Module 2 {Installation and Maintenance of Hardware and Its components}

Topic: User Management

1. **What is user management?**
   - User management deals with managing and controlling user access to computer systems and resources within an organization. It includes creating and managing user accounts, authenticating users, determining user rights, and enforcing access controls based on roles and responsibilities. It's also important to disable or delete user accounts as needed. Password management and user training are critical to security. User controls and systems help monitor user activity for compliance and security purposes.
   - Proper user management is essential to protect data integrity, confidentiality and availability and reduce the risk of unauthorized access or data breach. It plays an important role in enhancing overall security and protecting sensitive information.

2. **Why is user management needed?**
   - User management is essential for maintaining the security, integrity, and confidentiality of computer systems and resources within an organization. It includes creating and managing user accounts, defining identities, and assigning access rights based on roles and responsibilities. User management implements access control, preventing unauthorized access and potential data leakage, ensuring compliance with laws and regulations, and blocking data. It ensures efficient allocation of resources, supports accountability by monitoring user actions, and supports business continuity by securing critical operations. In addition, user management increases overall security against threats by enabling organizations to enforce strong password policies and multiple authentication methods.

Module 2 {Installation and Maintenance of Hardware and Its components}

3. **Where can we access the user management?**
    - 1. Process: On desktop or server operating systems such as Windows, macOS, or Linux, user control tools are usually found in System Settings or Control Panel. You can access them to create, update, and delete user accounts, set permissions, and manage passwords.

    - Web applications: Web applications usually have the ability to manage the user through an administration dashboard. Site administrators or administrators can use dashboards to manage user accounts, roles, and permissions.

    - 3. Cloud Platform: Cloud service providers such as AWS (Amazon Web Services), Microsoft Azure or Google Cloud Platform are dedicated to user management consoles. These consoles allow administrators to create, modify, and delete user accounts, as well as provide access rights to various cloud services.

    - 4. Content Management Systems (CMS): CMS platforms such as WordPress, Joomla or Drupal include user management. Site administrators can use these interfaces to manage user accounts, roles, and access to various areas of the site.

    - 5. Database Management System: User management for databases is done by a database management system (eg database management system).For example, MySQL, PostgreSQL, Microsoft SQL Server). Database administrators can create, modify, and delete user rights to control access to the database and its tables.

    - 6. Business applications: Enterprise software systems, such as customer relationship management (CRM) or enterprise resource planning (ERP) software, often have user management to control access to certain models or functions.

- Access to user management often requires administrative privileges or credentials to enable only authorized personnel to make changes to user accounts and access rights. The exact steps to access user management may vary depending on the platform, application or system you are using, so if you need assistance we recommend that you consult the relevant documentation or contact your administrator.

4. What are the features of user management?

- 1. User Creation: The ability to create new user accounts with unique characters such as username or email address and provide initial credentials (password or temporary login).

- 2. Authentication and access: Secure authentication mechanisms such as username/password combination or multi-factor authentication to authenticate the user at the time of access.

- 3. User role and contact group: user group in the role or group of contacts with predefined rules and regulations. This simplifies administration by allowing groups rather than individual users.

- 4. Access Rights: Ability to assign specific rights and access rights to users or user groups based on their role or responsibilities in the organization.

- 5. Identity Management: Use password rules such as minimum length, complexity, and expiration rules and allow users to reset their passwords if they forget or are affected.

Module 2 {Installation and Maintenance of Hardware and Its components}

- 6.User deactivation and deletion: Ability to disable or delete user accounts when they are no longer needed to ensure that automated user accounts are not used for unauthorized access.

- 7. User Control and Logging: Monitoring and logging of user activities, including login attempts, accessing certain resources and changing user settings for security, and processing by purpose.

- 8. Account Lockout and Security Precautions: To prevent unauthorized access, use security measures such as locking accounts after multiple failed login attempts.

- 9. User Profile Management: Allows users to manage profile information such as contact information, preferences and notification settings.

- 10. Single Sign-On (SSO): Combined with external authentication systems to allow users to access multiple applications and services using a single set of credentials.

- 11.Self-Service: Provide users with self-service to update their passwords, restore their account, or manage other account-related settings without interrupting administration.
-
- 12. Import/Export Function: Ability to batch import or export user data for easy migration or integration with other systems.

- 13. API Integration: The Application Programming Interface (API) encourages integration with other systems and allows users to manage processes.
- 14. Compliance and Reporting: Generate reports on user activity, access rights, and compliance to assist with audits and compliance.

Module 2 {Installation and Maintenance of Hardware and Its components}

5. **Do a practical to create a user from user management.**

- Creating a User on Windows:
- Go to the "Control Panel" or "Settings" on your Windows computer.
- Look for "User Accounts" or "User Accounts and Family Safety."
- Click on "Add or remove user accounts" or "Manage another account."
- Select "Add a new user account" or "Add a user account."
- Choose whether the user is a "Standard user" or "Administrator" (admin users have more privileges).
- Enter the desired username for the new user.
- If necessary, add a password for the user account (recommended for security).
- Follow the on-screen instructions to complete the user creation process.

6. **Do a practical to change the password of the administrator from the user management tool.**

- Changing Administrator Password on Windows:
- Press the "Windows key + R" on your keyboard to open the "Run" dialog box.
- Type "lusrmgr.msc" and press Enter. This will open the "Local Users and Groups" management console.
- In the left pane, click on "Users" to see a list of user accounts on the right pane.
- Locate the "Administrator" account from the list of users.
- Right-click on the "Administrator" account and select "Set Password."

- A warning prompt will appear informing you that changing the password will lose all encrypted files and data associated with the account. Click "Proceed" if you understand the implications.
- In the "Set Password for Administrator" window, enter the new password and confirm it by typing it again.
- Click "OK" to set the new password for the Administrator account.

Topic: File and Folder Permission

1. **What is file folder permission?**
    - Files and permissions are access controls that determine who can view, edit, or play files and folders on a computer. These permissions fall into three categories: owner, group, and others. Each group can grant special permissions such as read, write or execute. The owner who created the document has the most control. Group permissions allow multiple users to have the same access rightsOthers include all users who are not owners or groups.
    - These permissions are important for managing data security and controlling user access to resources. By setting appropriate permissions, administrators can reduce the risk of modification or unauthorized removal by ensuring that only authorized users have access to sensitive data. File and folder permissions are important to protect data integrity, privacy, and system security in multi-user environments.

2. **What is the use of file and folder permission?**
    - Files and permissions play an important role in computer systems by controlling access to files and directories and determining which users or groups can read, write paper or complete special resources. The primary purpose of file and folder permissions is to increase data security and protect the confidentiality, integrity, and availability of data.

- By setting appropriate permissions, administrators can ensure that sensitive data is accessed only by authorized users, thus preventing unauthorized access rules and information leaks. This helps prevent important information from being intercepted, deleted or viewed by unauthorized persons.
- Documentation and permissions are especially important in a multi-user environment because different users can have different permission levels.
- These permissions allow efficient allocation of resources, allowing users to access the files and directories required for their role while restricting their access to other property areas.

3. **wirte down the steps to give a folder read only permission.**

- To give a folder read-only permission, you can follow these steps on a Windows operating system:
- Locate the Folder: Identify the folder for which you want to set read-only permissions.
- Right-Click on the Folder: Right-click on the folder to open the context menu.
- Select "Properties": From the context menu, choose "Properties" at the bottom. This will open the Properties dialog box for the folder.
- Go to the "Security" Tab: In the Properties dialog box, click on the "Security" tab.
- Click "Edit": Click on the "Edit" button to modify the permissions for the folder.
- Add or Select User/Group: In the "Permissions for [Folder Name]" window, click on "Add" to add a user or group for which you want to set read-only permissions. Alternatively, you can select an existing user or group from the list.
- Set Read-Only Permission: In the "Permission Entry" window, find and check the "Read" box under "Allow." This grants the selected user/group read-only access to the folder.
- Click "OK" to Save Changes: After setting the read-only permission, click "OK" in the "Permission Entry" window, then again in the "Permissions for [Folder Name]" window to apply the changes.
- Confirm Changes: You may need to confirm the changes in the Security dialog box by clicking "Yes" or "OK."

4. **Write a step to give a file only admin permission.**
    - Locate the File: Identify the file for which you want to set admin-only permissions.
    - Right-Click on the File: Right-click on the file to open the context menu.
    - Select "Properties": From the context menu, choose "Properties" at the bottom. This will open the Properties dialog box for the file.
    - Go to the "Security" Tab: In the Properties dialog box, click on the "Security" tab.
    - Click "Edit": Click on the "Edit" button to modify the permissions for the file.
    - Add or Select Administrators Group: In the "Permissions for [File Name]" window, click on "Add" to add the Administrators group.
    - Set Admin-Only Permission: In the "Permission Entry" window, find and check the "Full control" box under "Allow" for the Administrators group. This grants the Administrators full control over the file.
    - Click "OK" to Save Changes: After setting the admin-only permission, click "OK" in the "Permission Entry" window, then again in the "Permissions for [File Name]" window to apply the changes.
    - Confirm Changes: You may need to confirm the changes in the Security dialog box by clicking "Yes" or "OK."

5. **Do a practical to give the folder permission of read only in network.**

- Share the Folder: First, you need to share the folder on the network. Right-click on the folder you want to share, select "Properties," go to the "Sharing" tab, and click "Advanced Sharing." Check the "Share this folder" option and set the share name.

- Set Permissions: After sharing the folder, click on the "Permissions" button in the "Advanced Sharing" window. Here, you can set specific permissions for users and groups accessing the shared folder.

- Add or Select Users/Groups: Click on the "Add" button to add the users or groups for whom you want to set read-only permissions. You can also select existing users or groups from the list.

- Set Read Permission: In the "Permissions" window, select the added user/group, and under the "Allow" column, check the "Read" permission. This grants read-only access to the shared folder for the selected user/group.

- Click "OK" to Save Changes: After setting the read-only permission, click "OK" in the "Permissions" window to apply the changes.

- Configure Network Share Settings: Back in the "Advanced Sharing" window, you can set additional settings for permissions. Click "OK" to close the "Advanced Sharing" window and apply the settings.

6. **Do a practical to change the ownership of the folder and the sub folders in it**

    - Open File Explorer: Navigate to the parent folder containing the subfolders you want to change ownership for using the File Explorer.

    - Identify the Target Folder: Locate the main folder that you want to change ownership of and all its subfolders.

    - Right-Click on the Folder: Right-click on the folder and select "Properties" from the context menu.

    - Go to the "Security" Tab: In the Properties dialog box, click on the "Security" tab.

- Click "Advanced": Click on the "Advanced" button to access advanced security settings.
- Change Owner: In the "Advanced Security Settings" window, click on the "Change" link next to the owner's name.
- Enter New Owner: In the "Select User or Group" window, enter the name of the new owner (e.g., Administrator) or click "Advanced" to search for the user.
- Check Names and Click "OK": After entering the new owner's name, click "Check Names" to validate the name and then click "OK."
- Apply Changes to Subfolders and Files: In the "Advanced Security Settings" window, check the box "Replace owner on subcontainers and objects" to apply the new ownership to all subfolders and files.
- Confirm and Apply Changes: Click "OK" to close the "Advanced Security Settings" window, then click "OK" again in the Properties dialog box to apply the changes.

Topic: Install OS

1. **What is OS?**
    - The operating system (OS) is the underlying software that manages computer hardware and acts as an interface between the user and the computer. It facilitates the execution of applications, manages hardware such as processors, memory and storage devices, and provides a user interface for users to interact with the system. Operating system processes manage memory allocation and data management, ensuring efficient operations and data organization. The device driver in the operating system provides the functionality of peripheral devices by supporting communication between hardware and software components. Different operating systems such as Windows, macOS, Linux, iOS and Android keep track of different devices and user preferences.Operating system selection

can affect computer performance, user experience, and software and hardware compatibility.

2. **What are the types of OS?**
    - There are different types of operating systems (OS), performing different functions and supporting different devices. General-purpose operating systems such as Windows, macOS, and Linux are usually found on desktop and laptop computers, while mobile operating systems such as Android and iOS are designed for smartphones and tablets. The real-time operating system (RTOS) kernel takes care of time, and the server operating system manages network services and shared processes in the server environment. Embedded operating systems are lightweight and suitable for specialized equipment, deploying the operating system to control connected computers. Multi-user functionality allows simultaneous access by multiple users, while time-sharing and time-sharing manage the job and user tasks, respectively.
    - A network operating system simplifies network management. Each operating system type has its own unique features and applications that make users unique in the digital world.

3. **Do a practical to create bootable pendrive for kali Linux**
    - Download Rufus: If you don't have Rufus installed on your PC, download it from the official website (https://rufus.ie/).

    - Insert the USB Pendrive: Insert the USB pendrive into an available USB port on your PC.

    - Run Rufus: Run the Rufus application (no installation is required).

    - Select the USB Drive: In Rufus, under "Device," select your USB pendrive from the dropdown menu.

    - Choose Kali Linux ISO: Under "Boot selection," click on "Select" and browse to the Kali Linux ISO file you downloaded.

