# Лабораторная работа № 4

# Основы безопасности в Linux

Пользователь является ключевым понятием в системе доступа Linux. Как правило, у ОС домашнего компьютера не может быть больше 1-2 пользователей, однако в случае распределённых локальных систем учётных записей может быть десятки или даже сотни. В Ubuntu, как, впрочем, и в Windows, у пользователя есть своё выделенное пространство – рабочая или домашняя директория, доступ к которой имеет только он и пользователь с расширенными правами доступа (администратор). Но он также может иметь доступ к общим программам и утилитам – и здесь важно организовать всё правильно с точки зрения безопасности файлов и данных.

В данной работе мы рассмотрим процесс создания и удаления пользователей, назначению файлам прав доступа, а также некоторым важным аспектам работы в ОС.

Полезные ссылки

* [*https://sysadminium.ru/groups\_and\_users\_in\_linux/*](https://sysadminium.ru/groups_and_users_in_linux/)- про пользователей и группы
* [*https://habr.com/ru/post/469667/*](https://habr.com/ru/post/469667/)- про права доступа к файлам
* [*https://habr.com/ru/post/423049/*](https://habr.com/ru/post/423049/)- про процессы

Необходимое ПО:

* Любая ОС, на которую можно установить VirtualBox
* VirtualBox
* Образ Ubuntu версии 16.04 или выше

## Оформление отчета

В отчете опишите процесс выполнения работы, сопроводив его скриншотами.

## Ход работы

Перед началом работы

Включите запись терминала командой:

$script –a l4\_result

Если вы работаете в нескольких терминалах, то запустите запись в каждом, назвав файлы l4\_result\_<пользователь1>, l4\_result\_<пользователь2> и т.д. Обязательно приложите файлы к отчёту!

Root права

В Unix-подобных системах пользователь с правами root всемогущ – он обладает доступом ко всему, что можно делать в системе, в том числе, сделать с ней что-нибудь непоправимое. Поэтому правами root следует пользоваться с осторожностью, чтобы не навредить другим пользователям в системе. Пользователь с данными правами создаётся автоматически при установке системы.

Чтобы выполнить команду от имени пользователя root, добавьте в начало команды sudo. К примеру, попробуйте обратиться к файлу etc/passwd:

$ sudo cat /etc/passwd

Опишите структуру файла и поля, которые в нём содержатся.

Пользователи

Создание и удаление пользовательских учётных записей – рутинная работа администратора. При создании нового пользователя в Ubuntu происходит три вещи:

1. Заводится запись в файле \etc\passwd, в которой указано уникальное имя пользователя, UID и другие данные.
2. Создаётся домашний каталог, в которому применяются соответствующие права доступа.
3. Вся система получает обновление конфигурационных файлов, а в домашний каталог помещаются файлы инициализации командной оболочки.

Поскольку создание пользователей подразумевает изменения в системных файлах, создать пользователя можно, только обладая root-правами. Для того, чтобы создать пользователя, наберите:

$ adduser username

Чтобы удалить пользователя, воспользуйтесь командой userdel:

$ userdel username

Пользователей можно объединять в группы – так гораздо удобнее устанавливать права доступа. Чтобы сразу создать пользователя, принадлежащего к группе, нужно указать флаг --ingroup:

$ adduser username --ingroup groupname

Создать новую группу можно через:

$ groupadd groupname

За группы отвечает файл etc/group – в нём появится запись о созданной группе. Теперь можно добавить в неё существующих пользователей:

$ usermod -aG groupname username

Для того, чтобы сменить пользователя, наберите

$ su username

Или

$ su - username

**Задание**

Посмотрите структуру команды adduser и создайте трёх обычных пользователей <ваше\_имя\_на\_латинице>(1-3) – например, ivanov1, ivanov2 и ivanov3. Для удобства можно открыть несколько вкладок терминала – в Ubuntu Mate это делается при помощи сочетания клавиш Ctrl+Shift+T. Первых двух пользователей оставьте обычными, а третьему дайте root-права при помощи команды:

$ sudo su

Первого и второго пользователей объедините в созданную группу Students. Это можно сделать от имени третьего пользователя с root-правами. Проверьте с помощью команды groups, что пользователи действительно состоят в группе.

