Лабораторная работа №4

Дискреционное разграничение прав в Linux. Расширенные атрибуты.

Пономарева Лилия Михайловна

Содержание

Список иллюстраций

Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов[1].

Теоретическое введение

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов к объектам, которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ, которые работают от лица псевдопользовательских учетных записей.

В рамках дискреционного разграничения доступа каждому файлу назначен пользователь-владелец и группа-владелец файла.

В метаданных каждого объекта содержится список разрешений на доступ к нему для разных категорий субъектов.

Атрибуты Minimal ACL поддерживают три базовых класса субъектов доступа к файлу (класс All объединяет все три класса):

User access (u) – доступ для владельца файла;

Group access (g) – доступ для группы, владеющей файлом;

Other access (o) – доступ для остальных пользователей (кроме пользователя root);

All access (a) – доступ для всех субъектов доступа (u, g, o).

Для каждого из этих классов определены три типа разрешений:

На чтение содержимого файла (read) – символ «r».

На запись внутри файла или изменения его содержимого (write) – символ «w».

На исполнение файла (если это бинарный исполняемый файл или файл сценария интерпретатора (execute)) – символ «x».

Для директорий трактовка типов разрешений иная:

r – разрешение на «открытие» директории, то есть на чтение списка файлов, которые содержит эта директория.

w – разрешение на модификацию этого списка файлов (создание/удаление/переименование/
файлов этой директории.

x – разрешение на «исполнение» директории, то есть на возможность перейти в нее.

Чтобы изменить расширения для определенного файла используется команда chmod с соответствующими аргументами.

Расширенные атрибуты.

chattr изменяет атрибуты файлов в файловой системе Linux.

Формат символьного режима: +-=[aAcCdDeFijmPsStTux].

Оператор «+» вызывает добавление выбранных атрибутов к существующим атрибутам файлов; «-» заставляет их удалить; и «=» делает их единственными атрибутами файлов.

Буквы «aAcCdDeFijmPsStTux» выбирают новые атрибуты для файлов:

только добавление (a), без обновлений времени (A), сжатие (c), без копирования при записи (C), без дампа (d), синхронные обновления каталогов (D), формат экстента (e), поиск в каталогах без учёта регистра (F), неизменяемый (i), ведение журнала данных (j), без сжатия (m), иерархия проекта (P), безопасное удаление (s), синхронные обновления (S), без слияния хвостов (t), вершина иерархии каталогов (T), возможность восстановления после удаления (u) и прямой доступ к файлам (x).

a

Файл с установленным атрибутом «a» можно открыть только в режиме добавления для записи. Только суперпользователь или процесс, обладающий возможностью CAP_LINUX_IMMUTABLE, может установить или очистить этот атрибут.

i

Файл с атрибутом «i» не может быть изменён: его нельзя удалить или переименовать, нельзя создать ссылку на этот файл, большую часть метаданных файла нельзя изменить, и файл нельзя открыть в режиме записи. Только суперпользователь или процесс, обладающий возможностью CAP_LINUX_IMMUTABLE, может установить или очистить этот атрибут.

Выполнение лабораторной работы

1. От имени пользователя guest определила расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /home/guest/dir1/file1 (рис. 1).

Рис. 1: Определение расширенных атрибутов файла

2. Установила командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла (рис. 2).

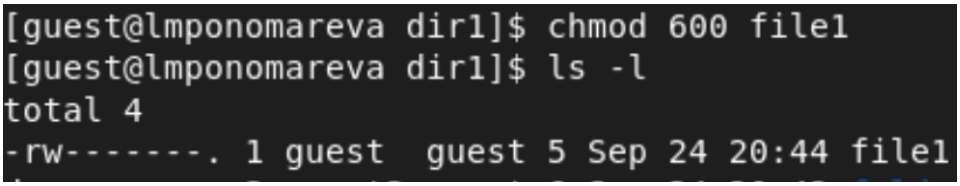

Рис. 2: Права, разрешающие чтение и запись для владельца

3. Попробовала установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest: chattr +a /home/guest/dir1/file1 (рис. 3).

