TERM-1 CompTIA A+ Assignment

Module 2

[Installation and maintenance of hardware and its components]

BHARGAV DARJI

**User Management**

What is user management?

By establishing, modifying, and removing user accounts and allocating permissions, user management pertains to regulating user access to digital resources

Why is user management needed?

Efficiency: Simplifies procedures like onboarding, saving time and money.

Security: Ensures only authorized people access sensitive data, decreasing risks.   
Compliance: Assists in fulfilling legal obligations by keeping correct documentation   
Productivity: Efficient resource allocation boosts productivity

Where can we access the user management?

Open control panel

Open user accounts

Open user management

What are the features of user management?

Creating Accounts: This feature enables administrators to make user accounts.   
Permission Assignment: Provides the ability to grant users access according to their jobs.   
User Monitoring: Tools for user activity monitoring are provided by user monitoring.   
Access Control: Manages user permissions to restrict access to

digital resources.   
Password management: Enables password resets and policies.   
User authentication: Confirms the identities of users prior to allowing access.   
User Deactivation: Allows for the deactivation of user accounts as needed.

Do a practical to create a user from user management.

How to Create a User from User Management in Practice   
1. Go to the tool for managing users.   
2. Go to the "Users" or "User Administration" area.   
3. Search for a "Add New User" or comparable option.   
4. Enter the necessary data, including your role, email address, and login.   
5. Assign suitable degrees of access and permissions.   
6. To create the new user, save the changes.

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

1. Open the tool for managing users.   
2. Look through the user list to find the administrator account.   
To change or manage the administrator account, choose that option.   
3. Search for a password-changing option.   
4. After entering the new password, enter the existing one.   
5. To update the administrator's password, save the modifications.

**File and Folder Permission**

What is file folder permission?

Permissions for files and folders specify the degree of access that individuals or organizations are allowed to have when engaging with these resources on a computer system or network.

What is the use of file and folder permission?

Security: Preserves sensitive data by limiting access to files and folders to authorized users only.   
Control: Gives administrators the ability to set access restrictions and stop illegal additions or deletions.

write down the steps to give a folder read only permission.

Right-click on the folder you want to set permissions for.

Select "Properties" from the context menu.

Go to the "Security" tab.

Click on "Edit" to modify permissions.

Click "Add" to add a user or group.

Select the user or group you want to set read-only permission for.

Check the "Read" permission in the permissions list.

Click "OK" to save the changes

Write a step to give a file only admin permission.

Right-click on the file you want to set permissions for.

Select "Properties" from the context menu.

Go to the "Security" tab.

Click on "Edit" to modify permissions.

Click "Add" to add a user or group.

Select the user or group you want to set admin permission for.

Check the "Full Control" permission in the permissions list.

Click "OK" to save the changes.

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

Access the shared folder on the network.

Right-click on the folder and select "Properties."

Navigate to the "Security" tab.

Click on "Edit" to modify permissions.

Add the user or group you want to set read-only permission for.

Check the "Read" permission for that user or group.

Click "OK" to save the changes.

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

Right-click on the folder and select "Properties."

Go to the "Security" tab and click on "Advanced."

Navigate to the "Owner" tab and click "Change."

Enter the name of the new owner and click "Check Names."

Click "OK" to change the owner.

Check "Replace owner on sub containers and objects" and click "OK."

Confirm the action and wait for the process to complete.

**Install OS**

What is OS?

Software called an operating system (OS) controls computer hardware and offers shared services for software. It facilitates communication and resource management by operating as a go-between for user applications and computer hardware.

What are the types of OS?

Single users and one task at a time are supported by single-user, single-task systems (e.g., MS-DOS).   
Single-user, multitask: Allows one user to work on several tasks at once (e.g., Windows, macOS).   
Multi-user: Allows several users to access the system at once (e.g., Linux, UNIX).   
Real-time: Offers key processes (like RTOS) guaranteed response times.   
Embedded: Made for particular, low-resource devices (like iOS and Android).

Do a practical to create bootable pen drive for kali Linux

Download Kali Linux ISO.

Use a tool like Rufus or Etcher to burn the ISO onto a USB drive.

Set the USB drive as the primary boot device in BIOS/UEFI.

