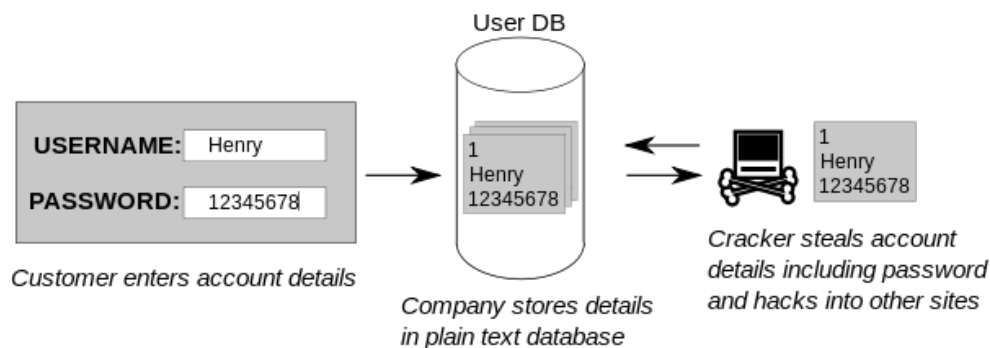
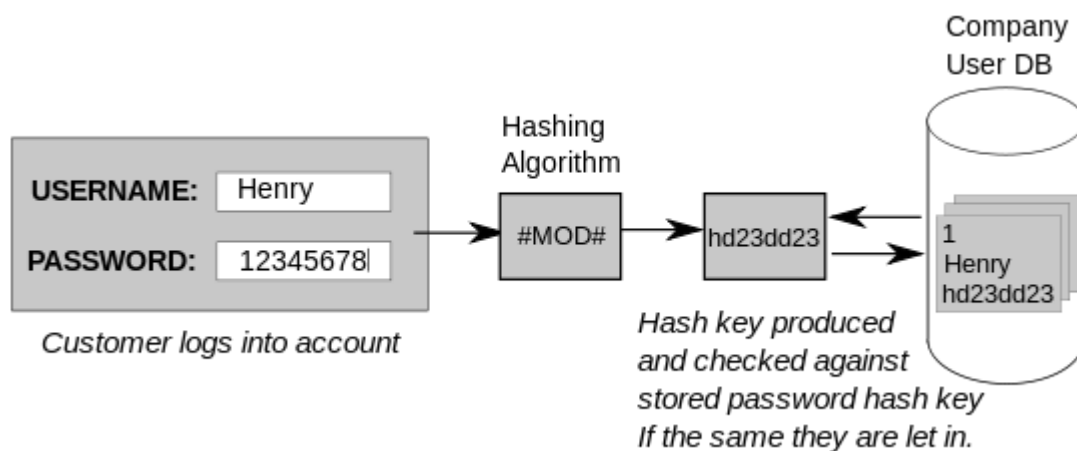


```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
```

Мы с вами уже не раз обращались к файлу `/etc/passwd`, наконец-то пришло время разобраться, что же там написано — `cat /etc/passwd`. Каждая строчка содержит информацию о каком-то пользователе. Двоеточие в данном файле выступает в роли разделителя – специального символа, который делит строку на столбцы. В первом столбце у нас логин пользователя, во втором – икс-ы. Очень давно здесь хранились пароли пользователей в хэшированном виде. Вообще, хэширование используется не только для паролей, но сейчас нас интересует именно хэширование паролей.



И так, что это вообще такое? Думаю все согласятся, что хранить пароли пользователя в открытом виде нельзя, иначе их с лёгкостью узнает любой пользователь с правами суперпользователя. Но система должна знать пароли, чтобы их подтвердить, когда вы логинитесь – поэтому пароли нужно преобразовать в какой-то нечитаемый вид. Но если это сделать так, чтобы можно было преобразовать обратно в читаемый вид – то опять же любой пользователь с правами рута сможет это сделать и получить первоначальный пароль.



