COSA

1. Explain Linux Directory Structure in detail.
    - The Linux/Unix file system hierarchy base begins at the root and everything starts with the root directory.

/bin	**binary or executable programs**
/etc	system configuration files.
/home	home directory. It is the default current directory.
/opt	optional or third-party software.
/tmp	temporary space, typically cleared on reboot.
/usr	User related programs.
/var	log files.
/boot	It contains all the boot-related information files and folders such as conf, grub, etc.
/dev	It is the location of the device files such as dev/sda1, dev/sda2, etc.
/lib	It contains kernel modules and a shared library.
/lost+found	It is used to find recovered bits of corrupted files.
/media	It contains subdirectories where removal media devices are inserted.
/mnt	It contains temporary mount directories for mounting the file system.
/proc	contains info about the running processes with a specific process ID or PID.
/run	It stores volatile runtime data.
/sbin	binary executable programs for an administrator.
/srv	It contains server-specific and server-related files.
/sys	It is a virtual file system for modern Linux distributions to store and allows modification of the devices connected to the system.

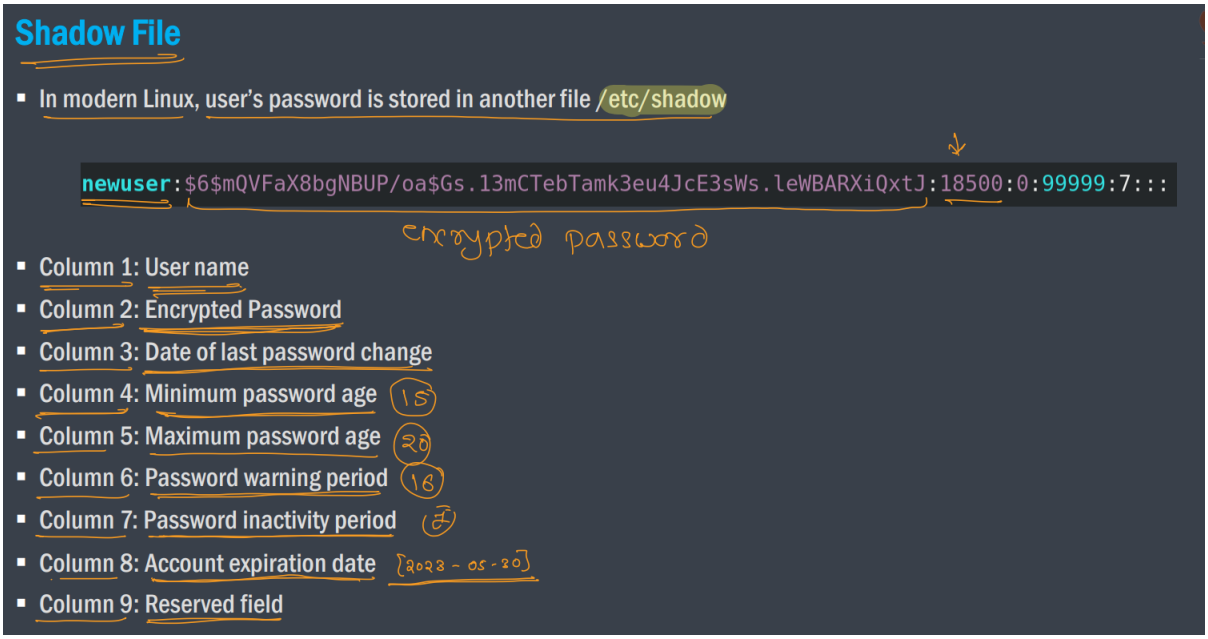
2. What is SSH? What is its default port? Why SSH is secure?

    - SSH, which stands for Secure Shell, is a cryptographic network protocol used for secure remote access to computers and servers over a network.
    - It provides a secure and encrypted communication channel between a client (your local machine) and a server (remote machine) to enable secure data exchange and remote command execution.
    - Port Number - 22
    - SSH is secure because it uses a combination of encryption and authentication to protect data in transit.