Boot from the USB drive to install Kali Linux

Do a practical to create a bootable pen drive for windows 7

Download Windows 7 ISO.

Use Rufus or Windows USB/DVD Download Tool to create a bootable USB drive.

Set the USB drive as the primary boot device.

Boot from the USB drive to install Windows 7

Do pen drive for creating a pen drive for mac OS Mojave with Uni beast.

Download macOS Mojave installer.

Use Disk Utility to format the USB drive.

Download Uni beast and run it.

Follow Uni beast prompts to create the bootable USB drive

Do a practical to install Kali Linux

Boot from the Kali Linux bootable USB.

Follow the installation wizard to install Kali Linux on your system.

Do a practical to install windows 10

Boot from the Windows 10 bootable USB.

Follow the on-screen instructions to install Windows 10.

Do a practical to install Mac OS X

Boot from the macOS X bootable USB.

Follow the installation wizard to install macOS X on your Mac.

**Clean Install**

What is clean install?

A clean install is the process of installing an operating system on a computer without retaining any previous data or applications. It involves wiping the hard drive and starting fresh with a clean system

What is the process for clean install?

Boot the computer from the installation media (e.g., USB drive or DVD).

Follow the on-screen prompts to access the installation options.

Choose the option to format the hard drive.

Select the newly formatted drive as the installation destination.

Follow the prompts to complete the installation, including setting up user accounts and preferences.

what are the benefits of clean install?

Improved performance: Removes unnecessary files and applications that may slow down the system.

Stability: Helps resolve software issues caused by corrupted system files or conflicts.

Security: Ensures a fresh start with no malware or unwanted programs.

Customization: Allows users to set up the system exactly as they want from the beginning.

Do a clean installation of windows XP

Boot from the Windows XP installation CD or USB.

Follow the on-screen instructions to delete existing partitions and format the hard drive.

Choose the newly formatted drive as the installation destination.

Follow the prompts to complete the installation, including entering the product key and setting up user accounts.

Do a clean installation of windows 8

Boot from the Windows 8 installation DVD or USB.

Access the installation options and choose to format the hard drive.

Select the formatted drive as the installation destination.

Follow the on-screen prompts to complete the installation, including customizing settings and creating user accounts.

Upgrade installation

What is upgrade installation?

Upgrade installation refers to the process of installing a newer version of an operating system on top of an existing older version. This process retains user data, settings, and applications from the previous installation.

What is the benefit of upgrade installation?

Preservation of data and settings: User data, settings, and installed applications are retained, reducing the need for manual backup and reinstallation.

Faster deployment: Upgrading an existing installation is often faster than performing a clean installation, as it requires less setup time.

Write down the steps of upgrade installation.

Backup: Before starting the upgrade process, it's advisable to back up important files and data to prevent any potential loss.

Download Windows 10: Download the Windows 10 installation files from Microsoft's official website or use the Windows Update tool.

Run the Installer: Double-click on the downloaded installation file to begin the upgrade process.

Follow On-Screen Prompts: The installation wizard will guide you through the upgrade process. Follow the prompts and select the option to keep your files, settings, and applications.

Do a practical to upgrade from windows 8 to windows 10

Download the Windows 10 upgrade tool from Microsoft's website.

Run the upgrade tool and follow the on-screen instructions.

Select the option to keep files, settings, and applications when prompted.

Wait for the upgrade process to complete, and follow any additional prompts as necessary.

After the upgrade is finished, configure any remaining settings and check that everything is working correctly.

**Partition & Formatting**

What is partitioning?

Partitioning is the process of dividing a hard drive into multiple sections, each treated as a separate unit. These sections are called partitions and can be used to organize data, install different operating systems, or improve performance

What is partition?

A partition is a logical division of a hard drive created during the partitioning process. Each partition behaves like a separate disk drive, with its own file system and storage space

What is format?

Formatting is the process of preparing a partition or storage device for use by creating a file system on it. It erases all existing data on the partition and sets up the necessary structures for storing files.

Do a Practical of MBR partition.

Use a disk management tool like Disk Management in Windows or Disk Utility in macOS.

Right-click on the disk you want to partition and select "Initialize Disk" if it's new.