- Partition Scheme and File System: For most modern PCs, the default settings will work fine. Ensure that "Partition scheme" is set to "MBR" and "File system" is set to "FAT32."
- Volume Label: You can give a name to your USB pendrive in the "Volume label" field, or leave it blank for the default name.
- Create Bootable Disk: Click on the "Start" button in Rufus to initiate the process of creating the bootable USB.
- Confirmation: A warning message will appear, notifying you that all data on the USB drive will be destroyed. Confirm and proceed.
- Wait for Completion: Rufus will format the USB drive and write the Kali Linux ISO file onto it. This process may take a few minutes.
- Boot from the USB: Once Rufus completes the process, safely eject the USB drive from your PC. Now, you can boot your computer from the USB pendrive to install Kali Linux.

To boot from the USB pendrive:

- Insert the bootable USB into your computer.
- Restart your computer.
- During the boot process, access the BIOS or UEFI settings (usually by pressing F2, F12, Delete, or Esc, depending on your computer's manufacturer).
- In the BIOS/UEFI settings, change the boot order to prioritize the USB drive.
- Save the changes and exit the BIOS/UEFI settings.
- Your computer will boot from the USB pendrive, and you can follow the on-screen instructions to install Kali Linux.

4. **Do a practical to create a bootable pendrive for windows 7**

Module 2 {Installation and Maintenance of Hardware and Its components}

- Download Rufus: If you don't have Rufus installed on your PC, download it from the official website (https://rufus.ie/).
- Insert the USB Pendrive: Insert the USB pendrive into an available USB port on your PC.
- Run Rufus: Run the Rufus application (no installation is required).
- Select the USB Drive: In Rufus, under "Device," select your USB pendrive from the dropdown menu.
- Choose Windows 7 ISO: Under "Boot selection," click on "Select" and browse to the Windows 7 ISO file you have obtained.
- Partition Scheme and File System: For most modern PCs, the default settings will work fine. Ensure that "Partition scheme" is set to "MBR" and "File system" is set to "NTFS."
- Volume Label: You can give a name to your USB pendrive in the "Volume label" field, or leave it blank for the default name.
- Create Bootable Disk: Click on the "Start" button in Rufus to initiate the process of creating the bootable USB.
- Confirmation: A warning message will appear, notifying you that all data on the USB drive will be destroyed. Confirm and proceed.
- Wait for Completion: Rufus will format the USB drive and write the Windows 7 ISO file onto it. This process may take a few minutes.
- Boot from the USB: Once Rufus completes the process, safely eject the USB drive from your PC. Now, you can boot your computer from the USB pendrive to install Windows 7.
- **To boot from the USB pendrive:**
- Insert the bootable USB into your computer.

  - Restart your computer.
  - During the boot process, access the BIOS or UEFI settings (usually by pressing F2, F12, Delete, or Esc, depending on your computer's manufacturer).
  - In the BIOS/UEFI settings, change the boot order to prioritize the USB drive.
  - Save the changes and exit the BIOS/UEFI settings.
  - Your computer will boot from the USB pendrive, and you can follow the on-screen instructions to install Windows 7.

5. **Do pendrive for creating a pendrive for mac os Mojave with unibeast**

- First, you need to Download macOS Mojave from App Store then Download UniBeast.
- Press command+space to open spotlight then search Disk Utility and hit enter.
- Select your USB installer then erase it with the following options.

- Name: USB
- Format: Mac OS Extended Journaled
- Scheme: GUID Partition Map
- Now open UniBeast App and click Continue for a couple of times.
- Agree to terms and conditions.
- Select your USB Installer.
- Select macOS Mojave and click Continue.
- As a bootloader configuration mode, it’s recommended to select UEFI Boot mode. However, if your device doesn’t support UEFI then select Legacy Boot mode.
- Verify the installation options and if you agree click Continue.
- Type the password for your username and click OK button.
- Wait for a couple of minutes to complete the process. It’ll take some time so just be patient and wait. Also, it depends on your speed of your USB. Mostly USB 3.0 or 3.1 is much faster than USB 2.0

6. **Do a practical to install Kali Linux**

Module 2 {Installation and Maintenance of Hardware and Its components}

- Kali Linux ISO - Download the latest Kali Linux ISO from the official website (https://www.kali.org/downloads/).
- USB Pendrive (8GB or more) - You'll use this to create a bootable Kali Linux installer.
- A PC or laptop - Ensure your system meets the minimum requirements to run Kali Linux.
- Step-by-step Guide:
- Create a Bootable USB Installer:
    - Download Rufus (https://rufus.ie/) and install it on your Windows PC. For macOS, you can use Etcher (https://www.balena.io/etcher/).
    - Insert the USB pendrive into your computer.
    - Run Rufus (or Etcher) and select the Kali Linux ISO you downloaded.
    - Choose the USB pendrive as the target device.
    - Start the process to create a bootable USB installer. This will erase all data on the USB drive, so back up any important files.
- Boot from the USB Installer:
    - Insert the bootable USB pendrive into the PC or laptop on which you want to install Kali Linux.
    - Restart the computer and access the BIOS or UEFI settings during boot-up (usually by pressing F2, F12, Delete, or Esc, depending on your computer's manufacturer).
    - In the BIOS/UEFI settings, change the boot order to prioritize the USB drive.
    - Save the changes and exit the BIOS/UEFI settings.
- Kali Linux Installation:
    - The Kali Linux boot menu should appear on your screen. Select "Install" and press Enter.
    - Choose your preferred language, location, and keyboard layout during the installation process.
    - Configure the network settings (Wi-Fi or Ethernet) if required.
- Disk Partitioning:
    - Select the disk on which you want to install Kali Linux.

  - Choose the partitioning scheme (use the guided option for most users).
  - Create the necessary partitions for Kali Linux (root, swap, etc.). If you're unsure, you can use the default settings.
- Install Kali Linux:
  - Confirm the changes to the disk (Note: This will erase all data on the selected disk).
  - The installation process will begin. You may be prompted to configure additional settings, such as setting up a user account and password.
- Complete the Installation:
  - Once the installation is complete, you will be prompted to remove the USB pendrive and press Enter to reboot the system.
  - Remove the USB pendrive and press Enter to reboot the computer.
- Boot into Kali Linux:
  - After the computer restarts, the GRUB boot menu should appear, allowing you to select Kali Linux as the operating system to boot into.
  - Choose Kali Linux from the list, and the system will boot into Kali Linux.

7. **Do a practical to install windows 10**
- Create a Bootable USB Installer:
  - Download Rufus (https://rufus.ie/) and install it on your Windows PC.
  - Insert the USB pendrive into your computer.
  - Run Rufus and select the Windows 10 ISO you downloaded.
  - Choose the USB pendrive as the target device.
  - Start the process to create a bootable USB installer. This will erase all data on the USB drive, so back up any important files.
- Boot from the USB Installer:
  - Insert the bootable USB pendrive into the PC or laptop on which you want to install Windows 10.

  - Restart the computer and access the BIOS or UEFI settings during boot-up (usually by pressing F2, F12, Delete, or Esc, depending on your computer's manufacturer).
  - In the BIOS/UEFI settings, change the boot order to prioritize the USB drive.
  - Save the changes and exit the BIOS/UEFI settings.
- Windows 10 Installation:
  - The Windows 10 setup screen should appear on your screen.
  - Select your language, time, currency, and keyboard preferences.
  - Click "Next" to continue.
- Enter Product Key:
  - If prompted, enter your Windows 10 product key. You can also choose to skip this step and activate Windows later.
- Accept License Terms:
  - Read and accept the license terms by checking the "I accept the license terms" box.
  - Click "Next" to continue.
- Choose Custom Installation:
  - Select "Custom: Install Windows only (advanced)."
- Disk Partitioning:
  - Choose the disk or partition where you want to install Windows 10.
  - If the drive is unallocated or needs to be reformatted, click "New" to create a new partition.
  - Select the newly created partition and click "Next" to begin the installation.
- Install Windows 10:
  - The installation process will begin. The computer will reboot several times during the process.
  - Follow the on-screen instructions to complete the installation.
- Set Up Windows 10:
  - After the installation is complete, you'll be prompted to set up Windows 10.
  - Follow the on-screen instructions to customize your settings, create a user account, and choose privacy settings.

- Log In and Complete Setup:
- Once you complete the setup process, you'll be logged into Windows 10.
- Install any necessary drivers and software for your hardware and enjoy using Windows 10.

8. **Do a practical to install Mac os X**

- Backup Data: Before proceeding with the installation, it's essential to back up all your important data to prevent data loss.
- Download macOS Installer: Download the macOS installer from the Mac App Store or other trusted sources.
- Create a Bootable macOS Installer:
    - Insert a USB pendrive (16GB or more) into your Mac.
    - Open "Disk Utility" (you can find it in the Applications > Utilities folder).
    - Select the USB pendrive from the left sidebar in Disk Utility.
    - Click on the "Erase" button and format the pendrive with the "Mac OS Extended (Journaled)" file system and "GUID Partition Map" scheme.
    - Once the format is complete, close Disk Utility.
- Create Bootable Installer using Terminal:
    - Open "Terminal" (you can find it in the Applications > Utilities folder).
    - Use the "createinstallmedia" command to create a bootable macOS installer on the USB pendrive. Replace "Path_to_MacOS_Installer" with the path to the macOS installer application.
    - sudo /Path_to_MacOS_Installer/Contents/Resources/createinstallmedia --volume /Volumes/USB_Name --nointeraction
    - Enter your administrator password when prompted.
    - Wait for the process to complete; it may take a while.

- Boot from USB Installer:
    - Insert the bootable USB pendrive into your Mac.
    - Restart your Mac while holding down the "Option" key.
    - This will bring up the Startup Manager, allowing you to choose the USB installer as the boot device.
- Install macOS:
    - Once the Mac boots from the USB installer, you'll see the macOS Utilities window.
    - Choose "Install macOS" to start the installation process.
    - Follow the on-screen instructions to select the destination drive, agree to the license terms, and start the installation.
- Complete the Installation:
    - The installation process may take some time to complete. Your Mac will restart multiple times during this process.
    - After the installation is finished, follow the on-screen setup instructions to set up macOS with your preferences, language, Wi-Fi, Apple ID, etc.

Topic: Clean Install

1. **What is clean install?**
    - A clean install is the process of installing an operating system (OS) or software on a computer or device without saving any data or settings from a previous installation. In other words, it involves starting from scratch, deleting all existing files and settings, and installing the operating system or software as it was originally installed.

    - During a fresh installation, all hard drives or storage devices are usually formatted, removing all existing partitions and files. After formatting, the installation process starts and the operating system or software is installed on the new clean drive. This ensures that the new installation does not contain any conflicts, errors or residuals from the previous installation.

- A clean install is usually done to fix software-related problems, remove malware or viruses, upgrade to a newer version of the operating system, or reboot the system to a clean and tidy system. However, it is important to recover important data before performing a clean install, as all data on the drive will be permanently deleted during operation.

2. What is the process for clean install?

- Create a Backup: Save all your important files, documents, photos, and any other data you want to keep to an external storage device or a cloud service.
- Obtain Installation Media: Obtain the installation media for the operating system you want to install. This can be a bootable USB drive or a DVD containing the OS installer.
- Boot from Installation Media: Insert the installation media into your computer's appropriate drive, then restart your computer. You'll need to boot from the installation media, and this often requires changing the boot order in the BIOS/UEFI settings to prioritize the USB or DVD drive.
- Begin Installation: Once your computer boots from the installation media, follow the on-screen instructions to begin the installation process. You'll typically be asked to choose your language, time zone, and keyboard layout.
- Partitioning the Drive: During the installation process, you'll come across the option to choose where to install the OS. At this stage, you'll have to partition your hard drive. You can either let the installer do it automatically or manually create partitions. A common configuration is to have one partition for the OS and another for your personal data, which can help you keep your data separate and easier to manage in the future.
- Format the Drive: After partitioning, you'll have the option to format the drive(s). Formatting will erase all existing data on the selected partition, so be careful and ensure you've backed up everything you need.

- Install the OS: Once the drive is ready, continue with the installation process. Follow the prompts, enter any necessary information (such as your product key for licensed OS versions), and wait for the installation to complete. This may take some time.
- Install Drivers and Updates: After the OS installation is complete, you'll likely need to install drivers for your hardware, such as graphics cards, network adapters, etc. Check your device manufacturer's website for the latest drivers and install them. Additionally, run system updates to ensure you have the latest security patches and improvements.
- Reinstall Applications: Now that you have a fresh OS, you'll need to reinstall your desired applications and software. This includes productivity tools, web browsers, media players, and any other software you regularly use.
- Restore Data: Finally, transfer your backed-up data from the external storage or cloud service back to your computer.

3. what are the benefits of clean install?

