Отчёт по лабораторной работе №5

дисциплина: Информационная безопасность

Абрамян Артём Арменович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

2 Теоретическое введение

Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (http://www.gentoo.ru/); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: /afs/dk.sci.pfu.edu.ru/common/files/iso/.

В операционной системе Linux есть много отличных функций безопасности, но одна из самых важных - это система прав доступа к файлам. Изначально каждый файл имел три параметра доступа: Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги Выполнение - невозможно выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу Каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это

группа владельца, хотя для файла можно назначить и другую группу Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла

Команды, которые могут понадобиться при работе с правами доступа: “ls -l” - для просмотра прав доступа к файлам и каталогам “chmod категория действие флаг файл или каталог” - для изменения прав доступа к файлам и каталогам (категорию действие и флаг можно заменить на набор из трех цифр от 0 до 7) Значения флагов прав: — - нет никаких прав –x - разрешено только выполнение файла, как программы, но не изменение и не чтение -w- - разрешена только запись и изменение файла -wx - разрешено изменение и выполнение, но в случае с каталогом, невозможно посмотреть его содержимое r– - права только на чтение r-x - только чтение и выполнение, без права на запись rw- - права на чтение и запись, но без выполнения rwx - все права

3 Выполнение лабораторной работы

1. Убедился, что компилятор gcc установлен, исолпьзуя команду “gcc -v”. Затем отключил систему запретов до очередной перезагрузки системы командой “sudo setenforce 0”, после чего команда “getenforce” вывела “Permissive” (рис. 3.1)

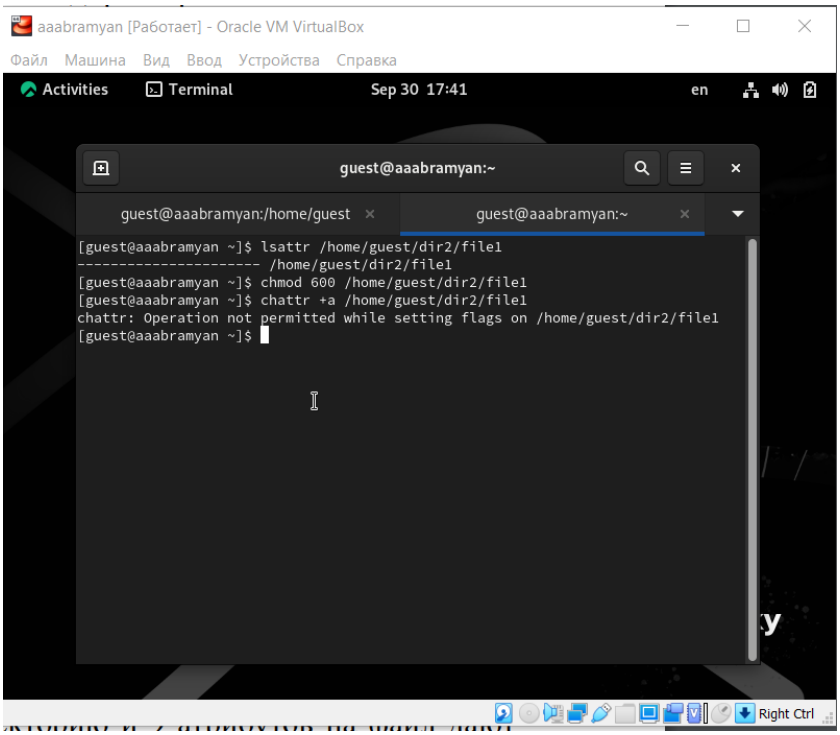


Рис. 3.1: Предварительная подготовка

2. Проверил успешное выполнение команд “whereis gcc” и “whereis g++”. (рис. 3.2)

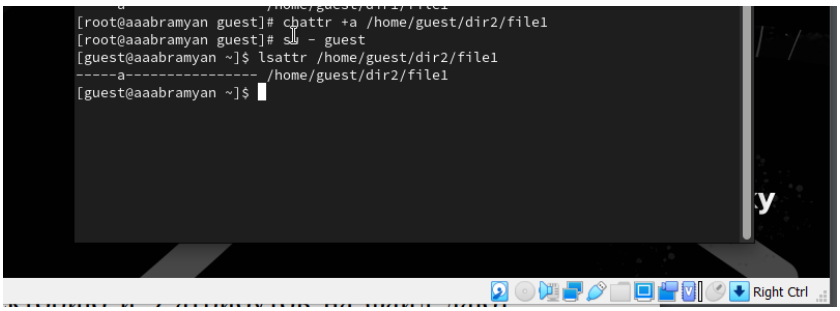


Рис. 3.2: Команда “whereis”

