Лабораторная работа №2

Дисциплина: информационная безопасность

Студент: Подорога Виктор Александрович

Цель работы

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.

Выполнение лабораторной работы

1. Добавляем гостевого пользователя:

```
[podorogava@PodorogaVA ~]$ useradd guest
useradd: Permission denied.
```

Рис. 1. Добавление гостевого пользователя

2. Настраиваем пароль для гостевого пользователя:

```
[podorogava@PodorogaVA ~]$ passwd guest
passwd: только root может выбрать имя учетной записи.
```

Рис. 2. Настройка пароля для гостевого пользователя

3. Заходим в суперпользователя root и проделываем то же самое, чтобы разрешить доступ:

```
[podorogava@PodorogaVA ~]$ sudo bash

Мы полагаем, что ваш системный администратор изложил вам основы
безопасности. Как правило, всё сводится к трём следующим правилам:

    №1) Уважайте частную жизнь других.
    №2) Думайте, прежде что-то вводить.
    №3) С большой властью приходит большая ответственность.

[sudo] пароль для podorogava:
[root@PodorogaVA podorogava]# useradd guest
[root@PodorogaVA podorogava]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@PodorogaVA podorogava]#
```

Рис. 3. Те же действия от root

4. Заходим в гостевого пользователя:

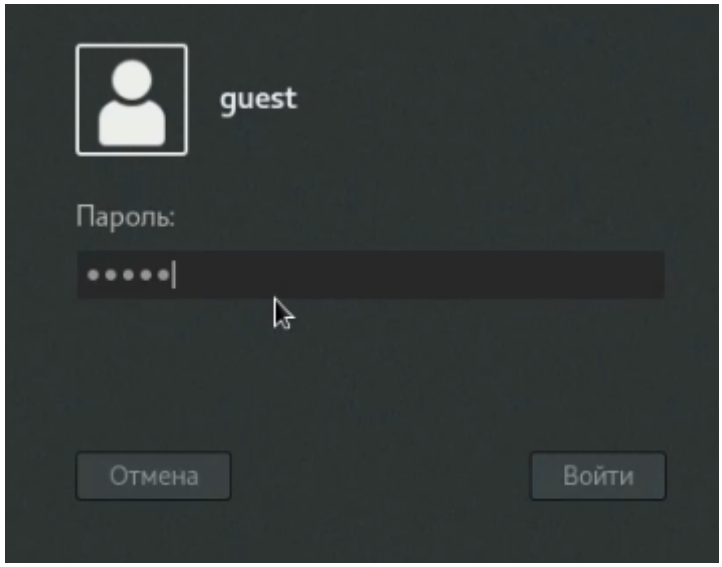

Рис. 4. Логин

5. Командой pwd проверяем путь до директории, в которой оказались:

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

Рис. 5. Проверка pwd

6. Уточняем имя нашего пользователя командой whoami:

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

Рис. 6. Уточнение имени пользователя

7. Уточняем имя нашего пользователя, его группу, а также группы, куда входит пользователь, командой id и groups:

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

Рис. 7. Уточнение с помощью id и groups

В результате получает одни и те же группы пользователя (в обоих случаях guest)

8. Просмотрим файл /etc/passwd командой cat /etc/passwd:

```
[guest@PodorogaVA ~]$ 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/no
login
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
saned:x:996:994:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
```

