Лабораторная работа №4

Дисциплина: Основы информационной безопасности

Первойкин Илья Сергеевич

Содержание

Список иллюстраций

Список таблиц

Цель работы

Цель данной лабораторной работы — Получить навыки работы в консоли с расширенными атрибутами файлов.

Теоретические данные

Атрибуты — это набор основных девяти битов, определяющих какие из пользователей обладают правами на чтение, запись и исполнение. Первые три бита отвечают права доступа владельца, вторые — для группы пользователей, последние — для всех остальных пользователей в системе.

Установка атрибутов производится командой chmod. Установка бита чтения (r) позволяет сделать файл доступным для чтения. Наличие бита записи (w) позволяет изменять файл. Установка бита запуска (x) позволяет запускать файл на исполнение.

Расширенные атрибуты — это система дополнительной информации, которая может быть добавлена к файлу или директории в файловой системе.

Некоторые примеры расширенных атрибутов:

- a — файл можно открыть только в режиме добавления.
- A — при доступе к файлу его запись atime не изменяется.
- c — файл автоматически сжимается.
- e — файл использует экстенты.
- E — файл, каталог или символьная ссылка зашифрованы файловой системой.
- F — поиски путей в директории выполняются без учёта регистра.
- i — файл не может быть изменён.
- m — файл не сжимается.

Установка атрибутов производится командой chmod. Установка бита чтения (r) позволяет сделать файл доступным для чтения. Наличие бита записи (w)

позволяет изменять файл. Установка бита запуска (x) позволяет запускать файл на исполнение.

В ОС Linux, группа — это набор пользователей. Основная цель групп — это определить права на чтение, запись и исполнение сразу для нескольких пользователей, состоящих в группе. Так же пользователи могут быть добавлены в уже существующие группы для получения их прав.

Группы бывают двух видов:

- Первичная группа — это группа, приписанная к файлам, созданным пользователем. Обычно имя первичной группы совпадает с именем пользователя. У каждого пользователя может быть только одна первичная группа.
- Вторичная группа — используется для определения прав для набора пользователей. Пользователь может состоять в нескольких вторичных группах или не состоять ни в одной.

Задание

1.Определить расширенные атрибуты файла в Виртуальной машине. 2.Установка расширенного атрибута “a” на файл 3.Снять расширенные атрибуты “a” с файла

Выполнение лабораторной работы

1). От имени пользователя guest1 просмотрел расширенные атрибуты файла file1 с помощью команды lsattr. После этого изменил права на этот файл с помощью команды chmod 600 file1, сделав его доступным только для чтения и записи. Далее при попытке добавить расширенный атрибут с помощью команды chattr я получил сообщение об ошибке.

Рис. 1: Проверка расширенных атрибутов

2). От имени администратора в другой консоли добавил файлу file1 аттрибут a командой chattr +a. Также убедился в корректном установлении атрибута с помощью команды lsattr.

```
[guest1@localhost ~]$ sudo chattr +a /home/guest1/dir1/file1

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for guest1:
guest1 is not in the sudoers file.  This incident will be reported.
[guest1@localhost ~]$ su
Password:
[root@localhost guest1]# sudo chattr +a /home/guest1/dir1/file1
[root@localhost guest1]#
```

Рис. 2: Установка расширенного атрибута a

```
[root@localhost guest1]# lsattr /home/guest1/dir1/file1
-----a---------- /home/guest1/dir1/file1
[root@localhost guest1]# echo "test" /home/guest1/
.bash_logout   .config/       Documents/     .local/        Public/
.bash_profile  .dbus/         Downloads/     .mozilla/      .redhat/
.bashrc        Desktop/       .esd_auth      Music/         Templates/
.cache/        dir1/          .ICEauthority  Pictures/      Videos/
[root@localhost guest1]# echo "test" /home/guest1/dir1/file1
test /home/guest1/dir1/file1
[root@localhost guest1]#
```