- A clean install of the operating system offers several benefits that can significantly improve the performance and stability of your computer. Here are some of the key advantages:
- Improved Performance: Over time, as you use your computer and install/uninstall software, the system can become cluttered with temporary files, registry entries, and other data. A clean install removes all this accumulated junk, resulting in a faster and more responsive system.
- Enhanced Stability: A fresh installation ensures that the operating system starts with a clean slate, free from any potential conflicts or corrupted files that may have arisen over time. This can lead to a more stable and reliable system, reducing the likelihood of crashes and errors.
- Increased Security: Some malware or viruses can be deeply embedded in the system, making them difficult to remove completely. A clean install eliminates any lurking threats and ensures that your system starts with a clean, secure environment.

- Elimination of Bloatware: Many pre-installed computers come with unnecessary software or bloatware that can slow down your system and take up valuable storage space. A clean install allows you to get rid of all these unwanted applications and start with only the necessary software.
- Better Privacy: With a clean install, you can be confident that no remnants of your previous activities or personal data are left behind, providing better privacy and security.
- Easier Troubleshooting: When encountering issues on your computer, a clean install can help you identify whether the problem is due to a software conflict or a hardware issue. If the problem persists even after a clean install, it's more likely to be related to hardware.
- Customization Opportunity: A clean install allows you to set up your system exactly the way you want it from the beginning. You can choose the preferred settings, organize your files, and configure the system according to your needs without any pre-existing influences.
- Extended Hardware Support: Upgrading your hardware, such as replacing your motherboard or CPU, can sometimes lead to compatibility issues. A clean install ensures a fresh start and better integration with the new hardware.
- Long-term Maintenance: Starting with a clean installation provides a solid foundation for your computer's long-term maintenance. Regular system backups and periodic clean installs can help keep your system running smoothly over the years.

4. Do a clean installation of windows XP

- Obtain Windows XP Installation Media: You'll need a valid Windows XP installation CD or a bootable USB drive with the Windows XP setup files.
- Backup Your Data: Before proceeding, make sure to back up all your important files to an external storage device or a cloud service.
- Change Boot Order: Insert the Windows XP installation media into your computer and restart it. Make sure the boot order in the BIOS/UEFI settings is set to boot from the CD/DVD drive or USB drive, depending on your installation media.

- Begin Installation: The computer should boot from the installation media, and the Windows XP setup will start. Follow the on-screen instructions to begin the installation process.
- Partition and Format the Drive: During the installation, you'll be prompted to partition your hard drive and format the partition where you want to install Windows XP. Formatting will erase all data on the selected partition.
- Enter Product Key: When prompted, enter your Windows XP product key. You should have a valid license key to activate the installation.
- Select Region and Language: Choose your preferred language and regional settings.
- Complete Installation: Follow the remaining on-screen instructions to complete the installation of Windows XP. This process may take some time.
- Install Drivers and Software: After the Windows XP installation is complete, you'll need to install drivers for your hardware, such as graphics cards, network adapters, etc. Additionally, you'll need to install any necessary software or applications.

5. Do a clean installation of windows 8

- Obtain Windows 8 Installation Media: You'll need a valid Windows 8 installation DVD or a bootable USB drive with the Windows 8 setup files.

- Backup Your Data: Before proceeding, make sure to back up all your important files to an external storage device or a cloud service.

- Change Boot Order: Insert the Windows 8 installation media into your computer and restart it. Ensure the boot order in the BIOS/UEFI settings is set to boot from the CD/DVD drive or USB drive, depending on your installation media.

- Begin Installation: The computer should boot from the installation media, and the Windows 8 setup will start. Follow the on-screen instructions to begin the installation process.

- Partition and Format the Drive: During the installation, you'll be prompted to partition your hard drive and format the partition where you want to install Windows 8. Formatting will erase all data on the selected partition.

- Enter Product Key: When prompted, enter your Windows 8 product key. You should have a valid license key to activate the installation.

- Select Region and Language: Choose your preferred language and regional settings.

- Complete Installation: Follow the remaining on-screen instructions to complete the installation of Windows 8. This process may take some time.

- Install Drivers and Software: After the Windows 8 installation is complete, you'll need to install drivers for your hardware, such as graphics cards, network adapters, etc. Additionally, you'll need to install any necessary software or applications.

Topic: Upgrade installation

1. **What is upgrade installation?**
    - An upgrade installation is the process of installing a new version of the operating system over an existing version of the operating system. It allows you to save files, applications and settings while updating the file system and configuring it to be compatible with new functions. While it's quick and easy, it's important to back up your data before upgrading. A clean install is recommended for stability and optimization, especially when migrating from a large operating system or experiencing major issues.

2. **What is the benefit of upgrade installation?**
    - The benefits of upgrade installation include:

- Convenience: Upgrade installations are generally easier and more convenient than clean installs. They save you the effort of backing up and reinstalling all your applications and settings.
- Time-Saving: Upgrading is quicker since you don't have to go through the entire installation process or reinstall applications.
- Preserve Settings and Applications: Your files, applications, and personalized settings from the previous OS version are retained, making the transition to the new OS seamless.
- Compatibility: Upgrade installations update system files, drivers, and configurations to ensure compatibility with the new OS version.
- Preserve User Data: All your files and documents remain intact, reducing the risk of data loss that might occur during a clean installation.
- Less Configuration: Since your settings are preserved, you don't have to reconfigure your applications and personalized preferences.
- Cost-Effective: Some OS upgrades may be available for free or at a lower cost compared to purchasing a new full license.
- App Compatibility: In some cases, certain applications might not be compatible with a new OS version. By upgrading, you can test if your existing applications continue to work without issues.
- Familiarity: If you are already accustomed to the previous OS version, upgrading allows you to stay within a familiar environment with some added features and improvements.

3. **Write down the steps of upgrade installation.**
    - Check System Requirements: Ensure that your computer meets the minimum system requirements for the new OS version you intend to upgrade to. Check the official documentation or website of the OS manufacturer for the specific requirements.

Module 2 {Installation and Maintenance of Hardware and Its components}

- Backup Your Data: Create a full backup of all your important files, documents, photos, and any other data you want to keep. You can use an external hard drive, USB flash drive, cloud storage, or a backup software tool.

- Check for Updates: Before starting the upgrade, make sure your current operating system is up to date with the latest software updates and patches. This ensures a smoother transition to the new OS version.

- Obtain the Upgrade Media: Obtain the installation media for the new OS version. This can be a physical disc or a bootable USB drive containing the upgrade files. In some cases, you might be able to download the upgrade directly from the OS manufacturer's website.

- Run Compatibility Check: Many OS upgrades come with a compatibility check tool that scans your system for potential issues with the new OS. Run this tool to identify any hardware or software conflicts that might arise during the upgrade.

- Start the Upgrade: Insert the upgrade installation media into your computer and run the setup program. Follow the on-screen instructions to begin the upgrade process.

- Enter Product Key (If Required): During the installation process, you might be prompted to enter a product key for the new OS version. If you purchased a new license for the upgrade, provide the product key when prompted.

- Accept License Terms: Review and accept the license terms and agreements for the new OS.

- Choose Installation Options: The setup may ask you to choose installation options, such as preserving your files and applications or performing a custom installation. Select the appropriate option based on your preferences.

- Begin the Upgrade: Once you've selected your preferences, the upgrade installation will begin. The process can take some time, depending on the speed of your computer and the complexity of the upgrade.

- Follow On-Screen Prompts: During the upgrade, you may be prompted to make certain choices or confirm certain actions. Follow the on-screen prompts and provide any necessary input.

- Completing the Upgrade: After the upgrade installation is complete, your computer will restart, and you should now be running the new OS version.

- Install Updates and Drivers: After the upgrade, it's essential to check for and install any updates and drivers specific to the new OS version. This ensures optimal performance and compatibility with your hardware and software.

- Restore Data: If necessary, transfer your backed-up data from the external storage or cloud service back to your computer.

4. **Do a practical to upgrade from windows 8 to windows 10.**
    - Check System Requirements: Ensure your computer meets the minimum system requirements for Windows 10. These requirements are generally similar to those of Windows 8 but may have some slight differences. Verify that your computer has sufficient processing power, RAM, and free disk space for Windows 10.
    - Backup Your Data: Before starting the upgrade, create a full backup of all your important files and data to an external storage device or a cloud service.
    - Check for Updates: Make sure your Windows 8 installation is up to date with the latest updates and patches.
    - Download Windows 10 Media Creation Tool: Visit the official Microsoft website and download the Windows 10 Media Creation Tool. You can find it by searching "Windows 10 Media Creation Tool" in your preferred search engine.
    - Run the Media Creation Tool: Double-click the downloaded Media Creation Tool to launch it.
    - Accept License Terms: Review and accept the license terms presented by the Media Creation Tool.
    - Choose Upgrade Option: Select the "Upgrade this PC now" option in the Media Creation Tool and click "Next."

- Check for Compatibility: The tool will check your system's compatibility with Windows 10. If any issues are detected, the tool will provide suggestions to resolve them.
- Download Windows 10: The Media Creation Tool will download the necessary files for Windows 10. This process may take some time, depending on your internet connection speed.
- Begin the Upgrade: Once the download is complete, the tool will prompt you to begin the upgrade. Click "Install" or "Start the upgrade" to initiate the process.
- Follow On-Screen Prompts: The upgrade process will proceed automatically, and you may be asked to confirm a few settings during the process. Follow the on-screen prompts and provide any necessary input.
- Completing the Upgrade: The upgrade may require several restarts. Allow the process to complete, and your computer should boot into Windows 10.
- Check for Updates and Drivers: After the upgrade, check for and install any Windows updates and drivers specific to your hardware. Visit the manufacturer's website for your computer and any additional peripherals to download the latest drivers.
- Restore Data: If necessary, transfer your backed-up data from the external storage or cloud service back to your computer.

Topic: Partition & Formatting

1. **What is partitioning?**
    - Partitioning is the process of dividing a physical disk into several areas called partitions, each acting as a separate drive with its own data. This allows users to better organize information and achieve more goals. A common use is to install multiple boot programs with different operating systems on a single disk. Partitions also improve data protection by separating system files from user files. It improves performance by reducing disk fragmentation and provides flexibility in choosing data systems for multiple partitions.

- It also helps with data backup and recovery by allowing backup options. However, you need to be careful when partitioning because incorrect operations can cause data loss. Users should recover data and use reliable partition tools or utility when replacing partition.

2. **What is partition?**
    - In the context of computing and data management, classification means dividing or dividing a larger logical or physical entity into smaller, manageable parts or subsets. Partitioning is often used in many areas such as disk storage, databases, and parallel processing.

    - **Disk Partitioning:**In disk storage, partitioning divides the physical hard disk drive or solid state drive into separate parts, each of which appears and functions as a standalone unit. These partitions allow the operating system to better manage files and data systems. Users can assign different files to each partition or use them for different purposes, such as one partition for the operating system and another for personal files.
    - **Database Partitioning:**Partitioning in a database environment is the technique used to divide large tables into smaller, more manageable parts called partitions. This approach improves query performance, simplifies data management, and enables more efficient use of resources. Each partition can be placed on a different device or server, which simplifies deployment and increases satisfaction.

    - **Parallel Processing Partitioning:**Parallel processing involves breaking down a complex task into smaller tasks that can be executed simultaneously by multiple processing units. Each subtask is divided into separate sections and the results are combined to form the final results.
    - This method is mainly used in high performance and distribution systems.

Module 2 {Installation and Maintenance of Hardware and Its components}

3. **What is format?**
   - In computing, formatting refers to the process of preparing a medium (such as a hard drive or USB) for data storage by creating a file. It deletes all existing data on the device and creates a new structure to organize and manage the data. This step is important to ensure proper operation and compatibility with the operating system. Users can choose between quick format and full format; the former is faster but potentially outperforms data recovery. Different operating systems support specific file systems, such as NTFS for Windows and APFS for macOS.
   - Formatting is a great way to clean up storage devices, start from scratch, or optimize a system or device. However, care should be taken as it deletes all data on the device, so backup important data first.

4. **Do a Practical of mbr partition.**

   Here's a step-by-step guide to creating an MBR partition using Disk Management on Windows:

   Open Disk Management:

   - Press Win + X on your keyboard and select "Disk Management" from the context menu.
   - Alternatively, you can right-click on "This PC" (or "My Computer" in older versions of Windows), select "Manage," and then navigate to "Disk Management" in the Computer Management window.
   - **Identify the Disk:**
   - In the Disk Management window, you will see a list of all connected disks.
   - Identify the disk where you want to create the MBR partition. Be cautious not to select the wrong disk, as it could lead to data loss.

   Delete Existing Partitions (Optional):

- If the disk already has partitions, and you want to create a new MBR partition, you might need to delete the existing partitions first.
- Right-click on each existing partition and select "Delete Volume" until the disk becomes "Unallocated."

Create MBR Partition:

- Right-click on the "Unallocated" space and select "New Simple Volume."
- Follow the on-screen instructions in the "New Simple Volume Wizard."
- Specify the size of the partition (if you want to use the entire disk, keep the default maximum size).
- Assign a drive letter or mount point (e.g., "D:" or "E:").
- Format the partition with the desired file system (e.g., NTFS).

Complete the Wizard:

- Complete the wizard, and the MBR partition will be created on the selected disk.