Значит пароль нужно так преобразовать, чтобы никак нельзя было узнать первоначальный вид. И когда пользователь введёт пароль, можно будет преобразовать введённый им пароль тем же способом, получить ровно такое же значение, сравнить эти значения, и если совпадают - пароль подходит. Но даже такой способ недостаточно безопасен – зачастую люди используют стандартные пароли и легко создать базу, где для каждого стандартного пароля будет его хэшированный вид. А потом можно будет попытаться найти в этой базе совпадающий хэш. Если пароль стандартный - это будет довольно просто. Поэтому при хэшировании к паролю ещё добавляют рандомные символы, называемые солью, благодаря чему даже два одинаковых пароля после хэширования будут выглядеть по-разному. Но это всё криптография. Я объяснил очень поверхностно, опуская много деталей, а если кому интересно, можете почитать по [ссылке](#).

Учитывая, что в `passwd` есть полезная информация о пользователях, скрывать этот файл от всех пользователей как-то нежелательно, но и хранить тут пароли, пусть даже в хэшированном виде, тоже как-то не правильно. Поэтому пароли из `/etc/passwd` перенесли в другой файл - `/etc/shadow`, `passwd` сделали читаемым для всех, а `shadow` доступен только для рут пользователя.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
```

Пойдём дальше. Третий столбик – уникальный идентификатор пользователя – user id - uid. Очень многое строится именно вокруг uid-a, а не логина пользователя. У root пользователя идентификатор всегда ноль. Обычно для базовых сервисных пользователей uid-ы назначаются ниже 100, для каких-то дополнительных сервисных пользователей – до 999, а с 1000 начинаются uid-ы обычных пользователей.

Дальше идёт идентификатор группы - group id – gid. У каждого пользователя есть одна основная группа. И у каждой группы есть свой уникальный идентификатор. Здесь отображается идентификатор этой основной группы пользователя, для самих групп есть файл /etc/group.

После идентификатора группы идёт небольшой комментарий о пользователе – тут иногда пишут полное имя пользователя, его телефонный номер или какой-то комментарий. Как видите, для некоторых пользователей этот столбец не имеет значения.

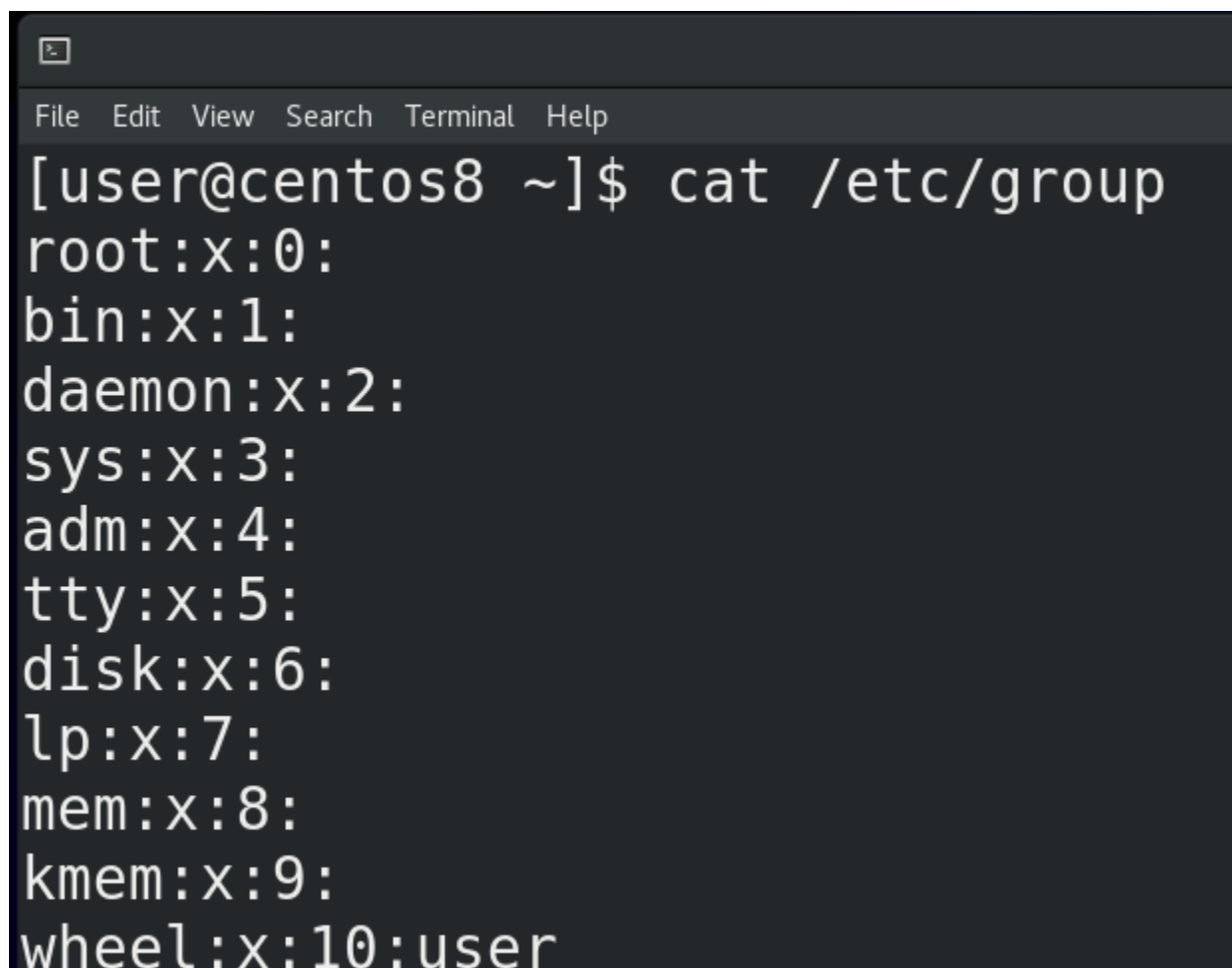
Следующий столбец – домашняя директория пользователя. Мы привыкли, что обычно домашняя директория хранится внутри директории /home , но это не обязательно и те же сервисные пользователи используют в качестве домашней директории абсолютно другие пути. У суперпользователя домашняя директория - /root.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ grep mail /etc/passwd  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
[user@centos8 ~]$ sudo su mail  
This account is currently not available.  
[user@centos8 ~]$ grep vboxadd /etc/passwd  
vboxadd:x:975:1::/var/run/vboxadd:/bin/false  
[user@centos8 ~]$ sudo su vboxadd
```

