CompTIA A+

- **A+**
    - CompTIA A+ certified professionals are proven problem solvers. They support today's core technologies from security to networking to virtualization and more. CompTIA A+ is the industry standard for launching IT careers into today's digital world. *(CompTIA.org)*

- **Exam Description**

  CompTIA A+ 220-1102 covers operating systems, security, software and operational procedures.
- **Four Domains**
    - 31% Operating Systems
    - 25% Security
    - 22% Software Troubleshooting
    - 22% Operational Procedures

- **Exam Details**
    - Up to 90 questions in 90 minutes
        - Multiple-choice
        - Drag and drops
        - Performance-based/Simulations
            - Requires a 700 out of 900
            - Recommended Experience:
            - 9 to 12 months hands-on experience in the lab or field

    - Released: April 2022

- **Are You Ready?**
    - Take practice exams
    - Did you score at least 85% or higher?
    - If you need more practice, take additional practice exams to hone your skills before attempting the exam

- **What kind of jobs can I get?**

Operating System Types

Objective 1.8

- **Operating System Types**

- **Windows**

    - **Windows**
        - A graphical operating system developed and published by Microsoft
        - One of the most popular operating systems in the world
            - **windows 1.01**
                - The very first version

                    - Windows 1.01
                    - Windows 2.01
                    - Windows 3.01
                    - Windows 95
                    - Windows 98
                    - Windows 2000
                    - Windows Me
                    - Windows XP
                    - Windows Vista
                    - Windows 7
                    - Windows 8
                    - Windows 8.1
                    - Windows 10
                    - Windows 11

        - The oldest one that we're going to support is known as **windows 8.1**

        - **Windows 10** support is going to continue to operate until October of 2025

        - When you're dealing with **windows server 2016**, this'll be supported by Microsoft up until January of 2027

- **Windows server 2019** will be supported all the way up through January of 2029

- **Windows server 2022** will be supported all the way up until October of 2031

- **Windows** used to have a **90%** market share when it came to home computer operating systems

- **Linux**

  - **Linux**
    - Made by lots and lots of different companies, organizations, and individual people
    - Known as an open-source operating system
    - You have access to all the underlying code and you can make any changes you want

      - **Unix**
        - A different type of operating system
    - Some distributions use a subscription based model with they only give you access to their code

      - **Ubuntu**
        - A free software you can install on your desktop or your server

      - **Fedora, Debbie and mint, arch or cent OS**
        - Community supported distributions

  - **Two different formats for lifecycle support**

    - **Standard release model**
      - A version number associated with

    - **Rolling release model**

        - There is no long-term support version and there's no version numbers at all because you're dealing with this constant update Android

- **Android**
    - **Android operating system**
        - A specific operating system that was designed to be able to support the smartphone and tablet market
        - Originally released by the open handset Alliance, which is primarily backed and driven by Google
        - Uses a much shorter lifecycle than does desktop or server environments
        - Older devices can't necessarily support the newer operating systems
            - Android is based on Linux
            - Each manufacturer can make their own version of Android
- **Chrome**
    - **Chrome OS**
        - Proprietary operating system developed by Google
        - Developed to run specifically on laptops and desktop hardware created by Google
        - This hardware was designed to keep costs very low
        - Chrome OS devices have built-in virus protection and firewalls
        - Chrome OS is extremely safe and secure
        - Automatic updates

        1. Proprietary operating system created by Google
        2. Designed to run on specific hardware
        3. Stripped down operating system
        4. Primarily uses web applications and supports Android apps

- **macOS**
    - **macOS**
        - Operating system used on Mac computers, built by Apple
            - iMac
            - Mac desktop
            - MacBook

        - macOS was previously called OSX

    - Desktop operating system that only operates on Apple devices

- **iOS and iPadOS**
    - **iOS and iPad iOS**
        - Developed by apple for their smartphones and tablets
            - **iOS operating system**
                - Developed as a closed source operating system
                - Have a very high percentage of total market share for mobile devices
            - **iPad iOS**
                - Developed as a fork of the mean iOS branch

- **Filesystem Types**
    - Organize data and information on a hard drive, solid state drive, or other storage device
    - File systems have to be created before you can install an operating system or storage device like a hard disk drive
    - Windows operating systems use NTFS, FAT32, or exFAT
    - Linux will use ext3, ext4, or exFAT for your filesystem
    - macOS uses the Apple file system known as APFS

1. **New technology filesystem, also known as NFTS**

    - Linux and macOS cannot read NTFS by default, you would have to use third party utilities to read and write NTFS

- NTFS is considered a 64-bit filesystem that allows for large volumes and very large file sizes
- NTFS has a lot of key features such as journaling, snapshots, security, POSIX compliance, indexing, and dynamic discsJournaling allows forfaster recovery from power outages and crashes
- Snapshots allow you to make a read-only copy of a file, even if it is already locked
- NTFS has a higher security level and allows you access to audit trails, quota management, and an encrypting filesystem
- Each file can be protected against unauthorized access
- POSIX supports Unix and Linux compatibility between NTFS and a Unix or Linux filesystem
- Windows and NTFS are not case sensitive
- JASON and jason would be the same file to NTFS
- Windows doesn't rely on case sensitivity when reading NTFS but Linux and Unix will
- Indexing is a catalog of file and folder locations to help speed up searches
- Dynamic discs can combine physical discs into one larger disc that is understood by the operating system

2. File allocation table 32, also known as FAT32

- You can only have a total drive size of up to 2 TB and the maximum file size is 4 GB
- FAT is limited due to it being a 32-bit allocation table, where the maximum file size is around 4.2 billion bytes or 4 GB
- FAT is supported by Windows, Unix, Linux, and macOS
- FAT32 is usually used on removable drives like external hard drives or USB flash drives

3. Extended file type system, also known as ext3 and ext4

- These are supported by Linux and Unix systems, but not by Windows or macOS by default
- ext3 has a maximum volume size of 32 TB and maximum file size of 2 TB
- ext4 has a maximum volume size of 1 EB and maximum file size of 16 TB

4. **Apple file system or APFS**

    - APFS has been the default file system of macOS since 2018
    - APFS is considered a journaled filesystem, and provides same journaling benefits as in NTFS
    - APFS has a higher level of performance when dealing with SSD than a traditional HDD

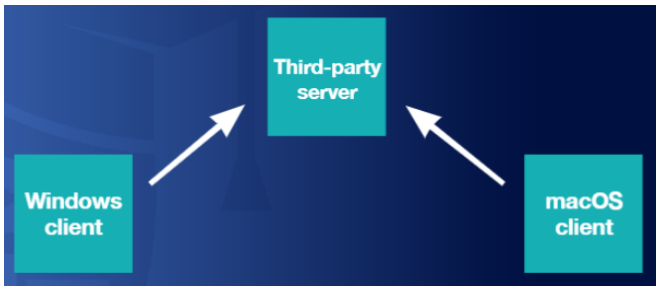
5. **Extensible file allocation table, also known as exFAT**