3. Explain each field of /etc/passwd. What is /etc/shadow?

- /etc/passwd

- /etc/shadow



4. Why we use LVM in Linux & what are its benefits?

- lvcreate --type

> **17. What is LVM? Its a requirement in Linux?**
>
> LVM, which stands for Logical Volume Manager, is a storage management technology used in Linux and other Unix-like operating systems. It provides a flexible and advanced method for managing storage devices, allowing administrators to create, resize, and manage logical volumes that span multiple physical disks.
>
> Key concepts and features of LVM include:
>
> 1. **Physical Volumes (PVs):** Physical volumes are the underlying physical storage devices, such as hard drives or solid-state drives. LVM combines multiple physical volumes into a single storage pool.
> 2. **Volume Groups (VGs):** Volume groups are created by grouping one or more physical volumes together. A volume group acts as a container for logical volumes.
> 3. **Logical Volumes (LVs):** Logical volumes are created within volume groups. They represent the virtual partitions that users can use as if they were physical partitions. Logical volumes can be resized and moved easily, providing flexibility in storage management.

5. Explain Postfix Mail Server. What is default port used for postfix?

    - Postfix is a free and open-source mail transfer agent (MTA) that is known for its flexibility, security, reliability, scalability, and ease of use.
    - It is one of the most popular MTAs in use today, and is used by many large organizations, including Google, Yahoo, and eBay.
    - port 25
    - In short, Postfix is a powerful and reliable MTA that can be used to send and receive email for a variety of different environments.

6. What Is Dovecot? Can it be used with Postfix?

    - Dovecot is a free and open-source IMAP and POP3 server. It is designed to be secure, reliable, and efficient. Dovecot is also highly scalable, and can be used to serve a large number of users.
    - Dovecot can be used with Postfix to provide a complete email solution. Postfix can be used to send and receive email, while Dovecot can be used to store and manage email messages.

7. What is mounting in Linux? Write a command to mount FAT formatted pen-drive in /mnt? How can you auto-mount it each time you boot the system?

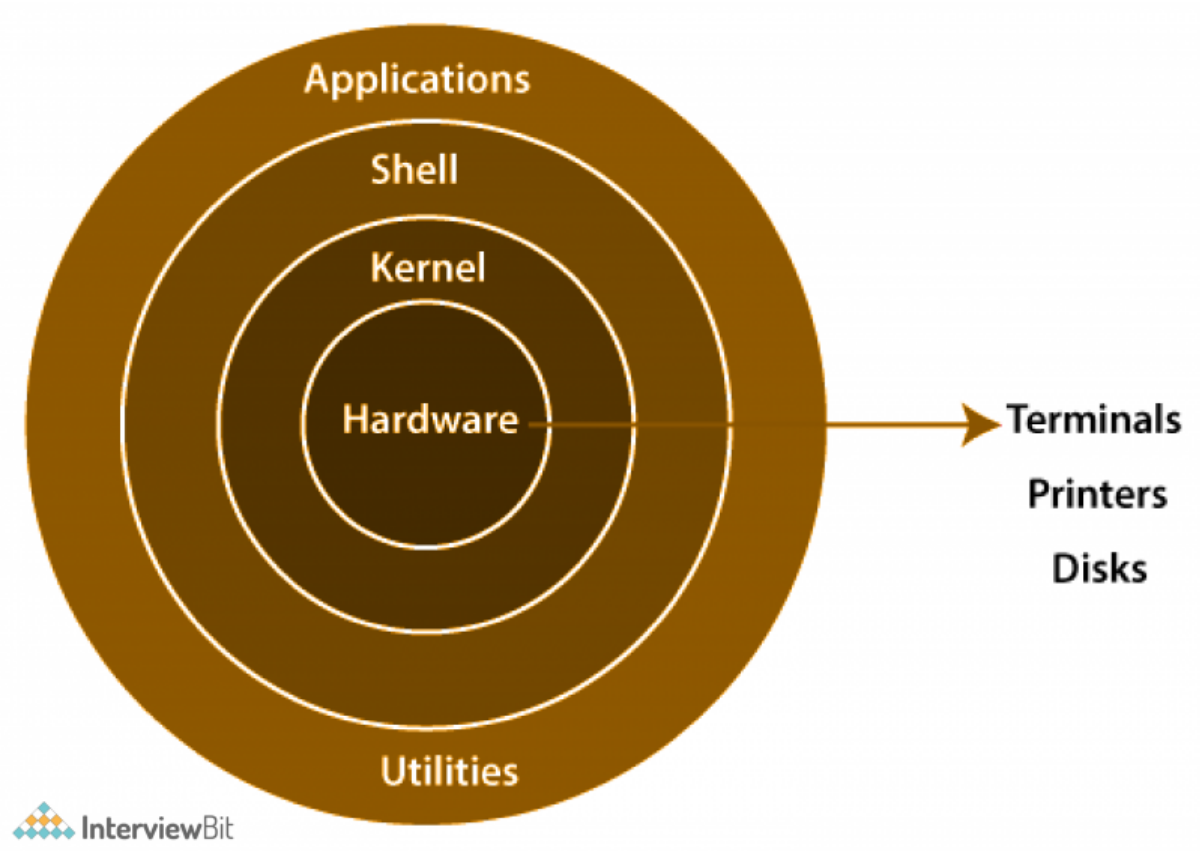
    - Mounting in Linux is the process of making a file system or device available to the operating system. Once a file system is mounted, it can be accessed like any other part of the Linux filesystem.
    - command : sudo mount /dev/sdb1 /mnt
    - To auto-mount your pen drive each time you boot the system, you can add the following line to the "/etc/fstab" file:
        - /dev/sdb1 /mnt vfat defaults,auto,user 0 0

