**Лабораторная работа №4**

**Цель:** получить навыки управления пользователями и правами в ОС Linux

**Задачи:**

Изучить команды работы с пользователями \*Nix систем

**Теоретическая часть**

**Права собственности**

Файловая система хранит информацию о правах собственности для каждого фала и каталога. Включая информацию о пользователе и группе, которым принадлежит файл. Самый простой способ просмотреть эту информацию - воспользоваться ls:

# ls -l /usr/bin/wc

-rwxr-xr-x 1 root bin 7368 Jul 30 1999 /usr/bin/wc

Нас интересуют третий и четвёртый столбцы. Они содержат информацию о именах пользователя и группы, которым принадлежит файл. В приведённом примере файл принадлежит пользователю root и группе bin.

Владельца файла можно изменить при помощи chown(1) (что значит ''change owner'' - изменить владельца), а группу при помощи chgrp (''change group'' - изменить группу). Чтобы изменить владельца фала на ''daemon'', мы выполним команду:

# chown daemon /usr/bin/wc

А чтобы изменить группу на ''root'':

# chgrp root /usr/bin/wc

chown так же может быть использована для задания и пользователя и группы, которым принадлежит файл:

# chown daemon.root /usr/bin/wc

Принадлежность фалов - это очень важная часть использования Linux системы, даже если вы единственный пользователь. Иногда вам придётся исправлять права владения файлами и узлами (nodes) устройств.

**Права доступа**

Права доступа - это ещё одно проявление многопользовательских основ файловой системы. С их помощью вы можете указать, кто может читать, изменять и выполнять фалы.

Права доступа хранятся в виде четырёх восьмеричных чисел, каждое из которых устанавливает права для отдельного блока. Блоки представляют права владельца, права группы и права всего остального мира. Четвёртое восьмеричное число используется для хранения специальной информации, такой как ID владельца, ID группы и ''sticky''бит. Значения этих чисел соответствуют правам доступа (им так же сопоставляются буквы, которые выводятся такими программами, как ls и могут быть использованы программой chmod:

|  |  |  |
| --- | --- | --- |
| Тип | Восьми-битовое значение | Буква |
| ''sticky'' bit | 1 | t |
| set user ID (ID пользователя) | 4 | s |
| set group ID (ID группы) | 2 | s |
| read (чтение) | 4 | r |
| write (запись) | 2 | w |
| execute (выполнение) | 1 | x |

Для каждой из групп права складываются. Например, если вы хотите, чтобы права группы были ''read'' и ''write'', вы воспользуетесь ''6'' в части соответствующей группе прав доступа.

Права по умолчанию для bash:

$ ls -l /bin/bash

-rwxr-xr-x 1 root bin 477692 Mar 21 19:57 /bin/bash

Первый дефис для каталогов принимает значение, равное ''d''. Три группы прав (владелец, группа и весь мир) отображаются следующими. Из примера мы видим, что владелец имеет права для чтения, записи и выполнения (rwx). Группа имеет только право на чтение и выполнения файла (r-x). И все остальные имеют только права на чтение и выполнение фала (r-x).

Как же нам присваивать права файлам? Вначале давайте создадим файл для примеров:

$ touch /tmp/example

$ ls -l /tmp/example

-rw-rw-r- 1 david users 0 Apr 19 11:21 /tmp/example

Мы воспользуемся chmod(1) (что означает ''change mode'' - изменить режим), для того чтобы установить права доступа для файла примера. Сложите восьмизначные числа, для прав, которые вы хотите. Для того, чтобы владелец имел права чтения, записи и выполнения, получится 7. Чтение и выполнение соответствует числу 5. Установим права:

$ chmod 755 /tmp/example

$ ls -l /tmp/example

-rwxr-xr-x 1 david users 0 Apr 19 11:21 /tmp/example

Для задания специальных прав, сложите числа вместе, и расположите их в первом столбце:

$ chmod 6755 /tmp/example

$ ls -l /tmp/example

-rwsr-sr-x 1 david users 0 Apr 19 11:21 /tmp/example

Если вас смущают восьми-битовые числа, вы можете пользоваться буквами. Группы прав представляются, как:

|  |  |
| --- | --- |
| Владелец | u |
| Группа | g |
| Мир (все остальные) | o |
| Все вышеперечисленные | a |

Чтобы проделать то же, что и выше, нам понадобится выполнить команду несколько раз:

$ chmod a+rx /tmp/example

$ chmod u+w /tmp/example

$ chmod ug+s /tmp/example

Некоторые предпочитают работать с буквами. Но в любом случае, результат - это тот же самый набор прав доступа.