Ну и последний столбик – shell – оболочка пользователя. Допустим, у нашего юзера или рута оболочкой выступает bash. Есть ещё другие оболочки – zsh, csh и т.п. - у всех свои преимущества. У сервисных пользователей, как правило, вместо оболочки указан nologin – и если кто-то попытается залогиниться этими пользователями - увидит текст о том, что нельзя. И этот текст можно заранее прописать в файле /etc/nologin.txt. В некоторых случаях вместо оболочки можно встретить /bin/false – тоже не позволяет логиниться, но работает немного по другому принципу. /bin/false – программа, которая ничего не делает и просто выдаёт ошибку – обычно нужна для каких-нибудь скриптов. И если это указать в /etc/passwd – при логине пользователя с /bin/false он просто получит ошибку и всё.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ id  
uid=1000(user) gid=1000(user) groups=1000(user),10(wheel) context=unconfined_u:  
unconfined_r:unconfined_t:s0-s0:c0.c1023  
[user@centos8 ~]$ id user  
uid=1000(user) gid=1000(user) groups=1000(user),10(wheel)  
[user@centos8 ~]$ id user2  
uid=1001(user2) gid=1001(user2) groups=1001(user2)
```

Зачастую при работе может понадобится узнать uid пользователя или группы, в которых он состоит – и не обязательно для этого искать нужные строки в /etc/passwd – можно использовать утилиту id - id, id user, id user2.

A terminal window with a dark background and light text. The window has a title bar with a small icon and a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command prompt shows '[user@centos8 ~]\$ cat /etc/group'. The output lists system groups: root:x:0:, bin:x:1:, daemon:x:2:, sys:x:3:, adm:x:4:, tty:x:5:, disk:x:6:, lp:x:7:, mem:x:8:, kmem:x:9:, and wheel:x:10:user.

