Лабораторная работа № 3.

Тема: управление пользователями и группами.

Цель лабораторной работы: овладеть базовыми навыками управления пользователями в операционной системе Linux.

Файлы **/etc/passwd**, **/etc/group** и **/etc/shadow** являются основными конфигурационными файлами в системах Linux и содержат информацию о пользователях, группах и паролях. рассмотрим каждый из них:

/etc/passwd: Этот файл содержит базовую информацию о пользователях.

/etc/passwd

```
vvv@userver:~$ less /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

Каждая строка файла /etc/passwd содержит семь полей, разделенных запятыми:

1. Username. Строка, которую вы вводите при входе в систему. Каждое имя пользователя должно быть уникальной строкой на компьютере. Максимальная длина имени пользователя ограничена 32 символами.
2. Password. В старых системах Linux зашифрованный пароль пользователя хранился в файле /etc/passwd. В большинстве современных систем это поле имеет значение x, и пароль пользователя сохраняется в файле /etc/shadow.
3. UID. Идентификатор пользователя — это номер, назначенный каждому пользователю. Он используется операционной системой для обращения к пользователю.
4. GID. Номер идентификатора группы пользователя, относящийся к основной группе пользователя. Когда пользователь создает файл, группа файла устанавливается на эту группу. Как правило, имя группы совпадает с именем пользователя. Пользователя вторичные группы перечислены в файле /etc/groups.
5. GECOS или полное имя пользователя. Это поле содержит список значений через запятую со следующей информацией:
    - Полное имя пользователя или название приложения.
    - Номер комнаты.
    - Рабочий номер телефона.
    - Домашний телефон.
    - Другая контактная информация.
6. Home directory. Абсолютный путь к домашнему каталогу пользователя. Он содержит файлы пользователя и конфигурации. По умолчанию домашние каталоги пользователей именуются по имени пользователя и создаются в каталоге /home.
7. Login shell. Абсолютный путь к оболочке входа пользователя. Это оболочка, которая запускается, когда пользователь входит в систему. В большинстве дистрибутивов Linux оболочкой входа по умолчанию является Bash.

/etc/group: Этот файл содержит информацию о группах пользователей.

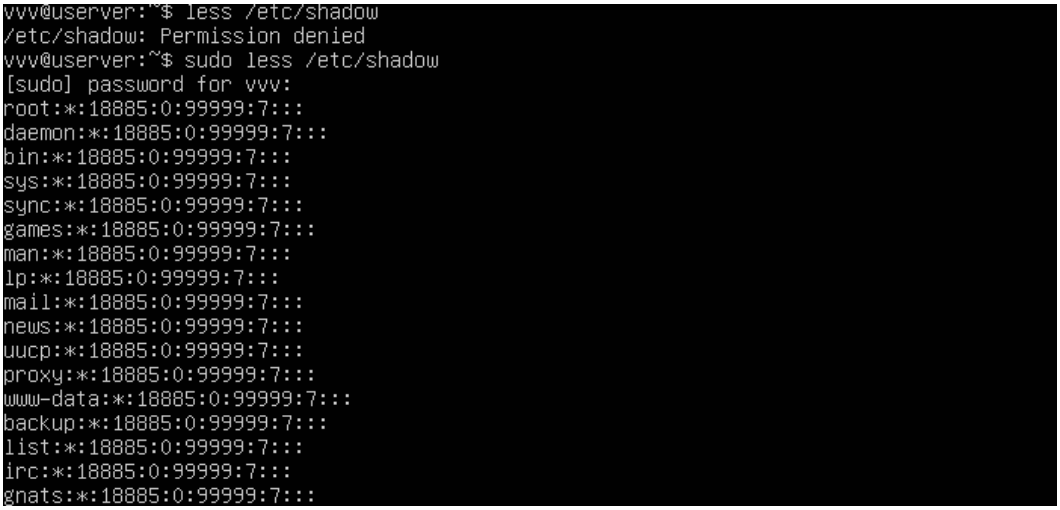
/etc/group

1. Имя группы.
2. Зашифрованный пароль. "x" - для группы пароль не установлен.
3. Идентификатор группы или сокращенно GID.
4. Пользователи, которые являются частью группы.

/etc/shadow: Этот файл хранит зашифрованные пароли пользователей.

- Доступ к файлу **/etc/shadow** имеют только привилегированные пользователи (например, root).

/etc/shadow



1.Имя пользователя
2. Хэш пароля.
3. Последнее изменение пароля (последнее изменение): дни с 1 января 1970 г., когда последний раз меняли пароль.
4. Минимум: минимальное количество дней, необходимое для смены пароля, то есть количество дней, оставшихся до того, как пользователю будет разрешено изменить свой пароль.
5. Максимум: максимальное количество дней, в течение которых пароль действителен (после того, как этот пользователь будет вынужден изменить свой пароль)
6. Предупреждение: количество дней до истечения срока действия пароля, в течение которого пользователя предупреждают о необходимости изменения пароля.

7. Неактивность: количество дней после истечения срока действия пароля, в течение которого учетная запись отключена.
8. Срок действия: дни с 1 января 1970 года, когда эта учетная запись отключена, то есть абсолютная дата, указывающая, когда логин больше не может использоваться.

Основные команды для работы с пользователями и группами

Управление пользователями:

1. **Добавление пользователя:**
   `sudo useradd username`
2. **Установка пароля для пользователя:**
   `sudo passwd username`
3. **Изменение информации о пользователе:**
   `sudo usermod -options username`
   Примеры:
   - Изменение домашнего каталога пользователя:
     `sudo usermod -d /new/home/directory username`
   - Изменение оболочки пользователя:
     `sudo usermod -s /bin/bash username`
4. **Удаление пользователя:**
   `sudo userdel username`
   При этом команда **userdel** удаляет только учетную запись пользователя, но не его домашний каталог. Если вы хотите удалить и домашний каталог, используйте **-r**:
   `sudo userdel -r username`
5. **Просмотр списка пользователей:**
   `cat /etc/passwd`
6. **Просмотр информации о конкретном пользователе:**
   `id username`

Управление группами:

1. **Добавление группы:**
   `sudo groupadd groupname`
2. **Изменение информации о группе:**
   `sudo groupmod -options groupname`
   Пример:
   - Изменение имени группы:
     `sudo groupmod -n newgroupname oldgroupname`
3. **Удаление группы:**
   `sudo groupdel groupname`
4. **Добавление пользователя в группу:**
   `sudo usermod -aG groupname username`
5. **Удаление пользователя из группы:**
   `sudo deluser username groupname`
6. **Просмотр списка групп:**
   `cat /etc/group`

Общие команды:

1. **Проверка принадлежности пользователя к группам:**
   `groups username`
2. **Просмотр информации о текущем пользователе:**
   `whoami`
3. **Просмотр информации о текущих группах:**
   `groups`
4. **Смена пользователя:**
   `su username`
5. **Смена пользователя с сохранением окружения:**
   `sudo -i -u username`
6. **Просмотр информации о себе (текущем пользователе):**
   `id`

Эти команды предоставляют базовый набор инструментов для управления пользователями и группами в Linux. Каждая команда имеет множество опций, которые могут быть использованы для более точной настройки.

Файл sudoers

Файл **sudoers** в системах Linux является конфигурационным файлом, который определяет правила использования утилиты **sudo**. Утилита **sudo** позволяет обычным пользователям выполнить команды с привилегиями суперпользователя (root) или другого пользователя, как определено в файле **sudoers**. Давайте рассмотрим основные аспекты файла **sudoers**:

Расположение файла sudoers:

Файл **sudoers** обычно располагается в директории **/etc/sudoers**. Рекомендуется редактировать этот файл с использованием команды **visudo**, которая обеспечивает блокировку файла и предотвращает возможные ошибки, что может быть критично для его работы.

Синтаксис файла sudoers:

Синтаксис файла **sudoers** достаточно гибкий и позволяет определить различные правила для разных пользователей или групп пользователей. В общем, каждая строка в файле **sudoers** имеет следующий формат:

```
user host=(runas) command
```

Где:

- **user**: Имя пользователя или группы пользователей, для которых применяется данное правило.
- **host**: Определяет на каком хосте (компьютере) это правило будет применяться. Обычно используется **ALL** для всех хостов.
- **runas**: Пользователь, от имени которого команда может быть выполнена. Обычно используется **ALL** для любого пользователя.
- **command**: Команда или группа команд, которые могут быть выполнены с использованием **sudo**.

Примеры правил в файле sudoers:

1. **Определение правил для конкретного пользователя:**

```
john ALL=(ALL:ALL) /bin/ls
```

В этом примере, пользователь **john** может выполнить команду **/bin/ls** от имени любого пользователя на любом хосте.

2. **Определение правил для группы пользователей:**

```
%admin ALL=(ALL:ALL) ALL
```

Группа пользователей **admin** может выполнять любые команды от имени любого пользователя на любом хосте.

3. **Разрешение выполнения команд без пароля для конкретного пользователя:**

```
jane ALL=(ALL:ALL) NOPASSWD: ALL
```

Пользователь **jane** может выполнять любые команды от имени любого пользователя на любом хосте без запроса пароля.

Осторожность при редактировании sudoers:

- **Не редактируйте файл sudoers напрямую.** Всегда используйте команду **visudo** для редактирования.
- **Ошибки в файле sudoers могут заблокировать доступ к команде sudo.** Поэтому будьте осторожны при внесении изменений.

Файл **sudoers** предоставляет мощные инструменты для управления привилегиями пользователей в системе Linux. Однако, использование его требует внимания и осторожности, чтобы избежать ошибок, которые могут повлиять на безопасность системы.

Задание:

1. Управление пользователями:
- создать тестового пользователя, используя утилиту useradd;
- создать второго пользователя с таким же паролем как у первого, сравнить хэши;
- установите срок действия учетной записи, например 7 дней, посмотрите изменения в файле /etc/shadow;
- удалить пользователя, используя утилиту userdel;
- создать пользователя через adduser. Заполните все поля, посмотрите запись в файле /etc/passwd

2. Управление группами:
- создать группу с использованием утилит и в ручном режиме;
- добавить пользователя в группу, не меняя основной, использую утилиту usermod;
- смените основную группу у пользователя;
- удалить пользователя из группы.

3. Создать пользователя с правами суперпользователя. Сделать так, чтобы sudo не требовал пароль для выполнения команд.