    - exFAT supports large volumes of up to 128 PB in size and file sizes of up to 16 EB
    - exFAT is considered cross platform capable and can be used on Windows, Unix, Linux, or macOS

        - Windows
            - NTFS
        - Linux
            - ext4
        - macOS
            - APFS

- **Compatibility Concerns**

    - Every software application is coded to run on a specific operating system
    - Devices that are running different operating systems can communicate on the same data network
    - Most computers can talk the same language using TCP/IP



- The ability of end users to use different operating systems
- A traditional user may be used to work with just one or two operating systems
- Train users to understand how to use your operating system

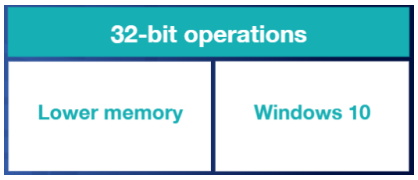
Windows Version

Objective 1.1 and 1.7

- **OBJ 1.1:** Identify basic features of Microsoft Windows editions
- **OBJ 1.7:** Given a scenario, apply application installation and configuration concepts

- **Windows Versions**
    - **64-bit vs 32-bit Versions**
        - **Windows 11**
            - **64-bit version**
        - **Windows 10**
            - **32-bit or 64-bit version**
        - **32-bit Version**
            - **32-bit programs**
        - **64-bit Version**
            - **32-bit or 64-bit programs**

        - **Each piece of hardware will be 32-bit or 64-bit based on the processor**
        - **Choose the version of the operating system that will align with your processor**
        - **32-bit version of Windows has lower memory requirements**
        - **Have a minimum of 4 GB of RAM to run Windows**
        - **Check if your processor can support 32-bit or 64-bit operations**



- **Windows Home**
  - **Windows Home**
    - Basic edition of the Windows operating system
    - Not designed to be used in a business environment
    - Upgrade to Windows Pro or Windows Enterprise for additional business features
    - Storage device encryption
    - Support for WIP
    - Business management features
    - Windows 11 Home edition is only in 64-bit version
    - Windows Home edition support multi-core processors
    - A multi-core processor has 2, 4, 6, 8, or even up to 64 cores
    - It does support hyper-threading
    - 64-bit can support large amounts of memory

      - **OEM**
        - The OEM license is used by the original manufacturers
      - **Retail**

    - You can move up from Windows 10 to 11 using the same edition

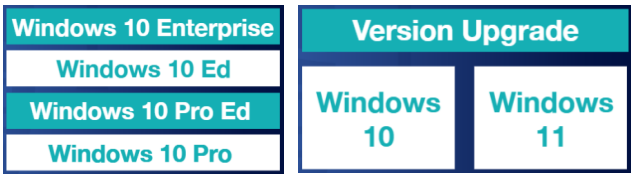
- **Windows Pro**
  - **Windows Pro**
    - Windows operating system that focuses on business use
    - Windows Pro can be used in a domain environment
  - **BitLocker**
    - Full disk drive encryption schema that is provided inside of Windows Pro and Windows Enterprise editions
  - **Group Policy Editor**
    - Creates and applies operating system and software application settings across all the users
    - **The group policy editor is not available within the Home edition**
  - **Remote Desktop Protocol (RDP)**

        - Remotely connect to your Windows Pro machine from anywhere in the world
    - **Windows Information Protection (WIP)**
        - Helps identify and protect against potential data leakage or data exfiltration

    - **OEM** is the original equipment manufacturer license
    - **Retail** license allows you to buy one license for one particular piece of hardware
    - **Windows Pro** is designed to be used by small and medium-sized businesses
    - **Windows Pro for Workstations** is an improved version of the Windows Pro edition
        - It provides support for additional hardware
        - Windows Pro for Workstations can support up to four-way multiprocessing

- **Windows Enterprise and Education**
    - **Windows Enterprise** is a fully featured version of Windows
    - Enterprise edition can only use **volume licensing**
    - Application virtualization under a tool known as **App-V**
        - **App-V** protects the rest of the operating system from any kind of malware
    - **UE-V** is used to capture, save, and manage Windows 10 operating system
    - Allows multiple people to use the same machine but separates all their settings
    - Direct access is used to allow connectivity for remote users without the use of a VPN
    - Credential guard allows for virtualization-based security and only grants access to privileged systems
    - **Windows To Go** creates an image version of a corporate Windows 10 environment that can be run on a user's personal computer
    - Windows Enterprise edition has a limit of **6 TB** of memory
    - Windows Enterprise supports up to **4 physical processors**
    - Both are only going to be using a volume licensing
    - Windows Education and Windows Pro Education are the same as Windows Enterprise and Windows Pro editions

- **Upgrading Windows**
  - In-place upgrade means the setup program for the new version will be launched within the current operating system
  - Verify the system meets the minimum requirements for the new operating system
  - Download the Windows 11 installation media and place it on a USB drive
  - Launch the setup program from that USB within Windows 10 and then perform a full upgrade
  - Data-only upgrade keeps all personal files, but not any applications or settings
  - Clean install will delete all personal settings, files, and folders



Windows Installation

Objective 1.9

- **OBJ 1.9:** Given a scenario, perform OS installations and upgrades in a diverse OS environment

- **Windows Installation**
  - **Installation Types**
    - **Clean installation**
      - When an operating system is installed onto a new computer
      - In this type of installation, all data, user settings, and programs will be deleted
    - **In-place upgrade**
      - Changes the current version of the operating system into a newer version
      - Clean installation does not bring over any of your data, applications, or user settings
    - **Attended installation**
      - Requires a system administrator to sit in front of the computer during the installation process
    - **Unattended installation**
      - Used by the system administrator when multiple machines needs the installation
    - **Image deployment**
      - Copies an image file of a hard drive onto the new system
      - This image can be stored on a DVD or USB media
    - **Remote network installation**
      - The image to be used will be sent over the network

  - **Upgrade Considerations**
    - Look at the system requirements
      - Hardware compatibility
      - Application support
      - Backup files and user preferences
      - Third-party drivers

- Make sure the processor, chipset, and memory can support the new OS
  - In Windows 11, 64-bit edition, the hardware requirements are doubled from Windows 10
  - x86 or x64
- Verify the new operating system has support for the peripherals that you need
- Run the PC Health Check app before performing an in-place upgrade

1. Remain with the older operating system
2. Replace the peripheral to something supported by the new operating system

- **Run a backup first**
- Obtain any third-party drivers that you may need
- Make sure to obtain the right third-party drivers

- **Product Lifecycle**
  - **Mainstream support** is for every version of the operating system for a minimum of five years
  - **Extended support** is the additional period for some of the products that can extend another three to five years
  - **End of life means that product is no longer supported**

  - **Legacy Operating System**
    - A product that is no longer supported and considered abandoned or orphaned

