

Презентация №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Аскеров А.Э.

02 марта 2024

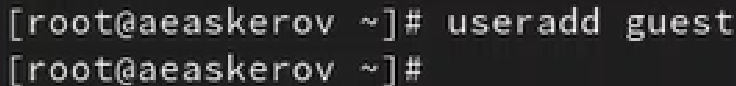
Российский университет дружбы народов, Москва, Россия

Вступление

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 лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора).



```
[root@aeaskerov ~]# useradd guest  
[root@aeaskerov ~]#
```

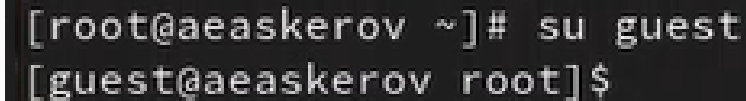
Рис. 1: Создание учётной записи guest

Зададим пароль для пользователя guest.

```
[root@aeaskerov ~]# passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@aeaskerov ~]#
```

Рис. 2: Указание пароля

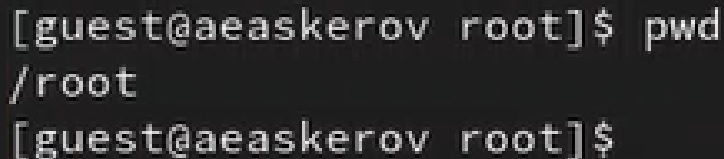
Войдём в систему от имени пользователя guest.

A terminal window with a dark background and light-colored text. The first line shows the prompt '[root@aeaskerov ~]#' followed by the command 'su guest'. The second line shows the new prompt '[guest@aeaskerov root]\$' after the command is executed.

```
[root@aeaskerov ~]# su guest  
[guest@aeaskerov root]$
```

Рис. 3: Переключение на пользователя guest

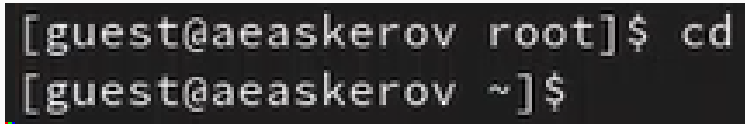
Определим директорию, в которой находимся, командой `pwd`.

A terminal window with a black background and white text. The prompt is [guest@aeaskerov root]\$. The command pwd is entered, followed by a newline. The output /root is displayed. Another newline is entered, and the prompt [guest@aeaskerov root]\$ is shown again.

```
[guest@aeaskerov root]$ pwd
/root
[guest@aeaskerov root]$
```

Рис. 4: Текущая директория

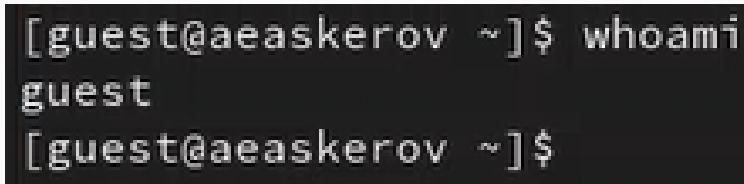
Отображённая директория не является домашней, поэтому теперь перейдём в домашнюю.

A terminal window with a black background and white text. The first line shows the prompt '[guest@aeaskerov root]\$' followed by the command 'cd'. The second line shows the prompt '[guest@aeaskerov ~]\$', indicating a successful transition to the home directory.

```
[guest@aeaskerov root]$ cd  
[guest@aeaskerov ~]$
```

Рис. 5: Переход в домашнюю директорию

Уточним имя пользователя командой `whoami`.

A terminal window with a dark background and light gray text. The prompt is `[guest@aeaskerov ~]$`. The command `whoami` has been entered, and the output `guest` is displayed on the next line. The prompt `[guest@aeaskerov ~]$` appears again on the third line.

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

Рис. 6: Отображение имени пользователя

Дискреционное разграничение прав в Linux

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

```
[guest@aeaskerov ~]$ id
uid=1007(guest) gid=100(users) groups=100(users) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@aeaskerov ~]$
```

Рис. 7: Команда `id`

Выполним команду `groups`.

```
[guest@aeaskerov ~]$ groups
users
[guest@aeaskerov ~]$
```

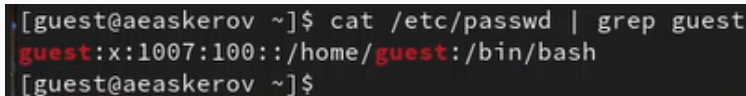
Рис. 8: Команда `groups`

Дискреционное разграничение прав в Linux

Команда `groups` просто показывает, к каким группам относится текущий пользователь. А команда `id` используется для определения имен пользователей и групп, а также числовых идентификаторов (UID или идентификатор группы) пользователя.

Полученная информация об имени пользователя и данные, выводимые в приглашении командной строки, совпадают.