Рис. 3: Установка расширенного атрибута от имени обычного пользователя

В ответ получила отказ в выполнении операции.

4. Попробовала установить расширенный атрибут a на файл /home/guest/dir1/file1 от имени суперпользователя: chattr +a /home/guest/dir1/file1 (рис. 4).

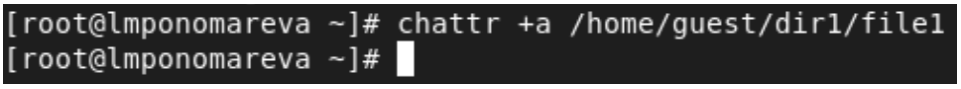

Рис. 4: Установка расширенного атрибута от имени суперпользователя

5. От пользователя guest проверила правильность установления атрибута: lsattr /home/guest/dir1/file1 (рис. 5).

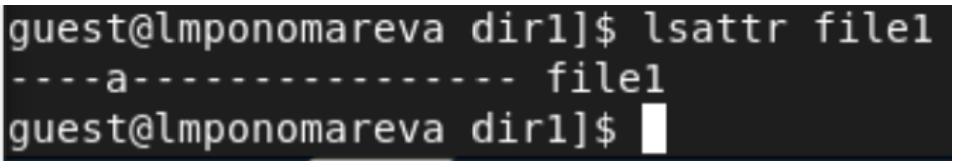

Рис. 5: Правильность установления атрибута

6. Выполнила дозапись в файл file1 слова «test» командой echo “test” » /home/guest/dir1/file1 и выполнила чтение файла file1 командой cat /home/guest/dir1/file1 (рис. 6).

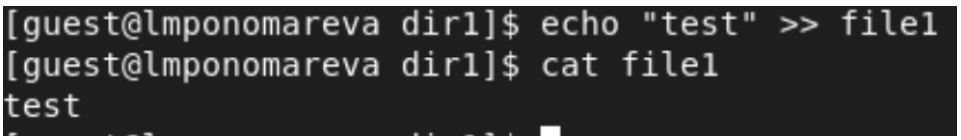

Рис. 6: Запись и чтение файла

7. Попробовала удалить файл file1 (рис. 7).

```
[guest@lmponomareva dir1]$ rm file1
rm: cannot remove 'file1': Operation not permitted
[guest@lmponomareva dir1]$
```

Рис. 7: Попытка удаления файла файла

Попробовала переименовать файл (рис. 8).

```
[guest@lmponomareva dir1]$ mv file1 file2
mv: cannot move 'file1' to 'file2': Operation not permitted
[guest@lmponomareva dir1]$
```

Рис. 8: Попытка переименовать файл

Попробовала перезаписать файл (рис. 9).

```
[guest@lmponomareva dir1]$ echo "test" > file1
bash: file1: Operation not permitted
```

Рис. 9: Запись в файл

8. Попробовала с помощью команды chmod 000 file1 установить на файл file1 права, запрещающие чтение и запись для владельца файла (рис. 10).

```
[guest@lmponomareva dir1]$ chmod 000 file1
chmod: changing permissions of 'file1': Operation not permitted
[guest@lmponomareva dir1]$
```

Рис. 10: Попытка изменения прав доступа файла

9. Сняла расширенный атрибут a с файла /home/guest/dirl/file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1 (рис. 11).

```
[root@lmponomareva ~]# chattr -a /home/guest/dir1/file1
[root@lmponomareva ~]#
```

Рис. 11: Снятие расширенного атрибута a

Повторила операции, которые ранее не удавалось выполнить (рис. 12).