Рис. 8.1. Просмотр файла

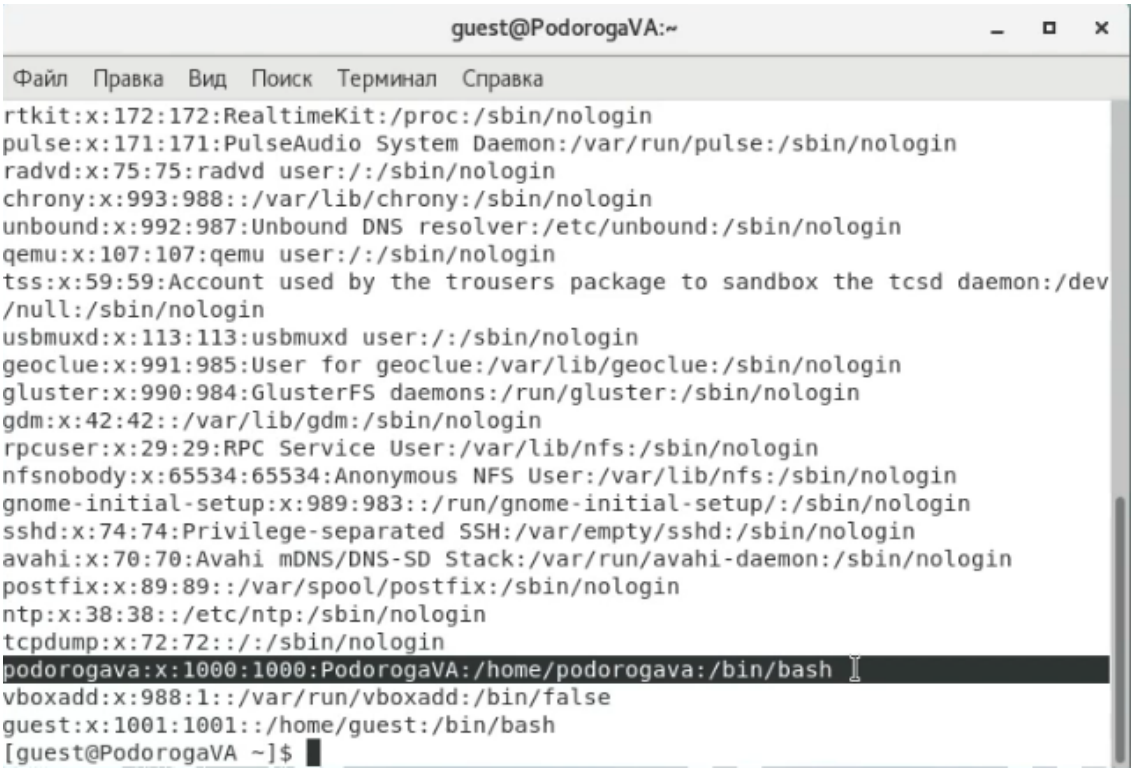

Рис. 8.2. Мой пользователь

9. Определим существующие в системе директории командой ls -l /home/:

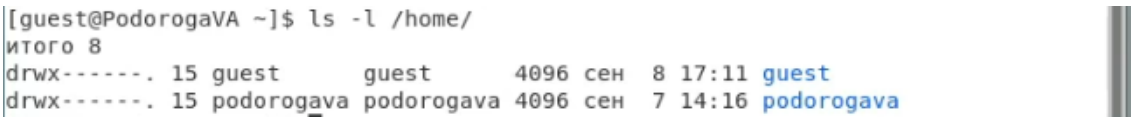

Рис. 9. Определение существующих в системе директорий

Список директорий получен, на директориях установлены права чтения, записи и исполнения, что соответствует атрибуту 700 в таблице.

10. Проверим расширенные атрибуты командой lsattr /home:

Рис. 10. Проверка расширенных атрибутов

Расширенные атрибуты увидеть не удалось - гостевому пользователю отказано в доступе.

11. Создадим в домашней директории поддиректорию dir1 командой mkdir dir1 и определим атрибуты:

Рис. 11.1. Создание dir1

Рис. 11.2. Определение атрибутов

12. Снимем с директории dir1 все атрибуты командой chmod 000 dir1 и проверим правильность командой ls -l:

```
[guest@PodorogaVA ~]$ chmod 000 dir1
[guest@PodorogaVA ~]$ ls -l
итого 0
d---------. 2 guest guest 6 сен  8 17:20 dir1
drwxr-xr-x. 2 guest guest 6 сен  8 17:10 Видео
drwxr-xr-x. 2 guest guest 6 сен  8 17:10 Документы
drwxr-xr-x. 2 guest guest 6 сен  8 17:10 Загрузки
drwxr-xr-x. 2 guest guest 6 сен  8 17:10 Изображения
drwxr-xr-x. 2 guest guest 6 сен  8 17:10 Музыка
drwxr-xr-x. 2 guest guest 6 сен  8 17:10 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен  8 17:10 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен  8 17:10 Шаблоны
[guest@PodorogaVA ~]$
```

Рис. 12. Снятие всех атрибутов и проверка

13. Попытаемся создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1:

```
[guest@PodorogaVA ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@PodorogaVA ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@PodorogaVA ~]$
```

Рис. 13. Попытка создания файла

Файл создать не удается, это связано с тем, что у директории dir1 отсутствует право на создание в ней файлов, ее атрибуты 000.

14. Выполняя команды 14.1 - 14.4, анализируем атрибуты директории и файла в ней:

```
[guest@PodorogaVA ~]$ chmod 000 dir1/file1
[guest@PodorogaVA ~]$ chmod 000 dir1
[guest@PodorogaVA ~]$ ls -l dir1
ls: невозможно открыть каталог dir1: Отказано в доступе
[guest@PodorogaVA ~]$ ls -l /dir1/file1
ls: невозможно получить доступ к /dir1/file1: Нет такого файла или каталога
[guest@PodorogaVA ~]$ ls -l dir1/file1
ls: невозможно получить доступ к dir1/file1: Отказано в доступе
```

Рис. 14.1. Обнуляем права директории

```
[guest@PodorogaVA ~]$ chmod 100 dir1
[guest@PodorogaVA ~]$ ls -l dir1/file1
----------. 1 guest guest 5 сен  8 17:33 dir1/file1
[guest@PodorogaVA ~]$ ls -l dir1
ls: невозможно открыть каталог dir1: Отказано в доступе
```