5. **Do a Practical of gpt partition**
    - Press Windows + X on your keyboard and select "Disk Management" from the menu that appears. This will open the Disk Management utility.
    - In the Disk Management window, you will see a list of all available disks on your system. Locate the disk you want to partition. Be careful not to select the wrong disk, as partitioning will erase its contents.
    - If the disk is new or uninitialized, you will need to initialize it first. Right-click on the disk's label (Disk 0, Disk 1, etc.) in the list and select "Initialize Disk." Choose the appropriate partition style, which should be GPT for modern systems.

- Once the disk is initialized as GPT, right-click on the "Unallocated" space on the disk and select "New Simple Volume."
- The New Simple Volume Wizard will appear. Click "Next" to start the wizard.
- Specify the size of the partition you want to create. In most cases, you'll want to use the entire available space for a single partition. Click "Next."
- Assign a drive letter to the new partition. You can choose an available letter or leave it to Windows to assign one automatically. Click "Next."
- Format the partition with a filesystem. For most use cases, you can select "NTFS" as the file system. You can also provide a volume label for the partition. Click "Next."
- Review your settings, and when you're ready, click "Finish" to create the partition.
- Windows will create the partition and format it with the specified filesystem. Once the process is complete, you'll see the new partition in the Disk Management window.

6. **Do a practical using cmd**
   - Press Windows + X on your keyboard and select "Windows Terminal" or "Command Prompt" from the menu that appears. You can also search for "cmd" in the Start menu and run Command Prompt as an administrator.
   - In the Command Prompt, type diskpart and press Enter. This will open the DiskPart utility, which allows you to manage disks and partitions from the command line.
   - Type list disk and press Enter. This command will display a list of all available disks on your system. Identify the disk number of the disk you want to partition. Be sure to double-check the disk number and ensure you have the correct disk before proceeding.

- Type select disk X, where X is the disk number you identified in the previous step. Press Enter. For example, if your disk number is 1, you would type select disk 1.

- Type clean and press Enter. This command will remove all existing partitions and data on the selected disk.

- Type convert gpt and press Enter. This command will convert the disk to the GPT partitioning style.

- Type create partition primary and press Enter. This command will create a new primary partition on the disk that spans the entire available space.

- Type format fs=ntfs quick and press Enter. This command will format the partition with the NTFS file system. The quick parameter performs a fast format.

- Type assign letter=X, where X is the drive letter you want to assign to the new partition. For example, assign letter=E will assign the letter E to the partition.

- Type exit and press Enter to exit the DiskPart utility.

- Close the Command Prompt.

7. **covert a partition to gpt by cmd.**
    - Press Windows + X on your keyboard and select "Windows Terminal" or "Command Prompt" (Admin) from the menu that appears. You can also search for "cmd" in the Start menu, right-click on "Command Prompt," and choose "Run as administrator."

    - In the Command Prompt, type diskpart and press Enter. This will open the DiskPart utility, which allows you to manage disks and partitions from the command line.

    - Type list disk and press Enter. This command will display a list of all available disks on your system. Identify the disk number of the disk containing the partition you want to convert to GPT.

- Type select disk X, where X is the disk number of the disk containing the partition you want to convert. Press Enter.
- Type list partition and press Enter. This command will list all partitions on the selected disk.
- Identify the partition number of the partition you want to convert to GPT.
- Type select partition X, where X is the partition number you want to convert to GPT. Press Enter.
- Type convert gpt and press Enter. This command will convert the selected partition to the GPT partitioning style. Note that this operation will erase all data on the selected partition, so make sure you have backed up any important data.
- Once the conversion process is complete, you can close the Command Prompt.

8. **Format a partition using cmd.**
    - Press Windows + X on your keyboard and select "Windows Terminal" or "Command Prompt" (Admin) from the menu that appears. You can also search for "cmd" in the Start menu, right-click on "Command Prompt," and choose "Run as administrator" to open an elevated Command Prompt.
    - In the Command Prompt, type diskpart and press Enter. This will open the DiskPart utility, which allows you to manage disks and partitions from the command line.
    - Type list volume and press Enter. This command will display a list of all available volumes (partitions) on your system, along with their associated drive letters.
    - Identify the volume (partition) you want to format based on its drive letter or other characteristics.

- Type select volume X, where X is the number of the volume you want to format. Press Enter. For example, if the volume number of the partition you want to format is 2, you would type select volume 2.
- Now, you need to choose the file system format for the partition. To format it as NTFS, type format fs=ntfs quick and press Enter. The quick parameter performs a fast format, which is usually sufficient for most cases. If you want a full format (which checks for bad sectors), omit the quick parameter.
- The system will display a warning that all data on the volume will be lost. Type y and press Enter to confirm that you want to proceed with the format.
- The format process will begin, and you'll see a progress indicator. Depending on the size of the partition, it may take some time to complete.
- Once the format is complete, the Command Prompt will display a message confirming the successful formatting of the partition.
- Close the Command Prompt.

Topic: Transferring Files

1. **What is transferring Files?**
    - Data transfer refers to the process of transferring data from one place to another, usually on a device or a network. It allows users to share information, news or other digital content. File transfers usually involve copying files from local devices to a USB drive, uploading files to a cloud storage service, sending attachments via email, or using file transfer methods such as FTP or HTTP. It is essential for data transfer, collaboration, data backup and data sharing between computers and devices. It plays an important role in modern computing by providing seamless communication and data exchange between multiple platforms and networks.

Module 2 {Installation and Maintenance of Hardware and Its components}

2. **What are the ways of transferring files?**

- There are several ways of transferring files, and the choice of method depends on factors like the file size, transfer speed, security, and the devices involved. Here are some common ways of transferring files:
- USB Drive: Using a USB flash drive or an external hard drive to physically copy and transfer files between devices.
- Cloud Storage: Uploading files to cloud storage services like Google Drive, Dropbox, OneDrive, etc., and accessing them from any connected device.
- Email Attachments: Sending files as attachments through email. This method is suitable for smaller file sizes.
- File Transfer Protocols: a. FTP (File Transfer Protocol): Transferring files over the internet using FTP clients. b. SFTP (SSH File Transfer Protocol): A secure version of FTP that uses encryption for enhanced security. c. HTTP/HTTPS: Downloading or uploading files via web browsers.
- Network File Sharing: Sharing files within a local network using shared folders or network-attached storage (NAS) devices.
- Peer-to-Peer (P2P): Directly transferring files between two devices using software like BitTorrent or Airdrop.
- Bluetooth: Transferring files wirelessly between nearby devices equipped with Bluetooth capabilities.
- QR Codes: Using QR codes to transfer files between devices equipped with cameras.
- NFC (Near Field Communication): A short-range wireless technology used for sharing files between compatible devices.
- Remote Access: Accessing files on one device from another using remote desktop software or cloud-based remote access tools.

Module 2 {Installation and Maintenance of Hardware and Its components}

3. **How do we transfer files from one system to another?**
    - USB Drive:
        - Copy the files to be transferred to a USB flash drive or an external hard drive on the source system.
        - Safely eject the USB drive from the source system.
        - Connect the USB drive to the destination system.
        - Copy the files from the USB drive to the desired location on the destination system.
    - Cloud Storage:
        - Upload the files to a cloud storage service like Google Drive, Dropbox, or OneDrive on the source system.
        - Access the cloud storage service from the destination system using a web browser or the respective client application.
        - Download the files to the destination system from the cloud storage service.
    - Email Attachments:
        - Compose a new email on the source system.
        - Attach the files to the email.
        - Send the email to your own email address.
        - Access the email from the destination system and download the attachments.
    - Network File Sharing (Local Network):
        - Ensure that both systems are connected to the same local network.

  - On the source system, share the desired files or folders by right-clicking on them and selecting "Share" or "Properties > Sharing."
  - On the destination system, navigate to the network locations and access the shared files or folders.
- File Transfer Protocol (FTP):
  - Set up an FTP server on the source system or use a public FTP service.
  - Install an FTP client on the destination system.
  - Connect to the FTP server from the destination system using the FTP client and transfer the files.
- Bluetooth or NFC (for Mobile Devices):
  - Enable Bluetooth or NFC on both mobile devices (e.g., smartphones).
  - On the source device, select the files to be transferred and choose the option to share via Bluetooth or NFC.
  - Accept the file transfer request on the destination device to complete the transfer.
- Remote Access:
  - Use remote desktop software or cloud-based remote access tools to access the source system from the destination system.
  - Copy the files from the source system to the destination system using the remote access interface.

Module 2 {Installation and Maintenance of Hardware and Its components}

4. **Types of file transferring media.**
    - There are several ways of transferring files, and the choice of method depends on factors like the file size, transfer speed, security, and the devices involved. Here are some common ways of transferring files:
    - USB Drive: Using a USB flash drive or an external hard drive to physically copy and transfer files between devices.
    - Cloud Storage: Uploading files to cloud storage services like Google Drive, Dropbox, OneDrive, etc., and accessing them from any connected device.
    - Email Attachments: Sending files as attachments through email. This method is suitable for smaller file sizes.
    - File Transfer Protocols: a. FTP (File Transfer Protocol): Transferring files over the internet using FTP clients. b. SFTP (SSH File Transfer Protocol): A secure version of FTP that uses encryption for enhanced security. c. HTTP/HTTPS: Downloading or uploading files via web browsers.
    - Network File Sharing: Sharing files within a local network using shared folders or network-attached storage (NAS) devices.
    - Peer-to-Peer (P2P): Directly transferring files between two devices using software like BitTorrent or Airdrop.
    - Bluetooth: Transferring files wirelessly between nearby devices equipped with Bluetooth capabilities.
    - QR Codes: Using QR codes to transfer files between devices equipped with cameras.
    - NFC (Near Field Communication): A short-range wireless technology used for sharing files between compatible devices.
    - Remote Access: Accessing files on one device from another using remote desktop software or cloud-based remote access tools.

Module 2 {Installation and Maintenance of Hardware and Its components}

5. **Do a practical to transfer files from one system to another via network.**

- On the Source System (Sender):
- Identify the files you want to transfer and place them in a folder for easy sharing.
- Right-click on the folder containing the files you want to share and select "Properties."
- In the Properties window, go to the "Sharing" tab.
- Click on the "Share" button, and a new window will appear.
- Choose the users or groups you want to share the folder with. You can select "Everyone" to share it with all users on the network.
- Set the permission level (Read or Read/Write) for the shared folder. Read allows users to only view the files, while Read/Write allows them to modify or add files to the folder.
- Click "Share" to apply the settings and share the folder.
- On the Destination System (Receiver):
- Open File Explorer and navigate to the network locations.
- You should see the name of the source system or its IP address listed under "Network." Double-click on it to access the shared folders.
- Locate the shared folder you want to access and open it.
- You can now copy the files from the shared folder to any location on the destination system.
- That's it! The files have been transferred from the source system to the destination system via the local network. Remember to disable file sharing or restrict access as needed once the transfer is complete to ensure the security of your network resources.

6. **DO a practical to transfer data from one hard disk to another.**
    - Make sure you have both the source and destination hard disks connected and recognized by your computer.
    - Steps to Transfer Data via Copy and Paste:
    - Open File Explorer by pressing Windows + E on your keyboard.
    - In File Explorer, navigate to the location of the data you want to transfer. This could be specific files, folders, or an entire directory.

- Once you have located the data, right-click on it and select "Copy" from the context menu.
- Now, navigate to the destination hard disk where you want to transfer the data. You can select a specific folder or the root directory of the disk.
- Right-click in the destination location and select "Paste" from the context menu.
- The copying process will begin, and depending on the amount of data being transferred, it may take some time to complete.
- Once the copying process is done, verify that the data has been successfully transferred to the destination hard disk.
- Optionally, you can compare the source and destination data to ensure the transfer was successful.
- Safely eject the source and destination hard disks once the transfer is complete.

Topic: Administrative tools

1.What are administrative tools?

- Management tools are software systems and management consoles that are included in the operating system (especially Windows) to facilitate project management. These tools provide maximum resources for managing hardware, software, network configuration and physical operations. Some management tools include Computer Management, Disk Management, Device Manager, Event Viewer, and Task Scheduler. It enables system administrators and users to perform important tasks such as creating and managing network partitions, setting up user accounts, monitoring system health, and setting policies. These tools provide centralized access to key management, simplifying troubleshooting, improving management, and ensuring proper computer management and security from start to finish.

Module 2 {Installation and Maintenance of Hardware and Its components}

2. What is the use of administrative tools?

- System Management: Administrative tools enable tasks like disk management, device management, and user account management. They allow administrators to create, format, and manage disk partitions, install and update device drivers, and configure user permissions.

- Troubleshooting: These tools provide access to system logs, event viewers, and performance monitors, helping administrators identify and diagnose issues, errors, and warnings. This aids in proactive problem-solving and system optimization.

- Network Management: Administrative tools assist in network-related tasks, such as configuring network settings, setting up group policies, and managing network services.

- Automation: Tools like Task Scheduler allow the automation of tasks, scripts, and programs, reducing manual intervention and improving system efficiency.

- Security Management: Administrative tools include features for managing security settings, such as Windows Firewall configuration and access controls, to safeguard the system and network from potential threats.