Right-click on the unallocated space and select "New Simple Volume."

Follow the wizard to specify the partition size, assign a drive letter, and format the partition.

Do a Practical of GPT partition

Use a disk management tool like Disk Management in Windows or Disk Utility in macOS.

Right-click on the disk you want to partition and select "Convert to GPT Disk" if it's currently using the MBR partition style.

Right-click on the unallocated space and select "New Simple Volume."

Follow the wizard to specify the partition size, assign a drive letter, and format the partition.

Do a practical using cmd.

Open Command Prompt with administrator privileges.

Use the disk part command to open the disk partitioning tool.

Use commands like list disk, select disk [number], create partition primary, and format fs=NTFS quick to partition and format the disk as desired.

covert a partition to GPT by cmd.

Open Command Prompt with administrator privileges.

Use the disk part command to open the disk partitioning tool.

Use commands like list disk, select disk [number], and convert GPT to convert the selected disk to the GPT partition style.

Format a partition using cmd.

Open Command Prompt with administrator privileges.

Use the format command followed by the drive letter of the partition you want to format (e.g., format D:) and specify the desired file system (e.g., NTFS). Add /q for quick format.

**Transferring Files**

What is transferring Files?

Transferring files involves moving data from one location or system to another. This could be done between computers, devices, or storage mediums.

What are the ways of transferring files?

Files can be transferred using various methods including:

Network Transfer: Over a local network or the internet.

External Storage Devices: Such as USB flash drives, external hard drives, or memory cards.

Cloud Storage: Utilizing online storage services like Google Drive, Dropbox, or OneDrive.

Email: Sending files as attachments via email.

File Transfer Protocols: Using protocols like FTP, SFTP, or SCP.

Bluetooth: For wireless transfer between devices.

How do we transfer files from one system to another?

Using a network transfer:

Connect both systems to the same network.

Share files/folders on the source system.

Access shared files/folders from the destination system over the network.

Types of file transferring media.

Types of file transferring media

Wired: Ethernet cables, USB cables.

Wireless: Wi-Fi, Bluetooth, Infrared.

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

Ensure both systems are connected to the same network.

Share the files/folders you want to transfer on the source system.

On the destination system, open File Explorer (Windows) or Finder (macOS).

Navigate to the network location or IP address of the source system.

Access the shared files/folders and copy them to the desired location on the destination system.

DO a practical to transfer data from one hard disk to another.

Connect both hard disks to the same system.

Open File Explorer (Windows) or Finder (macOS).

Copy the files/folders from the source hard disk and paste them into the destination hard disk.

**Administrative tools**

What are administrative tools?

Administrative tools are software utilities provided by operating systems to manage various aspects of system configuration, maintenance, and troubleshooting. They are typically used by system administrators to perform tasks that require elevated privileges.

What is the use of administrative tools?

Administrative tools are used for:

Configuring system settings and preferences.

Managing user accounts and permissions.

Monitoring system performance.

Troubleshooting and diagnosing issues.

Managing hardware devices and drivers.

List out the administrative tools.

Control Panel: Centralized hub for system settings and configurations.

Computer Management: Provides access to various system tools and utilities.

Task Scheduler: Allows scheduling automated tasks and scripts.

Event Viewer: Logs and monitors system events and errors.

Device Manager: Manages hardware devices and drivers.

Disk Management: Manages disk partitions and volumes.

Performance Monitor: Monitors system performance metrics.

Services: Controls system services and their settings.

Local Security Policy: Configures security settings and policies.

Group Policy Editor: Manages group policies for system configurations.

What is disk management tools.

Disk management tools are utilities used to manage disk partitions and volumes on a computer's hard drive. They allow users to create, delete, resize, and format partitions, as well as assign drive letters and change partition properties.

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

Open Device Manager from Administrative Tools.

Locate the driver you want to delete under the appropriate category.

Right-click on the driver and select "Uninstall device."

Follow the uninstallation prompts and restart the system if required.

After restarting, open Device Manager again and select "Action" > "Scan for hardware changes" to reinstall the driver automatically.

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

Open Disk Management from Administrative Tools.

Right-click on the partition you want to delete and select "Delete Volume."

