Отчет по лабораторной работе №5

Основы информационной безопасности

Назармамадов Умед Джамшедович

Содержание

Список иллюстраций

Список таблиц

Элементы списка иллюстраций не найдены.

Цель работы

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в кон- соли с дополнительными атрибутами.

Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Теоретическое введение

Дополнительные атрибуты файлов Linux В Linux существует три основных вида прав — право на чтение (read), запись (write) и выполнение (execute), а также три категории пользователей, к которым они могут применяться — владелец файла (user), группа владельца (group) и все остальные (others). Но, кроме прав чтения, выполнения и записи, есть еще три дополнительных атрибута. [@u]

Sticky bit

Используется в основном для каталогов, чтобы защитить в них файлы. В такой каталог может писать любой пользователь. Но, из такой директории пользователь может удалить только те файлы, владельцем которых он является. Примером может служить директория /tmp, в которой запись открыта для всех пользователей, но нежелательно удаление чужих файлов.

SUID (Set User ID)

Атрибут исполняемого файла, позволяющий запустить его с правами владельца. В Linux приложение запускается с правами пользователя, запустившего указанное приложение. Это обеспечивает дополнительную безопасность т.к. процесс с правами пользователя не сможет получить доступ к важным системным файлам, которые принадлежат пользователю root.

SGID (Set Group ID)

Аналогичен suid, но относиться к группе. Если установить sgid для каталога, то все файлы созданные в нем, при запуске будут принимать идентификатор группы каталога, а не группы владельца, который создал файл в этом каталоге.

Обозначение атрибутов sticky, suid, sgid

Специальные права используются довольно редко, поэтому при выводе программы ls -l символ, обозначающий указанные атрибуты, закрывает символ стандартных прав доступа.

Пример: rwsrwsrwt

где первая s — это suid, вторая s — это sgid, а последняя t — это sticky bit

В приведенном примере не понятно, rwt — это rw- или rwx? Определить это просто. Если t маленькое, значит x установлен. Если T большое, значит x не установлен. То же самое правило распространяется и на s.

В числовом эквиваленте данные атрибуты определяются первым символом при четырехзначном обозначении (который часто опускается при назначении прав),

например в правах 1777 — символ 1 обозначает sticky bit. Остальные атрибуты имеют следующие числовое соответствие:

1 — установлен sticky bit 2 — установлен sgid 4 — установлен suid

Компилятор GCC GCC - это свободно доступный оптимизирующий компилятор для языков C, C++. Собственно программа gcc это некоторая надстройка над группой компиляторов, которая способна анализировать имена файлов, передаваемые ей в качестве аргументов, и определять, какие действия необходимо выполнить. Файлы с расширением .cc или .C рассматриваются, как файлы на языке C++, файлы с расширением .c как программы на языке C, а файлы с расширением .o считаются объектными.

Выполнение лабораторной работы

обновляю пакеты и ставлю утилиту e2fsprogs (там есть chattr и lsattr) (рис. [-@fig:001]).

```
umedn@HUAWEI: sudo apt update && sudo apt install -y e2fsprogs
```

обновляю пакеты

обновляю пакеты

захожу в домашний каталог пользователя guest, создаю каталог dir1 и файл file1.

```
umedn@HUAWEI: su - guest
umedn@HUAWEI: mkdir -p ~/dir1
umedn@HUAWEI: echo "start" > ~/dir1/file1
```

захожу в домашний каталог

захожу в домашний каталог

смотрю расширенные атрибуты файла.

```
umedn@HUAWEI: lsattr ~/dir1/file1
```

смотрю расширенные

смотрю расширенные

проверяю права доступа.

```
umedn@HUAWEI: ls -l ~/dir1/file1
```

проверяю права

проверяю права

пробую поставить a (append-only) как guest. Должно выдать отказ.

```
umedn@HUAWEI: chattr +a ~/dir1/file1
```

пробую поставить

пробую поставить

выхожу из guest и ставлю a с sudo.

```
umedn@HUAWEI: exit
umedn@HUAWEI: sudo chattr +a /home/guest/dir1/file1
```

выхожу из guest

выхожу из guest

проверяю, что a появился.

```
umedn@HUAWEI: su - guest
umedn@HUAWEI: lsattr ~/dir1/file1
```

проверяю

проверяю

дозаписываю строку в файл (>>).

```
umedn@HUAWEI: echo "append" >> ~/dir1/file1
umedn@HUAWEI: cat ~/dir1/file1
```

проверяю

проверяю

пробую перезаписать файл (>). Должно выдать отказ.

```
umedn@HUAWEI: echo "newtext" > ~/dir1/file1
```

проверяю

проверяю

пробую удалить файл. Должно выдать отказ.

```
umedn@HUAWEI: rm ~/dir1/file1
```

проверяю

проверяю

снимаю атрибут a от root.

```
umedn@HUAWEI: exit
umedn@HUAWEI: sudo chattr -a /home/guest/dir1/file1
```

снимаю атрибут

снимаю атрибут

пробую снова перезаписать и удалить. Теперь должно работать.

```
umedn@HUAWEI: su - guest
umedn@HUAWEI: echo "newtext" > ~/dir1/file1
umedn@HUAWEI: rm ~/dir1/file1
```

снимаю атрибут

снимаю атрибут

создаю заново файл и ставлю i.

```
umedn@HUAWEI: echo "immutable" > ~/dir1/file1
umedn@HUAWEI: exit
umedn@HUAWEI: sudo chattr +i /home/guest/dir1/file1
```

создаю заново файл

создаю заново файл

проверяю атрибуты

```
umedn@HUAWEI: su - guest
umedn@HUAWEI: lsattr ~/dir1/file1
```

проверяю

проверяю

пробую дозапись, перезапись, chmod, rename и удаление. Всё должно запрещаться.

```
umedn@HUAWEI: echo "add" >> ~/dir1/file1
umedn@HUAWEI: echo "replace" > ~/dir1/file1
umedn@HUAWEI: chmod 000 ~/dir1/file1
umedn@HUAWEI: mv ~/dir1/file1 ~/dir1/file2
umedn@HUAWEI: rm ~/dir1/file1
```

пробую дозапись

пробую дозапись

снимаю i от root и удаляю файл.

```
umedn@HUAWEI: exit
umedn@HUAWEI: sudo chattr -i /home/guest/dir1/file1
umedn@HUAWEI: rm /home/guest/dir1/file1
```

пробую дозапись

пробую дозапись

Выводы

В ходе работы было изучено, как изменяются идентификаторы пользователей и процессов, а также применены SetUID- и Sticky-биты. Получены практические навыки работы в консоли с дополнительными атрибутами. Рассмотрено действие механизма смены идентификаторов процессов, а также влияние Sticky-бита на операции записи и удаления файлов.

Список литературы