Под первым пользователем поменяйте себе пароль при помощи команды passwd.

Под вторым пользователем попробуйте зайти в каталог /root и объясните результат.

Третьим пользователем выйдите из root-прав командой exit.

Файлы

Обычно владельцем файла является создавший его пользователь. У файлов есть два типа владельцев: пользователи и группы. Под первым пользователем создайте файл schedule, куда при помощи редактора nano поместите следующий текст:

10:00 Maths

11:40 Physics

13:30 Economics

15:20 Programming

Затем назначьте владельцем этого файла группу Students через команду

$ chgrp Students schedule

Убедитесь, что файл доступен пользователю 2, зайдя под его учётной записью. Попробуйте добавить в этот файл строку:

17:00 Databases

Теперь зайдите под третьим пользователем. Создайте от его имени файл important, где будет записан текст:

All students need to be in recreation area at 18:00! Sign below if you got this message.

Теперь сделаем его доступным остальным пользователям через изменение прав доступа при помощи утилиты chmod.

Следует обратить внимание, что в Unix-системах есть три типа доступа:

R – read, доступ к чтению файла или просмотру содержимого каталога.

W – write, доступ к записи в файл или добавлению файлов в каталог.

X – execute, доступ к запуску как исполняемого файла или возможность зайти в каталог командой cd.

По команде ls с ключом -la вы можете увидеть права доступа к файлам вида:

drw-r–r– 2 adam adam 96 2007-09-05 18:04 blob  
drwxr-xr-x 2 adam adam 176 2007-09-04 15:57 tapety  
-rw-r–r– 1 adam adam 125 2007-08-29 18:31 fme.py

Символ d в начале означает директорию, а “-“ -- файл. Записи прав доступа приводятся в следующем порядке: Пользователи (Users), Группы(Groups), Остальные (Others). То есть, запись:

drw-r–r– 2 adam adam 96 2007-09-05 18:04 blob

можно расшифровать как «папке blob разрешены чтение и запись для пользователей, чтение для групп и чтение для остальных». Команда на изменение прав выглядит, например, так:

$ chmod u+x script.sh

Здесь мы добавляем у файла script.sh доступ на исполнение для пользователей. Права можно как добавлять (+), так и удалять (-).

Итак, вернёмся к третьему пользователю. Он не состоит в группе Students, поэтому ему нужно сделать этот файл доступным для записи остальным (Others). Воcпользуйтесь командой chmod для этого, но сперва **запомните, какие права есть у файла по умолчанию**.

Зайдя под первым и вторым пользователями, проверьте доступность файла и отпишитесь в конце этого файла о получении сообщения.

Снова дайте третьему пользователю root-права и создайте файл very important! с текстом:

All personal! University will be closed tomorrow!

Посмотрите права на этот файл через ls -la. Чем они отличаются от стандартных прав на файл, созданный пользователем?

Процессы

Как и в Windows, в Unix-системах существует браузер процессов, запущенных в системе. Чтобы вывести на экран список действующих процессов, наберите:

$ ps

Список процессов можно фильтровать, к примеру:

-a #Выдать все процессы системы, включая лидеров сеансов.

-d #Выдать все процессы системы, исключая лидеров сеансов.

-e #Выдать все процессы системы.

-o #Определяет формат вывода в виде списка полей, разделенных символом «,».

-u #Выдать процессы, принадлежащие указанному пользователю.

Процессами можно управлять. К примеру, можно запускать программы в фоновом режиме, указывая после имени программы символ &. Чтобы перевести процесс из фонового на передний план, то нужно воспользоваться командой fg, а наоборот – bg. Наконец, командой kill можно завершить процесс, а killall завершает всю группу.

**Задание**

Здесь можно пользоваться только одним терминалом.

1. Используя перенаправление, выведите список процессов от имени пользователя root в файл proc\_list. Приложите его к отчёту.
2. Проверьте команду kill -9 1.
3. В окне терминала запустите программу firefox. Изучите команду pstree и получите с помощью неё информацию о дереве процессов и их идентификаторах. Найдите поддерево для процесса firefox, изучите список составляющих его процессов.
4. Завершите процесс firefox при помощи kill.
5. Завершите все процессы текущего пользователя, набрав:

$ killall -u имя\_пользователя