Confirm the deletion if prompted.

Right-click on the unallocated space and select "New Simple Volume."

Follow the wizard to create the partition with desired size, file system, and drive letter.

Do a practical to create user with administrative tool.

Open Computer Management from Administrative Tools.

Navigate to "Local Users and Groups" > "Users."

Right-click in the right pane and select "New User."

Enter the user details, including username and password.

Click "Create" to create the user account.

**Windows Feature**

What is windows features?

Windows Features are optional software components and tools that can be installed or removed from a Windows operating system to customize its functionality based on user preferences and requirements.

List out the windows features.

Internet Information Services (IIS).

.NET Framework

Hyper-V.

Telnet Client.

Windows Subsystem for Linux (WSL).

Internet Explorer

Windows Media Player

Windows PowerShell

Remote Server Administration Tools (RSAT

Windows Defender Features.

Windows Subsystem for Android (WSA)

Windows Subsystem for Linux 2 (WSL 2)

What is the use of IIS?

Internet Information Services (IIS) is a Windows feature that serves as a web server, allowing users to host websites and web applications on Windows-based servers. It provides support for various web technologies and protocols, including HTTP, HTTPS, FTP, SMTP, and more.

Do a practical to re install IIS with windows feature.

Open "Control Panel" > "Programs" > "Programs and Features."

Click on "Turn Windows features on or off" from the left pane.

Scroll down and locate "Internet Information Services (IIS)" in the list of features.

Check the box next to "Internet Information Services (IIS)" to enable it if it's not already enabled.

Click "OK" and follow the prompts to install IIS.

Once installation is complete, IIS will be available for use.

Do a practical to install dotnet framework 3.5 with Windows feature.

Open "Control Panel" > "Programs" > "Programs and Features."

Click on "Turn Windows features on or off" from the left pane.

Check the box next to ".NET Framework 3.5 (includes .NET 2.0 and 3.0)" in the list of features.

Click "OK" and follow the prompts to install .NET Framework 3.5.

Once installation is complete, .NET Framework 3.5 will be available for use.

Do a practical to disable internet explorer in windows feature

Open "Control Panel" > "Programs" > "Programs and Features."

Click on "Turn Windows features on or off" from the left pane.

Uncheck the box next to "Internet Explorer 11" in the list of features.

Click "OK" and follow the prompts to apply the changes.

Once disabled, Internet Explorer will no longer be available for use.

**Disk management**

What is Disk Management?

Disk Management is a built-in utility in Windows operating systems that allows users to manage their hard drives and storage devices. It enables users to view, create, delete, format, and manage disk partition111111s.

What is the use of Disk Management?

The primary use of Disk Management is to manage disk partitions on a computer's hard drive or storage device. It allows users to allocate and reallocate disk space, format disks, create new partitions, extend or shrink existing partitions, change drive letters, and set partition attributes.

What are the merits of Disk Management tool?

Some merits of the Disk Management tool include:

User-friendly interface: It provides a simple and intuitive interface for managing disk partitions.

Built-in utility: As a built-in tool in Windows, it eliminates the need for third-party partition management software.

Comprehensive features: Disk Management offers a wide range of features for managing disk partitions, making it suitable for most disk management tasks.

Compatibility: It works with various disk formats, including NTFS, FAT32, and exFAT, ensuring compatibility with different storage devices.

Where can we find the Disk Management tool?

The Disk Management tool can be found in the Windows Administrative Tools. To access it:

Open the Control Panel.

Navigate to Administrative Tools.

Click on Computer Management.

In Computer Management, select Disk Management under the Storage section.

List out the operations we can do with the Disk Management tool

Operations that can be performed with the Disk Management tool include:

Creating new partitions

Deleting existing partitions

Formatting partitions

Changing drive letters

Extending partitions

Shrinking partitions

Assigning or changing partition attributes

Practical to create a new partition with Disk Management tool:

To create a new partition with Disk Management:

Open Disk Management as described in the Intermediate level.

Right-click on the unallocated space on the disk where you want to create the new partition.

Select "New Simple Volume" from the context menu.

Follow the wizard to specify the partition size, assign a drive letter, choose a file system, and format the partition.