8. What is hard link and symbolic link? How to create them?

	Soft Link (Symbolic Link)	Hard Link
Type of Link	A reference to the target file/directory	Additional directory entry to the same file
Data	Does not contain the actual data	Shares the same data with the original file
Impact on Target	Deleting the link does not affect target	Deleting any link does not affect data or other links
Cross File Systems	Can span across different file systems	Limited to the same file system
Supported for	Works for both files and directories	Only supported for files, not directories

    - To create a hard link, you can use the "ln" command
        - ```
          ln [source_file] [link_file]
          ```
    - To create a symbolic link, you can also use the "ln" command
        - ```
          ln -s [source_file] [link_file]
          ```
            - The "-s" option tells the "ln" command to create a symbolic link.

9. What is SELinux?
    - SELinux, or Security-Enhanced Linux, is a Linux kernel security module that provides a mechanism for supporting access control security policies, including mandatory access controls (MAC).
    - It is a set of kernel modifications and user-space tools that have been added to various Linux distributions.
10. What is NFS? What is root_squash?
    - NFS stands for Network File System. It is a protocol that allows users to access files over a network as if they were stored on their local machine.
    - NFS is a distributed file system, which means that the files are stored on one or more servers, but can be accessed by clients as if they were stored locally.
    - "NFS is a popular way to share files between Linux and Unix systems, but it can also be used to share files between Windows and Mac systems. NFS is also used in cloud computing environments to allow users to access files stored on cloud servers."
    - root_squash
        - Root squash is a security feature in NFS that prevents root users on client machines from accessing files on the NFS server with root privileges.
        - It does this by mapping the root user on the client machine to a non-privileged user on the NFS server.
        - It can help to protect your NFS server from unauthorized access and modification.
11. What is Network Information Service (NIS) in Linux?
    - Network Information Service (NIS) is a distributed directory service that allows you to maintain consistent configuration files throughout your network.
    - It is a client-server system, with the server storing a database of configuration information and the clients querying the server for that information.
    - NIS is typically used to store and manage user accounts, hostnames, and other system configuration information.
    - It can be useful for organizations that have a large number of Linux hosts, as it allows you to manage all of the system configuration information from a single location.
12. What is .bashrc and .profile in Linux?
    - .bashrc
        - The .bashrc file is executed every time a user opens a new terminal window.
        - The .bashrc file is typically used to store aliases, functions, and other environment variables that are specific to the user's interactive shell.
    - .profile
        - The .profile file is executed only once when a user logs in to the system.
        - The .profile file is typically used to store environment variables that are needed by all of the user's processes, such as the PATH variable, which specifies the directories where the shell looks for executable files.
13. Explain Linux architecture. What is name of kernel?
    - The Linux architecture is a layered system that consists of several components, each with a specific function.



