

Лабораторная работа №2

Дисциплина: Основы информационной безопасности

Жибицкая Евгения Дмитриевна

Содержание

| | | |
|----------|---------------------------------------|-----------|
| 1 | Цель работы | 5 |
| 2 | Выполнение лабораторной работы | 6 |
| 3 | Выводы | 14 |
| | Список литературы | 15 |

Список иллюстраций

| | | |
|-----|--|----|
| 2.1 | Создание нового пользователя | 6 |
| 2.2 | Учетная запись guest | 7 |
| 2.3 | Данные uid и gid | 7 |
| 2.4 | Права директорий | 7 |
| 2.5 | Новая директория | 8 |
| 2.6 | Обнуление всех прав | 8 |
| 2.7 | Запись в файл | 9 |
| 2.8 | Проверка прав | 9 |
| 2.9 | Проверка прав | 10 |

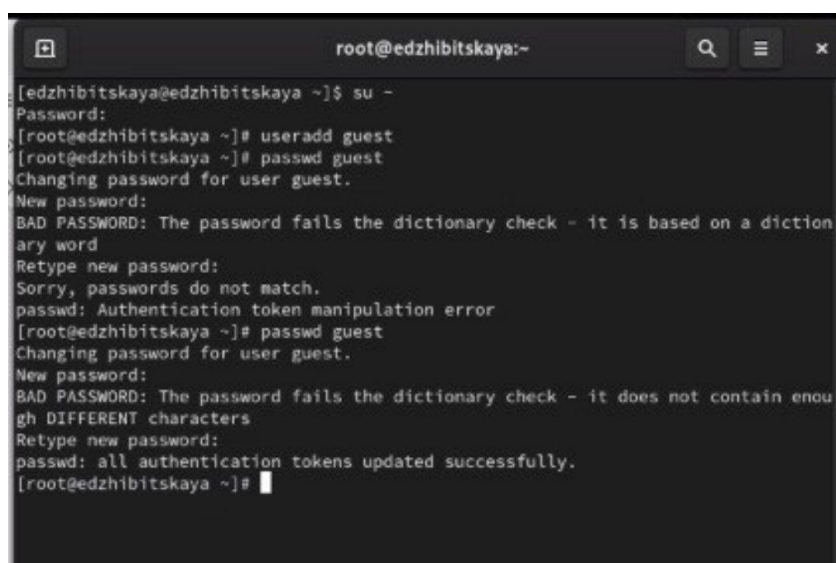
Список таблиц

1 Цель работы

Получение навыков работы с атрибутами файлов через консоль, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Выполнение лабораторной работы

Получим права администратора и создадим нового пользователя - guest. Зададим ему пароль(рис. 2.1).

A terminal window titled 'root@edzhbitskaya:~' with search, menu, and close icons in the title bar. The terminal shows the following commands and output:

```
[edzhbitskaya@edzhbitskaya ~]$ su -
Password:
[root@edzhbitskaya ~]# useradd guest
[root@edzhbitskaya ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[root@edzhbitskaya ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password fails the dictionary check - it does not contain enough DIFFERENT characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@edzhbitskaya ~]#
```

Рис. 2.1: Создание нового пользователя

Далее переходим в его учетную запись, переключаемся на домашнюю директорию, уеждаемся, что находимся в его аккаунте и получаем информацию об id и группах(рис. 2.2).

```
[guest@edzhbitskaya ~]$ pwd
/home/guest
[guest@edzhbitskaya ~]$ cd ~
[guest@edzhbitskaya ~]$ whoami
guest
[guest@edzhbitskaya ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@edzhbitskaya ~]$ groups
guest
[guest@edzhbitskaya ~]$
```

Рис. 2.2: Учетная запись guest

Затем получаем информацию из файла /etc/passwd о пользователе(рис. 2.3).

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

Рис. 2.3: Данные uid и gid

Определяем существующие директории вместе с правами и проверяем, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home(рис. 2.4).

```
[guest@edzhbitskaya ~]$ ls -l /home/
total 8
drwx-----, 17 edzhbitskaya edzhbitskaya 4096 Feb 15 13:12 edzhbitskaya
drwx-----, 14 guest          guest      4096 Feb 18 11:29 guest
[guest@edzhbitskaya ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/edzhbitskaya
----- /home/guest
[guest@edzhbitskaya ~]$
```