3. Вошел в систему от имени пользователя guest командой “su - guest”. Создал программу simpleid.c командой “touch simpleid.c” и открыл её в редакторе командой “gedit /home/guest/simpleid.c” (рис. 3.3)

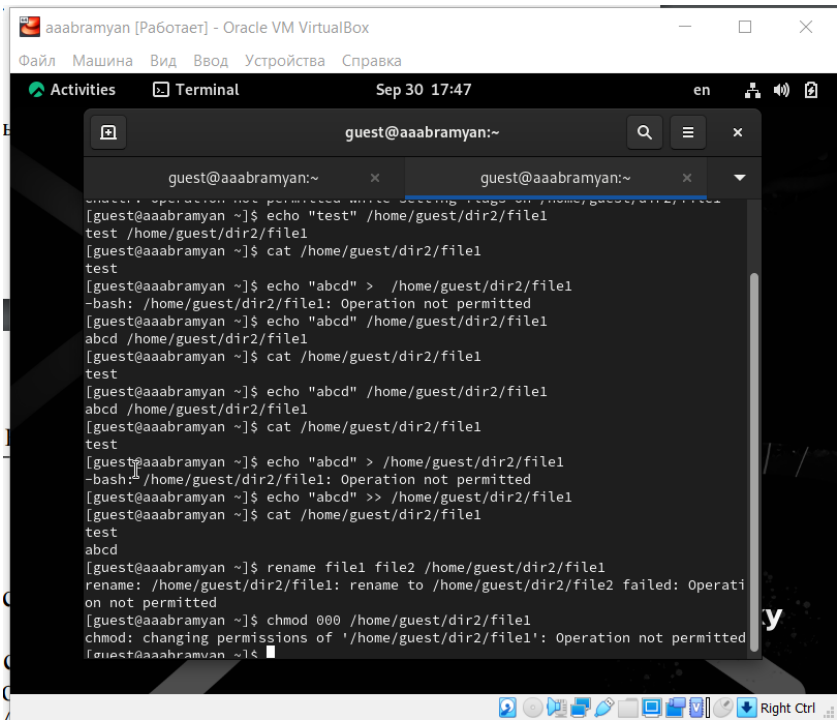
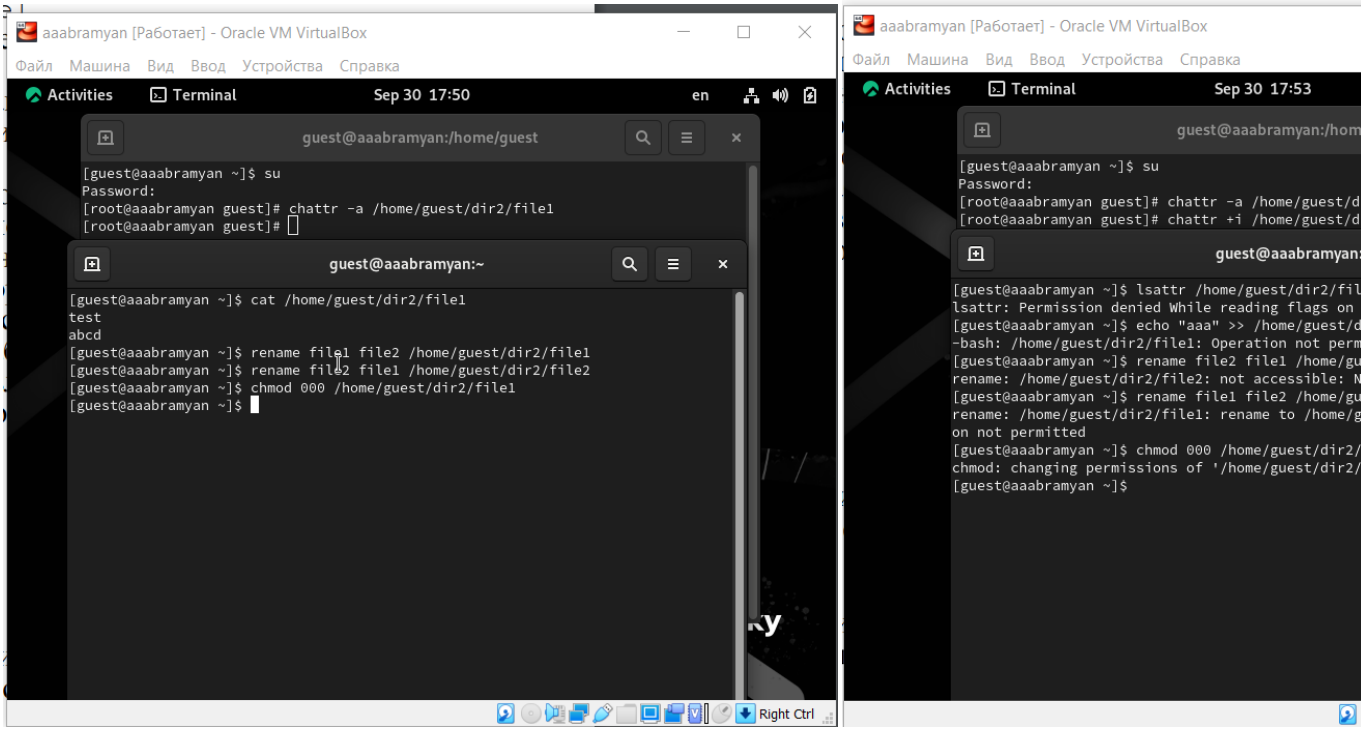