```
[user@centos8 ~]$ cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:user
```

Что касается групп - давайте заглянем в `/etc/group`. Тут синтаксис похож на `passwd` – тот же разделитель в виде двоеточия, но меньше столбцов. Однако первый столбец – это не имя пользователя, а имя группы. Вы, возможно, заметили, что имена пользователей и групп совпадают. При создании какого-то пользователя по умолчанию создаётся группа с таким же названием – личная группа пользователя (User Private Group – UPG). Это сделано в целях безопасной, но удобной совместной работы с файлами. Станет понятнее, когда пройдем права на файлы.

Дальше у нас `x` – как и в `passwd`, речь про пароль, который хранится в хэшированном виде в файле `/etc/gshadow`. Как и у пользователей, у групп можно поставить пароль с помощью утилиты `grpasswd`. И потом, с помощью этого пароля, кто-то из другой группы может временно получить права этой группы, используя утилиту `newgrp`. Но это очень специфичная задача и я пока не видел реальных примеров использования.

Потом у нас идентификатор группы – `gid`. А в конце – список пользователей в этой группе, через запятую. Пока что у нас тут пусто, только в группе `wheel` есть пользователь `user`.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ sudo head /etc/shadow  
[sudo] password for user:  
root:$6$vZHP0JgArwLt9ZU$BviUXYv8EzzKeC6BbUvrfWDm058GcNSG.  
/gFidjzVQHpf8HrFEc0oYdBZ11vaP31::0:99999:7:::  
bin:*:18358:0:99999:7:::  
daemon:*:18358:0:99999:7:::  
adm:*:18358:0:99999:7:::  
lp:*:18358:0:99999:7:::
```

Ну и давайте ещё заглянем в файл /etc/shadow — `sudo cat /etc/shadow`. Тут у нас хранится информация о пароле пользователя и всё, что относится к паролю:

- пользователь;
- пароль в хэшированном виде, причём в начале указывается хэш функция, например, \$6\$ - это sha512 – то есть каким алгоритмом был хэширован пароль. Также тут вместо пароля может быть * или ! или два восклицательных знака – может зависеть от дистрибутива. Обычно это означает, что аккаунт заблокирован. Как правило, это относится к сервисным или новым аккаунтам, у которых нет паролей.

- Days since **epoch** of last password change
- Days until change allowed
- Days before change required
- Days warning for expiration
- Days after no logins before account is locked
- Days since epoch when account expires
- Reserved and unused

Дальше у нас идёт информация о том, когда менялся пароль, когда заблокируется и всё такое.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ chage -l user  
Last password change : never  
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
```

Эту информацию не очень удобно читать из файла – легче использовать утилиту `chage -l user`.