Рис. 2.4: Права директорий

Создадим новую директорию, посмотрим доступные ей разрешения и атрибуты(рис. 2.5).

```

[guest@edzhibitskaya ~]$ mkdir dir1
[guest@edzhibitskaya ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Desktop
drwxr-xr-x. 2 guest guest  6 Feb 18 11:40 dir1
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Documents
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Downloads
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Music
drwxr-xr-x. 2 guest guest 147 Feb 18 11:39 Pictures
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Public
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Templates
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Videos
[guest@edzhibitskaya ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@edzhibitskaya ~]$

```

Рис. 2.5: Новая директория

Обнулим все разрешения у каталога, посмотрим, что теперь их правда нет(рис. 2.6).

```

[guest@edzhibitskaya ~]$ chmod 000 dir1
[guest@edzhibitskaya ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Desktop
d----- . 2 guest guest  6 Feb 18 11:40 dir1
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Documents
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Downloads
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Music
drwxr-xr-x. 2 guest guest 4096 Feb 18 11:41 Pictures
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Public
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Templates
drwxr-xr-x. 2 guest guest  6 Feb 18 11:29 Videos
[guest@edzhibitskaya ~]$

```

Рис. 2.6: Обнуление всех прав

Попытаемся теперь записать что-то в файл, создав и его, но, столкнемся, что права на это у нас нет. Перейти в директорию и посмотреть созданся ли файл также невозможно(рис. 2.7).


```
[guest@edzhibitskaya ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@edzhibitskaya ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@edzhibitskaya ~]$
```

Рис. 2.7: Запись в файл

Примеры выполнения команд, необходимых для заполнения таблицы(рис. ??) и (рис. 2.8) и (рис. 2.9).

```
[guest@edzhibitskaya ~]$ chmod 600 dir1
[guest@edzhibitskaya ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@edzhibitskaya ~]$ chmod 700 dir1
[guest@edzhibitskaya ~]$ rm dir1/file1
[guest@edzhibitskaya ~]$
```

```
[guest@edzhibitskaya ~]$ chmod 500 dir1
[guest@edzhibitskaya ~]$ ls -l /home/guest/dir1
total 4
-rw-r--r--. 1 guest guest 5 Feb 18 12:02 file1
[guest@edzhibitskaya ~]$ touch file1
[guest@edzhibitskaya ~]$ chmod 200 file1
[guest@edzhibitskaya ~]$ echo "Hello" > file1
[guest@edzhibitskaya ~]$ rm file1
```

Рис. 2.8: Проверка прав

```

[guest@edzhibitskaya ~]$ chmod 200 dir1
[guest@edzhibitskaya ~]$ touch dir1/file1
touch: cannot touch 'dir1/file1': Permission denied
[guest@edzhibitskaya ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@edzhibitskaya ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@edzhibitskaya ~]$ chmod 300 dir1
[guest@edzhibitskaya ~]$ touch dir1/file1
[guest@edzhibitskaya ~]$

[guest@edzhibitskaya ~]$ echo "test" > /home/guest/dir1/file1
[guest@edzhibitskaya ~]$ cd dir1/
[guest@edzhibitskaya dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest@edzhibitskaya dir1]$ cd ~
[guest@edzhibitskaya ~]$ rmdir dir1
rmdir: failed to remove 'dir1': Directory not empty
[guest@edzhibitskaya ~]$ rm dir1/file1
[guest@edzhibitskaya ~]$ rmdir dir1
[guest@edzhibitskaya ~]$

```

Рис. 2.9: Проверка прав

Заполним таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-».

| Права ди- ректо- рии | Права фай- ла | Созда- ние фай- ла | Удале- ние фай- ла | За- пись в файл | Чте- ние фай- ла | Сме- на ди- ректо- рии | Про- смотр фай- лов в ди- ректо- рии | Переиме- нование фай- ла | Сме- на атри- бутов фай- ла |
|-------------------------------|---------------------|-----------------------------|-----------------------------|--------------------------|---------------------------|------------------------------------|--|-----------------------------------|--|
| d(000) | (000) | - | - | - | - | - | - | - | - |
| d(000) | (100) | - | - | - | - | - | - | - | - |
| d(000) | (200) | - | - | - | - | - | - | - | - |
| d(000) | (300) | - | - | - | - | - | - | - | - |
| d(000) | (400) | - | - | - | - | - | - | - | - |