Рис. 14.2. Выдаем директории право на исполнение

```
[guest@PodorogaVA ~]$ chmod 200 dir1
[guest@PodorogaVA ~]$ ls -l dir1/file1
ls: невозможно получить доступ к dir1/file1: Отказано в доступе
[guest@PodorogaVA ~]$ ls -l dir1
ls: невозможно открыть каталог dir1: Отказано в доступе
```

Рис. 14.3. Выдаем директории право на запись

```
[guest@PodorogaVA ~]$ chmod 300 dir1
[guest@PodorogaVA ~]$ ls -l dir1/file1
----------. 1 guest guest 5 сен  8 17:33 dir1/file1
[guest@PodorogaVA ~]$
```

Рис. 14.4. Выдаем директории право на исполнение и запись

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименовывание файла	Смена атрибутов файла
d---------(000)	0	-	-	-	-	-	-	-	-
d--x------(100)	0	-	-	-	-	+	-	-	+
d-w-------(200)	0	-	-	-	-	-	-	-	-
d-wx------(300)	0	+	+	-	-	+	-	+	+
dr--------(400)	0	-	-	-	-	-	+	-	-
dr-x------(500)	0	-	-	-	-	+	+	-	+
drw-------(600)	0	-	-	-	-	-	+	-	-
drwx------(700)	0	+	+	-	-	+	+	+	+
d---------(000)	--x------ (100)	-	-	-	-	-	-	-	-
d--x------(100)	--x------ (100)	-	-	-	-	+	-	-	+
d-w-------(200)	--x------ (100)	-	-	-	-	-	-	-	-
d-wx------(300)	--x------ (100)	+	+	-	-	+	-	+	+
dr--------(400)	--x------ (100)	-	-	-	-	-	+	-	-
dr-x------(500)	--x------ (100)	-	-	-	-	+	+	-	+
drw-------(600)	--x------ (100)	-	-	-	-	-	+	-	-
drwx------(700)	--x------ (100)	+	+	-	-	+	+	+	+
d---------(000)	-w------- (200)	-	-	-	-	-	-	-	-
d--x------(100)	-w------- (200)	-	-	+	-	+	-	-	+
d-w-------(200)	-w------- (200)	-	-	-	-	-	-	-	-
d-wx------(300)	-w------- (200)	+	+	+	-	+	-	+	+
dr--------(400)	-w------- (200)	-	-	-	-	-	+	-	-
dr-x------(500)	-w------- (200)	-	-	+	-	+	+	-	+
drw-------(600)	-w------- (200)	-	-	-	-	-	+	-	-
drwx------(700)	-w------- (200)	+	+	+	-	+	+	+	+
d---------(000)	-wx------ (300)	-	-	-	-	-	-	-	-
d--x------(100)	-wx------ (300)	-	-	+	-	+	-	-	+
d-w-------(200)	-wx------ (300)	-	-	-	-	-	-	-	-
d-wx------(300)	-wx------ (300)	+	+	+	-	+	-	+	+
dr--------(400)	-wx------ (300)	-	-	-	-	-	+	-	-
dr-x------(500)	-wx------ (300)	-	-	+	-	+	+	-	+
drw-------(600)	-wx------ (300)	-	-	-	-	-	+	-	-
drwx------(700)	-wx------ (300)	+	+	+	-	+	+	+	+
d---------(000)	r-------- (400)	-	-	-	-	-	-	-	-
d--x------(100)	r-------- (400)	-	-	-	+	+	-	-	+
d-w-------(200)	r-------- (400)	-	-	-	-	-	-	-	-
d-wx------(300)	r-------- (400)	+	+	-	+	+	-	+	+
dr--------(400)	r-------- (400)	-	-	-	-	-	+	-	-
dr-x------(500)	r-------- (400)	-	-	-	+	+	+	-	+
drw-------(600)	r-------- (400)	-	-	-	-	-	+	-	-
drwx------(700)	r-------- (400)	+	+	-	+	+	+	+	+
d---------(000)	r-x------ (500)	-	-	-	-	-	-	-	-
d--x------(100)	r-x------ (500)	-	-	-	+	+	-	-	+
d-w-------(200)	r-x------ (500)	-	-	-	-	-	-	-	-
d-wx------(300)	r-x------ (500)	+	+	-	+	+	-	+	+
dr--------(400)	r-x------ (500)	-	-	-	-	-	+	-	-
dr-x------(500)	r-x------ (500)	-	-	-	+	+	+	-	+
drw-------(600)	r-x------ (500)	-	-	-	-	-	+	-	-
drwx------(700)	r-x------ (500)	+	+	-	+	+	+	+	+

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

Рис. 14.5. Таблица атрибутов

Вывод

В ходе лабораторной работы я получил практические навыки работы с атрибутами файлов и директории с использованием консоли операционной системы CentOS Linux, а также закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.