Лабораторная работа 5

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.1.

Ким Эрика Алексеевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов1

2 Теоретическое введение

Более подробно про Unix см. в [1–4].

3 Выполнение лабораторной работы

1. От имени пользователя guest определили расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /home/guest/dir1/file1 (рис. 3.1).

Рис. 3.1: 1

2. Установили командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла (рис. 3.2).

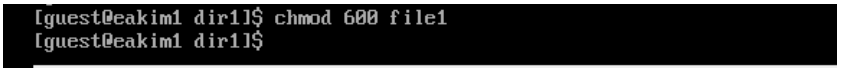

Рис. 3.2: 2

3. Попробовали установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest: chattr +a /home/guest/dir1/file1 (рис. 3.3).

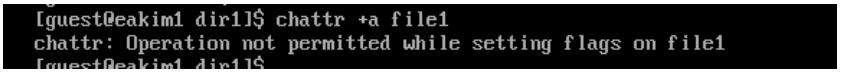

Рис. 3.3: 3

4. Зашли на третью консоль с правами администратора либо повысили права с помощью команды su. Попробовали установить расширенный атрибут a на файл /home/guest/dir1/file1 от имени суперпользователя: chattr +a /home/guest/dir1/file1 (рис. 3.4).

Рис. 3.4: 4

5. От пользователя guest проверили правильность установления атрибута: lsattr /home/guest/dir1/file1 (рис. 3.5).

Рис. 3.5: 5

6. Выполнили дозапись в файл file1 слова «test» командой echo “test” /home/guest/dir1/file1. После этого выполнили чтение файла file1 командой cat /home/guest/dir1/file1. Убедились, что слово test было успешно записано в file1. (рис. 3.6).

Рис. 3.6: 6

7. Попробовали удалить файл file1 либо стереть имеющуюся в нём информацию командой echo “abcd” > /home/guest/dirl/file1.Попробовали переименовать файл. (рис. 3.7).

Рис. 3.7: 7

8. Попробовали с помощью команды chmod 000 file1 установить на файл file1 права, например, запрещающие чтение и запись для владельца файла. Команда сработала. (рис. 3.8).

Рис. 3.8: 8

9. Сняли расширенный атрибут a с файла /home/guest/dirl/file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1. (рис. 3.9).

Рис. 3.9: 9

10. Повторили операции, которые ранее не удавалось выполнить. (рис. 3.10).

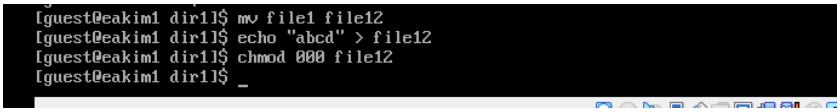

Рис. 3.10: 10

4 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. Составили наглядные таблицы, поясняющие какие операции возможны при тех или иных установленных правах.

Список литературы

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.
2. Robbins A. Bash Pocket Reference. O'Reilly Media, 2016. 156 с.
3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
4. Newham C. Learning the bash Shell: Unix Shell Programming. O'Reilly Media, 2005. 354 с.