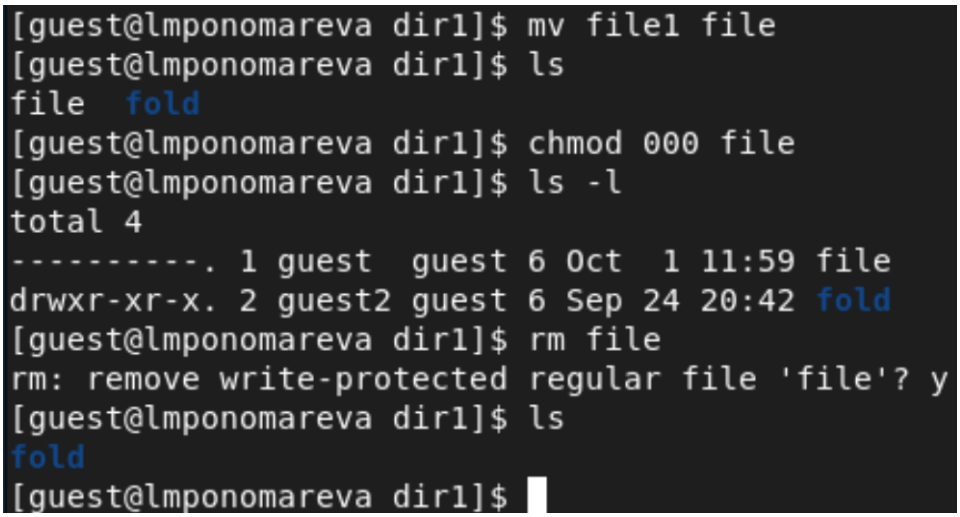

Рис. 12: Повтор операций

Теперь у нас есть возможность менять права доступа, название файла, а также можем его удалить.

10. Повторила свои действия, заменив атрибут «a» атрибутом «i» (рис. 13).

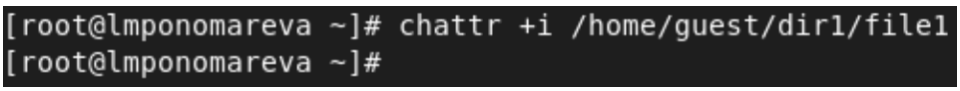

Рис. 13: Добавление атрибута i

На этот раз мы не можем производить никакие действия над файлом, в том числе и дозапись (рис. 14).

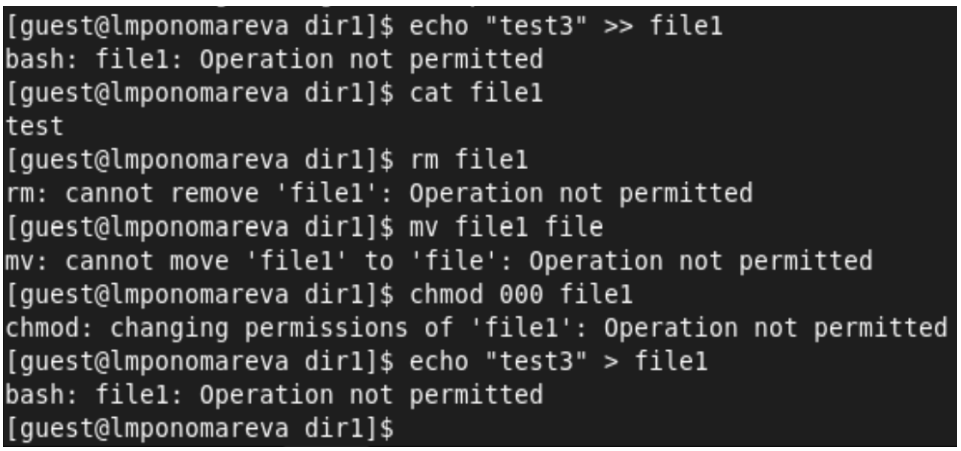

Рис. 14: Операции с новым атрибутом

Выводы

В результате выполнения работы вы повысили свои навыки использования интерфейса командой строки (CLI), познакомились на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имели возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux. Опробовали на практике действие расширенных атрибутов «a» и «i».

Список литературы

1. Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3.