```
File Edit View Search Terminal Help  
[user@centos8 ~]$ useradd -D  
GROUP=100  
HOME=/home  
INACTIVE=-1  
EXPIRE=  
SHELL=/bin/bash  
SKEL=/etc/skel  
CREATE_MAIL_SPOOL=yes
```

До этого мы уже создавали пользователя с помощью команды `useradd user2`. Как мы заметили, у пользователей есть много разных настроек, а значит `useradd` откуда-то взяла настройки по умолчанию. Настройки по умолчанию можно увидеть при помощи ключа `-D` — `useradd -D`. Сразу скажу, что первый параметр – `GROUP` – будет игнорироваться, для каждого пользователя создаётся его личная группа. Настройки по умолчанию распределены в двух файлах – `/etc/default/useradd` и `/etc/login.defs`. Если первый файл – сугубо параметры утилиты `useradd`, то `login.defs` содержит параметры для многих утилит, работающих с пользователями и группами.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ cat /etc/default/useradd  
# useradd defaults file  
GROUP=100  
HOME=/home  
INACTIVE=-1  
EXPIRE=  
SHELL=/bin/bash  
SKEL=/etc/skel  
CREATE_MAIL_SPOOL=yes
```

И так, в файле /etc/default/useradd у нас несколько параметров:

- GROUP – если мы не захотим создавать личную группу пользователя, то группа по умолчанию будет группа с gid 100 – это группа users;
- HOME – это внутри какой директории создастся домашняя директория пользователя. Т.е мы создаём пользователя user2 и для него создаётся директория user2 внутри директории /home.
- INACTIVE – это через сколько дней после устаревания пароля заблокируется аккаунт: -1 – никогда, 0 – сразу же, как устареет пароль, ну или указываете количество дней.
- EXPIRE – когда аккаунт заблокируется. Указывается как год, месяц, день (ГГГГ-ММ-ДД).
- SHELL – какой интерпретатор будет по умолчанию, в данном случае /bin/bash;

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ ls -la /etc/skel/  
total 24  
drwxr-xr-x.  3 root root  78 Oct  2 11:25 .  
drwxr-xr-x. 134 root root 8192 Jan 10 17:59 ..  
-rw-r--r--.  1 root root  18 Nov  8 2019 .bash_logout  
-rw-r--r--.  1 root root 141 Nov  8 2019 .bash_profile  
-rw-r--r--.  1 root root 312 Nov  8 2019 .bashrc  
drwxr-xr-x.  4 root root  39 Oct  2 11:24 .mozilla
```

- SKEL – путь к шаблонной директории, которая используется при создании пользователя. Тут у нас есть .bash_profile и .bashrc. Если вы хотите, чтобы у всех новых пользователей в домашней директории были какие-то файлы или директории, достаточно положить их в /etc/skel.
- CREATE_MAIL_SPOOL – создаёт специальный файл, куда будет попадать входящая почта для пользователя.


```
user@centos8:~  
File Edit View Search Terminal Help  
# PASS_WARN_AGE      Number of days warning given before  
#  
PASS_MAX_DAYS      99999  
PASS_MIN_DAYS       0  
PASS_MIN_LEN        5  
PASS_WARN_AGE       7  
  
#  
# Min/max values for automatic uid selection in useradd  
#  
UID_MIN             1000  
UID_MAX             60000  
# System accounts  
SYS_UID_MIN          201  
SYS_UID_MAX          999
```

Теперь что касается /etc/login.defs — cat /etc/login.defs:

- MAIL_DIR – директория, где создастся файл для входящей почты. Вообще тут есть разные варианты, но давайте пока не будем трогать почту.
 - PASS_MAX_DAYS – максимум дней, разрешённых на один пароль. Скажем, если поставить 30 – нужно будет менять пароль каждый месяц.
 - PASS_MIN_DAYS – минимум дней, необходимых для смены пароля. Допустим, если поставить 7 – то можно будет менять пароль максимум раз в неделю. Это нужно, если вы хотите защититься от того, чтобы ваши пользователи повторно не использовали старый пароль. Допустим, у вас может стоять политика, чтобы у пользователя пароли не совпадали как минимум с 10 предыдущими паролями. Без минимального времени смены пароля он может просто разом 10 раз ввести новые пароли и потом старый. Так что этот параметр защищает от таких любителей одного пароля.
 - PASS_MIN_LEN – минимальная длина пароля. Естественно, руту плевать на этот параметр, а вот юзеры должны будут придумать пароль указанной длины.
 - PASS_WARN_AGE – за сколько дней до устаревания пароля пользователю выйдет предупреждение о том, что ему стоит сменить пароль.
 - UID_MIN и UID_MAX – минимальный и максимальный uid, который будет выдан пользователю, если конечно вручную не указать другой uid. Максимальное значение примерно 65000.
 - SYS_UID_MIN и SYS_UID_MAX – uid-ы для сервисных пользователей.
 - CREATE_HOME – создавать ли домашнюю директорию при создании пользователя.
 - USERGROUPS_ENAB – тот самый параметр, отвечающий за создание приватной группы пользователя. Без этого параметра группа по умолчанию будет та, что указана в файле /etc/default/useradd.
 - ENCRYPT_METHOD – SHA512 – алгоритм, по которому хэшируются пароли для /etc/shadow.
- На самом деле для login.defs есть много других параметров, но пока что нам этого достаточно.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ sudo useradd user3  
[sudo] password for user:
```

