d w (400)	+	+	+	+	+	+	+	+
d w (200)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (400)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (800)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+
d w (200)	d w<000	+	+	+	+	+	+	+	+
d w<000	d w<000	+	+	+	+	+	+	+	+

11/13

Figure 11: 2.1

Выводы

Мной были получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.