1. **Analyze the structure of the /etc/passwd and /etc/group file, what fields are present in it, what users exist on the system? Specify several pseudo-users, how to define them?**

**/etc/passwd**

From the above image:

1. **Username**: It is used when user logs in. It should be between 1 and 32 characters in length.
2. **Password**: An x character indicates that encrypted password is stored in /etc/shadow file. Please note that you need to use the passwd command to computes the hash of a password typed at the CLI or to store/update the hash of the password in /etc/shadow file.
3. **User ID (UID)**: Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.
4. **Group ID (GID)**: The primary group ID (stored in /etc/group file)
5. **User ID Info (GECOS)**: The comment field. It allow you to add extra information about the users such as user’s full name, phone number etc. This field use by finger command.
6. **Home directory**: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes /
7. **Command/shell**: The absolute path of a command or shell (/bin/bash). Typically, this is a shell. Please note that it does not have to be a shell. For example, sysadmin can use the nologin shell, which acts as a replacement shell for the user accounts. If shell set to **/sbin/nologin** and the user tries to log in to the Linux system directly, the /sbin/nologin shell closes the connection.

**/etc/group:**

group\_name: It is the name of group. If you run ls -l command, you will see this name printed in the group field.

Password: Generally password is not used, hence it is empty/blank. It can store encrypted password. This is useful to implement privileged groups.

Group ID (GID): Each user must be assigned a group ID. You can see this number in your /etc/passwd file.

Group List: It is a list of user names of users who are members of the group. The user names, must be separated by commas.

1. What are the uid ranges? What is UID? How to define it?

Множество допустимых значений UID зависит от системы; в общем случае UID допускает использование значений от 0 до 65535 с некоторыми оговорками:

* Суперпользователь всегда должен иметь UID, равный нулю (0).
* Пользователю [nobody](https://ru.wikipedia.org/wiki/Nobody_(%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C)) обычно присваивается или наибольший из возможных UID (в противоположность суперпользователю), или один из системных UID (см. ниже).
* UID с 1 по 100 по соглашению резервируются под системные нужды; некоторые руководства рекомендуют резервировать UID со 101 по 499 (в [Red Hat](https://ru.wikipedia.org/wiki/Red_Hat)) или даже 999 (в [Debian](https://ru.wikipedia.org/wiki/Debian)).

A unique identifier (UID) is a numeric or alphanumeric string that is associated with a single entity within a given system. UIDs make it possible to address that entity, so that it can be accessed and interacted with.

Unique identifiers can be assigned to anything that needs to be distinguished from other entities, such as individual users, companies, machines or websites. These distinctive values are usually assigned depending on the needs of the specific application, but can either be randomly auto-generated with an algorithm, allocated incrementally or chosen by the user.

Uses of UIDs

The most widely known use of unique identifiers occurs when users register for a website or service. Customers are often provided with a username or user ID that allows the company they are registering with to differentiate them within their user logs. These identifiers are then also used for security and log on purposes.

In a database or spreadsheet, unique identifiers may be designated as a specific column or field to help make sorting and filtering through information easier. This also helps trace information back to a specific user or entity within the system.

Another popular application of UIDs is in a physical supply chain. Manufacturers often mark individual pieces of a larger component, such as computer parts, or an entire product with a serial number. This allows users to trace back the origin of the product in case of a malfunction, defect or recall.

3) What is GID? How to define it?

4) How to determine belonging of user to the specific group?

5) What are the commands for adding a user to the system? What are the basic

parameters required to create a user?

6) How do I change the name (account name) of an existing user?

7) What is skell\_dir? What is its structure?

8) How to remove a user from the system (including his mailbox)?

9) What commands and keys should be used to lock and unlock a user account?

10) How to remove a user's password and provide him with a password-free

login for subsequent password change?

11) Display the extended format of information about the directory, tell about

the information columns displayed on the terminal.

12) What access rights exist and for whom (i. e., describe the main roles)?

Briefly describe the acronym for access rights.

13) What is the sequence of defining the relationship between the file and the

user?

14) What commands are used to change the owner of a file (directory), as well

as the mode of access to the file? Give examples, demonstrate on the terminal.

15) What is an example of octal representation of access rights? Describe the

umask command.

16) Give definitions of sticky bits and mechanism of identifier substitution. Give

an example of files and directories with these attributes.

17) What file attributes should be present in the command script?