    - Windows 10 and 11 get mainstream support for at least five years
    - Feature updates usually occur every 6 to 12 months
    - Feature updates are not going to change the requirements for that operating system
    - Every product, including operating systems, has a defined life cycle
    - Windows will provide at least five years of mainstream support
    - Once that operating system reaches end of life, there will be no more security patches

- **Boot Methods**
  - Optical media
  - USB drives
  - SSDs
  - Flash drives
  - External/Hot swappable
  - Network boot
  - Internet boot
  - Internal partitions

  - **Optical Media is any type of disk that uses laser or light to read and write data**
    - Many newer computers don't have optical drives, so using optical media is less common

  - **USB connected drives can be many types of drives**
    - USB connected drives can be CDs, DVDs, Blu-ray, solid state drives, flash drives, or hot swappable hard drives
    - To make sure your USB device is bootable, you need a media creation tool to create the installation media

  - **Network boot devices take advantage of something inside your BIOS or UEFI**
    - This allows you to read boot media over the network
    - Windows generally use the PXE environment to boot up the setup program to install Windows
    - If you rely on network boot, you need to ensure you have DHCP enabled to get an IP address assigned to your server

  - **Internet-based boot method allows the system to boot up its system over the Internet**
    - The computer will boot up a minimalist version of an operating system that is used to download the setup files

  - **Internal hard disk drive partition is a hidden device partition created by your manufacturer**

- If your purchased Windows 11 laptop gets corrupted, do a clean install by booting from the internal hidden partition

- Configure your BIOS or UEFI to have the proper boot order
- If booting from a USB drive, you need to place it above the hard disk in the boot order

- **Partitioning Storage Devices**
  - Once you boot up the setup program, ensure the storage devices are properly partitioned

    - **Hard Disk Drives**
      - Also known as HDDs
    - **Solid State Devices**
      - Also known as SSDs

  - Both HDDs and SSDs require partitioning and formatting before using them to store an operating system
  - By default, at least one partition on a fixed disk is needed before you can perform a high-level disk format for your file system

  - There are two styles of partitioning
    - **Master Boot Record (MBR)**
      - The traditional style of doing partitions on a particular fixed storage device
      - The first 512 byte sector on a disk contains the MBR, which has the info about the physical disk on it
      - Inside the MBR, you will be able to carve up the physical disk into four primary partitions
      - Any of these partitions can be marked as active, which signals the system to look for the operating system to boot up
      - When booting up initially, it will read the first 512 byte sector from the hard disk which will have the MBR on it
      - That will be partition zero, but the boot loader will ask which device would you like to boot up, Windows or Linux

- You can also use partitioning to make multiple areas of storage instead of just having one single drive
- One drive for the operating system and one for the data in two different partitions
- MBR has limitations, such as only able to run four primary partitions and only supports a disk size of 2 TB

- **GUID Partition Table (GPT)**
  - Provides a more up-to-date schema to address MBR limitations
  - Windows can support up to 128 partitions with GPT
  - GUID partition table can support drives over 2 TB,which is good for its 128 partitions
  - The system must support UEFI as its boot method to be able to use GPT
  - Most systems use UEFI for its 64-bit processors since BIOS only supports 32-bit processors
  - Windows supports NTFS, macOS supports APFS, and Linux supports either ext3 or ext4 (depending on the distribution used)
  - Choose the file system that works best with your operating system, like Windows with NTFS or macOS with APFS
  - This may be a good reason to have two partitions, if you are using macOS and Windows, or Linux and Windows
  - It is important to understand what limitations you have when choosing file systems

- **Recovery and Reset**
  - Recovery and Reset is used when your Windows has been corrupted with malware, or there is a system issue
    - **Recovery and reset** is helpful when there is some malware or you are going to sell your machine
    - Normally, a message will pop up with the required key, such as **F11 or CTRL + F11**
    - A text or graphics display will walk you through how to do a full recovery or repair

- With a **full recovery**, all files will be lost, unless you have them saved on a backup drive to bring back into the system
- The **factory recovery** only works if you have the original hard drive in the system
    - A disadvantage of a full recovery is you lose everything on the system
    - This can be an advantage when you're going to sell the machine though
        - Example, if you bought a laptop with Windows 8.1, and upgraded to Windows 10 before a full recovery, it will go back to Windows 8.1

- Under **refresh or repair mode**, your machine will reset and try to repair itself without doing a full recovery
- To **repair** instead of factory reset, you go to the same menu and just choose the repair/reset options
- With Windows, most hardware will include a **recovery partition** that you can boot up from

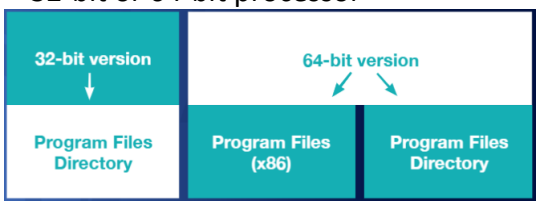
- **Using a Recovery Partition**

Application Configuration

Objective 1.7

- **OBJ 1.7:** Given a scenario, apply application installation and configuration concepts

- **Application Configuration**
  - **Application Requirements**
    - Every application is going to have different processing requirements
      - 32-bit or 64-bit processor



      - Processor speed and cores available
      - Memory available for that application
      - Have more than the minimum required for best performance
      - Amount of storage space available

    - **Graphic requirements**
      - Dedicated graphics card or integrated graphics card
      - VRAM available

    - Graphics cards can be embedded into the motherboard or into the processor
    - Integrated GPU can handle most day-to-day applications in an office environment
    - Dedicated graphics card is for more high-end graphics and intense applications
      - 8 to 16 gigabytes of RAM available
      - External Hardware Token
      - Digital key that can unlock an application

  - **Distribution Methods**
    - Download from the app store
    - Purchase on physical media

- Download from the Internet

- These app stores will handle all the installation process for you
- These app stores take precautions to ensure that the software is of good quality
- Not all applications can be found inside the app store
- Physical copy of the software
- CD or DVD as a distribution method is known as Physical Media
- Physical media is not the most convenient way to install sotware

1. Requires to be picked up at some retail location
2. Software is not going to be the most up to date version

- Downloadable software directly from the manufacturer

- **ISO File**
    - Digital file format used to replicate a physical CD, DVD or Blu-ray Disc
        - **Windows**
            - Right click and select "Mount"
        - **Mac**
            - Use the Disk Utility

- **Business Impacts**
    - **Licensing**
    - **Support**
    - **Training**

    - **Single user license** means you can install one copy of that application on one system
        - Some applications will support multiple copies being installed on multiple systems for use by a single user
        - Never install an application on a system without a valid license
        - Understand the terms of a software license
    - **Provide support for that application**
        - **Manufacturer's Support**
            - Extended support agreement between the company and the manufacturer

- **How are you going to be training your users?**
  - Third-party manufacturer who made that software to train your users
  - Make sure to budget for that in terms of time and costs

- **Operational Impacts**
  - **Single component**
  - **Larger network**
  - **Larger enterprise system**

  - Send a technician to every machine to manually update it
  - Use automation to push that software over the network to all the clients