Теперь, зная всё это, давайте рассмотрим утилиту useradd. При простом добавлении useradd user3 всё будет ровно с теми параметрами, которые мы рассматривали в файлах useradd и login.defs. Если же мы хотим сделать как-то по своему, то давайте я возьму пару параметров для примера, а остальное вы сами протестируйте.

```
use Laptop battery low  
Approximately 42 minutes remaining (10%)  
File Edit View Search Terminal Help  
[user@centos8 ~]$ sudo mkdir -p /home/company/it  
[user@centos8 ~]$ sudo useradd user4 -b /home/company/it  
-c "User Userovich" -g users -G wheel,user2 -u 1111
```

И так, sudo useradd ключ -b – base dir – это собственно директория, внутри которой создается домашняя директория пользователя, как параметр HOME в useradd. Допустим, если я укажу sudo useradd user4 -b /home/company/it, то внутри этой директории /home/company/it создается директория user4. Но нужно заранее создать эту директорию /home/company/it - mkdir -p /home/company/it. Если у меня уже есть какая-то директория для пользователя и я не хочу её создавать, я могу указать её с ключом -d - sudo useradd -d /home/olduser user4.

Ключ -c – для комментария. Ключ -g основная группа пользователя. Как мы говорили, если этот ключ не указывать, то создается приватная группа пользователя и она станет основной группой этого пользователя. Если же мы хотим существующую группу – то указываем после ключа -g - sudo useradd user4 -g groupname. Ключ -G большое – для дополнительных групп. Допустим, если вы хотите, чтобы пользователь кроме основной группы был также в группах wheel и users2 - sudo useradd user4 -g users -G wheel,users2. Вы можете сами задать uid для будущего пользователя - sudo useradd user4 -u 1111.

```
[user@centos8 ~]$ grep user4 /etc/passwd /etc/group  
/etc/passwd:user4:x:1111:100:User Userovich:/home/company/it/user4:/bin/bash  
/etc/group:wheel:x:10:user,user4  
/etc/group:user2:x:1001:user4  
[user@centos8 ~]$ id user4  
uid=1111(user4) gid=100(users) groups=100(users),10(wheel),1001(user2)
```

Теперь посмотрим, что у нас получилось - sudo useradd user4 -b /home/user/it -c “User Userovich” -g users -G wheel,user2; grep user4 /etc/passwd /etc/group, id user4. Как видим, всё так, как мы указывали. Но пока этого не достаточно – пока мы не зададим пароль пользователю, аккаунт будет недоступен.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ sudo passwd user4  
Changing password for user user4.  
New password:  
BAD PASSWORD: The password is a palindrome  
Retype new password:  
passwd: all authentication tokens updated successfully.
```

Для создания пароля используем команду `passwd - sudo passwd user4`. Можете также использовать утилиту `chage`, чтобы настроить времена для пароля – `chage user4`.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ sudo usermod user4 -d /var/user4 -m -aG user  
[user@centos8 ~]$ grep user4 /etc/passwd /etc/group  
/etc/passwd:user4:x:1111:100:User Userovich:/var/user4:/bin/bash  
/etc/group:wheel:x:10:user,user4  
/etc/group:user:x:1000:user4  
/etc/group:user2:x:1001:user4
```

