

Управление учетными записями.

Цель работы

Научиться основным действиям и командам, связанным с управлением пользователями Linux - добавление, удаление пользователя, изменение пароля, добавление в группу. Основные изучаемые команды - *adduser*, *passwd*, *su*, *sudo*.

Задания к работе

1. Ознакомиться с содержимым файлов:

```
/etc/passwd  
/etc/shadow  
/etc/group
```

2. Создать следующие группы:

```
workers  
teachers  
students
```

3. Создать пользователей `user_N`, где $N = 1, 2, \dots, 5$, `uid` учетной записи должен быть равен $2000+N$.
4. Пользователей с `N` равным 1 и 2 добавить в группу `workers` вручную внеся изменения в конфигурационный файл.
5. Пользователей с `N` равным 3, 4 и 5 добавить в группу `students` при помощи команд администрирования.
6. Создать пользователя `student`. В комментарии к учетной записи должны быть Ваше имя и фамилия. `uid` учетной записи должен быть равен 3000. Пользователя добавить в группу `students`.
7. Для всех пользователей задайте пароли, используя команду `passwd`.
8. Создать директорию `labs` в корневом каталоге. В нем создать каталоги `library` и `tests`
9. Создать файлы `book_[фамилия студента]_N` и поместить их в `library`
10. Создать текстовый файл `test_[имя студента]`, и поместить в `tests`. Файлы должны содержать скрипт на создание пользователя `user[номер варианта]` и задание ему пароля `pass[номер варианта]`. Сделайте эти файлы исполняемыми для пользователей группы `students`.
11. В директории `labs` создать файл `list`, который должен содержать список файлов директории `/etc`.
12. Дать право на изменение файла только пользователю `teacher`, а на чтение пользователям группы `workers`.

13. Настроить права доступа к каталогу `library` и `tests`, таким образом, чтобы пользователи группы `teachers` могли изменять и создавать там файлы, а пользователи группы `students` имели доступ на чтение

Методические указания

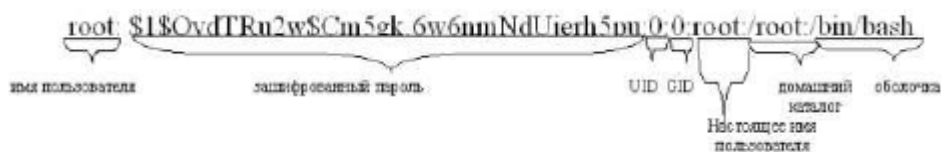
Linux, как и любая unix-подобная система, является не только многозадачной, но и многопользовательской, т.е. эта операционная система позволяет одновременно нескольким пользователям работать с ней. Но система должна как-то узнавать, какой или какие из пользователей работают в данный момент. Именно для этих целей в Linux существует два понятия – учетные записи и аутентификация, которые являются частями одного механизма.

Учетная запись пользователя – это необходимая для системы информация о пользователе, хранящаяся в специальных файлах. Информация используется Linux для аутентификации пользователя и назначения ему прав доступа.

Аутентификация – системная процедура, позволяющая Linux определить, какой именно пользователь осуществляет вход.

Вся информация о пользователе обычно хранится в файлах `/etc/passwd` и `/etc/group`.

`/etc/passwd` – этот файл содержит информацию о пользователях. Запись для каждого пользователя занимает одну строку:



```
root:$1$OvdTRu2w$Cm5gk6w6nmNdUierh5pu0:0:root:/root:/bin/bash
```

Имя пользователя зашифрованный пароль UID GID домашний каталог оболочка

Настоящее имя пользователя

имя пользователя – имя, используемое пользователем на все приглашения типа `login` при аутентификации в системе.

зашифрованный пароль – обычно хешированный по необратимому алгоритму MD5 пароль пользователя или символ `!`, в случаях, когда интерактивный вход пользователя в систему запрещен.

UID – числовой идентификатор пользователя. Система использует его для распределения прав файлам и процессам.

GID – числовой идентификатор группы. Имена групп расположены в файле /etc/group. Система использует его для распределения прав файлам и процессам.

Настоящее имя пользователя – используется в административных целях, а также командами типа finger (получение информации о пользователе через сеть).

Домашний каталог – полный путь к домашнему каталогу пользователя.

Оболочка – командная оболочка, которую использует пользователь при сеансе. Для нормальной работы она должна быть указана в файле регистрации оболочек /etc/shells.