  - The user doesn't have to be logged into the system and the administrator doesn't have to go to that system

  - What clients are on the network
  - What servers are being used
  - Windows Deployment Service
  - Microsoft Deployment Toolkit

  - Apple Business Manager
  - Private repositories

- **Device Impacts**
  - **Processing power**
  - **Memory**
  - **Storage**

  - Some applications are going to slow down the system
  - Some applications are going to be memory intensive
  - Some applications are going to take a lot of storage space
  - Test the applications on a sample system

- **Network Impacts**
  - Some applications will rely heavily on the network
  - What network impacts would there be when installing certain tools

- Backup tools will steal a lot of the network's performance by overwhelming the connection
- Consider the actual installation of the application itself

- Break down the deployment into small groups
- Use times that are the least impactful for the users

Windows Networking

Objective 1.6

- **OBJ 1.6:** Given a scenario, configure Microsoft Windows networking features on a client/desktop

- **Windows Networking**
  - **Wired Connections**
    - **Wired connections** can come in the form of copper or fiber
    - **Fiber** connects directly into a network interface card
    - **Copper connection** uses a Cat 5, Cat 6, Cat 7, or Cat 8 connector using a UTP or STP cable

  - **WWAN Connections**
    - Connects to a wide area network over a wireless connection, and is most commonly seen with cellular modems or cellular hotspots
    - Be aware of how much data your plan has as service providers can have different limits
    - Some are done on a monthly basis, some are unlimited, and some are allocated over a given time period
    - Additionally, some plans will cap your transferable data and cut off your connection

    - **Overage Fees**
      - Some cellphone carriers charge $10 to $20 per GB beyond the data cap
    - **Throttling**
      - With throttling, you will still be able to use data, but at a much lower speed
    - **Unlimited**
      - Unlimited plans have no data cap, you can use as much as you want and at the highest levels of speed

  - **VPN Connections**
    - Used to connect anyone or any resources from one private network to another over a public network

- VPNs will allow you to connect back to your office and access your data in a secure manner

- **Network Client Configuration**
  - Anytime you connect to a network, whether wired or wireless, you need to make sure the device has four basic items
    - IP address
    - Subnet mask
    - Gateway
    - DNS server

Windows Control Panel

Objective 1.4

- **OBJ 1.4:** Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility

- **Windows Control Panel**
  - **Devices and Printers**
    - Provide you with a wizard and an interface to add devices manually and create shortcuts to the different configuration pages
    - There is a lot you can do with devices, which are things like mice, keyboards, webcams, etc.
    - This area of the control panel is where you can edit the functionality of mice, keyboards, monitors, etc.

  - **Internet Options**
    - An older legacy applet that can be used to configure the old legacy web browser Internet Explorer
    - Most places don't use Internet Explorer anymore, and use things like Microsoft Edge or Google Chrome, but some places still rely on Internet Explorer
    - When using the Internet Options, you are only configuring Internet Explorer

  - **Network and Sharing Center**
    - Status of any network adapter
    - Change settings
    - Configure media streaming

  - **Windows Defender Firewall**
    - Software-based/ Host-based Firewall
    - Determines which processes, protocols, and hosts are allowed to communicate over a network

      - Public Networks
        - Airports, hotels, etc.
      - Private Networks

- Business/home networks

- **Mail**
  - Configures Microsoft Outlook, but not other mail apps like Thunderbird or web-based mail like Gmail
  - Mail only works with Microsoft Outlook and allows for the configuration of email clients under different profiles

- **Sound**
  - Used to select your input such as your microphone or your output

- **System**
  - The exam objectives list the system as part of the control panel

- **Device Manager**
  - Allows for the viewing and editing of properties of the different pieces of hardware installed on a system
  - Device Manager is a separate program that lets you view and edit the properties of hardware
  - installed on a given system

- **Administrative Tools**
  - Different tools that can be used for more in depth configuration or troubleshooting

- **Indexing Options**
  - Configures how the search capability inside File Explorer is going to work
  - Indexing options configure how things will be indexed to increase search speeds

- **Power Options**
  - Allows to control the power management on a Windows system
    - Turn off or reduce the power
    - Use less energy

  - Advanced Configuration and Power Interface

- Industry standard for power management services designed to allow software and hardware to have compatibility

- S3
  - Most of the devices are going to lose power
- S4
  - Power will be maintained to the memory
- S5
  - This applet conserves energy or maximizes performance by choosing how the computer will manage power

S0	Power ON
S1	Standby
S2	Standby
S3	Standby
S4	Hibernation
S5	Power OFF

- **Ease of Access**
  - Gives access to all sorts of settings to configure the input and output options
  - Accessibility area

Windows Settings

Objective 1.5

- **OBJ 1.5:** Given a scenario, use the appropriate Windows settings

- **Windows Settings**
    - **Windows Settings**
        - **Windows Setting**
            - Used to administer and configure the Windows 10 and 11 operating systems
            - The Windows Setting application provides easy to use applets

Windows Tools

Objective 1.3

- **OBJ 1.3:** Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS)

- **Windows tools**

    - **Task Manager**
        - Monitors the computer's key resources, like processing, memory, storage, and network capacity
        - Task Manager is used to monitor the computer's key resources, things like processing, memory, storage and network capacity

    - **Device Manager**
        - A tool used for investigating and troubleshooting system hardware, components, and peripherals
        - Device manager is used to investigate and troubleshoot all sorts of system hardware, components, and peripherals

    - **Disk Management Console**
        - Provides a summary of all the fixed and removable disks on the system, including HDDs, SSDs, and optical drives
        - This is a tool that formats disk drives, creates partitions, shrinks volumes, creates RAIDs, and more

    - **Disk Maintenance Tools**
        - **Fragmentation**
        - **Capacity**
        - **Damage**

        - Disk fragmentation only truly affects hard drives, and this is because of the way data is written
        - Capacity is the cap of data you are able to have on your disk
        - Damage can happen when you cut off power to a disk being read or written, or if you drop the device

- Disk defragmenter
- Disk cleanup utility

- **Task Scheduler**
  - Used to run commands and scripts automatically in the background at any given interval

- **Event Viewer**
  - Allows you to go through log files and see what has happened on a given Windows system

    - Information
    - Warning
    - Verbose
    - Error
    - Critical

- **Performance Monitor**
  - Provide real-time information about system resources by keeping track of what things are happening in the operating system
  - Monitor performance over time and find the issue by looking at some key counters

- **Local Users and Groups**
  - Provides the ability to create, modify, disable, and delete user accounts along with the setting or resetting of passwords

- **Group Policy Editor**
  - Provides a way of configuring different Windows settings across all machines in the network

- **Certificate Manager**
  - Looks at the different digital certificates installed on the system and provides a way of requesting and importing new certificates
  - Certificate manager provides the ability to manage all digital certificates on the system

- **System Information**
  - Produces a comprehensive report on the different pieces of hardware and software inside a Windows system