Посмотрим информацию о `guest` в файле `/etc/passwd`.



```
[guest@aeaskerov ~]$ cat /etc/passwd | grep guest
guest:x:1007:100::/home/guest:/bin/bash
[guest@aeaskerov ~]$
```

Рис. 9: Просмотр `/etc/passwd`

Дискреционное разграничение прав в Linux

UID равен 1007, GID равен 100. Эти значения совпадают со значениями, показанными командой `id`.

Определим существующие в системе директории.

```
[guest@aeaskerov ~]$ ls -l /home/  
total 4  
drwx-----. 15 aeaskerov aeaskerov 4096 Mar  2 16:25 aeaskerov  
drwx-----.  6 alice      users      146 Sep 20 18:54 alice  
drwx-----.  6 bob        users      146 Sep 24 18:58 bob  
drwx-----.  6 carol      users      146 Sep 20 18:54 carol  
drwx-----.  5 dan        users      111 Sep 20 12:35 dan  
drwx-----.  5 dave       users      111 Sep 20 12:35 dave  
drwx-----.  5 david      users      111 Sep 20 12:36 david  
drwx-----.  6 guest      users      125 Mar  2 16:46 guest  
drwx-----.  3 alice      alice       78 Sep  9 16:57 Hope  
drwx-----.  3 bob        bob         78 Sep  9 21:00 Tom  
drwxr-xr-x.  2 root       root         6 Sep 24 19:55 users  
[guest@aeaskerov ~]$
```

Рис. 10: Существующие в системе директории

Список поддиректорий директории /home получить не удалось.

Установленные права (read, write, execute) позволяют только владельцам взаимодействовать с директориями.

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

Дискреционное разграничение прав в Linux

```
[guest@aeaskerov ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/aeaskerov
lsattr: Permission denied While reading flags on /home/Hope
lsattr: Permission denied While reading flags on /home/Tom
lsattr: Permission denied While reading flags on /home/alice
lsattr: Permission denied While reading flags on /home/bob
lsattr: Permission denied While reading flags on /home/carol
lsattr: Permission denied While reading flags on /home/dan
lsattr: Permission denied While reading flags on /home/dave
lsattr: Permission denied While reading flags on /home/david
----- /home/users
----- /home/guest
[guest@aeaskerov ~]$
```

Рис. 11: Просмотр расширенных атрибутов директории

Их не удалось посмотреть из-за отказа в доступе как у guest, так и у других пользователей.

Создадим в домашней директории поддиректорию dir1.

A terminal window with a black background and white text. The prompt is [guest@aeaskerov ~]\$. The command mkdir dir1 is entered and executed. The prompt returns to [guest@aeaskerov ~]\$.

```
[guest@aeaskerov ~]$ mkdir dir1  
[guest@aeaskerov ~]$
```

Рис. 12: Создание поддиректории dir1

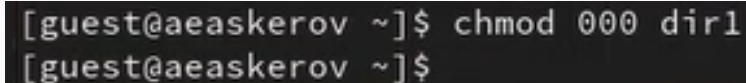
Дискреционное разграничение прав в Linux

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

```
[guest@aeaskerov ~]$ ls -l
total 0
drwxr-xr-x. 2 guest users 6 Mar  2 16:50 dir1
drwxr-xr-x. 2 guest users 6 Sep 12 10:17 Documents
drwxr-xr-x. 2 guest users 6 Sep 12 10:17 Pictures
[guest@aeaskerov ~]$ lsattr
----- ./Pictures
----- ./Documents
----- ./dir1
[guest@aeaskerov ~]$
```

Рис. 13: Права на директорию `dir1`

Снимем с директории dir1 все атрибуты.

A terminal window with a dark background and light gray text. The prompt is [guest@aeaskerov ~]\$. The command entered is chmod 000 dir1. The prompt after the command is [guest@aeaskerov ~]\$.

```
[guest@aeaskerov ~]$ chmod 000 dir1  
[guest@aeaskerov ~]$
```

Рис. 14: Изменение доступа к dir1

Отообразим права доступа к dir1.

```
[guest@aeaskerov ~]$ ls -l
total 0
d----- . 2 guest users 6 Mar  2 16:50 dir1
drwxr-xr-x. 2 guest users 6 Sep 12 10:17 Documents
drwxr-xr-x. 2 guest users 6 Sep 12 10:17 Pictures
[guest@aeaskerov ~]$
```

Рис. 15: Отображение прав доступа

Попытаемся создать в директории dir1 файл file1.

```
[guest@aeaskerov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@aeaskerov ~]$
```

Рис. 16: Попытка создания файла в dir1

В доступе отказано, так как мы запретили запись в директорию dir1.

Оценим, как сообщение об ошибке отразилось на создании файла.

```
[guest@aeaskerov ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@aeaskerov ~]$
```

Рис. 17: Попытка посмотреть содержимое dir1

Заключение

Получены практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.