Мы несколько раз упоминали упоминали права ''set user ID'' (установить ID пользователя) и ''set group ID'' (установить ID группы). Обычно, когда вы выполняете программу, она имеет все те же самые права, что и вы, как пользователь. То же справедливо и для группы. Когда вы запускаете программу, она выполняется с правами вашей текущей группы. При помощи ''set user ID'' вы можете заставить программу всегда выполнятся с правами её владельца (например ''root''). ''Set group ID'' работает так же, но для группы.

Будьте осторожны здесь, так как set user ID и set group ID могут открыть ''дыры '' в безопасности вашей системы. Если вы установите эти права на файл, принадлежащий root-у, вы позволяете всем запускать эту программу, и выполнять её, как root. Так как у пользователя root нет ограничений в системе, это ставит под вопрос целостность основной безопасности системы. Короче, пользоваться этими командами не плохо, но здравый смысл должен присутствовать.

**Пользователи и группы**

Самый простой способ манипулирования пользователями - при помощи поставляемых с дистрибутивом вспомогательных скриптов и программ. В Slackware для работы с пользователями есть такие программы: adduser, userdel(8), chfn(1),chsh(1) и passwd(1). А для работы с группами есть groupadd(8), groupdel(8) и groupmod(8). За исключением chfn, chsh и passwd перечисленные программы могут выполняться только пользователем root и поэтому расположены они в /usr/sbin. chfn, chsh и passwd могут быть выполнены кем угодно, а расположены они в каталоге /usr/bin.

Добавить пользователя можно при помощи программы **adduser**. Мы начнём с разбора процедуры, комментируя все вопросы, задаваемые программой и кратко описывая, что же всё это означает. Вариант ответа по умолчанию, предлагаемый программой практически на каждый из вопросов, показывается в скобках и может быть использован для ответа практически на все вопросы.

#adduser

Login name for new user (8 characters or less) []: jellyd

Это имя, которое пользователь будет использовать для входа в систему. Оно должно состоять из восьми или менее символов, так как все login утилиты рассчитаны на это. Обычно используются только маленькие буквы, но можно пользоваться и большими.

User id for jellyd [ defaults to next available]:

ID (UID) пользователя, это на самом деле то, с помощью чего в системе Linux определяется принадлежность файлов. Каждый пользователь имеет уникальный номер, начиная с 1000 в Slackware. Вы можете выбрать UID для нового пользователя, или вы можете просто позволить программе adduser присвоить пользователю следующий свободный номер.

Initial group for jellyd [users]:

Все пользователи по умолчанию попадают в группу users. Вы можете захотеть создать отдельную группу для каждого из пользователей, но это не рекомендуется.

Additional groups for jellyd (seperated with commas, no spaces) []:

Здесь вам предлагается добавить пользователя в дополнительные группы. Один пользователь может числиться в нескольких группах. Это полезно, если у вас есть разные группы для разных задач, например, для изменения файлов вэб-сайта, для игр и т.д.

jellyd's home directory [/home/jellyd]:

Домашние каталоги по умолчанию располагаются в /home каталоге. Если вы работаете в очень большой системе, возможно возникнет необходимость разместить домашние каталоги в другом месте. Эта опция позволяет вам уточнить, где должен располагаться домашний каталог пользователя. Вы можете так же парализовать пользователя, указав его домашним каталогом что-то вроде /usr/bin/false, но мы не рекомендуем пользоваться этим методом.

jellyd's shell [/bin/bash]:

bash это оболочка по умолчанию в Slackware Linux и подойдёт для большинства людей. Если ваш новый пользователь ранее пользовался Unix, он может быть захочет какую-то другую оболочку, к которой привык больше. Вы можете поменять оболочку сейчас, или же пользователь сделает это позже самостоятельно при помощи chsh команды.

jellyd's account expiry date (YYYY-MM-DD) []:

Вы можете задать дату, после которой пользователь не будет больше иметь доступа к системе. По умолчанию, это бесконечность. Например, эта опция может быть полезна для ISP, если они хотят создать пользователя до определённой даты, пока не получать плату за следующий год.