- **Resource Monitor**
  - Gives a better version of the type of monitoring provided by the task manager
  - Resource Monitor is essentially an enhanced or better version of the snapshot and overview monitoring inside the Task Manager

- **System Configuration**
  - Used to modify various settings and files that affect the way a computer boots up and loads Windows

- **Registry Editor**
  - **Windows Registry**
    - A database which has all the different settings and configurations across the entire operating system

- **Microsoft Management Console**
  - A container for plugins or snap-ins that can be used to create custom admin tools to configure a system

Windows Command

Objective 1.2

- **OBJ 1.2:** Given a scenario, use the appropriate Microsoft command-line tool

- **Windows Command**
  - **Windows Command Line Tools**
  -
  - **Using the GUI**
    - Command Line
    - Graphical User Interface

  - **Using the Command Prompt**
    - **Command Prompt**
      - Allows to run a series of different text-based commands and be able to run different tools or utilities
      - An administrative user can do a lot of things that may not be available to a standard user
        - Create a new user account
        - Access files or folders
      - Use the regular command prompt first

  - **Copying Commands**
    - Copying commands
    - Movement commands

  - **Shutdown**
    - This command can run at various times when the user is not at the computer

  - **System File Checker**
    - Provides a manual interface for verifying system files and restoring them from the cache

  - **Network Troubleshooting Commands**
    - **IPConfig**
      - IPConfig provides information about own network connection

- **Ping**
  - Ping verifies there is good connectivity between the client and the remote destination
- **Tracert**
  - Tracert shows each and every stop along the way by using multiple pings all the way out and all the way back
- **Path ping**
  - Path ping gives a more accurate round-trip time being calculated

- **Name Resolution Commands**
  - Host name
  - NS Lookup

- **The netstat Command**
  - Netstat is really helpful for malware removal or threat hunting against bad actors

Windows Share

Objective 1.2, 1.6 and 2.5

- **OBJ 1.2:** Given a scenario, use the appropriate Microsoft command-line tool
- **OBJ 1.6:** Given a scenario, configure Microsoft Windows networking features on a client/desktop
- **OBJ 2.5:** Given a scenario, manage and configure basic security settings in the Microsoft Windows OS

- **Windows Shares**
    - **Domain-Based**
        - Used for larger environments
    - **Workgroup-Based**
        - Used in a single computer environment

- **Workgroups and Domains**
    - **Workgroups and Domains**
        - Represent the two different methods for organizing workstations inside of a Windows-based computer network
        - The main difference between the two is how workstations and resources on the network are going to be managed
            - **Workgroup**
                - Decentralized model
            - **Domain**
                - Centralized architecture
        - When dealing with a workgroup, you're dealing with a decentralized model of administration, so there is no main computer in control
        - Workgroups are better used with smaller sized networks, all on the same network of less than about 15 to 20 computers

  - Domains are used for large scale networks, one or more computers acting as a server, which makes it easier to automatically connect to the network from anywhere

  - Domains can support hundreds of thousands of computers on a single domain

- **Printer Sharing**
  - Sharing a printer over a network is easier in a small office environment

macOS

Objective 1.10

- **OBJ 1.10:** Identify common features and tools of the macOS/desktop OS

- **macOS**
  - macOS generally has same features and functionality like Windows

    - **Time Machine**
      - A backup feature in macOS
    - **Finder**
      - macOS file management app (file explorer)
    - **Dock**
      - Used for managing applications from the desktop (taskbar)
    - **Spotlight**
      - Search function
    - **.pkg (Package)**
      - macOS installer that supports complex setup tasks using a setup wizard
    - **.dmg (Disc Image)**
      - macOS installer for copying self-contained apps to an app folder

- **Mission Control**
  - Enables the user to set up multiple virtual desktops with different sets of applications and backgrounds

- **File Vault**
  - Disk encryption tool that encrypts the data that's stored on the hard drive or solid-state device

- **Remote Disc**
  - Utility that allows to access an optical disc drive over the network
  - Most Mac computers don't have an internal optical drive
  - One requires CD or DVD drive installed on the network

- **Keychain**
  - Application designed to help manage passwords for all the different accounts

- **iCloud and Apple ID**
  - Apple's online storage solution for all its users

- **System Preferences**
  - Provides a centralized and standard location for mail, contacts, calendar, photos, notes, reminders, and more
  - The free account gives 5GB worth of storage

    - **Apple ID**
      - Account with Apple used across the entire Apple ecosystem

- **Managing macOS Applications**
  - **Mac App Store**
    - Central area that Apple and developers can use to distribute free and paid apps

- **Best Practices for macOS**
  - **Antivirus**
  - **Backups**
  - **Updates**
  - **Force quit apps**

  - Always have antivirus or antimalware on the system
  - Mac doesn't run the same types of software as Windows
  - There is no built in antivirus software for Mac system

  - **Apple Business Manager**
    - Supervises the use of macOS systems, restricts which apps can be installed, locates any systems, and ensures they're up to date with the latest security patches

Linux

Objective 1.11

- **OBJ 1.11:** Identify common features and tools of the Linux client/desktop OS

- **Linux**
  - **ls**
    - Used for listing file system objects
  - **pwd**
    - Used to print the current directory
  - **cd**
    - Used to change the directories
  - **mv**
    - Used to move files from one location to another
  - **cp**
    - Used to copy files from one location to another
  - **rm**
    - Used to delete files
  - The mv, cp, and rm commands are used in both files and directories in Linux
  - **df**
    - Used to display the amount of free disk space
  - **du**
    - Used to estimate the file space usage
  - **nano**
    - Easy to use command line text editor
  - **vi**
    - Old command that supports modal editing
  - **vim**
    - Supports normal, visual, insert, and command line mode
  - **pico**
    - Text editor that provides less features and less complexity
  - **cat**
    - Used to create, view, or concatenate files
  - **find**
    - Used to search the file system or directory

- **grep**
  - Used to search for characters within the specified file using regular expressions
- **su**
  - Used to switch users
- **sudo**
  - Used to switch to the root user
- **usermod**
  - Used to modify the user's account
- **userdel**
  - Used to delete a user's account
- **passwd**
  - Used to change or reset the password of the user's account
- **groupadd**
  - Used to add a new group
- **groupmod**
  - Used to modify a group
- **groupdel**
  - Used to delete a group
- **chmod**
  - Used to change the access permissions
- **chown**
  - Used to change the owner
- **apt-get**
  - Used to install and remove software on Debian
- **yum**
  - Used to install and remove software on Red Hat
- **dnf**
  - Updated version of yum command and used to install and remove software on Red Hat
- **rpm**
  - Low-level tool that is used to install and remove software on Red Hat
- **ps**
  - Used to display a list of currently running processes
- **top**
  - Task manager that is used to display information about CPU and memory
- **ip**