- Policy Implementation: With group policy management, administrators can define and apply policies that dictate the behavior and settings of computers within a network.

3. List out the administrative tools.

- Computer Management: Provides access to various system management tools like Device Manager, Disk Management, Event Viewer, and more.

- Disk Management: Allows administrators to create, format, and manage disk partitions and volumes.

- Device Manager: Facilitates managing hardware devices and their drivers, enabling installation, updating, or uninstallation.

Module 2 {Installation and Maintenance of Hardware and Its components}

- Event Viewer: Logs and monitors system events, errors, and warnings for troubleshooting and system analysis.
- Local Users and Groups: Manages user accounts and groups on the local computer.
- Task Scheduler: Enables the scheduling of tasks, scripts, and programs to run automatically at specific times or events.
- Services: Manages system services, allowing users to start, stop, and configure services.
- Group Policy Management: Configures and applies group policies to control the behavior and settings of computers in a network.
- Performance Monitor: Monitors system performance metrics and generates performance reports.
- Windows Firewall with Advanced Security: Provides advanced configuration options for the built-in Windows Firewall.
- Component Services: Manages COM+ applications and services for distributed applications.
- Device and Printers: Displays a list of installed devices and printers on the computer.
- System Configuration: Provides tools to manage system startup and configure system settings.
- Event Viewer: Monitors and displays detailed information about system events, logs, and errors.
- Resource Monitor: Provides real-time monitoring of system resource usage (CPU, memory, disk, network).

Module 2 {Installation and Maintenance of Hardware and Its components}

4. What is disk management tools.

- Disk Management is an administrative tool in Windows operating systems that allows users to manage and control the storage devices (hard drives, solid-state drives, etc.) connected to their computer. It provides a graphical user interface to perform various disk-related tasks, such as partitioning, formatting, and assigning drive letters.
- Key features of Disk Management tools include:
- Partitioning: Creating, deleting, shrinking, and extending disk partitions to organize storage space efficiently.
- Formatting: Preparing a partition or drive for use by choosing a file system (e.g., NTFS, FAT32) to store data.
- Assigning Drive Letters: Allocating drive letters to newly created partitions, making them accessible in File Explorer.
- Changing Volume Labels: Renaming the volumes to provide meaningful names for better identification.
- Extending and Shrinking Partitions: Adjusting partition sizes to accommodate changes in storage requirements.
- Converting Disk Types: Converting a Basic Disk to a Dynamic Disk for advanced storage features.
- Setting Active Partitions: Designating an active partition for booting the operating system.
- Mounting Virtual Hard Disks (VHD): Attaching and accessing VHD files as if they were physical disks.

Module 2 {Installation and Maintenance of Hardware and Its components}

5. Do a practical to delete a driver and reinstall it from administrative tools.

- Open Device Manager:
    - Press Windows + X on your keyboard and select "Device Manager" from the menu, or
    - Right-click on the "Start" button and choose "Device Manager," or
    - Press Windows + R, type devmgmt.msc, and click "OK."
- Locate the Driver:
    - In the Device Manager, expand the category that corresponds to the device whose driver you want to uninstall. For example, if you want to reinstall your graphics card driver, locate the "Display adapters" category.
- Uninstall the Driver:
    - Right-click on the device name and select "Uninstall device."
    - If prompted, choose "Delete the driver software for this device" to remove the driver completely.
- Reinstall the Driver:
    - After uninstalling the driver, you can either restart your computer to allow Windows to automatically reinstall the driver, or
    - Visit the manufacturer's website for the device and download the latest driver software for your operating system.
    - Install the downloaded driver by following the installation prompts.

Module 2 {Installation and Maintenance of Hardware and Its components}

6. Do a practical to delete a partition and again create it with administrative tool

- Open Disk Management:
  - Press Windows + X on your keyboard and select "Disk Management" from the menu.
  - Alternatively, you can right-click on "This PC" (or "My Computer" in older versions of Windows), select "Manage," then click on "Disk Management" under "Storage" in the Computer Management window.
- Identify the Partition:
  - In Disk Management, you will see a list of all connected disks and their partitions. Identify the partition you want to delete and create a new one. Be sure to double-check that you've selected the correct partition.
- Delete the Partition:
  - Right-click on the partition you want to delete.
  - Select "Delete Volume" from the context menu.
  - Confirm the action when prompted.
- Create a New Partition:
  - After deleting the partition, you will have "Unallocated" space.
  - Right-click on the unallocated space.
  - Select "New Simple Volume" from the context menu.
  - The New Simple Volume Wizard will open.
  - Click "Next" and follow the wizard to set the size, drive letter, and format the new partition with the desired file system (e.g., NTFS).
  - Complete the wizard to create the new partition.

- Finalize the Process:
  - Once the new partition is created, you will see it in Disk Management with the assigned drive letter.

7. **Do a practical to create user with administrative tool.**
   - Open Computer Management:
     - Press Windows + X on your keyboard and select "Computer Management" from the menu.
     - Alternatively, you can right-click on "This PC" (or "My Computer" in older versions of Windows), select "Manage," then click on "Computer Management" in the Computer Management window.
   - Navigate to Users and Groups:
     - In the Computer Management window, expand "Local Users and Groups" in the left pane.
     - Click on the "Users" folder.
   - Create a New User Account:
     - Right-click on the right pane and select "New User."
     - The "New User" window will open.
   - Enter User Details:
     - In the "New User" window, enter the required details for the new user account:
       - User name: Enter the desired username for the new account.
       - Full name: Add the full name of the user (optional).

        - Description: Add a description for the user (optional).
        - Password: Set a password for the account (optional).
        - Confirm Password: Confirm the password.

- Configure User Properties:
    - If you want the user account to be an administrator, do the following:
        - Click on the "Member of" tab.
        - Click "Add."
        - Type "Administrators" (without quotes) and click "Check Names" to verify the name.
        - Click "OK."
- Create the User Account:
    - Click "Create" to create the new user account.
- Finish:
    - You will see a confirmation message that the user account has been created.
    - Close the Computer Management window.

Module 2 {Installation and Maintenance of Hardware and Its components}

Topic: Windows Feature.

1. **What is windows features?**
    - **Windows Features, also known as Windows Components or Optional Products, are additional software products and features that can be installed or removed from the Windows operating system. These features expand the capabilities of the Windows operating system and allow users to customize their computing experience according to their specific needs.**

    - **Windows features may include many tools, services, and applications that are not installed by default but can be added as needed. Some Windows features include:**
    - **Internet Information Services (IIS): Provides support for web servers that host websites and web applications.**
    - **Hyper-V: A virtualization platform that enables users to create and manage virtual machines.**
    - **Windows Media Player: Multimedia player for audio and video files.**
    - **Telnet Client: A tool for accessing remote computers.**
    - **Windows Subsystem for Linux (WSL): Allows running a Linux distribution under Windows.**
    - **.NET Framework: A software framework for building and running Windows applications.**
    - **Remote Desktop Services (RDS): Provides remote access to Windows-based applications or desktops.**
    - **Windows PowerShell: An advanced command line shell and script.**
    - **Windows Fax and Scan: Allows you to send and receive faxes and copy documents.**
    - **Windows Defender: Built-in antivirus and anti-malware protection.**
    - **To manage Windows features:**
    - **Open Control Panel and go to Programs > Programs and Features.**
    - **On the left, click Turn Windows features on or off.**

- **A list of available jobs will be displayed. Check or uncheck the box next to a feature to install or remove it.**
- **Click OK and follow the further instructions to apply the changes.**

2. **List out the windows features.**
   - File Explorer: The file management tool for navigating and organizing files and folders on your computer.
   - Start Menu: The central access point to launch applications, search for files, and access various system features.
   - Taskbar: The bar typically located at the bottom of the screen, providing quick access to frequently used applications and system notifications.
   - Cortana/Search: Microsoft's virtual assistant and search tool, which allows you to perform searches and access information using voice commands or text input.
   - Action Center: A notification center that displays system and app notifications, as well as quick access to various settings.
   - Microsoft Store: An app store that allows you to download and install various applications, games, and utilities.
   - Windows Update: The feature that keeps your Windows operating system and installed Microsoft products up to date with the latest security patches and feature updates.
   - Control Panel: A central hub for configuring various system settings and options.
   - Settings: A more modern and user-friendly version of the Control Panel, providing access to system settings and configurations.
   - Task Manager: A utility that provides real-time information about the running processes, performance, and resource usage of your computer.

Module 2 {Installation and Maintenance of Hardware and Its components}

- System Restore: A feature that allows you to revert your system to a previous state in case of issues or errors.
- Windows Defender (or Microsoft Defender): The built-in antivirus and antimalware software for protecting your system from threats.
- User Account Control (UAC): A security feature that prompts you for permission when changes are made to the system that require administrator privileges.
- Windows Firewall: A built-in firewall that helps protect your computer from unauthorized network access.
- Remote Desktop: Allows you to connect to another computer remotely, either within a local network or over the internet.
- BitLocker: A feature that enables full-disk encryption for data protection.
- Windows Hello: A biometric authentication feature that allows you to log in to your device using your fingerprint, face, or iris.
- DirectX: A collection of APIs for multimedia and gaming tasks on Windows.
- Windows Media Player: A multimedia player that allows you to play audio and video files.
- Windows Ink: A set of features designed to work with touchscreens and stylus input for digital inking.

Module 2 {Installation and Maintenance of Hardware and Its components}

3. **What is the use of IIS?**

- IIS stands for Internet Information Services. It is a web server software application developed by Microsoft and is included with most versions of the Windows operating system. The primary use of IIS is to host and serve websites and web applications on the internet or on a local network. Here are some of the key uses and functionalities of IIS:
- Web Hosting: IIS allows you to host websites, web applications, and web services on a Windows server. It handles incoming HTTP requests and serves the appropriate web pages or content to the client's web browser.
- ASP.NET Support: IIS is optimized to work with Microsoft's ASP.NET framework, which enables the development of dynamic and interactive web applications.
- PHP and Other Technologies: While initially developed for ASP.NET, IIS also supports various other web technologies, including PHP, Python, and other scripting languages, making it versatile in hosting different types of web applications.
- FTP Server: IIS includes an FTP (File Transfer Protocol) server, which allows you to upload and manage files on your server through FTP clients.
- Security Features: IIS provides robust security features, such as authentication methods, SSL/TLS support, and request filtering, to ensure the safe and secure transmission of data between the server and clients.
- Virtual Hosting: With IIS, you can set up and manage multiple websites or web applications on a single server using different domain names or IP addresses. This is known as virtual hosting.
- Application Pooling: IIS uses application pools to separate and manage different web applications or websites, providing better isolation and stability. If one application encounters an issue, it won't affect others in separate application pools.
- Performance Monitoring and Logging: IIS offers tools for performance monitoring and logging, allowing administrators to track server performance, diagnose issues, and optimize the server's performance.
- URL Rewriting and Redirection: IIS allows administrators to rewrite URLs and set up redirection rules, which can be useful for search engine optimization (SEO) and managing page URLs.

- Server-Side Includes: IIS supports Server-Side Includes (SSI), which enables the inclusion of dynamic content in web pages, such as headers, footers, and common elements.

4. **Do a practical to re install IIS with windows feature.**
    - Open the Control Panel:
        - In Windows 10 or Windows 11, right-click on the Start button and select "Settings." Then, go to "Apps" > "Optional Features" > "Add a feature."
        - In Windows 8.1 or Windows 7, click on the Start button, then open the Control Panel.
    - In the Control Panel, select "Programs" (or "Programs and Features" in Windows 7).
    - In the Programs and Features window, click on "Turn Windows features on or off" on the left side.
    - A dialog box labeled "Windows Features" will appear, showing a list of various Windows components you can enable or disable.
    - Scroll down the list and look for "Internet Information Services (IIS)." It might be located under "Internet Information Services."
    - Check the box next to "Internet Information Services (IIS)" to enable it. You may also see some sub-components of IIS that you can select based on your requirements.
    - After checking the appropriate boxes, click the "OK" button to start the installation.
    - Windows will install the selected IIS components, and this process may take a few minutes.

- Once the installation is complete, you may be prompted to restart your computer. If so, save any unsaved work and restart your computer.
- After the restart, IIS will be installed and ready to use on your Windows computer.

5. **Do a practical to install dotnet framework 3.5 with Windows feature.**
    - Open the "Control Panel" on your computer. You can do this by typing "Control Panel" in the search bar or accessing it through the Start menu.
    - In the Control Panel, click on "Programs" or "Programs and Features," depending on your Windows version.
    - On the left side of the window, click on "Turn Windows features on or off." This will open the "Windows Features" dialog box.
    - In the "Windows Features" dialog box, you will see a list of optional features that you can enable or disable. Scroll down to find ".NET Framework 3.5 (includes .NET 2.0 and 3.0)" and check the box next to it.
    - When you check the box, a small window might pop up, indicating that Windows needs to download the required files from Windows Update. Click on "Download files from Windows Update" (if available) to proceed with the installation.
    - Windows will download and install the necessary files for .NET Framework 3.5. This process may take some time, depending on your internet speed and computer performance.
    - Once the installation is complete, you might be prompted to restart your computer. If so, go ahead and restart.
    - After the restart, the .NET Framework 3.5 should be installed and ready to use on your Windows machine.