Practical to convert from MBR to GPT using Disk Management tool:

Converting from MBR to GPT involves data loss, so ensure you have backups. To do this:

Open Disk Management.

Right-click on the disk you want to convert.

Select "Convert to GPT Disk."

Practical to create a new partition from an existing partition:

To create a new partition from an existing partition:

Open Disk Management.

Right-click on the existing partition you want to shrink to create space for the new partition.

Select "Shrink Volume" and follow the wizard to specify the amount of space to shrink.

Once the shrink process is complete, right-click on the unallocated space and select "New Simple Volume" to create a new partition.

**Device Management**

What is Device Management?

Device Management refers to the process of managing and controlling hardware devices connected to a computer system or network. It involves tasks such as installing, configuring, monitoring, updating, and troubleshooting devices to ensure their proper functioning.

What is the need for Device Management?

The need for Device Management arises from the increasing complexity and diversity of hardware devices used in computer systems. It ensures that devices are correctly installed, configured, and maintained to optimize performance, reliability, and security. Without proper device management, systems may experience compatibility issues, performance degradation, security vulnerabilities, and difficulties in troubleshooting hardware-related problems.

What are the benefits of Device Management?

Some benefits of Device Management include:

Improved system performance and reliability: Properly managed devices contribute to the overall stability and efficiency of computer systems.

Enhanced security: Device Management helps ensure that devices are configured securely, reducing the risk of security breaches and unauthorized access.

Simplified administration: Centralized management of devices streamlines administrative tasks such as device installation, configuration, and updates.

Better resource utilization: Effective Device Management helps optimize resource allocation, ensuring that hardware devices are used efficiently.

Reduced downtime: Proactive monitoring and maintenance of devices minimize the likelihood of hardware failures and downtime.

Where can we access Device Management?

Device Management can be accessed through the Device Manager utility in the Windows operating system. To access Device Manager:

Right-click on the Start button.

Select "Device Manager" from the context menu.

List out the devices connected to Device Management.

The devices connected to Device Management (Device Manager) typically include:

Display adapters

Network adapters

Sound, video, and game controllers

Printers and scanners

Disk drives

Universal Serial Bus (USB) controllers

Human Interface Devices (HID)

Imaging devices

Ports (COM & LPT)

Other devices

Practical to add a device with Device Management tool:

To add a device using Device Manager:

Open Device Manager.

Right-click on the category under which the new device should be added.

Select "Scan for hardware changes" from the context menu. Windows will search for new devices and automatically install them if drivers are available.

Practical to delete a driver from the Device Management tool:

To delete a driver using Device Manager:

Open Device Manager.

Locate the device whose driver you want to delete.

Right-click on the device and select "Uninstall device" from the context menu.

Follow the on-screen prompts to uninstall the driver.

**Physical security**

Why is physical security needed?

Physical security is essential to protect physical assets, including people, hardware, software, networks, and data, from physical threats such as theft, vandalism, natural disasters, and unauthorized access. It ensures the safety and integrity of resources and prevents potential damage or loss.

What is physical security?

Physical security refers to the measures and mechanisms implemented to safeguard physical assets, facilities, and resources from unauthorized access, damage, or theft. It encompasses various strategies, policies, and technologies designed to protect physical infrastructure, personnel, and information assets.

List out the ways of physical security:

Physical security methods include:

Perimeter security: Fencing, gates, walls, and barriers to control access to facilities.

Access control: Locks, keys, access cards, biometric authentication, and security guards to regulate entry to buildings and restricted areas.

Surveillance: Video cameras, motion sensors, and alarms to monitor and detect unauthorized activities.

Lighting: Adequate lighting to deter intruders and enhance visibility.

Security patrols: Regular patrols by security personnel to monitor premises and respond to incidents.

Intrusion detection systems (IDS): Sensors and alarms to detect unauthorized entry or breaches.

Environmental controls: Fire suppression systems, temperature control, and humidity control to protect against environmental hazards.

Backup power: Uninterruptible Power Supply (UPS) systems and generators to maintain power during outages.

Secure storage: Safes, vaults, and secure cabinets to store valuable assets and sensitive information.

Security policies: Establishing policies and procedures for access control, visitor management, and incident response.