        - Used for configuring network interfaces
    - **ping**
        - Used to test a host's reachability on an IP-based network
    - **traceroute**
        - Used to display the route and transmit time across an IP-based network
    - **dig**
        - Used to query the DNS to get information about the different DNS records
    - **man**
        - Used for accessing and searching online reference manuals
    - **--help**
        - Written after the name of a command to give information on how to use a specific command
    - **Samba**
        - Cross-platform file sharing protocol that supports the SMB

- **Linux Navigation**
    - When it comes to Linux terminal environment, can use the LS, PWD, and CD commands

- **Disk Usage Commands**
    - **DF**
    - **DU**

    - **Free space**
    - **Filesystem**
    - **Total size**
    - **Space used**
    - **% used**
    - **Mount point**

    - The DU command shows the disk usage and how the device is used

- **Text Manipulation**
    - Nano and Pico are both considered visual editors and are easy for anyone to use
    - VI and VIM are more difficult to use, but they have a lot more capabilities if you are able to use them

- The cat command is used for concatenating or displaying the contents of a file to the screen

- **Search Commands**
  - **Find**
    - Search for a file
  - **Grep**
    - Search for content within a file

- **Resource Management Commands**
  - PS and top are the two commands you should be aware of for resource management

- **Best Practices for Linux**
  - **Update and patches**
  - **Antivirus**
  - **Backups**
  - **Samba**

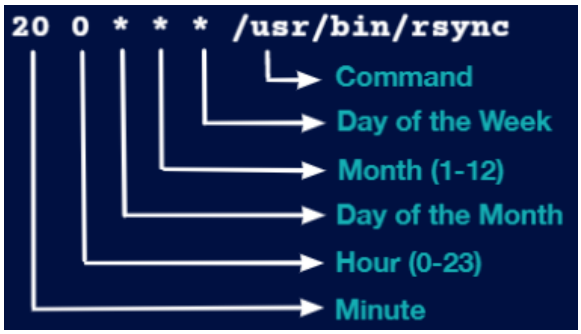
  - **Debian**
    - apt-get
  - **Red Hat**
    - rpm, yum, dnf

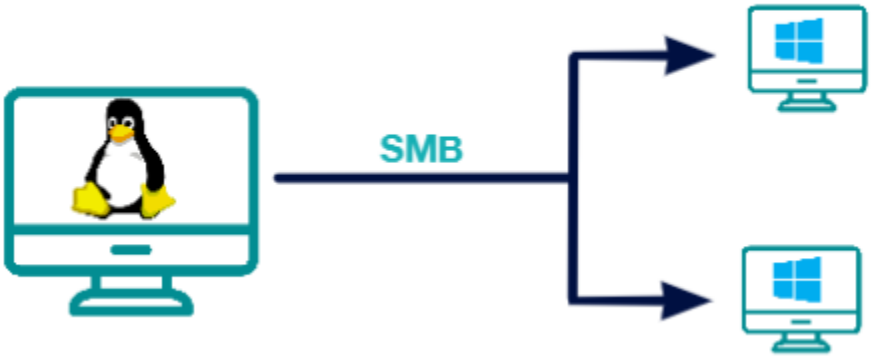
  - Linux and Windows malware do not affect each other's systems
  - Linux is more secure, but it is not risk-free

  - **Clam AntiVirus**
  - **Snort**
  - **IDS/IPS**

  - Use a Task Scheduler to run a backup
  - Cron is the Linux scheduling service

  - **tar**
  - **gzip**





- Install samba on a Linux device to communicate with a Windows host or server

Threats and Vulnerabilities

Objective 2.4

- **OBJ 2.4:** Explain common social-engineering attacks, threats, and vulnerabilities

- **Threats and Vulnerabilities**
- **CIA Triad**
- **Vulnerabilities**
- **Zero-day Attack**
- **DoS and DDoS**
- **Spoofing**
- **On-path Attack**
- **SQL Injection**
- **Cross-site Scripting**
- **Password Cracking**
- **Insider Threat**

Malware

Objective 2.3

- **OBJ 2.3:** Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods

- **Malware**
  - Software that is designed to infiltrate and damage a system
    - Viruses, Worms, and Trojans

- **Viruses, Worms, and Trojans**
  - **Viruses require user action in order to reproduce and spread**
  - **Boot sector**
    - Viruses that are stored in the first sector of a hard drive and are loaded into memory upon boot
  - **Macro**
    - Virus embedded into a document and is executed when the document is opened by the user
  - **Program**
    - Program viruses seek out executables or application files to infect
  - **Multipartite**
    - Virus that combines boot and program viruses to first attach itself to the boot sector and system files before attacking other files on the computer
  - **Encryption**
    - This virus is gonna use a cipher to encrypt the contents of itself to avoid detection by any antivirus software
  - **Polymorphic**
    - Advanced version of an encrypted virus that change its code each time it's executed by altering the decryption module in order for it to evade detection
  - **Metamorphic**
    - Viruses that are able to rewrite themselves entirely before it attempts to infect a file
  - **Stealth**
    - Stealth viruses are a category of a virus protecting itself
  - **Armored**

        - Virus that has a layer of protection to confuse a program or a person who's trying to analyze it
    - **Hoax**
        - Hoax virus tries to trick a user to infect their own machine
    - **Worm**
        - Malicious software, like a virus, but can replicate itself without any user interaction
        - Worms can spread and replicate really fast
    - **Trojan**
        - Are a piece of malicious software that are disguise as a piece of harmless or desirable software
    - **Remote Access Trojan (RAT)**
        - Provides the attacker with remote control of a victim computer

- **Ransomware**
    - Malware that restricts access to a victim's computer system until a ransom is received
    - Keep backups of all the systems and files
    - Ransomware uses a vulnerability in your software to gain access and then encrypts your files
- **Spyware**
    - Malware that secretly gathers information about the user without their consent
        - **Adware**
            - Displays advertisements based upon its spying on you
        - **Grayware**
            - Software that isn't benign nor malicious and tends to behave improperly without serious consequences

- **Rootkits**
    - Software designed to gain administrative level control over a system without detection

        - DLL injection is commonly used by rootkits to maintain their persistent control

            - **DLL Injection**

- Malicious code is inserted into a running process on a Windows machine by taking advantage of Dynamic Link Libraries that are loaded at runtime

- **Driver Manipulation**
  - An attack that relies on compromising the kernel-mode device drivers that operate at a privileged or system level

- **Shim**
  - A piece of software code that is placed between two components to intercept calls and redirect them

- **Botnets and Zombies**
  - A collection of compromised computers under the control of a master node

  - **DDoS**
    - Occurs when many machines target a single victim and attack them at the exact same time

  - **Botnets** can be utilized in other processor intensive functions and activities

- **Symptoms of Infection**
  - Your computer might have been infected if it begins to act strangely
  - Hard drives, files, or applications are not accessible anymore
    - Strange noises
    - Unusual error messages
    - Display looks strange
    - Jumbled printouts
  - Double file extensions are being displayed, such as textfile.txt.exe
  - New files and folders have been created or files and folders are missing/corrupted
  - System Restore will not function

