Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

Задание

Выполнить задания лабораторной работы и проанализировать полученные результаты.

Теоретическое введение

Дискреционное управление доступом (англ. discretionary access control, DAC) — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа. Также используются названия избирательное управление доступом, контролируемое управление доступом и разграничительное управление доступом.

Для каждой пары (субъект — объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа, то есть тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту).

Возможны несколько подходов к построению дискреционного управления доступом:

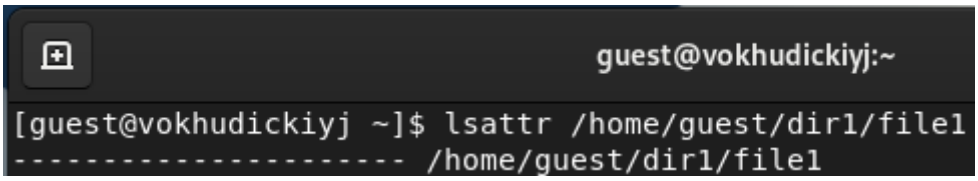
- Каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту.
- Система имеет одного выделенного субъекта — суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.
- Субъект с определённым правом доступа может передать это право любому другому субъекту.

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем, например Unix.

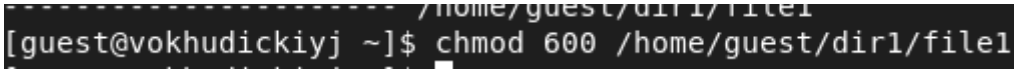
Избирательное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.

Выполнение лабораторной работы

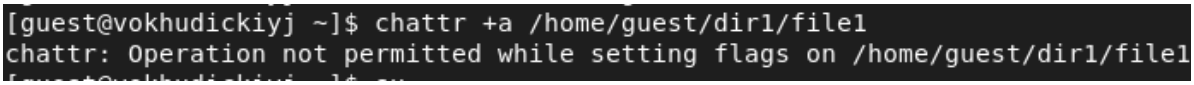
1. От имени пользователя guest определил расширенные атрибуты файла /home/guest/dir1/file1 командой *lsattr /home/guest/dir1/file1:*



2. Установил командой *chmod 600 /home/guest/dir1/file1* на файл file1 права, разрешающие чтение и запись для владельца файла:



3. Попробовал установить на файл /home/guest/dir1/file1 расширенный атрибут **a** от имени пользователя guest командой *chattr +a /home/guest/dir1/file1*. В ответ получил отказ от выполнения операции:

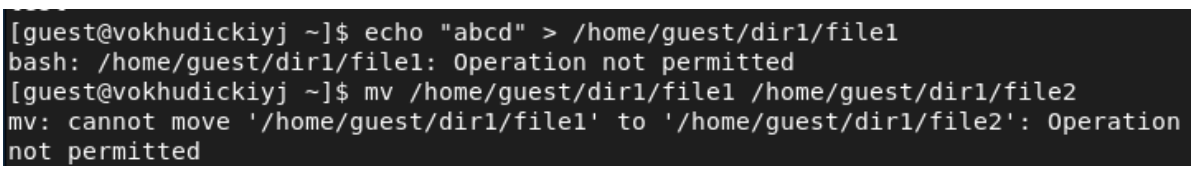


4. Повысил свои права с помощью команды *su*. Установил расширенный атрибут **a** на файл /home/guest/dir1/file1 от имени суперпользователя командой *chattr +a /home/guest/dir1/file1*:

5. От пользователя guest проверил правильность установления атрибута командой *lsattr /home/guest/dir1/file1*:

6. Выполнил дозапись в файл file1 слова «test» командой *echo "test" >> /home/guest/dir1/file1*. После этого выполнил чтение файла file1 командой *cat /home/guest/dir1/file1*. Убедился, что слово test было успешно записано в file1.

7. Попробовал стереть имеющуюся в файле file1 информацию командой *echo "abcd" > /home/guest/dirl/file1*. Попробовал переименовать файл командой *mv /home/guest/dirl/file1 /home/guest/dirl/file2*. Команды не удалось выполнить:



8. Попробовал с помощью команды *chmod 000 /home/guest/dirl/file1* установить на файл file1 права, запрещающие чтение и запись для владельца файла. Успешно выполнить указанную команду не удалось:

```
[guest@vokhudickiyj ~]$ chmod 000 /home/guest/dir1/file1
chmod: changing permissions of '/home/guest/dir1/file1': Operation not permitted
```

9. Снял расширенный атрибут **a** с файла /home/guest/dirl/file1 от имени суперпользователя командой *chattr -a /home/guest/dir1/file1*.
   Повторил операции, которые ранее не удавалось выполнить. Теперь их удалось выполнить:

```
[root@vokhudickiyj guest]# chattr -a /home/guest/dir1/file1
[root@vokhudickiyj guest]# su guest
[guest@vokhudickiyj ~]$ echo "abcd" > /home/guest/dir1/file1
[guest@vokhudickiyj ~]$ mv /home/guest/dir1/file1 /home/guest/dir1/file2
[guest@vokhudickiyj ~]$ cat /home/guest/dir1/file2
abcd
[guest@vokhudickiyj ~]$ chmod 000 /home/guest/dir1/file2
```

10. Повторил действия по шагам, заменив атрибут «a» атрибутом «i». Дозаписать информацию в файл не удалось. Также не удалось изменить название файла и права доступа.

```
[guest@vokhudickiyj ~]$ chmod 600 /home/guest/dir1/file2
[guest@vokhudickiyj ~]$ chattr +i /home/guest/dir1/file2
chattr: Operation not permitted while setting flags on /home/guest/dir1/file2
[guest@vokhudickiyj ~]$ su
Password:
[root@vokhudickiyj guest]# chattr +i /home/guest/dir1/file2
[root@vokhudickiyj guest]# su guest
[guest@vokhudickiyj ~]$ lsattr /home/guest/dir1/file2
----i----------------- /home/guest/dir1/file2
[guest@vokhudickiyj ~]$ echo "test" > /home/guest/dir1/file2
bash: /home/guest/dir1/file2: Operation not permitted
[guest@vokhudickiyj ~]$ mv /home/guest/dir1/file2 /home/guest/dir1/file1
mv: cannot move '/home/guest/dir1/file2' to '/home/guest/dir1/file1': Operation
not permitted
[guest@vokhudickiyj ~]$ chmod 000 /home/guest/dir1/file2
chmod: changing permissions of '/home/guest/dir1/file2': Operation not permitted
[guest@vokhudickiyj ~]$
```

Выводы

В результате выполнения работы я повысил свои навыки использования интерфейса командой строки (CLI), познакомился на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имел возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux. Составил наглядные таблицы, поясняющие какие операции возможны при тех или иных установленных правах. Опробовал действие на практике расширенных атрибутов «a» и «i».

Список литературы

- Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №4. Дискреционное разграничение прав в Linux. Расширенные атрибуты