Презентация по лабораторной работе №2

Первойкин Илья Сергеевич

16 Сентября 2023

РУДН, Москва, Россия

Цель лабораторной работы №2

Цель: Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Ход выполнения лабораторной работы

Создание нового пользователя в виртуальной машине

Создали нового пользователя guest командой useradd, затем установили для него пароль с помощью команды passwd guest.

```
[ispervoyjkin@localhost ~]$ su
Password:
[root@localhost ispervoyjkin]# useradd guest
[root@localhost ispervoyjkin]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ispervoyjkin]#
```

Рис. 1: Новый пользователь в Виртуальной машине

Проверка данных пользователя

С помощью команды id узнали uid пользователя и группы, в которых он состоит.

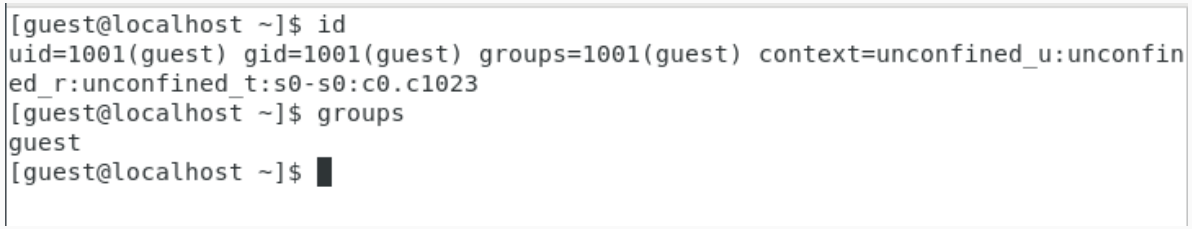

Рис. 2: Команда id

Просмотр атрибутов

С помощью команды ls рассмотрели атрибуты. С помощью команды lsattr рассмотрели расширенные атрибуты текущего пользователя.

```
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Desktop
drwxrwxr-x. 2 guest guest   6 Sep 16 18:15 dir1
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Documents
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Downloads
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Music
drwxr-xr-x. 2 guest guest 100 Sep 16 18:13 Pictures
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Public
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Templates
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Videos
[guest@localhost ~]$ lsattr
---------------- ./Desktop
---------------- ./Downloads
---------------- ./Templates
---------------- ./Public
---------------- ./Documents
---------------- ./Music
---------------- ./Pictures
---------------- ./Videos
---------------- ./dir1
[guest@localhost ~]$
```

Рис. 3: Работа с каталогом /home

Смена прав доступа

Поменяли права доступа директории dir1 с помощью команды chmod 000.

```
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Desktop
d---------. 2 guest guest   6 Sep 16 18:15 dir1
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Documents
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Downloads
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Music
drwxr-xr-x. 2 guest guest 147 Sep 16 18:15 Pictures
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Public
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Templates
drwxr-xr-x. 2 guest guest   6 Sep 16 18:09 Videos
[guest@localhost ~]$
```

Рис. 4: Меняем директории dir1 атрибуты

Разрешённые действия

Изучив все атрибуты, составили таблицу «Установленные права и разрешённые действия».

Установленные права и разрешённые действия (таб. 2.1)

