Управление учетными записями пользователей в *Linux*

В системе *Linux centOS* существует три типа пользователей.

- Суперпользователь (*root, su*)
- Системные пользователи (назначение – выполнение процессов)
- Обычный пользователь (человек, имеет учетную запись).

Когда обычный пользователь регистрируется в системе (проходит процедуру авторизации, например, вводя системное имя и пароль), он идентифицируется с учётной записью, в которой хранится следующая информация:

Системное имя (*user name***)** — имя, которое вводит пользователь в ответ на приглашение «*login*:». Оно может содержать только латинские буквы и знак "_". Это имя используется также в качестве имени учётной записи.

Идентификатор пользователя (*UID***)** — это положительное целое число, связанное с системными именем, по которому операционная система отслеживает пользователей. Обычно это число выбирается автоматически при регистрации учётной записи. *UID* от 1 до 500 и 65534 зарезервированы под системных пользователей (не имеют учетной записи). Пользователь root имеет *UID 0*.

Идентификатор группы (*GID***)** — группы пользователей применяются для организации доступа нескольких пользователей к определенным ресурсам. При создании учётной записи пользователя обычно создаётся и группа, имя которой совпадает с системным именем, эта группа будет использоваться как группа по умолчанию для этого пользователя. Пользователь может входить более чем в одну группу, но в учётной записи указывается только номер группы по умолчанию.

Принадлежность к группе определяет прав доступа для каждого файла. При этом для каждого файла также определены пользователь-владелец и группа-владелец.

Полное имя (*full name***)** — опционально, предназначено только чтобы иметь возможность определить, кому принадлежит учётная запись.

Домашний каталог (*home directory***)** — каталог, в котором он может хранить свои данные. Доступ других пользователей к домашнему каталогу пользователя может быть ограничен.

Начальная оболочка (*login shell***)** —запускается при входе пользователя в систему в текстовом режиме (например, на виртуальной консоли). Поскольку в *Linux* доступно несколько разных командных оболочек, в учётной записи указано, какую из командных оболочек нужно запустить для данного пользователя. Если специально не указывать начальную оболочку при создании учётной записи, она будет назначена по умолчанию, вероятнее всего это будет *bash*.

Все перечисленные данные об учётных записях хранятся в файле */etc/passwd*. Сведения о конкретной учётной записи пользователя можно получить с помощью утилиты *getent*, например при помощи запроса вида

$getent passwd user

user:x:506:506:Name Last Name:/home/user:/bin/bash

синтаксис ответа имеет следующую структуру:

user name: password:UID:GID:Full Name: home directory:login shell

В приведенном примере вместо пароля стоит символ *x,* потому что пароль находится в другом месте. В современных системах Linux обычно применяются так называемые «теневые пароли» (*shadow passwords*), которые хранятся отдельно от остальных сведений об учётной записи, а также позволяют назначать дополнительные ограничения, в частности, «срок годности» пароля. Как правило пароли храниться в общем файле */etc/shadow* (менее строго) или в отдельном файле *shadow* для каждого пользователя (более строгая политика безопасности).

Также отдельно хранится информация обо всех группах пользователей в системе, для этого предназначен файл /*etc/group*.

Информацию о конкретной группе можно получить с помощью запроса

$*getent group audio*

audio:x:81:user, user2

данная записать означает, что в группу audio входят два пользователя. Как видно из примера в общем случае каждая группа может также иметь пароль, но он используется очень редко.

Информацию о принадлежности пользователя той или иной группе можно получить при помощи запроса

groups или *groups имя_пользователя*

также информацию о каждом пользователе можно получить при помощи команды

id имя_пользователя

Процедура создания пользователя

Исходя из изложенного выше процедура создания пользователя предполагает следующие действия.

- создание записи в */etc/passwd*;
- создание домашнего каталога пользователя и обеспечение пользователю доступ к его домашнему каталогу (сделать его владельцем каталога);
- наполнение домашнего каталога (конфигурационные файлы из /*etc/skel*);
- модифицировать системные конфигурационные файлы, в частности, создать хранилище для приходящей почты для данного пользователя *(/var/spool/mail/tester*).

Все эти действия могут быть выполнены и вручную, однако для упрощения процедуры создания пользователя используется утилита *useradd*. С помощью дополнительных параметров при вызове *useradd* можно явно указать значение для того или иного поля учётной записи, также эта утилита позволяет модифицировать параметры создания пользователей по умолчанию. Также для модификации пользователей существуют утилиты *usermod* (модификация учетных записей) и *userdel* для удаления учетных записей, также пароль для каждой учетной записи может быть изменен командой *passwd*.

Следует отметить, что запрос *passwd* в режиме суперпользователя позволяет поменять пароль root, при этом предыдущий пароль будет полностью удален.

Аналогично процедуре создания пользователей может быть создана, отредактирована и удалена группа при помощи утили *groupadd, groupdel, groupmod*.

Особенности работы с суперпользователем.

Суперпользователь в Linux имеет особые права доступа к любым файлам и папкам, как системным, так и принадлежащим другим пользователям.