/etc/group – этот файл содержит информацию о группах, к которым принадлежат пользователи:

project:\$1\$QydTRu2w\$Cm5gk.6w6nnNdUjerh5pu:100:root,bin,daemon

Имя группы Шифрованный пароль GID Пользователи, включенные в несколько групп

Имя группы – имя, применяемое для удобства использования таких программ, как newgrp .

Шифрованный пароль – используется при смене группы командой newgrp. Пароль для групп может отсутствовать.

GID – числовой идентификатор группы. Система использует его для распределения прав файлам и процессам.

Пользователи, включенные в несколько групп – В этом поле через запятую отображаются те пользователи, у которых по умолчанию (в файле /etc/passwd) назначена другая группа.

На сегодняшний день хранение паролей в файлах passwd и group считается ненадежным.

В новых версиях Linux применяются так называемые теневые файлы паролей – shadow и gshadow. Права на них назначены таким образом, что даже чтение этих файлов без прав суперпользователя невозможно. Нужно учесть, что нормальное функционирование системы при использовании теневых файлов подразумевает одновременно и наличие файлов passwd и group. При использовании теневых паролей в /etc/passwd и /etc/group вместо самого пароля устанавливается символ 'x', что и является указанием на хранение пароля в /etc/shadow или /etc/gshadow.

Файл shadow хранит защищенную информацию о пользователях, а также обеспечивает механизмы устаревания паролей и учетных записей. Вот структура файла shadow :

cisco:\$1\$0AJZcVg0\$EGORy8Mh3swT1RfJeXUR0:13770:10:99999:7:30:99999:

The diagram shows the entry 'cisco:\$1\$0AJZcVg0\$EGORy8Mh3swT1RfJeXUR0:13770:10:99999:7:30:99999:' with brackets and letters below it: 'a' under 'cisco', 'б' under '\$1\$0AJZcVg0\$EGORy8Mh3swT1RfJeXUR0', 'в' under '13770', 'г' under '10', 'д' under '99999', 'е' under '7', 'ж' under '30', 'з' under '99999', and 'и' under the final colon.

а - имя пользователя ;

б - шифрованный пароль – применяются алгоритмы хеширования, как правило MD5 или символ '!', в случаях, когда интерактивный вход пользователя в систему запрещен;

в - число дней с последнего изменения пароля, начиная с 1 января 1970 года;

г - число дней, перед тем как пароль может быть изменен;

д - число дней, после которых пароль должен быть изменен;

е - число дней, за сколько пользователя начнут предупреждать, что пароль устаревает;

ж - число дней, после устаревания пар

В Linux, кроме обычных пользователей, существует один (и только один) пользователь с неограниченными правами. Идентификаторы UID и GID такого пользователя всегда 0 . Его имя, как правило, root , однако оно может быть легко изменено (или создано несколько символьных имен с одинаковым GID и UID), так как значение для применения неограниченных прав доступа имеет только GID 0 . Для пользователя root права доступа к файлам и процессам не проверяются системой. При работе с использованием учетной записи root необходимо быть предельно осторожным, т.к. всегда существует возможность уничтожить систему.

В Linux используется развитая система распределения прав пользователям. Но для точного опознания пользователя одного имени недостаточно с точки зрения безопасности. Именно поэтому используется и пароль – произвольный набор символов произвольной длины, обычно ограниченной лишь используемыми методами шифрования.

Сегодня в большинстве версий Linux пароли шифруются по алгоритмам 3DES и MD5 (устарело, теперь SHA512). Когда алгоритм 3DES является обратимым, то есть такой пароль можно расшифровать, MD5 – это необратимое преобразование. Пароли, зашифрованные по алгоритму 3DES не применяются при использовании теневого файла для хранения паролей.

При аутентификации, пароль, введенный пользователем, шифруется тем же методом, что и исходный, а потом сравниваются уже зашифрованные копии. Если они одинаковые, то аутентификация считается успешной.

Учитывая ежедневно увеличивающиеся требования к безопасности, в Linux есть возможность использовать скрытые пароли. Файлы `/etc/passwd` и `/etc/group` доступны для чтения всем пользователям, что является довольно большой брешью в безопасности системы. Именно поэтому в современных версиях Linux предпочтительнее использовать скрытые пароли. Такие пароли располагаются в файлах `/etc/shadow` и `/etc/gshadow`, для паролей пользователей и групп соответственно.