Module 2 {Installation and Maintenance of Hardware and Its components}

6. Do a practical to disable internet explorer in windows feature.

- Open the "Control Panel" on your computer. You can do this by typing "Control Panel" in the search bar or accessing it through the Start menu.
- In the Control Panel, click on "Programs" or "Programs and Features," depending on your Windows version.
- On the left side of the window, click on "Turn Windows features on or off." This will open the "Windows Features" dialog box.
- In the "Windows Features" dialog box, you will see a list of optional features that you can enable or disable. Scroll down to find "Internet Explorer 11" and uncheck the box next to it.
- When you uncheck the box, a small window might pop up, indicating that Windows needs to make changes to apply the feature change. Click on "Yes" to proceed.
- Windows will proceed to disable Internet Explorer. This process might take a moment.
- Once the process is complete, you might be prompted to restart your computer. If so, go ahead and restart.
- After the restart, Internet Explorer will be disabled on your Windows machine. It will no longer be accessible from the Start menu or taskbar.

Module 2 {Installation and Maintenance of Hardware and Its components}

Topic: Backup & Restore

1. **What is backup?**
   - Backup is the process of making copies of data to prevent data loss or corruption. Ensuring the integrity and availability of data is an important aspect of technology. Backups can be complete, incremental, or variable and can be stored locally or externally, including in the cloud. The main objective is to provide data recovery with minimal downtime and associated risks such as bankruptcy or legal troubles in case of equipment failure, deletion errors, cyber attacks or natural disasters. A good backup strategy should be in place, including regular testing and verification of backup data to ensure data can be recovered when needed.

2. **What is Restore?**
   - Restore is the process of restoring data from a backup to its original location or to another location. It is an essential part of data management and backup applications to protect lost, damaged or compromised data. Depending on the type of backup used (such as full, incremental, or differential), recovery includes accessing the backup file, selecting the appropriate backup version, initiating recovery, and verifying data integrity.
   - Effective recovery enables organizations to continue their normal operations and mitigate the effects of data loss or damage. Reliable backup and recovery processes are essential to ensure data availability and business continuity.

Module 2 {Installation and Maintenance of Hardware and Its components}

3. **What is the need of backup ?**
   - Backup is an important practice that involves copying data to prevent data loss or corruption. Data is vulnerable to various threats such as hardware failure, software errors, malicious deletion, data corruption, cyber attacks and natural disasters, so backup is needed. Through regular data backups, individuals, businesses and organizations can ensure data integrity, availability and continuity.

   - For businesses, data loss can be financially devastating and impacts operations, making data backups an essential part of disaster recovery and business continuity. In addition, having reliable backups in the face of ransomware attacks allows organizations to restore data without losing the ransom demand.
   - Business compliance is another important reason to manage data backups, as some businesses require special data storage and protection measures.

   - Backup also gives users peace of mind that their important data is safe and recoverable. They provide the additional benefits of data history and version control to retrieve data from a specific time point or previous state.

   - Additionally, data backups help facilitate data transfer to new systems or hardware. It acts as insurance against data-related events, giving users confidence to manage and use their data.

4. **What are the tools of backup?**
   - Backup tools will vary according to the specific needs and requirements of the system or data to be backed up. However, some backup tools are:

   - File-level backup software: This tool allows you to backup individual files and folders for easy retrieval of Private information when needed. Examples include Windows Backup, macOS Time Machine, and many third-party tools.

Module 2 {Installation and Maintenance of Hardware and Its components}

- Disk Imaging Software: A disk imaging tool that creates an exact copy (image) of an entire disk or partition. This allows you to customize the entire system, including functionality, apps, and data.
- For example Clonezilla and Macrium Reflect.

- Cloud backup services: Cloud backup services provide offsite backup solutions by storing data remotely over the Internet. Examples include Backblaze, Carbonite, and Google Backup and Sync.

- Network Attached Storage (NAS) Device: A NAS device is a dedicated storage device attached to a network and is typically used for centralized data backup and file sharing at home or business.

- External Hard Drive: An external hard drive is a storage device that can be connected to a computer for manual backup.These are a simple and easy backup solution.

- Tape Backup Systems: Although rare today, tape backup is still used for big data backup and storage.
- RAID (Redundant Array of Independent Disks): A RAID configuration can provide some data redundancy by acting as a backup in case of drive failure. However, RAID is not a replacement for regular backups.

- Database backup tools: For databases, special backup tools are often used to create backups of the data stored in them.
- Examples include mysqldump for MySQL databases and pg_dump for PostgreSQL databases.

- Version Control Systems: Primarily used for project management and collaboration, control systems such as Git can also act as backups for code repositories.

Module 2 {Installation and Maintenance of Hardware and Its components}

5. **How do we restore?**
    - The procedure for restoring data from a backup depends on the type of backup you made and the device you use for it. Recovery overview for different backup types:

    - **File-level backup recovery:**
        - If you have a file-level backup, you only need to navigate to one backup store (external drive, cloud service). VESAIR.).
        - Find the file or folder to be recovered and copy it back to its original location on the computer.

    - **Disk Image Recovery:**
        - To recover from a disk image backup, you need a bootable recovery media (such as a USB drive or CD/DVD) containing image software.
        - Start your computer using the recovery media.
        - Select Recovery from disk image and select the image file to use for recovery.
        - Follow the onscreen instructions to start the recovery process.
        - When the process is complete, your system returns to the state it was in when you created the image.

    - **Cloud backup recovery service:**
        - For cloud backup, visit the backup service's website or app.
        - Login to your account and go to Recovery.
        - Select the file or data to restore, and then choose a location to restore (for example, the original location on your computer).
        - Follow the instructions to start the recovery process.

- **Network Attached Storage (NAS) backup:**
  - If you are using a NAS device for backup, access the NAS management interface via a web browser or custom app.
  - A backup file or folder was found for editing. Copy data back to your computer or desired location usingNAS backup functionality.

- **Database Backup Restore:**
  - Database backups are usually restored using specialized database management tools. Chapter
  - For example, MySQL, PostgreSQL) and import the backup data into the database using the appropriate commands.

6. **How to create a restore point?**

- Creating a restore point is a feature primarily available on Windows operating systems. It allows you to save a snapshot of your computer's system settings and configuration, which can be used to restore your system to a previous state if any issues arise. Here's how you can create a restore point on Windows:

- **Open System Properties:**
  - Press the Windows key + R to open the Run dialog box.
  - Type sysdm.cpl and press Enter. This will open the System Properties window.

- **Navigate to the System Protection tab:**
  - In the System Properties window, go to the "System Protection" tab.

- **Create a restore point:**
  - Under the "Protection Settings" section, you'll see a list of available drives on your computer.

  - Select the drive where you want to create the restore point (typically the system drive, usually labeled as C:) and click on the "Create" button.

- **Name the restore point:**
  - You'll be prompted to provide a name or description for the restore point. It's best to give it a descriptive name so you can identify it easily in the future.
- **Create the restore point:**
  - Click the "Create" button after providing a name.
  - Windows will then create the restore point, and you'll see a progress bar indicating the status.
- **Finish:**
  - Once the restore point is created successfully, you'll see a confirmation message.
  - Click "Close" to exit the System Properties window.
  - Your restore point is now created, and you can use it to revert your system to this specific state if needed. To restore your system to a previous restore point, follow the same steps above, but this time, click on the "System Restore" button in the "System Protection" tab. From there, you can select the desired restore point and proceed with the restoration process.

7. **Do a practical to create restore point.**

- Creating a Restore Point on Windows 10:
- Press the Windows key on your keyboard to open the Start menu.
- Type "Create a restore point" and select the corresponding option from the search results. This will open the System Properties window with the "System Protection" tab selected.

- In the System Properties window, you'll see a list of available drives on your computer under the "Protection Settings" section. Select the drive where you want to create the restore point (typically the system drive, usually labeled as C:).
- Click on the "Create" button located at the bottom of the window.
- You will be prompted to provide a name or description for the restore point. It's recommended to give it a descriptive name that can help you identify it later.
- After entering the name, click "Create" to create the restore point. Windows will then start creating the restore point, and you'll see a progress bar indicating the status.
- Once the restore point is created successfully, you'll see a confirmation message. Click "OK" to close the confirmation window.

8. **Do a practical to restore from restore point.**
    - Restoring from a Restore Point on Windows 10:
    - Open System Properties:
    - Press the Windows key on your keyboard to open the Start menu.
    - Type "Create a restore point" and select the corresponding option from the search results. This will open the System Properties window with the "System Protection" tab selected.
    - Initiate System Restore:
    - In the System Properties window, click on the "System Restore" button. This will open the System Restore wizard.
    - Choose a Restore Point:
    - In the System Restore wizard, click "Next" to proceed.
    - You'll see a list of available restore points. Select the restore point you want to use for the restoration. Make sure to choose a restore point that was created before the issue you want to resolve occurred.
    - Click "Next" to continue.

- Confirm the Restore Point:
- Review the details of the selected restore point to ensure it's the one you want to use.

- Click "Finish" to confirm your selection. This will prompt a warning that the restore process cannot be interrupted.

- Start the Restoration:
- Click "Yes" to confirm that you want to start the restoration process.

- Windows will then begin the restoration, which may take some time. Your computer may restart during the process.

- Complete the Restoration:
- After the restoration is complete, your computer will restart automatically.

- You'll see a message indicating whether the restoration was successful or not.

9. **Do a practical to take backup from another system**

Taking Backup from One System to Another using a USB Flash Drive:

Step 1: Prepare the USB Flash Drive:

- Insert the USB flash drive into a USB port on the source system (the system from which you want to take the backup).

Step 2: Copy the Files to the USB Flash Drive:

- On the source system, navigate to the files or folders you want to back up.
- Select the files and folders you want to transfer.
- Right-click on the selected items, and then click on "Copy".

Step 3: Access the USB Flash Drive:

- Open File Explorer (Windows) or Finder (Mac) on the source system.

- Locate the USB flash drive under the list of drives or devices. It is usually labeled with a drive letter (e.g., E:, F:, etc.) on Windows or has a specific name on Mac.

Step 4: Paste the Files to the USB Flash Drive:

- Double-click on the USB flash drive to open it.
- Right-click on an empty area inside the USB flash drive window, and then click on "Paste". This will copy the files from the source system to the USB flash drive.

Step 5: Safely Eject the USB Flash Drive:

- Once the files have been copied to the USB flash drive, right-click on the USB flash drive icon in the system tray (Windows) or Finder (Mac).
- Click on "Eject" or "Safely Remove" to safely disconnect the USB flash drive from the source system.

Step 6: Transfer the USB Flash Drive to the Target System:

- Now, remove the USB flash drive from the source system and insert it into a USB port on the target system (the system to which you want to transfer the backup).

Step 7: Copy the Backup Files to the Target System:

- On the target system, open File Explorer (Windows) or Finder (Mac).
- Locate the USB flash drive in the list of drives or devices.
- Double-click on the USB flash drive to open it and view its contents.
- Select the files and folders you want to transfer to the target system.
- Right-click on the selected items, and then click on "Copy".

Step 8: Paste the Backup Files on the Target System:

- Navigate to the location on the target system where you want to store the backup files.
- Right-click on an empty area, and then click on "Paste" to copy the files from the USB flash drive to the target system.

Module 2 {Installation and Maintenance of Hardware and Its components}

Topic: Disk Management

1. **What is Disk management?**
   - Disk Management is a utility built into the Microsoft Windows operating system that allows users to manage disk drives and storage devices. With Disk Management, you can perform many tasks related to disks, partitions and volumes on your computer. It provides a graphical interface for viewing and updating hard drives and other data storage structures.

2. **What is the use of disk management?**
   - The main purpose of Disk Management is to manage and manage disks and storage devices on Windows computers. It provides a graphical interface for performing various disk-related tasks, allowing users to install, format, and manage storage resources.

3. **What are the merits of Disk management tool?**
   - Disk Management is a utility built into the Windows operating system that provides users with useful tools to manage disk drives and storage devices. It offers the ability to create, delete, format and modify partitions, allowing users to organize data efficiently. This tool simplifies the driver list so that different drivers can be easily accessed and identified. Also, users can change the partition to adjust the distribution as needed. Disk Management also provides basic disk management functions such as initializing new disks, converting basic disks to dynamic disks (and vice versa), and checking disk properties.
   - It comes as a pre-installed tool at no additional cost, and its compatibility with various versions of Windows makes it available to a wide range of users. However, users may need to look for third-party management tools or proprietary software for more advanced features.

Module 2 {Installation and Maintenance of Hardware and Its components}

4. **Where can we find the disk management tool?**

- Disk Management tool on Windows operating systems. It is a built-in utility provided by Microsoft for managing disk drives and storage devices. Here's how you can access the Disk Management tool:
- On Windows 10:
- Right-click on the Start button (Windows logo) located at the bottom-left corner of the screen.