OK, I'm about to make a new account. Here's

what you entered so far:

New login name: jellyd

New UID: [Next available]

Initial group: users

Additional groups: [none]

Home directory: /home/jellyd

Shell: /bin/bash

Expiry date: [no expiration]

This is it... if you want to bail out, hit Control-C.

Otherwise, press ENTER to go ahead and make the account.

Теперь вы видите всю введённую информацию и, если что-то не так, вы можете остановиться при помощи Control-C и начать всё сначала. Иначе вы можете нажать ввод, и пользователь будет создан.

Making new account...

Changing the user information for jellyd

Enter the new value, or press return for the default

Full Name []: Jeremy

Room Number []: Smith 130

Work Phone []:

Home Phone []:

Other:

Вся эта информация дополнительна, она используется для finger. Вы можете оставить пустыми эти поля. Пользователь может так же изменить эту информацию в любой момент при помощи chfn. Но может быть полезно указать по крайней мере имя и телефон, на тот случай, если вы захотите связаться с персоной.

Changing password for jellyd

Enter the new password (minimum of 5, maximum of 127 characters)

Please use a combination of upper and lower case letters and numbers.

New password:

Re-enter new password:

Password changed.

Done...

Вам придётся ввести пароль для нового пользователя. Если новый пользователь не присутствует при создании аккаунта, просто укажите какой-то пароль по умолчанию и скажите пользователю поменять его на что-то более надёжное.

**Выбор пароля**

*Выбор надёжного пароля – это первый шаг по защите системы от взлома. Пароль не должен быть легко угадываемым, так как в этом случае шансы несанкционированного проникновения в систему возрастают. Идеальный пароль – это случайный набор символов, включая большие и маленькие буквы, числа и другие символы. Имейте ввиду, что* ***tab*** *лучше не использовать, так как он трактуется по-разному разными системами, и при удалённом доступе могут возникнуть проблемы.*

*В общем, руководствуйтесь здравым смыслом: не выбирайте в качестве пароля чей-то день рождения, какую-то общую фразу, что-то что есть у вас на столе, что-то, что тесно связанно с вами. ''secure1'' так же плохой пароль.*

Удаление пользователя ещё более простая процедура. Просто запустите userdel и имя пользователя, которого вы хотите удалить. Вам необходимо убедиться, что пользователь в этот момент не в системе, и что нет процессов, выполняемых этим пользователем. Так же помните, что если вы удалили пользователя то его больше нет.

#userdel jellyd

Выполнив эту команду, вы удалите ''jellyd'' из вашей системы. Так ему и надо:) Команда удаляет пользователя из файлов /etc/passwd и /etc/group, но не удалит его домашний каталог. Если вы так же хотите удалить и домашний каталог, вы должны воспользоваться следующей командой:

#userdel -r jellyd

Временная парализация аккаунта, будет описана в разделе ''Изменение паролей'', так как это требует изменения пароля пользователя. Изменение регистрационной информации пользователя будет описано в разделах ''Изменения пароля'' и ''Изменение информации о пользователе''.

Программы для создания и удаления групп очень просты. groupadd просто создаст ещё одну группу в файле /etc/group, с уникальным group ID, а groupdel удалит указанную группу. Вам надо будет вручную добавить пользователей в созданную группу, путём редактирования /etc/group.

**Вручную**

Конечно, возможно добавлять, изменять и удалять пользователей и группы вручную. После того, как вы ознакомитесь с процедурой, возможно, вы найдёте, что использование скриптов сложнее, чем создание вручную.

Вначале, добавим нового пользователя в файлы /etc/passwd(5), /etc/shadow(5) и /etc/group(5). Файл passwd содержит некоторую информацию о пользователе, но не содержит их паролей. Этот файл должен быть доступен для чтения всем пользователям, но вы не хотите, чтобы пароли, даже закодированные, были доступны для чтения всему миру, так как это будет огромной помощью злоумышленникам. Поэтому закодированные пароли хранятся в теневом файле, который доступен для чтения только root пользователю, а в файле passwd пароли пользователей отображаются, как ''x''. Файл group показывает список всех групп, и кто из пользователей к каким группам относиться.