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов
d (000)	(000)	-	-	-	-	-	-	-	-
d -x (100)	(000)	-	-	-	-	+	-	-	-
d -w- (200)	(000)	-	-	-	-	-	-	-	-
d -wx (300)	(000)	+	+	-	-	+	-	+	-
dr- (400)	(000)	-	-	-	-	-	+	-	-
d r-x (500)	(000)	-	-	-	-	+	+	-	-
d rw-(600)	(000)	-	-	-	-	-	+	-	-
d rwx (700)	(000)	+	+	-	-	+	+	+	-
d (000)	(100)	-	-	-	-	-	-	-	-
d -x (100)	(100)	-	-	-	-	+	-	-	-
d -w-(200)	(100)	-	-	-	-	-	-	-	-
d -wx (300)	(100)	+	+	-	-	+	-	+	-
dr- (400)	(100)	-	-	-	-	-	+	-	-
d r-x (500)	(100)	-	-	-	-	+	+	-	-
d rw-(600)	(100)	-	-	-	-	-	+	-	-
d rwx (700)	(100)	+	+	-	-	+	+	+	-
d (000)	(200)	-	-	-	-	-	-	-	-
d -x (100)	(200)	-	-	+	-	+	-	-	-
d -w-(200)	(200)	-	-	-	-	-	-	-	-
d -wx (300)	(200)	+	+	+	-	+	-	+	-
dr- (400)	(200)	-	-	-	-	-	+	-	-
d r-x (500)	(200)	-	-	+	-	+	+	-	-
d rw-(600)	(200)	-	-	-	-	-	+	-	-
d rwx (700)	(200)	+	+	+	-	+	+	+	-
d (000)	(300)	-	-	-	-	-	-	-	-
d -x (100)	(300)	-	-	+	-	+	-	-	-
d -w-(200)	(300)	-	-	-	-	-	-	-	-
d -wx (300)	(300)	+	+	-	+	+	-	+	-
dr- (400)	(300)	-	-	-	-	-	+	-	-
d r-x (500)	(300)	-	-	+	-	+	+	-	-
d rw-(600)	(300)	-	-	-	-	-	+	-	-
d rwx (700)	(300)	+	+	+	-	+	+	+	-
d (000)	(400)	-	-	-	-	-	-	-	-

Разрешённые действия

d -x (100)	(500)	-	-	-	+	+	-	-	+
d -w-(200)	(500)	-	-	-	-	-	-	-	-
d -wx (300)	(500)	+	+	-	+	+	-	+	+
dr- (400)	(500)	-	-	-	-	-	+	-	-
d r-x (500)	(500)	-	-	-	+	+	+	-	+
d rw-(600)	(500)	-	-	-	-	-	+	-	-
d rwx (700)	(500)	+	+	-	+	+	+	+	+
d (000)	(600)	-	-	-	-	-	-	-	-
d -x (100)	(600)	-	-	+	+	+	-	-	+
d -w-(200)	(600)	-	-	-	-	-	-	-	-
d -wx (300)	(600)	+	+	+	+	+	-	+	+
dr- (400)	(600)	-	-	-	-	-	+	-	-
d r-x (500)	(600)	-	-	+	+	+	+	-	+
d rw-(600)	(600)	-	-	-	-	-	+	-	-
d rwx (700)	(600)	+	+	+	+	+	+	+	+
d (000)	(700)	-	-	-	-	-	-	-	-
d -x (100)	(700)	-	-	+	+	+	-	-	+
d -w-(200)	(700)	-	-	-	-	-	-	-	-
d -wx (300)	(700)	+	+	+	+	+	-	+	+
dr- (400)	(700)	-	-	-	-	-	+	-	-
d r-x (500)	(700)	-	-	+	+	+	+	-	+
d rw-(600)	(700)	-	-	-	-	-	+	-	-
d rwx (700)	(700)	+	+	+	+	+	+	+	+

Рис. 6: Таблица 2.1 «Установленные права и разрешённые действия»

Минимальные требования

На основании этой таблицы заполнили вторую таблицу «Минимальные права для совершения операций». В данной таблице указаны минимальные требования на права и директорию для выполнения тех или иных действий.

Минимальные права для совершения операция (таб. 2.2)

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

Рис. 7: Таблица 2.2 «Минимальные права для совершения операций»

Выводы

- Получили практические навыки работы в консоли с атрибутами файлов;
- Закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Библиография

СПИСОК ЛИТЕРАТУРЫ

1.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: http://bugtraq.ru/library/books/attack1/index.html

2.Теоеретические знания, приведённые в Лабораторной работе №2 - https://esystem.rudn.ru/pluginfile.php/2090123/mod_resource/conte lab_discret_attr.pdf

3.Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