Команда `login` запускает сеанс интерактивной работы в системе. Она проверяет правильность ввода имени и пароля пользователя, меняет каталог на домашний, выстраивает окружение и запускает командный интерпретатор. Команду `login` как правило не запускают из командной строки — это обычно за пользователя делают менеджеры консоли — например `getty` или `mgetty`.

Команда `su` (`switch user`) позволяет сменить идентификатор пользователя уже в процессе сеанса. Синтаксис ее прост: `su username`, где `username` – имя пользователя, которое будет использоваться. После этого программа запросит пароль. При правильно введенном пароле, `su` запустит новый командный интерпретатор с правами пользователя, указанного `su` и присвоит сеансу его идентификаторы. Если имя пользователя опущено, то команда `su` использует имя `root`.

```
[student@ns student]$ su root
Password:
[root@ns student]#_
```

При использовании команды `su` пользователем `root` она, как правило, не запрашивает пароль.

Команда `newgrp` аналогична по своим возможностям `su` с той разницей, что происходит смена группы. Пользователь должен быть включен в группу, которая указывается в командной строке `newgrp`. При использовании команды `newgrp` пользователем `root` она никогда не запрашивает пароль. Синтаксис команды аналогичен синтаксису команды `su`: `newgrp groupname`, где `groupname` – имя группы, на которую пользователь меняет текущую.

Команда `passwd` является инструментом для смены пароля в Linux. Для смены своего пароля достаточно набрать в командной строке `passwd`:

```
[student@ns student]$ passwd
Changing password for student
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully
[student@ns student]$_
```

Для смены пароля группы и управления группой используется команда `grpasswd`. Для смены пароля достаточно набрать в командной строке `grpasswd GROUPNAME`. Сменить пароль вам удастся только если Вы являетесь администратором группы. Если пароль не пустой, то для членов группы вызов `newgrp` пароля не требует, а не члены группы должны ввести пароль. Администратор группы может добавлять и удалять пользователей с помощью параметров `-a` и `-d` соответственно. Администраторы могут использовать параметр `-r` для удаления пароля группы. Если пароль не задан, то только члены группы с помощью команды `newgrp` могут войти в группу. Указав параметр `-R` можно запретить доступ в группу по паролю с помощью команды `newgrp` (однако на членов группы это не распространяется). Системный администратор (`root`) может использовать параметр `-A`, чтобы назначить группе администратора.

Команда `chage` управляет информацией об устаревании пароля и учетной записи. Обычный пользователь (не `root`) может использовать команду только для просмотра своих параметров устаревания пароля:

```
gserg@ADM:/$ chage -l gserg
Last password change : Май 03, 2007
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```

Суперпользователь же может использовать также иные параметры, такие как:

- `-d` дата (в формате системной даты, например ДД.ММ.ГГГГ) – устанавливает дату последней смены пароля пользователем.

- `-E` дата – установить дату устаревания учетной записи пользователя

- `-I N` – установить количество дней неактивности `N` с момента устаревания пароля перед тем как учетная запись будет заблокирована

- `-m N` – задает минимальное количество дней (`N`) между сменами пароля

- `-M N` – задает максимальное количество дней (`N`) между сменами пароля

-W N – задает количество дней, за которые будет выдаваться предупреждение об устаревании пароля.

Контрольные вопросы

1. Какие основные файлы хранят информацию о зарегистрированных в системе пользователях?
2. Как добавить пользователя в систему?
3. Зачем операционная система отслеживает дату назначения пароля пользователю?
4. Для чего служит пароль группы?
5. Каково назначения файла /etc/shadow?
6. Как поменять пароль пользователю? Кто может это сделать?
7. Почему возникает необходимость выполнить команду от имени другого пользователя?

Дополнительные задания

1. Определить значение umask, при котором создаваемые файлы будут доступны для исполнения всем.
2. Создать в домашнем каталоге подкаталог tmp, в котором сможет создавать, удалять и переименовывать файлы любой пользователь, входящий в группу student, но при этом его содержимое не должно быть видимым никому кроме владельца. Проверить правильность настроек доступа.
3. Создать в домашнем каталоге папку shared, в которой могут создавать файлы любые пользователи, но удалять файлы могут только те, кто их создал. Проверить правильность настроек доступа.