- **Removing Malware**
  - Scan the computer

1. Identify the symptoms of a malware infection

2. Quarantine the infected systems
3. Disable System Restore
4. Remediate the infected system
5. Schedule automatic updates and scans
6. Enable System Restore and create a new restore point
7. Provide end user security awareness training

- If a boot sector virus is suspected, reboot the computer from an external device and scan it
- Remove the hard drive from the victimized machine, connect it to a clean workstation as a secondary drive, and then scan it

- **Preventing Malware**
  - Continually doing your service packs and updates for your operating system
  - Have a good host-based Firewall
  - Worms, Trojans, and Ransomware are best detected with anti-malware solutions

  - Root kits are a type of malware that installs itself and tries to bypass the operating
  - system functions

  - Scanners can detect a file containing a rootkit before it is installed

  - Re-image the machine from a known good baseleine

  - Verify your email servers aren't configured as open mail relays or SMTP open relays

1. Remove email addresses from website
2. Use allowlist and blocklists
3. Train and educate end users

1. Update your anti-malware software automatically and scan your computer
2. Update and patch the operating system and applications regularly
3. Educate and train end users on safe internet surfing practices

Social Engineering

Objective 2.3 and 2.4

- **OBJ 2.3:** Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods
- **OBJ 2.4:** Explain common social-engineering attacks, threats, and vulnerabilities

- **Social Engineering**
  - Broad range of malicious activities accomplished through human interactions

- **Phishing Attacks**
  - **Phising**
  - **Spearphishing**
  - **Whaling**
  - **Smishing**
  - **Vishing**
  - **BEC**
  - **Pharming**

  - **Social Engineering**
    - Any attempt to manipulate users to reveal confidential information or perform actions detrimental to a system's security
    - End users and employees are the weakest link in an organization's security

  - **Phishing**
    - A social engineering attack where the malicious actor communicates with the victim from a supposedly reputable source to lure the victim into divulging sensitive information
    - 60-70% response rate

  - **Spearphishing**
    - Uses the same technology and techniques but is a more targeted version of phishing

  - **Whaling**

        - Focused on key executives within an organization or other key leaders, executives, and managers in the company

    - **Short Message Service (SMS)**
        - The text message service component on cellphones, smartphones, tablets, and other mobile devices

    - **Multimedia Messaging Service (MMS)**
        - A form of text messaging that also allows pictures, sounds, or videos to be sent

    - **Vishing**
        - Occurs when the message is being communicated to the target using the voice functions of a telephone

    - **Business Email Compromise (BEC)**
        - Occurs when an attacker takes over a high-level executive's email account and orders employees to conduct tasks

    - **Pharming**
        - Tricks users into divulging private information by redirecting a victim to a website controlled by the attacker or penetration tester

- **Spam**
    - The abuse of electronic messaging systems, most commonly through email
    - Spammers often exploit a company's open mail relays to send their messages
    - CAN-SPAM Act of 2003

- **Impersonation**
    - The act of pretending to be someone else in order to gain access or gather information
    - The goal is to use people's trust on a person in authority and people in uniform

        - **Elicitation**
            - The ability to draw, bring forth, evoke, or induce information from the victim

- **Pretexting**
    - **Train your employees not to fall for pretext and to not fill in the gaps for people when they're calling you or even in person**

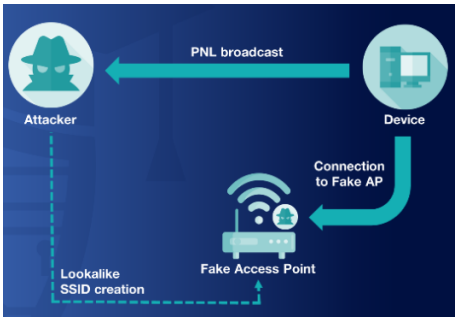
- **Social Engineering Attacks**
    - **Tailgating**
    - **Piggybacking**
    - **Shoulder Surfing**
    - **Eavesdropping**
    - **Dumpster Diving**

    - **Social Engineering**
        - Any attempt to manipulate users into revealing confidential information or performing other actions that are detrimental to that user or the security of our systems
        - The weakest link is our end users and employees

    - **Tailgating**
        - When an attacker attempts to enter a secure portion of a building by following an authorized person into that area, without their knowledge
    - **Piggybacking**
        - Similar to tailgating, but happens with the knowledge or consent of the employee
    - **Shoulder Surfing**
        - Using direct observation to obtain information from an employee
        - Not as obvious as standing over your shoulder, but it can be a quick glance at your screen
    - **Dumpster Diving**
        - Actually looking in garbage or recycling bins for personal or confidential information
- **Evil Twin**
    - A fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on your wireless communication

        - **Karma Attack**
            - Exploits the behavior of Wi-Fi devices due to a lack of access point authentication protocols being implemented

- **Preferred Network List (PNL)**
  - A list of the SSIDs of any access point the device has previously connected to and will automatically connect to when those networks are in range



- **Captive Portal**
  - A web page that the user of a public-access network is obligated to view and interact with before access is granted

- **Software Firewalls**
  - **Personal Firewall**
    - Software application that protects a single computer from unwanted Internet traffic
    - Host-Based Firewall

  - Windows Firewall
  - PF and IPFW
  - iptables

  - Many anti-malware suites contain software firewalls
  - It is better to run a personal software-based firewall and a network-based firewall to provide you with two layers of protection

- **User Education**
  - I can install all the technology I want, but if I don't fix the user, it's all gonna be for nothing
  - Never share your authentication information

    - **Clean Desk Policy**

- By end of day, employees clean their desks and leave nothing out that may be taken as a password or a PIN

- Train users how to encrypt emails and data
- Follow organizational data handling and disposal policies

Security Controls

Objective 2.3 and 2.4

- **OBJ 2.1:** Summarize various security measures and their purposes

- **Security Controls**
  - **Physical Controls**
    - Implemented to increase physical security posture
  - **Logical Controls**
    - Implemented through hardware or software to prevent or restrict access

      - **Auditing**
        - One-time
      - **Monitoring**
        - Ongoing

  - **Managerial Controls**
    - Implemented to manage the organization's personnel and assets

      - Data classification and labelling
      - Personnel supervision
      - Security awareness training

- **Perimeter Defense**
  - **Fences**
    - Designed in different formats, including see-through or not
    - See-through fences allow outsiders to see what's inside
    - Non-see-through fences prevent employees and guards from seeing incoming threats
    - Fences keep people away from areas that are under your control

  - **Bollards**
    - Type of barricade used to prevent terrorist attacks
    - Think about the type of aesthetic fence and bollards to install
    - Make sure that it is still friendly and inviting

  - **Lighting**

        - Use well-designed lighting around your perimeter
            - Always ON
            - Motion sensor

    - **Guards**
        - Protect the outside or inside of the building

- **Surveillance**
    - **Video Surveillance**
        - Used inside or outside of a building using cameras and CCTV
            - Motion
            - Sound
            - Light