- From the context menu that appears, select "Disk Management". This will open the Disk Management window.

  On Windows 8/8.1 and Windows 7:

- Right-click on Computer (Windows 7) or This PC (Windows 8/8.1) located on the desktop or in the Start menu.

- From the context menu, select "Manage". This will open the Computer Management window.

- In the Computer Management window, click on "Disk Management" under the Storage category in the left-hand pane.

- Alternatively, you can also search for "Disk Management" using the Windows search bar, and it should appear in the search results. Simply click on the "Disk Management" option to open the utility.

Module 2 {Installation and Maintenance of Hardware and Its components}

5. **List out the operations we can do with disk management tool**

- The Disk Management tool in Windows provides various operations to manage disk drives and storage devices. Here is a list of common operations that you can perform using Disk Management:
- Create New Partition: You can create a new partition on an unallocated space or shrink an existing partition to create a new one.
- Delete Partition: You can delete an existing partition to free up space or reorganize your disk.
- Format Partition: Formatting a partition prepares it for data storage by setting up the file system.
- Change Drive Letter and Paths: You can assign or change drive letters to partitions, making them easily accessible.
- Extend Partition: If there is unallocated space adjacent to a partition, you can extend it to use that space.
- Shrink Partition: You can reduce the size of a partition to free up space or create a new partition.
- Initialize New Disk: When you add a new disk to your system, you need to initialize it to make it ready for use.
- Convert Disk: You can convert a basic disk to a dynamic disk, which allows for advanced features like software RAID.
- View Disk Properties: Disk Management provides essential information about the disks installed on your computer, such as capacity, free space, and file system.
- View Volume Properties: For each partition, you can view properties such as file system, capacity, free space, and more.
- Change Volume Label: You can assign a custom label to a partition to help identify it easily.

- Mark Partition as Active: If you have multiple operating systems on different partitions, you can mark one partition as active for booting.

6. **Do a practical to create a new partition with disk management tool.**

   Creating a New Partition with Disk Management:

   Step 1: Open Disk Management:

   - Right-click on the Start button (Windows logo) located at the bottom-left corner of the screen.
   - From the context menu that appears, select "Disk Management". This will open the Disk Management window.

   Step 2: Locate Unallocated Space:

   - In the Disk Management window, you'll see a list of all your disk drives and their partitions.
   - Look for an area labeled as "Unallocated" or with black bars (unallocated space) on one of the disks. This is the space where you can create a new partition.

   Step 3: Create the New Partition:

   - Right-click on the unallocated space.
   - From the context menu, select "New Simple Volume...". The New Simple Volume Wizard will appear.

   Step 4: Wizard Welcome:

   - Click "Next" to proceed.

Step 5: Specify Volume Size:

- By default, the wizard will suggest using the maximum available space for the new partition. If you want to create a smaller partition, enter the desired size in megabytes (MB) in the "Simple volume size in MB" field.
- Click "Next" to continue.

Step 6: Assign Drive Letter or Path:

- You can choose to assign a drive letter to the new partition. A drive letter helps you access the partition easily in File Explorer. The system will suggest an available drive letter, but you can change it if needed.
- Click "Next" to proceed.

Step 7: Format Partition:

- Choose a file system for the new partition. For most use cases, it's best to use "NTFS" as it supports large file sizes and offers better security features.
- Enter a "Volume label" if you want to give the new partition a specific name (optional).
- Check the "Perform a quick format" box for faster formatting (recommended for new drives).
- Click "Next" to continue.

Step 8: Completing the Wizard:

- Review the information provided on the summary page.
- Click "Finish" to create the new partition.

Step 9: Confirmation:

- You will receive a message confirming that the new partition has been created successfully.

Module 2 {Installation and Maintenance of Hardware and Its components}

7. **Do a practical to convert from MBR to gpt from disk management tool**
    - To complete the disk conversion by using Disk Management, follow these steps.
    - Back up or move the data on the MBR disk prior to conversion.
    - Delete all partitions and volumes on the MBR disk.
    - For each partition or volume, select and hold (or right-click) the item, and select Delete Partition or Delete Volume.
    - Select and hold (or right-click) the MBR disk to convert to the GPT format, and select Convert to GPT Disk.

8. **Do a practical to create new partition from existing partition.**

    Step 1: Open Disk Management:

    - Right-click on the Start button (Windows logo) located at the bottom-left corner of the screen.
    - From the context menu that appears, select "Disk Management". This will open the Disk Management window.

    Step 2: Locate the Existing Partition:

    - In the Disk Management window, you'll see a list of all your disk drives and their partitions.
    - Identify the partition that you want to shrink to create space for the new partition.

    Step 3: Shrink the Existing Partition:

    - Right-click on the existing partition you want to shrink.
    - From the context menu, select "Shrink Volume...". The Shrink window will appear, showing the maximum amount of space available to shrink.

    Step 4: Enter Shrink Amount:

- Enter the amount of space you want to shrink from the existing partition. This will become unallocated space and can be used to create the new partition.
- Make sure to leave enough space on the existing partition to hold the data you want to keep.
- Click "Shrink" to proceed.

Step 5: Unallocated Space:

- After the shrink process is complete, you will see unallocated space next to the existing partition in the Disk Management window.

Step 6: Create a New Partition:

- Right-click on the unallocated space.
- From the context menu, select "New Simple Volume...". The New Simple Volume Wizard will appear.

Step 7: Wizard Welcome:

- Click "Next" to proceed.

Step 8: Specify Volume Size:

- By default, the wizard will suggest using the maximum available space for the new partition (the unallocated space). If you want to create a smaller partition, enter the desired size in megabytes (MB) in the "Simple volume size in MB" field.
- Click "Next" to continue.

Step 9: Assign Drive Letter or Path:

- You can choose to assign a drive letter to the new partition. A drive letter helps you access the partition easily in File Explorer. The system will suggest an available drive letter, but you can change it if needed.
- Click "Next" to proceed.

Step 10: Format Partition:

- Choose a file system for the new partition. For most use cases, it's best to use "NTFS" as it supports large file sizes and offers better security features.
- Enter a "Volume label" if you want to give the new partition a specific name (optional).
- Check the "Perform a quick format" box for faster formatting (recommended for new drives).
- Click "Next" to continue.

Step 11: Completing the Wizard:

- Review the information provided on the summary page.
- Click "Finish" to create the new partition.

Step 12: Confirmation:

- You will receive a message confirming that the new partition has been created successfully.

Topic: Device Management

1. **What is Device Management?**
   - Device Management refers to the process of managing and controlling various devices, typically within a network or an organization. It involves monitoring, configuring, securing, and maintaining devices to ensure their proper functioning and optimal performance. Device Management encompasses a wide range of devices, including computers, mobile phones, tablets, printers, routers, switches, IoT (Internet of Things) devices, and more.

Module 2 {Installation and Maintenance of Hardware and Its components}

2. **What is the need of device management?**
   - Device management is an essential process that solves device growth in today's IT environment. Efficient use of resources is important for centralized management and security. Because of the large number of devices used in an organization, device management provides a central platform to monitor, configure and secure them. It enables compliance management, simplifies IT operations, and enables remote management to improve customer productivity and support. In addition, equipment management facilitates efficient equipment installation, asset tracking, and decommissioning.
   - In the context of IoT devices, it is more important to monitor, update and secure different IoT elements. In general, asset management is essential for organizations to manage productivity, optimize resources, and protect technology assets.

3. **What are the benefits of Device management?**
   - Device management is very useful for organizations that manage many IT devices today. Device management provides overall security and protection against data breaches and cyber threats by enforcing security policies, installing firewalls, and applying updates. Centralized management simplifies IT operations, reduces manual effort and increases efficiency. The ability to remotely manage equipment improves productivity and support, allowing for quick troubleshooting and configuration updates from anywhere. Meets compliance and regulatory requirements with the ability to manage business and internal policies.
   - Additionally, organizations benefit from improved asset management, inventory management and cost reduction as they gain visibility into assets and usage. Effective equipment preparation and proper end-of-life disposal for new users or employees lead to efficient operation and good practice. For organizations using the Internet of Things (IoT), device management is essential to monitor, update and secure various IoT endpoints.

4. **Where can we access device management?**
   - The accessibility of Device Management depends on the type of devices being managed and the specific management tools or platforms being used. Here are some common scenarios for accessing Device Management:
   - Windows Device Management (PCs and Laptops):
     - On Windows PCs and laptops, you can access basic device management through the built-in "Device Manager." To open it, right-click on the Start button, select "Device Manager", and it will show a list of hardware devices installed on your computer.
     - For more advanced management, such as managing policies, security, and applications on Windows devices, organizations can use tools like Microsoft Endpoint Manager (formerly known as Microsoft Intune) or System Center Configuration Manager (SCCM).
   - Mobile Device Management (Smartphones and Tablets):
     - Mobile Device Management (MDM) platforms are used to manage smartphones and tablets. For example, Android devices can be managed through Google's Android Enterprise platform, and iOS devices can be managed through Apple's Mobile Device Management (MDM) solution.
     - Organizations use MDM platforms to enforce security policies, deploy apps, and remotely manage mobile devices.
   - Network Device Management (Routers, Switches, etc.):
     - Network devices like routers, switches, and access points are typically managed through their respective web-based user interfaces or command-line interfaces (CLI). Each manufacturer provides specific instructions for accessing and managing their devices.
   - Internet of Things (IoT) Device Management:
     - IoT devices may be managed through cloud-based IoT platforms or device management services provided by IoT solution providers. These platforms allow users to monitor, update, and control IoT devices remotely.
   - Cloud Device Management Platforms:

    - Cloud-based device management platforms, like Microsoft Azure Device Management, provide a centralized solution to manage a wide range of devices across different platforms and environments.
- Enterprise Device Management Solutions:
    - In enterprise environments, there are various comprehensive solutions available, like Microsoft Endpoint Manager (which includes both Configuration Manager and Intune), VMware Workspace ONE, IBM Endpoint Manager, and others. These platforms provide a holistic approach to managing devices across different operating systems and platforms.

5. **List out the devices connected to the device management.**
    - Windows Desktop Computers: Devices running Windows operating systems, such as desktop computers and workstations, can be managed through tools like Microsoft Endpoint Manager (Intune) or System Center Configuration Manager (SCCM).

    - Windows Laptops and Notebooks: Windows-based laptops and notebooks are included in the devices that can be managed through Device Management solutions.

    - Windows Servers: Windows Server machines, used for various server roles like file server, domain controller, web server, etc., can be managed through Windows Server management tools or enterprise management solutions like SCCM.

    - Windows Tablets: Tablets running Windows, such as Microsoft Surface devices or other Windows-based tablets, can be managed through MDM platforms or specific management tools.

    - Windows Mobile Devices: Windows Mobile devices, such as smartphones running Windows Mobile OS, can be managed through MDM platforms.

- Windows Embedded Devices: Specialized devices running Windows Embedded, like point-of-sale (POS) systems or kiosks, can be managed through specific Windows Embedded management tools.

- Windows IoT Devices: Internet of Things (IoT) devices based on Windows IoT Core or Windows 10 IoT Enterprise can be managed using Windows IoT management tools or MDM platforms.

- Printers and Multifunction Devices: Network-connected printers and multifunction devices can be managed using print management tools and drivers provided by the printer manufacturer or through Windows Server print management.

- Network Devices (for Monitoring): Windows-based devices functioning as network monitoring appliances, such as Network Operations Center (NOC) devices or network analyzers, can be managed through their respective management interfaces or Windows-specific monitoring tools.

- Virtual Machines: Virtual machines running Windows as guest operating systems on hypervisors like Hyper-V can be managed using Hyper-V Manager or through Windows Admin Center.

- Network Attached Storage (NAS) Devices: Windows-compatible NAS devices can be managed through their web-based interfaces or specific management utilities provided by the NAS manufacturer.

- External Storage Devices: External hard drives and storage devices connected to Windows computers can be managed through Disk Management tools in Windows.

Module 2 {Installation and Maintenance of Hardware and Its components}

6. Do a practical to delete a driver from the device management tool

- To uninstall a driver from a Windows device using Device Manager, you can follow these steps:
- Step 1: Open Device Manager:
- Right-click on the Start button (Windows logo) and select "Device Manager" from the context menu.
- Step 2: Locate the Driver:
- In Device Manager, locate the device for which you want to remove the driver. The device categories and their respective drivers are listed in the device tree.
- Step 3: Uninstall the Driver:
- Right-click on the device with the driver you want to remove and select "Uninstall device" from the context menu.
- Step 4: Confirmation:
- You will receive a confirmation prompt asking if you want to uninstall the device driver. Select "Uninstall" to proceed.

Module 2 {Installation and Maintenance of Hardware and Its components}

Topic: Physical security

1. **Why physical security needed?**
    - In the computing environment, physical security is essential for the physical protection of equipment, sensitive data, and critical resources. Protects computer hardware from theft, tampering and unauthorized access. Body safety maintains privacy and confidentiality in accordance with regulatory requirements by restricting physical access to sensitive areas and equipment. It helps prevent insider threats and prevents attackers from controlling devices. Data centers and network equipment are protected, helping business continuity and preventing outages.
    - Physical security is especially important to prevent data breaches and data loss. Physical security creates an important layer of protection in an effective security system for computer systems and IT environments, reducing the risk of theft, unauthorized access, and body tampering.