Если вы уже создали пользователя, но хотите изменить какие-то параметры – допустим, поменять комментарий, добавить в группу, переместить домашнюю директорию, поменять `uid` и т.п. - используйте утилиту `usermod`. Например, я хочу перенести домашнюю директорию пользователя и добавить его в группу - `sudo usermod user4 -d /var/user4 -m -aG user`. Ключ `-d` указывает на новую домашнюю директорию, но без ключа `-m` текущая домашняя директория не перенесётся на новое место. Что касается `-aG`, то `G` указывает дополнительные группы, но без ключа `-a` все текущие группы пользователя сбросятся и останется одна группа `user`.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ sudo userdel -r user2  
userdel: group user2 not removed because it has other members.
```

Чтобы удалить пользователя, используется команда `userdel`. Но без ключа `-r` после удаления пользователя останется его домашняя директория, личная группа и почтовый ящик, а с ключом всё это удалится - `sudo userdel -r user2`.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ sudo groupadd group1  
[user@centos8 ~]$ sudo gpasswd group1 -A user -M user4,root  
[user@centos8 ~]$ gpasswd -a user group1  
Adding user user to group group1  
[user@centos8 ~]$ gpasswd -d root group1  
Removing user root from group group1
```

Что касается групп – всё примерно также – команды `groupadd`, `groupmod` и `groupdel`. Для примера, давайте добавим группу `group1` – `sudo groupadd group1`. У группы можно назначить администратора и пользователей с помощью команды `gpasswd` – `sudo gpasswd group1 -A user -M user4,root`. А администратор группы может добавлять и удалять пользователей из группы уже без всяких прав суперпользователя – `gpasswd -a user group1`, `gpasswd -d root group1`.

```
user@centos8:~  
File Edit View Search Terminal Help  
[user@centos8 ~]$ sudo lid user  
wheel(gid=10)  
user(gid=1000)  
group1(gid=1003)  
[user@centos8 ~]$ sudo lid -g group1  
user4(uid=1111)  
user(uid=1000)
```

Чтобы посмотреть, какие группы у пользователя и какие пользователи в группе, можно использовать команду `lid` – `sudo lid user`, `sudo lid -g group1`.

```
user@centos8:~  
File Edit View Search Terminal Help  
Usage: useradd [options] LOGIN  
       useradd -D  
       useradd -D [options]  
  
Options:  
-b, --base-dir BASE_DIR      base directory for the home directory of the  
                               new account  
-c, --comment COMMENT        GECOS field of the new account  
-d, --home-dir HOME_DIR      home directory of the new account  
-D, --defaults                print or change default useradd configuration  
-e, --expiredate EXPIRE_DATE expiration date of the new account  
-f, --inactive INACTIVE       password inactivity period of the new account  
-g, --gid GROUP               name or ID of the primary group of the new  
                               account  
-G, --groups GROUPS           list of supplementary groups of the new  
                               account
```

Мы много чего разобрали – файлы `/etc/passwd` и `/etc/group`, где хранится информация о пользователях и группах, `/etc/shadow`, где хранится информация о паролях, файлы `/etc/default/useradd` и `/etc/login.defs`, где прописаны параметры для новых пользователей, а также различные утилиты для создания новых пользователей и групп, изменения их параметров, паролей и т.п. И хотя мы не стали задерживаться на различных ключах – для вас это практика – создавайте пользователей и группы с различными параметрами, если что не понятно – откройте ману – там многое объясняется. А если какие-то трудности – обращайтесь, вместе разберёмся.