Переход в режим суперпользователя может быть осуществлен командой *su* или *su –* (со сменой домашней директории на */root*). Также команда *su* позволяет переходить от одного пользователя к другому. При этом подразумевается как-бы переход в режим суеперпользователя и выход и него в другой режим. Также выйти из режима суперпользователя можно при помощи команд *exit, logout* или комбинацией клавиш *Ctl+D*.

Помимо команды *su*, единоразовые действия суперпользователя могут быть выполнены командой *sudo*. При отсутствии необходимости в постоянном доступе к правам суперпользователя рекомендуется использование именно этой команды. Однако, по умолчанию не все пользователи имеют доступ к правам суперпользователя. Список авторизованных пользователей содержится в файле /*ets/sudoers*. Также данный файл может

быть просмотрен командой *visudo* – данная команда рекомендуется для редактирования *sudoers* – по завершению работы с этой командой проводится проверка синтаксиса файла.

Файл sudoers состоит из трех частей.

1. Алиасы – списки пользователей и групп
    - *User_Alias* – пользователи, которым разрешено выполнять команды с помощью *sudo*.
    - *Host_Alias* - хосты, на которых разрешено выполнять команды с помощью sudo
    - *Comand_Alias* – команды.
2. Установки *sudo* по умолчанию (в том числе и пути к файлам)
3. пользовательская спецификация – команды пользователей и групп и их привилегии.

Так например, в данном разделе пописано, что root имеет права доступа везде (строчка *root ALL=(ALL) ALL***).**

Задание:

1. Создайте нового пользователя.
2. Поменяйте пароль пользователя.
3. Поменяйте группу пользователя, место расположения домашнего каталога
4. Создайте новую группу
5. Добавьте существующих пользователей в данную группу
6. Убедитесь в том, что внесенные вами изменения отобразились в системе.
7. Попробуйте переключиться на созданного пользователя при помощи команды

    su – user_name

    где *user_name* имя данного пользователя.
8. Попробуйте выполнить команду от лица суперпользователя
9. Вернитесь обратно или в режим суперпользователя
10. Добавьте нового пользователя в группу *wheel* и попробуйте повторить попытку.
11. Добавьте нового пользователя в группу audio вручную (файл */etc/group*)
12. Добавьте в файл *sudoer* в раздел спецификаций пользователя строку

    user_name ALL=(ALL) NOPASSWD: ALL

    где *user_name* имя данного пользователя. Попробуйте выполнить команду *sudo* от лица данного пользователя.
13. Разрешите созданному пользователю перезагружать компьютер.

14. Найдите в файле *etc/passwd* созданного пользователя и поменяйте домашнюю директорию на *usr/bin/nologin* – повторите попытку войти от лица данного пользователя в систему.
15. Верните домашнюю директорию обратно.
16. Найдите файл *shadow*, найдите в нем хэш пароля созданного пользователя обратите внимание на начало хэша.
17. Введите для созданного пользователя режим *usermod -L,* и попробуйте войти под ним в систему, посмотрите, что поменялось в файле *shadow*, посмотрите в справке *usermod* значение данной команды.
18. Удалите созданного пользователя.
19. Удалите созданную группу.

    Следует отметить, что вновь созданная учетная запись блокируется до тех пор, пока не будет выполнена команда *passwd*.

Задание 2:

1. Изучите устойчивость созданных паролей к атакам по словарю. Для этого воспользуйтесь программой «*John the Ripper*». Рекомендуется использовать специализированный дистрибутив *Kali Linux*, где эта программа предустановлена.
2. Используя документацию (*/usr/share/doc/john*), либо иные открытые источники, подготовьте краткий обзор по основным возможностям программы «*John the Ripper*». Какие существуют аналоги этого программного продукта?
3. Перенесите в отдельную папку следующие файлы: */etc/passwd* и */etc/shadow*
4. Сформируйте исходный файл для анализа

   #unshadow ./passwd ./shadow > passwd_src
5. Изучите файл словаря паролей*:*

   /usr/share/john/password.lst

   обратите внимание на пароль *"password"* и модификации (*Password, password1* и т.д.)
6. Запустите процедуру анализа паролей с использованием словаря паролей и правил их модификации, доступных по умолчанию.

   #john --wordlist=/usr/share/john/password.lst --rules /study/lab2/passwd_src

   Зафиксируйте продолжительность выполнения этой процедуры и полученный результат.
7. Откройте для редактирования файл */etc/john/john.conf* ; найдите строки:

   # "Single crack" mode rules [List.Rules:Single]

Над этими строками создайте аналогичную секцию (*Study*) для собственных правил и зарегистрируйте два указанных ниже правила:

 # StudyRules [List.Rules:Study] sa@ $1$9$[0-9]$[0-9]

8. Запустите процедуру анализа паролей с использованием собственных правил.

 # john --wordlist=/usr/share/john/password.lst --rules=Study /study/lab2/ passwd_src

Проследить за процессом работы программы (а также оценить примерную продолжительность) можно по лог-файлу: *./.john/john.log*. Если выполнение процедуры занимает слишком много времени, остановите процесс (*ctrl+c*) и измените второе правило на следующее: *$1$9$4$[0-9]*

Запустите процесс повторно. Зафиксируйте полученный результат и сделайте вывод.