- Kernel:
  - The kernel is the core of the Linux operating system. It is responsible for managing the system's resources, such as the CPU, memory, and disk storage.
  - The kernel also provides a set of interfaces that allow applications to interact with the system hardware.
  - Name of Kernel:
    - Monolithic Kernel
    - Micro kernels
    - Exo kernels
    - Hybrid kernels
- System libraries:
  - The system libraries are a collection of pre-written functions that can be used by applications to perform common tasks, such as reading and writing files, communicating over the network, and displaying graphics.
- Shell:
  - The shell is a command-line interpreter that allows users to interact with the Linux system.
  - Users can use the shell to start programs, run scripts, and perform other system administration tasks.
- Applications:
  - Applications are programs that run on the Linux system.
  - Applications can be used for a variety of purposes, such as word processing, web browsing, and playing games.

14. What is Kerberos? How does Kerberos work?

- Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users.

- Kerberos is a secure and reliable authentication protocol that is used in a wide variety of environments.
- It is a good choice for organizations that need to protect their networks from unauthorized access.
- Working:
  - Kerberos works by using a trusted third party, called the Key Distribution Center (KDC), to authenticate clients and servers.
  - The KDC issues tickets that prove the identity of clients and servers, allowing secure communication and preventing unauthorized access.

15. What is user? What are groups? How to check the logged in user?

- USER:
  - A user is a person who uses a computer or network service.
  - Some common types of users include:
    - End users
    - System administrators
- GROUP:
  - A group is a collection of users who share common characteristics or permissions.
  - Groups are often used to manage access to resources, such as files, folders, and applications.
- To check the logged-in user, you can use the following command:
  - ```
    whoami
    ```

16. What is root user and general user? How to create a user? How to add user in group? How to change user's privileges?

- root user:
  - The Root user has full administrative privileges and can access and modify any file or system setting on the system.
  - The root user is typically used to perform system administration tasks, such as installing software, configuring the network, and managing user accounts.
- general user:
  - General users are regular users of the Linux system.
  - They have limited privileges and can only access and modify the files and system settings that they are given permission to
- In short

Feature	**Root user**	**General user**
Privileges	Full administrative privileges	Limited privileges
Access to files and system settings	Can access and modify any file or system setting	Can only access and modify the files and system settings that they are given permission to
Typical use cases	System administration tasks	Everyday tasks

- Create User:
    ```

    - `useradd meet`
    - `adduser meet`

- Add in Group:
    - To add a user to a group, you can use the usermod command.
    - The following command will add the user "meet" to the "developers" group:
        - `usermod -G developers meet`

- Change user privileges:
    - `usermod -aG sudo meet`

17. What is default permission of directory and file? How to change it? What is umask in Linux?
    - The default permission of a "directory" in Linux is 755.
    - The default permission of a "file" in Linux is 644.
    - Change permission use "chmod" command
        - ex:
            - `chmod "permissions" "path to file or directory"`
            - `chmod 775 /home/meet`
    - umask:
        - The umask in Linux is a user-defined permission mask that is applied to all newly created files and directories.
        - To set the umask, you can use the umask command. The syntax for the umask command is as follows:
            - `umask "permission"`
        - ex: if umask: 002
            - permissions:
                - directory: 777-002 = 775
                - file : 666-002 = 664