Рис. 3.3: Вход в систему и создание программы

4. Скомпилировал программу и убедился, что файл программы был создан командой “gcc simpleid.c -o simpleid”. Выполнил программу simpleid командой “./simpleid”, а затем выполнил системную программу id командой “id”.

Результаты, полученные в результате выполнения обеих команд, совпадают (uid=1001 и gid=1001) (рис. **??**)



5. От имени суперпользователя выполнил команды “sudo chown root:guest /home/guest/simpleid2” и “sudo chmod u+s /home/guest/simpleid2”, затем выполнил проверку правильности установки новых атрибутов и смены владельца файла simpleid2 командой “sudo ls -l /home/guest/simpleid2”. Этими командами была произведена смена пользователя файла на root и установлен SetUID-бит. (рис. **??**)

Установка новых атрибутов (SetUID) и смена владельца файла

Рис. 3.4: Установка новых атрибутов (SetUID) и смена владельца файла

6. Поменял владельца у программы readfile и устанавил SetUID. Проверил, может ли программа readfile прочитать файл readfile.c командой “./readfile readfile.c”. Прочитать удалось. Проверил, можно ли прочитать файл /etc/shadow. Прочитать удалось (рис. 3.9)

Запуск программы readfile

Рис. 3.5: Запуск программы readfile

7. Командой “ls -l / | grep tmp” убедился, что атрибут Sticky на директории /tmp установлен. От имени пользователя guest создал файл file01.txt в директории /tmp со словом test командой “echo”test” > /tmp/file01.txt”. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей “все остальные” командами “ls -l /tmp/file01.txt” и “chmod o+rw /tmp/file01.txt” (рис. **??**)

Создание файла file01.txt

Рис. 3.6: Создание файла file01.txt

8. От имени пользователя guest2 попробовал прочитать файл командой “cat /tmp/file01.txt” - это удалось. Далее попытался дозаписать в файл слово test2, проверить содержимое файла и записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию - эти операции удалось выполнить только в случае, если еще дополнительно разрешить чтение и запись для группы пользователей командой “chmod g+rw /tmp/file01.txt”. От имени пользователя guest2 попробовал удалить файл - это не удается ни в каком из случаев, возникает ошибка (рис. **??**)

Попытка выполнить действия над файлом file01.txt от имени пользователя guest2

Рис. 3.7: Попытка выполнить действия над файлом file01.txt от имени пользователя guest2

9. Повысил права до суперпользователя командой “su -” и выполнил команду, снимающую атрибут t с директории /tmp “chmod -t /tmp”. После чего покинул режим суперпользователя командой “exit”. Повторил предыдущие

шаги. Теперь мне удалось удалить файл file01.txt от имени пользователя, не являющегося его владельцем (рис. **??**)

Удаление атрибута t (Sticky-бита) и повторение действий

Рис. 3.8: Удаление атрибута t (Sticky-бита) и повторение действий

10. Повысил права до суперпользователя командой “su -” и выполнил команду, снимающую атрибут t с директории /tmp “chmod -t /tmp”. После чего покинул режим суперпользователя командой “exit”. Повторил предыдущие шаги. Теперь мне удалось удалить файл file01.txt от имени пользователя, не являющегося его владельцем. Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp (рис. **??**)

Возвращение атрибута t (Sticky-бита)

Рис. 3.9: Возвращение атрибута t (Sticky-бита)

4 Выводы

В данной лабораторной работе мне успешно удалось Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

5 Библиографический список

1. Документация Rocky (https://docs.rockylinux.org/)