How to protect the system from malfunctioning due to electrical fluctuation?

To protect systems from malfunctioning due to electrical fluctuation, you can implement the following measures:

Use surge protectors: Install surge protectors or uninterruptible power supply (UPS) systems to regulate voltage and protect equipment from power surges and spikes.

Voltage regulators: Use voltage regulators to stabilize voltage levels and prevent damage caused by fluctuations.

Grounding: Ensure proper grounding of electrical systems to minimize the risk of electrical shocks and equipment damage.

Isolation transformers: Install isolation transformers to protect equipment from electrical noise and interference.

Backup power: Implement backup power solutions such as generators or battery backups to maintain power during outages and prevent data loss or system downtime.

Regular maintenance: Conduct regular inspections and maintenance of electrical systems to identify and address potential issues before they cause damage.

Training and awareness: Educate users about the risks of electrical fluctuations and the importance of following best practices to protect equipment and data

**Firewall settings**

What is a firewall?

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and protect against cyber threats.

Why is a firewall needed?

Firewalls are needed to enhance the security of computer networks by:

- Filtering incoming and outgoing traffic to prevent unauthorized access and protect against cyber attacks such as malware, viruses, and hacking attempts.

- Enforcing security policies to control network communication and ensure compliance with organizational guidelines.

- Monitoring network traffic for suspicious activities and alerting administrators to potential security breaches.

- Safeguarding sensitive data and resources from unauthorized access or disclosure.

- Providing a layer of defense against various network threats and vulnerabilities, thereby improving overall network security.

What are the features of a firewall?

The features of a firewall typically include:

- Packet filtering: Examining network packets and allowing or blocking them based on predefined rules.

- Stateful inspection: Tracking the state of active connections and allowing only legitimate traffic.

- Application layer filtering: Analyzing network traffic at the application layer to detect and block specific types of traffic or applications.

- VPN support: Facilitating secure remote access through Virtual Private Networks (VPNs) by encrypting data and authenticating users.

- Intrusion detection and prevention: Identifying and blocking suspicious or malicious network activity to prevent security breaches.

- Logging and reporting: Recording firewall activities and generating reports for analysis and auditing purposes.

- High availability and scalability: Ensuring uninterrupted network connectivity and supporting the expansion of network infrastructure as needed.

Describe types of firewall:

Types of firewalls include:

- Packet-filtering firewall: Examines packets based on predefined rules, such as source/destination IP addresses, ports, and protocols, and allows or blocks them accordingly.

- Stateful inspection firewall: Tracks the state of active connections and makes decisions based on the context of the traffic, offering better security than packet-filtering firewalls.

- Proxy firewall: Acts as an intermediary between internal and external networks, forwarding requests on behalf of clients and filtering traffic at the application layer.

- Next-generation firewall (NGFW): Combines traditional firewall functionality with Advanced features such as intrusion prevention, application awareness, and deep packet inspection to provide comprehensive security.

- Unified Threat Management (UTM) firewall: Integrates multiple security features, including firewall, antivirus, intrusion detection/prevention, content filtering, and VPN, into a single appliance or software solution.

Practical to allow AnyDesk through firewall:

To allow AnyDesk through Windows Firewall:

- Open Windows Firewall settings.

- Click on "Allow an app or feature through Windows Firewall."

- Click on "Change settings" and then "Allow another app."

- Browse and select the AnyDesk executable file (usually located in Program Files).

- Click "Add," then ensure both public and private checkboxes are checked for AnyDesk.

- Click "OK" to save the changes.

Practical to turn off the services of the firewall:

To turn off Windows Firewall:

- Open Windows Firewall settings.

- Click on "Turn Windows Defender Firewall on or off" in the left panel.

- Select "Turn off Windows Defender Firewall" for both private and public network settings.

- Click "OK" to apply the changes.

Practical to block IP Messenger from accessing the network:

To block IP Messenger through Windows Firewall:

- Open Windows Firewall settings.

- Click on "Advanced settings" in the left panel.

- In the inbound or outbound rules section, create a new rule to block a program.

- Browse and select the IP Messenger executable file.

Choose to block the connection and apply the rule to both public and private networks.

Save the rule and exit the firewall settings.