| | | | | | | | | | |
|--------|-------|---|---|---|---|---|---|---|---|
| d(000) | (500) | - | - | - | - | - | - | - | - |
| d(000) | (600) | - | - | - | - | - | - | - | - |
| d(000) | (700) | - | - | - | - | - | - | - | - |
| d(100) | (000) | - | - | - | - | + | - | - | + |
| d(100) | (100) | - | - | - | - | + | - | - | + |
| d(100) | (200) | - | - | + | - | + | - | - | + |
| d(100) | (300) | - | - | + | - | + | - | - | + |
| d(100) | (400) | - | - | - | + | + | - | - | + |
| d(100) | (500) | - | - | - | + | + | - | - | + |
| d(100) | (600) | - | - | + | + | + | - | - | + |
| d(100) | (700) | - | - | + | + | + | - | - | + |
| d(200) | (000) | - | - | - | - | - | - | - | - |
| d(200) | (100) | - | - | - | - | - | - | - | - |
| d(200) | (200) | - | - | - | - | - | - | - | - |
| d(200) | (300) | - | - | - | - | - | - | - | - |
| d(200) | (400) | - | - | - | - | - | - | - | - |
| d(200) | (500) | - | - | - | - | - | - | - | - |
| d(200) | (600) | - | - | - | - | - | - | - | - |
| d(200) | (700) | - | - | - | - | - | - | - | - |
| d(300) | (000) | + | + | - | - | + | - | + | + |
| d(300) | (100) | + | + | - | - | + | - | + | + |
| d(300) | (200) | + | + | + | - | + | - | + | + |
| d(300) | (300) | + | + | + | - | + | - | + | + |
| d(300) | (400) | + | + | - | + | + | - | + | + |
| d(300) | (500) | + | + | - | + | + | - | + | + |
| d(300) | (600) | + | + | + | + | + | - | + | + |
| d(300) | (700) | + | + | + | + | + | - | + | + |
| d(400) | (000) | - | - | - | - | - | + | - | - |

| | | | | | | | | | |
|--------|-------|---|---|---|---|---|---|---|---|
| d(400) | (100) | - | - | - | - | - | + | - | - |
| d(400) | (200) | - | - | - | - | - | + | - | - |
| d(400) | (300) | - | - | - | - | - | + | - | - |
| d(400) | (400) | - | - | - | - | - | + | - | - |
| d(400) | (500) | - | - | - | - | - | + | - | - |
| d(400) | (600) | - | - | - | - | - | + | - | - |
| d(400) | (700) | - | - | - | - | - | + | - | - |
| d(500) | (000) | - | - | - | - | + | + | - | + |
| d(500) | (100) | - | - | - | - | + | + | - | + |
| d(500) | (200) | - | - | + | - | + | + | - | + |
| d(500) | (300) | - | - | + | - | + | + | - | + |
| d(500) | (400) | - | - | - | + | + | + | - | + |
| d(500) | (500) | - | - | - | + | + | + | - | + |
| d(500) | (600) | - | - | + | + | + | + | - | + |
| d(500) | (700) | - | - | + | + | + | + | - | + |
| d(600) | (000) | - | - | - | - | - | + | - | - |
| d(600) | (100) | - | - | - | - | - | + | - | - |
| d(600) | (200) | - | - | - | - | - | + | - | - |
| d(600) | (300) | - | - | - | - | - | + | - | - |
| d(600) | (400) | - | - | - | - | - | + | - | - |
| d(600) | (500) | - | - | - | - | - | + | - | - |
| d(600) | (600) | - | - | - | - | - | + | - | - |
| d(600) | (700) | - | - | - | - | - | + | - | - |
| d(700) | (000) | + | + | - | - | + | + | + | + |
| d(700) | (100) | + | + | - | - | + | + | + | + |
| d(700) | (200) | + | + | + | - | + | + | + | + |
| d(700) | (300) | + | + | + | - | + | + | + | + |
| d(700) | (400) | + | + | - | + | + | + | + | + |

| | | | | | | | | | |
|--------|-------|---|---|---|---|---|---|---|---|
| d(700) | (500) | + | + | - | + | + | + | + | + |
| d(700) | (600) | + | + | + | + | + | + | + | + |
| d(700) | (700) | + | + | + | + | + | + | + | + |

Таблица 2.1.

На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполним табл. 2.2

| Операция | Минималь- ные права на директорию | Минималь- ные права на файл |
|-----------------------------|---|-----------------------------------|
| Создание файла | d(300) | (000) |
| Удаление файла | d(300) | (000) |
| Чтение файла | d(100) | (400) |
| Запись в файл | d(100) | (200) |
| Переименова- ние файла | d(300) | (000) |
| Создание под- директории | d(300) | (000) |
| Удаление под- директории | d(300) | (100) |

Таблица 2.2.

3 Выводы

В ходе работы был создан новый пользователь, определены необходимые права доступа к файлам и директориям, приобретены навыки по работе с ними.

Список литературы

ТУИС