2. **what is physical security?**
    - computer systems, physical security refers to the measures taken to protect the physical components of the IT infrastructure, such as hardware devices, servers, data centers, and networking equipment. It aims to prevent unauthorized access, theft, tampering, and damage to the physical assets that house and support the computer systems.

3. **list out the ways of physical security**

- Physical security for computer systems involves various measures to protect the physical components of the IT infrastructure. Here is a list of common ways physical security is implemented for computers:

Module 2 {Installation and Maintenance of Hardware and Its components}

- Access Control: Restricting physical access to computer rooms, data centers, and sensitive areas using access control systems like keycards, biometric scanners, or PIN codes.
- Surveillance Cameras: Installing security cameras to monitor and record activities in critical areas, providing a visual record of any unauthorized access or suspicious behavior.
- Security Guards: Employing security personnel to monitor and control access to computer facilities, providing an additional layer of protection and response to incidents.
- Locks and Enclosures: Using physical locks and secure enclosures to protect computer hardware, servers, and networking equipment from unauthorized access and tampering.
- Cable Management: Properly organizing and securing cables to prevent accidental disconnections and potential damage to hardware.
- Data Center Protection: Implementing multi-layered security measures, including access controls, video surveillance, environmental monitoring, and fire suppression systems, to safeguard data centers.
- Environmental Controls: Ensuring proper temperature and humidity levels in computer rooms and data centers to prevent hardware overheating and damage.
- Equipment Tracking: Maintaining an accurate inventory of computer hardware and using asset tracking systems to prevent theft and manage equipment effectively.
- Secure Disposal: Properly disposing of decommissioned hardware, ensuring that data is securely erased before recycling or disposal.
- Visitor Management: Implementing visitor management procedures to track and control the entry of guests into computer facilities.
- Alarms and Alerts: Installing intrusion detection systems and alarms to detect unauthorized access and trigger immediate responses.

- Physical Barriers: Using physical barriers like fences, bollards, or crash barriers to prevent unauthorized vehicle access to computer facilities.

- Backup and Disaster Recovery: Implementing robust backup and disaster recovery plans to ensure data availability and continuity of operations in case of physical incidents.

- User Education: Conducting employee training on physical security best practices to raise awareness and promote a security-conscious culture.

4. **How to protect system from malfunctioning due to electrical fluctuation?**
    - Uninterruptible Power Supply (UPS): Install a UPS between the power source and your system. A UPS provides battery backup and surge protection, ensuring continuous power supply during short power outages and protecting against voltage spikes and surges.
    - Surge Protectors: Use surge protectors for all electronic devices, including your computer and peripherals. Surge protectors absorb excess voltage and divert it away from your equipment.

    - Voltage Stabilizers: If your area experiences frequent voltage fluctuations, consider using a voltage stabilizer or a voltage regulator. These devices help maintain a stable voltage supply to your system.

    - Power Conditioners: Power conditioners filter the incoming power, removing noise and interference, which can help protect your system from voltage irregularities.

    - Isolation Transformers: Isolation transformers provide electrical isolation between the power source and your system, protecting it from ground loops and certain electrical disturbances.

    - Proper Grounding: Ensure your electrical system is correctly grounded to minimize the risk of electrical issues caused by ground faults.

- Regular Maintenance: Perform regular maintenance on your system, including cleaning the internal components and checking for loose connections, which can help prevent issues caused by dust and debris buildup.
- Backup and Surge Protection for Network Equipment: Install surge protectors and battery backups for network equipment like routers and switches to protect against network disruptions.
- Shutdown Procedures: Implement proper shutdown procedures during power outages to avoid data corruption and potential damage to the system.
- Power Quality Monitoring: Consider using power quality monitoring devices to identify electrical issues in your environment and take necessary actions to rectify them.
- Backup and Redundancy: Implement data backup and redundancy measures to protect critical data in case of system failures.

Topic: Firewall settings

1. **What is firewall?**
   - A firewall is a security device or software that creates a barrier between a trusted network (such as a private company or home network) and an untrusted external network (usually Not the Internet). Its main purpose is to control and monitor network entrances and exits according to predefined security rules.

   - The primary purpose of the firewall is to improve network security by preventing unauthorized access, protecting sensitive data and preventing malicious or malicious access or leaving the network protected. It does this by analyzing data files as they come in, determining their location, location, transactions, and other characteristics, and then enforcing pre-order rules on whether or not the data should be allowed.

2. **Why is firewall needed?**
   - Firewalls are essential for network security by acting as barriers between trusted networks and untrusted outsiders such as the Internet. It controls inputs and outputs according to defined rules, prevents unauthorized access, and protects against cyber threats such as malware and hackers. Firewalls protect sensitive data and limit the impact of security breaches by segmenting the network and controlling data flow. It provides advanced features such as next-generation firewalls, application control and deep packet inspection. They also help to comply with business rules.

   - Firewalls help identify security events and conduct investigations by logging and monitoring network connections. Firewalls, which are an important part of the security system, provide important protection against cyber risks.

3. **What are the features of firewall?**
   - Firewalls come with various features designed to provide robust network security and protect against cyber threats. The specific features may vary depending on the type of firewall and its capabilities, but here are some common features found in modern firewalls:
   - Packet Filtering: The firewall examines the headers of data packets to allow or deny traffic based on predefined rules for source and destination IP addresses, port numbers, and protocols.

- Stateful Inspection: This feature maintains a record of active connections and their states, allowing the firewall to monitor the context of traffic and make more informed decisions about allowing or blocking packets.

- Application Layer Filtering: Next-generation firewalls can analyze application-layer data and filter traffic based on specific applications and services, providing granular control over network access.

- Intrusion Detection and Prevention: Firewalls with IDS/IPS capabilities can detect and block malicious activities or suspicious patterns in network traffic.

- Virtual Private Network (VPN) Support: Firewalls can handle secure VPN connections, enabling remote access to the network while ensuring data encryption and authentication.

- Proxying: Some firewalls act as intermediaries between clients and servers, hiding internal IP addresses and enhancing security by inspecting and filtering traffic at the proxy.

- Content Filtering: Firewalls can block or allow web content based on predefined categories or keywords, helping to enforce web usage policies and prevent access to malicious or inappropriate sites.

- Bandwidth Management and Quality of Service (QoS) Control: Firewalls can prioritize certain types of traffic or limit bandwidth usage for specific applications or users.

- Logging and Reporting: Firewalls maintain detailed logs of network activity, allowing administrators to analyze and investigate security incidents and generate reports on network usage.

- Threat Intelligence Integration: Advanced firewalls can integrate with threat intelligence feeds to stay updated on the latest known threats and adapt their security policies accordingly.

- User Authentication: Firewalls can enforce user authentication before granting access to the network, adding an extra layer of security.
- High Availability and Failover: Firewalls can be configured in redundant setups to ensure continuous operation and seamless failover in case of hardware or software issues.

4. **Describe types of firewall**
    - Firewalls come in various types, each offering specific functionalities and security features to meet different network protection needs. Here are some common types of firewalls:
    - Packet Filtering Firewall: This is the most basic type of firewall that operates at the network layer (Layer 3) of the OSI model. It examines the headers of individual packets and makes decisions based on source/destination IP addresses, port numbers, and protocols. It allows or blocks packets based on predefined rules, providing a simple form of access control.
    - Stateful Inspection Firewall: This type of firewall operates at the network layer but adds the ability to maintain a state table of active connections. It keeps track of the state of network sessions and can differentiate between legitimate packets of an established connection and unauthorized attempts, thereby providing better security and context-aware filtering.
    - Proxy Firewall: Proxy firewalls operate at the application layer (Layer 7) and act as intermediaries between clients and servers. They receive requests from internal clients and forward them to external servers on behalf of the clients, and vice versa. By doing so, they hide the internal network details and add an extra layer of security by inspecting and filtering traffic at the proxy.
    - Next-Generation Firewall (NGFW): NGFWs are advanced firewalls that combine traditional firewall capabilities with additional features like intrusion prevention,

deep packet inspection, application awareness, and integration with threat intelligence feeds. They offer more granular control over network traffic and application-level security.

- Application-Aware Firewall: These firewalls identify specific applications or services used in network traffic and apply policies based on application type. This level of visibility allows administrators to control applications beyond traditional port-based filtering.
- Proxy Server Firewall: Proxy server firewalls are similar to proxy firewalls but mainly focus on handling web traffic. They can cache web content, filter URLs, and block potentially harmful web pages, providing web security and content filtering capabilities.
- Hardware Firewall: Hardware firewalls are standalone devices specifically designed for network security. They often provide high-performance packet processing and are commonly used at the network perimeter.
- Software Firewall: Software firewalls are applications or programs installed on individual devices (such as computers or servers) and provide protection for that specific device. They are commonly used on personal computers and can control traffic for that particular device.
- Cloud Firewall: Cloud firewalls are hosted in the cloud and protect cloud-based infrastructure and services. They are particularly useful for securing virtual machines, containers, and cloud resources.

5. **Do a practical to allow anydesk through firewall.**
    - Open Windows Defender Firewall Settings:
        - Press the Windows key + R on your keyboard to open the Run dialog box.
        - Type control firewall.cpl and click "OK" or press Enter. This will open the Windows Defender Firewall settings.

- Allow AnyDesk Inbound Rule:
  - In the Windows Defender Firewall window, click on "Advanced settings" on the left-hand side. This will open the Windows Defender Firewall with Advanced Security window.
  - In the left pane of the Advanced Security window, click on "Inbound Rules."
  - In the right pane, click on "New Rule..." to create a new inbound rule.
- Configure Inbound Rule:
  - In the New Inbound Rule Wizard that appears, select the "Port" option and click "Next."
  - Choose "TCP" and specify the port used by AnyDesk. By default, AnyDesk uses port 7070 for TCP. If you have changed the default port, enter the specific port used by your AnyDesk installation. Click "Next."
  - Select the "Allow the connection" option and click "Next."
  - Choose when the rule applies. For simplicity, you can select all three options: "Domain," "Private," and "Public." Click "Next."
  - Give the rule a name (e.g., "Allow AnyDesk") and add an optional description. Click "Finish" to create the rule.
- Confirm the New Rule:
  - The new inbound rule to allow AnyDesk should now be created and enabled in the list of inbound rules.
- Test AnyDesk Connection:
  - Open AnyDesk on your computer and try to connect to another device or have another device connect to your computer using AnyDesk. The rule you created should allow the connection to go through the firewall.

Module 2 {Installation and Maintenance of Hardware and Its components}

6. **do a practical to turn off the services of firewall.**
    - Open Windows Defender Firewall Settings:
    - Press the Windows key + R on your keyboard to open the Run dialog box.
    - Type control firewall.cpl and click "OK" or press Enter. This will open the Windows Defender Firewall settings.
    - Turn Off Firewall:
    - In the Windows Defender Firewall window, click on "Turn Windows Defender Firewall on or off" on the left-hand side.
    - Select the option "Turn off Windows Defender Firewall" for both "Private network settings" and "Public network settings."
    - Click "OK" to confirm and turn off the firewall.
    - Warning and Confirmation:
    - A warning message will appear, notifying you that turning off the firewall might make your computer more vulnerable to unauthorized access. If you are sure you want to proceed, click "Yes" to confirm.
    - Firewall Status:
    - Once the firewall is turned off, you will see that both the "Private network" and "Public network" sections show "Off" under the Windows Defender Firewall status.

7. **Do a practical to block ip messenger to access the network.**
    - Open Windows Defender Firewall Settings:
    - Press the Windows key + R on your keyboard to open the Run dialog box.
    - Type control firewall.cpl and click "OK" or press Enter. This will open the Windows Defender Firewall settings.
    - Create an Outbound Rule:
    - In the Windows Defender Firewall window, click on "Advanced settings" on the left-hand side. This will open the Windows Defender Firewall with Advanced Security window.

Module 2 {Installation and Maintenance of Hardware and Its components}

- In the left pane of the Advanced Security window, click on "Outbound Rules."
- In the right pane, click on "New Rule..." to create a new outbound rule.
- Configure Outbound Rule:
- In the New Outbound Rule Wizard that appears, select the "Custom" option and click "Next."
- Choose "This program path:" and browse to the location of the IP Messenger executable file (usually "ipmsg.exe"). If you're not sure of the exact path, you can find it by right-clicking the IP Messenger shortcut, selecting "Properties," and then checking the "Target" field.
- Click "Next."
- Block the Connection:
- Select the "Block the connection" option and click "Next."
- Choose When to Apply the Rule:
- Choose when the rule applies. For simplicity, you can select all three options: "Domain," "Private," and "Public." Click "Next."
- Name the Rule:
- Give the rule a name (e.g., "Block IP Messenger") and add an optional description. Click "Finish" to create the rule.
- Confirm the New Rule:
- The new outbound rule to block IP Messenger should now be created and enabled in the list of outbound rules.