

Лабораторная работа № 2

Тарусов Артём Сергеевич

2023, Москва

Целью данной работы является 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 новую учетную запись guest.
2. Выполнить ряд операций в новой учетной записи.
3. Сформировать таблицу “Установленные права и разрешенные действия”.
4. Сформировать таблицу “Минимальные права для совершения операций”.

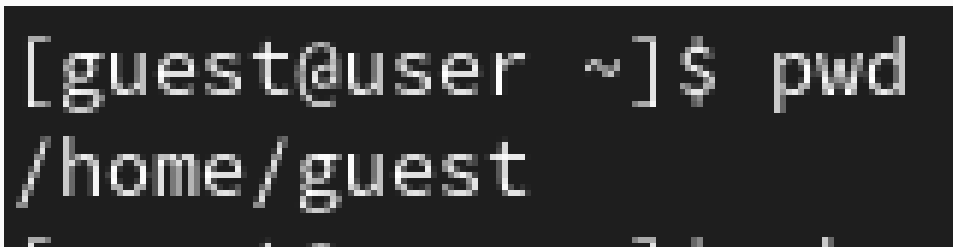
Создадим учетную запись пользователя guest и зададим пароль.

```
[astarusov@user ~]$ sudo su
[sudo] password for astarusov:
[root@user astarusov]# useradd guest
[root@user astarusov]# passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Рис. 1: Создание и настройка учетной записи guest

Войдем в систему от имени пользователя guest

Определим директорию, в которой мы находимся.

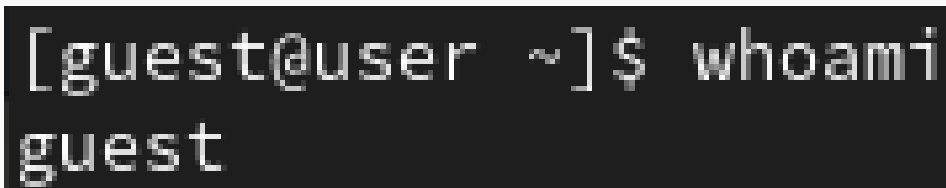
A terminal window with a black background and white text. The prompt is '[guest@user ~]\$'. The command 'pwd' has been entered, and the output is '/home/guest' on the next line.

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

Рис. 2: Определение текущей директории

Директория является домашней.

Уточним имя пользователя.

A terminal window with a black background and white text. The prompt is '[guest@user ~]\$' and the command entered is 'whoami'. The output of the command is 'guest' on the next line.

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

Рис. 3: Уточнение имени пользователя

Уточним имя пользователя, его группу, а также группы, куда входит пользователь.

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

Рис. 4: Уточнение информации о пользователе

Имя пользователя совпадает с приглашением в командной строке.

Просмотрим файл /etc/passwd.

```
[guest@user ~]$ 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
```

Рис. 5: Содержимое файла /etc/passwd

Найдем в нём свою учётную запись.

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

Рис. 6: Учетная запись guest в файле /etc/passwd

uid = 1001, gid = 1001. Совпадают со значениями, найденными в предыдущих пунктах.

Определим существующие в системе директории.

```
[guest@user ~]$ ls -l /home/  
total 8  
drwx-----. 18 astarusev astarusev 4096 Sep 14 11:27 astarusev  
drwx-----. 14 guest      guest      4096 Sep 14 11:27 guest
```

Рис. 7: Существующие в системе директории

Удалось получить список поддиректорий директории /home. На обеих директориях установлены права drwx——.

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home.

```
[guest@user ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/astarusov
----- /home/guest
```

Рис. 8: Расширенные атрибуты, установленные на поддиректориях /home

Удалось увидеть расширенные атрибуты директории текущего пользователя, но не удалось увидеть атрибуты директории другого пользователя.

Создадим в домашней директории поддиректорию `dir1` и выведем права доступа и расширенные атрибуты.

```
[guest@user ~]$ mkdir dir1
[guest@user ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 14 11:36 dir1
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Documents
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Music
drwxr-xr-x. 2 guest guest 53 Sep 14 11:30 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Public
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Templates
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Videos
[guest@user ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
```

Рис. 9: Создание поддиректории и информация о ней

Снимем с директории `dir1` все атрибуты.

```
[guest@user ~]$ chmod 000 dir1
[guest@user ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Desktop
d------. 2 guest guest 6 Sep 14 11:36 dir1
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Documents
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Music
drwxr-xr-x. 2 guest guest 53 Sep 14 11:30 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Public
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Templates
drwxr-xr-x. 2 guest guest 6 Sep 14 11:27 Videos
```

Рис. 10: Снятие всех атрибутов

Попытаемся создать в директории dir1 файл file1.

```
[guest@user ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@user ~]$ ls -l /home/guest/dir1
```

Рис. 11: Создание файла file1

Мы получили отказ, так как у нас нет прав на создание. Из-за этого файл не был создан.

Заполним таблицу «Установленные права и разрешённые действия».

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файла в директории	Переименование файла	Смена атрибутов файла
(000)	(000)	-	-	-	-	-	-	-	-
(100)	(000)	-	-	-	-	+	-	-	+
(200)	(000)	-	-	-	-	-	-	-	-
(300)	(000)	+	+	-	-	+	-	+	+
(400)	(000)	-	-	-	-	-	+	-	-
(500)	(000)	-	-	-	-	+	+	-	+
(600)	(000)	-	-	-	-	-	+	-	-
(700)	(000)	+	+	-	-	+	+	+	+
(000)	(100)	-	-	-	-	-	-	-	-
(100)	(100)	-	-	-	-	+	-	-	+
(200)	(100)	-	-	-	-	-	-	-	-
(300)	(100)	+	+	-	-	+	-	+	+
(400)	(100)	-	-	-	-	-	+	-	-

Рис. 12: Фрагмент таблицы 2.1

Заполним таблицу «Минимальные права для совершения операций».

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	(300)	(000)
Удаление файла	(300)	(000)
Чтение файла	(100)	(400)
Запись в файл	(100)	(200)
Переименование файла	(300)	(000)
Создание поддиректории	(300)	(000)
Удаление поддиректории	(300)	(000)

Рис. 13: Фрагмент таблицы 2.2

В рамках данной лабораторной работы были изучены средства ограничения прав для отдельных учетных записей.