Давайте рассмотрим /etc/passwd файл и и разберёмся, как добавить кого-то. Типичная строка файла выглядит таким образом:

chris:x:1000:100:Chris Lumens,Room 2,,:/home/chris:/bin/bash

Каждая строка, соответствует пользователю. Поля в каждой линии разделены двоеточием. Поля в порядке слева на право: имя для входа в систему, закодированный пароль (''x'' для всех в Slackware системе, так как мы пользуемся пакетом для теневых файлов паролей), ID пользователя, ID группы, дополнительная информация о пользователе, разделённая запятыми, домашний каталог и оболочка. Что вам надо сделать, так это добавить в конец файла строчку, заполнив все перечисленные поля соответствующими новому пользователю значениями.

Убедитесь, что пароль x, что ID пользователя уникален, что пользователь входит в группу 100 (''users'' группа в Slackware) и что выбрана правильная оболочка.

Теперь добавим строку в /etc/shadow, который содержит пароли. Типичная строка этого файла выглядит вот так:

chris:$1$w9bsw/N9$UWLr2bRER6YyBS.CAEp7R.:11055:0:99999:7:::

Опять-таки, каждая строка соответствует одному пользователю, и поля разделены двоеточием. Поля: имя входа в систему, закодированный пароль, количество дней со дня Эпохи (1 Января 1970) до дня, когда пароль был изменён последний раз. количество дней, после которых пароль может быть изменён, количество дней после которых пароль должен быть изменён, количество дней до истечения аккаунта, время когда пользователь получит сообщение о закрытии его аккаунта, дни после истечения аккаунта, после которых аккаунт полностью блокируется, дни с момента Эпохи, когда аккаунт должен быть заблокирован и зарезервированное поле.

Как вы видите, это в основном информация об истечении аккаунта. Если вы не пользуетесь информацией об истечении аккаунта, вам надо только заполнить некоторые из полей со специальными значениями. Иначе, вам понадобится произвести вначале некоторые вычисления и принять некоторые решения, до того, как вы сможете заполнить все эти поля. Для нашего нового пользователя впишите какой-то мусор в поле пароля. Не волнуйтесь о том, какой именно сейчас установлен пароль, так как через минуту мы изменим это. В пароле могут быть использованы любые символы кроме двоеточия. Оставьте ''количество дней, с момента изменения пароля'' пустым. Введите 0, 99999 и 7 как это указанно в примере выше (в те же поля), и оставьте остальные поля пустыми.

Так как все являются членами ''users'' группы по умолчанию, вам не надо добавлять нового пользователя в неё. Если вы захотите создать новую группу или добавить нового пользователя в другие группы, вам необходимо будет отредактировать /etc/group. Вот типичная строка файла:

cvs::102:chris,logan,david,root

Поля: имя группы, пароль группы, ID группы и члены группы. Создание новой группы, это всего лишь добавление ещё одной строчки, с уникальным ID и указанием списка пользователей, которых вы хотите включить в группу, в этот файл. Все из перечисленных пользователей, если они в данный момент в системе, вынуждены будут выйти и снова войти в систему, чтобы изменения вступили в силу.

Теперь давайте вернёмся к команде passwd, чтобы создать пароль для созданного нами пользователя. Затем воспользуемся mkdir, чтобы создать домашний каталог там, где мы указали, что он будет расположен в /etc/passwd файле.

Если вы установили sendmail(8), вам необходимо будет создать новый файл с соответствующими правами, принадлежащий новому пользователю в /var/spool/mail каталоге. Вот пример:

#touch /var/spool/mail/jellyd

#chown jellyd.users /var/spool/mail/jellyd

#chmod 660 /var/spool/mail/jellyd25

Эти команды создадут файл очереди почты (mail spool файл) для нового пользователя ''jellyd'' и установят правильные права и принадлежность файла.

Для удаления пользователя, просто удалите всё, что вы вводили при создании. Удалите упоминания о пользователе из /etc/passwd и /etc/group. Удалите его login имя, из всех групп в /etc/group, удалите его очередь почты, если таковая имеется, и так же не забудьте удалить домашний каталог пользователя, если есть необходимость.

Удаление групп проще. Просто удалите строку, определяющую группу из файла /etc/group.