Рис. 3: Проверка корректнсти установки атрибута +a

3). Дозаписал в конец файла новую информацию с помощью команды echo » и проверил, что это действительно произошло, используя команду cat. После этого попытался стереть информацию в файле с помощью команды echo >, на что получил ошибку. Мне также не удалось переименовать файл и изменить его атрибуты командой chmod из-за той же ошибки в правах доступа.

```
[root@localhost guest1]# echo "test" /home/guest1/dir1/file1
test /home/guest1/dir1/file1
[root@localhost guest1]# cat /home/guest1/dir1/file1
[root@localhost guest1]# echo "abcd" /home/guest1/dir1/file1
abcd /home/guest1/dir1/file1
[root@localhost guest1]# cat /home/guest1/dir1/file1
[root@localhost guest1]# echo "test" >> /home/guest1/dir1/file1
[root@localhost guest1]# echo "abcd" >> /home/guest1/dir1/file1
[root@localhost guest1]# cat /home/guest1/dir1/file1
test
abcd
[root@localhost guest1]# echo "abcd" > /home/guest1/dir1/file1
bash: /home/guest1/dir1/file1: Operation not permitted
[root@localhost guest1]# rename file1 file2 /home/guest1/dir1/file1
rename: /home/guest1/dir1/file1: rename to /home/guest1/dir1/file2 failed: Opera
tion not permitted
[root@localhost guest1]# chmod 000 /home/guest1/dir1/file1
chmod: changing permissions of ‘/home/guest1/dir1/file1’: Operation not permitte
d
[root@localhost guest1]#
```

Рис. 4: Проверка действий при наличии атрибута a

4). Снял расширенный атрибут “a” командой chattr -a от лица администратора. При повторе ранее описанных действий теперь не произошло ошибок и они все выполнились.

```
[root@localhost guest1]# sudo chattr -a /home/guest1/dir1/file1
[root@localhost guest1]# echo "abcd" > /home/guest1/dir1/file1
[root@localhost guest1]# rename file1 file2 /home/guest1/dir1/file1
[root@localhost guest1]# /home/guest1/dir1/file1
bash: /home/guest1/dir1/file1: No such file or directory
[root@localhost guest1]# rename file2 file1 /home/guest1/dir1/file2
[root@localhost guest1]# chmod 000 /home/guest1/dir1/file1
[root@localhost guest1]#
[root@localhost guest1]# chmod 000 /home/guest1/dir1/file1
[root@localhost guest1]#
```

Рис. 5: Проверка действий при отсутствии атрибута a

5). От имени адмистратора добавил файлу расширенный атрибут i и повторил действия, описанные раннее. В итоге получил, что в этом случае файл можно только читать, но его нельзя никак изменить.

```
[root@localhost guest1]# chattr +i /home/guest1/dir1/file1
[root@localhost guest1]#
```

Рис. 6: Установка атрибута i

```
[root@localhost guest1]# lsattr /home/guest1/dir1/file1
----i----------- /home/guest1/dir1/file1
[root@localhost guest1]# echo "12345" /home/guest1/dir1/file1
12345 /home/guest1/dir1/file1
[root@localhost guest1]# echo "12345" >> /home/guest1/dir1/file1
bash: /home/guest1/dir1/file1: Permission denied
[root@localhost guest1]# cat /home/guest1/dir1/file1
abcd
[root@localhost guest1]# echo "abcd" >> /home/guest1/dir1/file1
bash: /home/guest1/dir1/file1: Permission denied
[root@localhost guest1]# rename file1 file2 /home/guest1/dir1/file1
rename: /home/guest1/dir1/file1: rename to /home/guest1/dir1/file2 failed: Opera
tion not permitted
[root@localhost guest1]# chmod 000 /home/guest1/dir1/file1
chmod: changing permissions of ‘/home/guest1/dir1/file1’: Operation not permitte
d
[root@localhost guest1]#
```

Рис. 7: Проверка действий при наличии атрибута i

Выводы

Приобрел практические навыки работы с расширенными атрибутами файлов через консоль, опробовал на практике действия с файлами с установленными на них расширенными атрибутами a и i .

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 №4 - https://esystem.rudn.ru/pluginfile.php/2090127/mod_resource/content/3/004-lab_discret_extattr.pdf

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

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

1.[Электронный ресурс] - доступ: https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux

2.[Электронный ресурс] - доступ: https://debianinstall.ru/diskretsionnoe-razgranichenie-dostupa-linux/