Отчёт по лабораторной работе №4

Основы информационной безопасности

Бережной Иван Александрович

Содержание

Список иллюстраций

# 1 Цель работы

Получить практические навыки работы в консоли с расширенными атрибутами файлов.

# 2 Задание

1. Проверка расширенного атрибута a
2. Проверка расширенного атрибута i

# 3 Теоретическое введение

1. Типы прав доступа 1.1. Чтение (r): Разрешает просмотр содержимого файла или списка файлов в каталоге.

* 1.2. Запись (w): Разрешает изменение содержимого файла или создание/удаление файлов в каталоге.
* 1.3. Выполнение (x): Разрешает выполнение файла как программы или вход в каталог.

1. Категории пользователей
   * Владелец (Owner): Пользователь, который создал файл или каталог.
   * Группа (Group): Набор пользователей, которые имеют общие права доступа к файлу или каталогу.
   * Остальные (Others): Все остальные пользователи, не являющиеся владельцем или членом группы.
2. Представление прав доступа Права доступа отображаются в виде символов или цифр:

Символьное представление: rwxr-xr–

Первые три символа (rwx) — права владельца.

Следующие три (r-x) — права группы.

Последние три (r–) — права остальных.

Цифровое представление: Каждое право имеет числовое значение:

r = 4

w = 2

x = 1 Например, rwxr-xr– в цифровом виде: 754.

1. Команды для управления правами доступа chmod: Изменяет права доступа.

Пример: chmod 755 file.txt — устанавливает права rwxr-xr-x.

chown: Изменяет владельца файла или каталога.

Пример: chown user:group file.txt — изменяет владельца и группу.

chgrp: Изменяет группу файла или каталога.

Пример: chgrp group file.txt.

1. Особые права доступа SUID (Set User ID): Если установлен для файла, он выполняется с правами владельца.

SGID (Set Group ID): Если установлен для файла, он выполняется с правами группы. Для каталога — новые файлы наследуют группу каталога.

Sticky Bit: Если установлен для каталога, только владелец файла может удалить или переименовать файл в этом каталоге.

# 4 Выполнение лабораторной работы

## 4.1 Проверка расширенного атрибута a

Зайдём в терминал от имени пользователя guest и определим расширенные атрибуты файла dir1/file1 (рис. 1). Как видим, прав нет. Установим на файл file1 права на чтение, запись для владельца файла командой chmod 600 dir1/file1 (рис. 2).

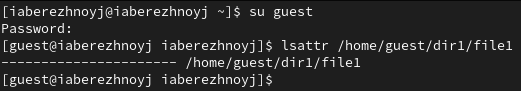


Рис. 1: Определение атрибутов

Рис. 2: Установка прав 600

Рис. 2: Установка прав 600

Установим на упомянутый файл расширенный атрибут a от имени guest. Получили ошибку (рис. 3). Попробуем повторить действие от имени другого пользователя с правами администратора (рис. 4). Получилось.

Рис. 3: Попытка установки расширенного атрибута

Рис. 3: Попытка установки расширенного атрибута

Рис. 4: Установка расширенного атрибута

Рис. 4: Установка расширенного атрибута

От имени пользователя guest проверим правильность установления атрибута (рис. 5).

Рис. 5: Проверка расширенного атрибута

Рис. 5: Проверка расширенного атрибута

Выполним дозапись текста в файл file1 (рис. 6). Работает.

Рис. 6: Дозапись в файл

Рис. 6: Дозапись в файл

Попробуем стереть имеющуюся информацию в файле - неудача (рис. 7). Попробуем переименовать файл - также безуспешно (рис. 8). И, наконец, попробуем изменить права доступа к файлу. Впрочем, ничего неожиданного (рис. 9).

Рис. 7: Попытка стереть файл

Рис. 7: Попытка стереть файл

Рис. 8: Попытка переименовать файла

Рис. 8: Попытка переименовать файла

Рис. 9: Попытка изменения прав

Рис. 9: Попытка изменения прав

Снимем расширенный атрибут с помощью администратора (рис. 10). Попробуем повторить неудавшиеся действия. Всё получилось (рис. 11).

Рис. 10: Отмена атрибута a

Рис. 10: Отмена атрибута a

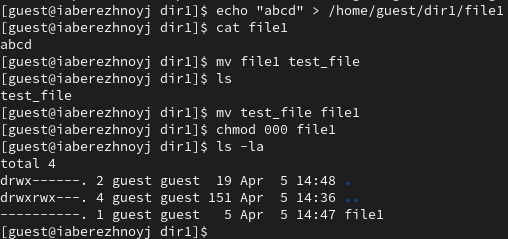


Рис. 11: Повтор действий

## 4.2 Проверка расширенного атрибута i

Выдадим расширенный атрибут i, как это было с a (рис. 12) и повторим проделанные действия (рис. 13). Ничего не работает.

Рис. 12: Расширенный атрибут i

Рис. 12: Расширенный атрибут i

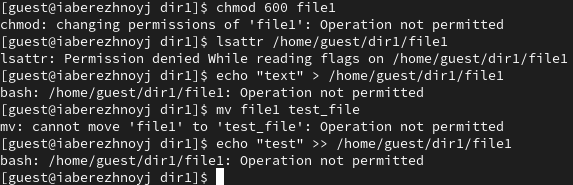


Рис. 13: Повтор действий 2

# 5 Выводы

В результате выполнения работы мы 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. Опробовали действие на практике расширенных атрибутов «а» и «i».