**Изменение паролей**

Программа passwd изменяет пароль, модифицируя /etc/shadow файл. Этот файл содержит все пароли системы в закодированной форме. Для того, чтобы изменить ваш пароль, выполните:

$ passwd Changing password for chris

Old password:

Enter the new password (minumum of 5, maximum of 127 characters)

Please use a combination of upper and lower case letters and numbers.

New password:

Как видите, вас просят ввести ваш старый пароль. Он не появится на экране, как и при входе в систему. Затем вам необходимо ввести новый пароль. passwd произведёт много различных проверок вашего пароля, и пожалуется вам, если найдёт ваш пароль ненадёжным. Вы можете проигнорировать эти сообщения, если пожелаете. Затем вам предложат ввести пароль опять, для подтверждения.

Если вы root, то вы можете изменить чей угодно пароль:

# passwd ted

Вам надо будет пройти через ту же самую процедуру, за исключением того, что не понадобится указывать старый пароль. (Одно из преимуществ пользователя root...).

Если у вас в системе есть пользователи, которые насаждают вам, вы можете временно заблокировать их эккаунты. Позже вы можете опять активизировать их. Как блокировка, так и последующее включение пользователя могут быть произведены при помощи passwd. Чтобы отключить эккаунт, как root, выполните следующее:

# passwd -l david

Это изменит пароль david-а на что-то, что не может быть подобрано. Для возвращения пользователя, выполните следующее:

# passwd -u david

Теперь эккаунт david-а опять работает, как и раньше. Приостановка эккаунта может быть полезна, если пользователь играет не по правилам, установленным в вашей системе или если они экспортировали очень большую копию xeyes(1) на ваш рабочий стол X.

**Изменение информации пользователя**

Пользователи могут поменять в любой момент времени свою оболочку и свою finger информацию. В Slackware Linux chsh (change shell - изменить оболочку) и chfn (change finger - изменить finger) используются для этого.

Пользователь может выбрать любую из оболочек, перечисленных в /etc/shell. Для большинства bash будет идеальным выбором. Кто-то может быть знаком с оболочками, встречающимися в других Unix системах используемых. Выбрать оболочку можно при помощи chsh:

$ chsh

Password:

Changing the login shell for chris

Enter the new value, or press return for the default

Login Shell [/bin/bash]:

После ввода пароля введите полный путь к новой оболочке. Убедитесь вначале, что она перечислена в /etc/shells(5). root может так же изменить оболочку пользователя, указав как аргумент программе chsh имя пользователя.

finger информация – это необязательная информация. Она содержит такие поля, как полное имя, номера телефона и номер кабинета. Она может быть изменена при помощи chfn, так же, как и при создании эккаунта. Как всегда, root может изменить finger информацию для любого пользователя.

**Получение прав суперпользователя**

При использовании системы в повседневной жизни строго рекомендуют использовать аккаунт обычного пользователя, даже если вы администратор. Но, бывают задачи, которые могут быть решены только имея права суперпользователя.

Для получения прав суперпользователя можно использовать две команды su и sudo. Но, конечно, нужно знать пароль root. Поведение этих команд можно настроить и в разных системах параметры по-умолчанию могут отличаться. sudo используется в Debian-подобных системах, su почти во всех дистрибутивах Linux.

su позволяет вам временно залогиниться под root

sudo позволяет вам выполнить команду под root

В обоих случаях система вам предложит ввести пароль суперпользователя.

test@darkstar:~$ su

Password:

root@darkstar:/home/test# who

test tty1 Oct 16 15:21

root@darkstar:/home/test# whoami

root

Обратите внимание, что команда who говорит, что на терминале 0 работает пользователь test. А команда whoami говорит, что работает пользователь root. Кроме того, обратите внимание на приглашение командной строки

$ - для обычных пользователей

# - для суперпользователя

Для завершения сеанса можно скомандовать exit или комбинацией Ctrl+D

**Правильное выключение компьютера**

Очень важно выключать компьютер правильно. Простое отключение питания может вызвать серьёзные повреждения системы. Пока компьютер включён, даже если вы ничего не делаете, некоторые файлы открыты системой. Помните, что в фоновом режиме всегда выполняются какие-то системные процессы. Эти процессы управляют системой, и много файлов открыты этими программами всё время. Если просто отключить питание, эти файлы не закрываются правильно, и из-за этого могут повредиться. В зависимости от того, какие из файлов были повреждены, система может быть серьёзно повреждена. В любом случае, вам придётся пройти через длительную процедуру проверки системы при следующей загрузке системы.

Так что, если вы собираетесь выключить, или перезагрузить компьютер, очень важно делать это правильно. Есть несколько путей сделать это. Большинство способов, используемых для выключения так же могут быть использованы для перезагрузки.

Первый метод это программа shutdown(8) и наверное это самый распространённый метод. shutdown может быть использована для выключения или пере-загрузки в определённое время, и может выдать сообщение всем пользователям системы, говорящее, что система будет выключена.

Обычный вариант использования shutdown:

# shutdown -h now

В этом случае мы не послали специфическое сообщение пользователям; они увидят стандартное сообщение shutdown программы. ''now'' это время, когда мы хотим выключить систему, а ''-h'' значит halt (остановить) систему. Это не очень вежливый способ выключения многопользовательской системы, но для вашего домашнего компьютера, этого больше чем достаточно. Более вежливо на многопользовательской системе будет заранее предупредить пользователей:

#shutdown -h +60

Эта команда перезагрузит компьютер через час (60 минут), что вполне нормально на обычной многопользовательской системе. Действительно важные системы должны заранее создавать расписание пере-загрузки и предоставлять его в /etc/motd(5).

Для перезагрузки используется та же команда, но с ключом ''-r'' вместо ''-h'':

#shutdown -r now

Вы можете использовать тот же формат для времени с shutdown -r, что и с shutdown -h. Есть много других действий, которые вы можете выполнять при помощи shutdown, чтобы контролировать, когда именно перезагрузить или выключить компьютер. Смотрите man страницу для подробностей.

Второй способ выключения или пере-загрузки компьютера, это использование halt(8) и reboot(8) программ. halt немедленно выключит ваш компьютер, а reboot перезагрузит его. Вызываются команды – вот так:

#halt

#reboot

Более низко уровневый способ перезагрузки компьютера, это общение напрямую с init. Все остальные методы, это лишь более удобные способы общения с init, но вы можете так же и напрямую сказать init-у, чего вы хотите, при помощи telinit(8). Использование telinit сообщит init-у, в какой из уровней загрузки (runlevel) перейти, что в свою очередь, вызовет выполнение соответствующего сценария. Этот сценарий убьёт или породит процессы, в соответствии с выбранным уровнем загрузки. Это может быть использовано для выключения или пере-загрузки, так как оба этих процесса являются определёнными уровнями загрузки.

#telinit 0

Уровень загрузки 0 - это режим выключения. Сказав init войти в режим загрузки 0, мы заставим его убить все процессы, размонтировать файловые системы и остановить систему. Это отличный способ выключения компьютера. На многих laptop-ах это так же вызовет отключение питания.

#telinit 6

Уровень загрузки 6 - это режим перезагрузки. Все процессы будут «убиты», файловые системы размонтированы, и компьютер перезагрузится. Это самый ''правильный'' метод перезагрузки.

Есть ещё один способ перезагрузки компьютера. Все остальные (вышеперечисленные) методы могут быть выполнены только пользователем root. Тем не менее, можно перезагрузить компьютер, если вы не root, в том случая, если у вас есть физический доступ к клавиатуре. Выполнение комбинации из трёх пальцев (control-alt-delete) вызовет немедленную пере-загрузку компьютера. что действительно происходит в этом случае, так это выполнение программы /usr/sbin/ctrlaltdel(8). Так что если у программы какие-то странные права доступа, или если она отсутствует, нажатие этих кнопок ни к чему не приведёт

**Практическая часть**

1. Создать двух пользователей
2. Прочитать информацию о пользователе
3. Войти в систему под одним из этих пользователей. Создать файл, дать права на чтение всем, для записи только себе и группе.
4. Войти в систему под другим пользователем, проверить, можно ли прочитать файл и можно ли внести изменения.
5. Изменить группу второго пользователя - отличную от первого (воспользоваться su)
6. Выйти из режима su, проверить, можно ли внести изменения в файл.
7. Те же операции проделать для каталогов.
8. Понять, как права доступа работают с каталогами и файлами.
9. Удалить пользователей.