    - **Circuit-based System**
        - Alarm system that sounds anytime the circuit is open or closed

    - **Motion Sensors**
        - Allows to play motion sensor in different areas

            - **Proximity**
                - Alarm that turns off when there is a movement in one of the tagged objects within the area

            - **Duress**
                - Alarm that can be triggered by someone when there is a threat

    - **Magnetometer**
        - Type of metal detector that is deployed at airports and public buildings
        - Walk-through magnetometer detects the presence of metal

- **Physical Access Controls**
    - **Door locks**
        - **Key Operated**
            - Uses a key to lock or unlock the door
        - **Mechanical Operated**

- Uses a PIN to lock or unlock the door
- Mechanically operated lock is usually referred to as a cipher lock

- **Electronic Operated**
  - Requires a PIN entered on an electronic keypad to unlock

    - Mechanical
    - No power needed
    - Electronic
    - Needs power

- **Badge Reader**
  - Uses a token to unlock the door
  - Badge reader can be combined with two-factor authentication

- **Biometric Door Lock**
  - Uses biometric data to unlock the door

    - Fingerprint readers are considered a hygiene issue

    - **Palm Print Scanner**
      - Uses a camera to scan the palm print by using infrared lights
      - Palm print scanners are much larger in size

    - **Retina Scanner**
      - Uses infrared light that is shown into an eye

- **Equipment locks**
  - Prevents theft and unauthorized physical access to servers, network appliances

    - **Lockable Rack Cabinet**
      - Controls access to servers, switches, and routers installed in standard networking racks
        - Chassis Locks
        - Faceplates

        - Lockable rack cabinet protects all the devices in one server rack

    - **Kensington Lock**
        - A cable that uses a tie to secure smaller devices

- **Access control vestibules**
    - Serves as a way to limit the people that go in or out of an organization

- **Badge readers**
    - Badge readers can be used as a way to log in to a computer
        - Magnetic Strip
        - Smart Card
        - RFID
    - Badge reader systems use contact-based badge reading

- **Security Principles**
    - **Least Privilege**
        - Uses the lowest level of permissions needed to complete a job function

    - **Role-based Access**
        - **Discretionary Access Control (DAC)**
            - Access control method where access is determined by the owner of the resource
            1. Every object in a system has to have an owner
            2. Each owner must determine the access rights and permissions for each object

        - **Mandatory Access Control (MAC)**
            - Access control policy where the computer system decides who gets access
                - Unclassified
                - Confidential
                - Secret
                - Top secret

- MAC is reserved for highly classified information within the military

- **Role-Based Access Control (RBAC)**
  - Access model that is controlled by the system that focuses on a set of permissions versus an individual's permissions
  - Creating groups makes it easy to control permissions based around actual job functions

- **Power User**
  - User who is not a normal user and also not a normal administrator
-
- **Zero-Trust**
  - Security framework that requires the users to be authenticated, authorized, and validated
    1. Reexamine all default access controls
    2. Employ a variety of prevention techniques and defense in depth
    3. Enable real-time monitoring and controls to identify and stop malicious activity
    4. Ensure the network's zero-trust architecture aligns with a broader security strategy

- **Multifactor Authentication**
  - **Multifactor Authentication (MFA)**
    - Uses two or more factors to prove a user's identity
      - **Knowledge**
        - Something you know
      - **Ownership**
        - Something you have
      - **Characteristic**
        - Something you are
      - **Location**
        - Somewhere you are
      - **Action**
        - Something you do

  - **High security systems often use multifactor authentication**

- **Time-Based One-Time Password (TOTP)**
  - Computes password from a shared secret and the current time
- **HMAC-Based One-Time Password (HOTP)**
  - Computes password from a shared secret and is synchronized across the client and the server
- **In-Band Authentication**
  - Relies on an identity signal from the same system requesting the user authentication
- **Out-of-Band Authentication**
  - Uses a separate communication channel to send the OTP or PIN
- **Implement 2FA or MFA that relies on OOB authentication system**

- **Enterprise Mobility Management (EMM)**
  - Enables centralized management and control of corporate mobile devices
    - Tracking
    - Controlling
    - Securing
  - **EMM**
    - Policies and tools
  - **MDM**
    - Technical controls
      - **Application Control**
      - **Passwords and passcode functionality**
      - **MFA Requirement**
      - **Token-based Access**
      - **Patch Management**
      - **Remote Wipe**
  - **Remote Wipe**

        - Used to send remote commands to a mobile device from an MDM solution to delete its data settings
        - A device must have an Internet connection to receive the remote wipe
        - Incorrect password or passphrase entered too many times
        - Device tries to connect to a network and does not meet the baseline requirements

    - **Firmware Update**
        - Updates the baseband of the radio modem used for cellular, Wi-Fi, Bluetooth, NFC, and GPS connectivity

- **Active Directory Security**
    - **Domain-based**
    - **Security Group**
    - **Organizational Unit**
    - **Group Policies**
    - **Login Scripts**
    - **Home Folders**
    - **Folder Redirection**

    - **Have at least one Windows server as a domain controller**

    - **Active Directory (AD)**
        - Allows to get information from the network about the systems, users, and computers
            - Users
            - Groups
            - Computers
        - Use Active Directory inside Windows-based networks for high levels of security

    - **Security Group**
        - Allows to easily assign permissions to a set of users or worskstations
        - Groups have different permissions applied using ACLs, group policies, and login scripts

    - **Organizational Unit (OU)**

- Way of dividing the domain into different administrative realms

- **Group Policies**
  - Allows to configure computer settings and user profile settings for the set of users
  - Settings can be templated

- **Home Folder**
  - Private drive that is mapped to a network share

- **Folder Redirection**
  - Allows to change the target of a personal folder

Wireless Security

Objective 2.3 and 2.4

- **OBJ 2.3:** Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods
- **OBJ 2.4:** Explain common social-engineering attacks, threats, and vulnerabilities

- **Wireless Encryption**
  - **Pre-Shared Key**
    - Same encryption key is used by the access point and the client
  - **Wired Equivalent Privacy**
    - Original 802.11 wireless security standard that claims to be as secure as a wired network
    - WEP's weakness is its 24-bit IV (Initialization Vector)
  - **Wi-Fi Protected Access (WPA)**
    - Replacement for WEP, which uses TKIP, Message Integrity Check (MIC), and RC4 encryption
    - WPA was flawed, so it was replaced by WPA2
  - **Wi-Fi Protected Access version 2 (WPA2)**
    - 802.11i standard to provide better wireless security featuring AES with a 128-bit key, CCMP, and integrity checking
    - If we make operations easier, then security is reduced
  - **Wi-Fi Protected Setup (WPS)**
    - Automated encryption setup for wireless networks at a push of a button, but is severely flawed and vulnerable
    - Always disable WPS
    - Encryption and VPNs are always a good idea

- **WPA3**
  - **Wi-Fi Protected Access 3 (WPA3)**
    - Latest and most secure version of wireless network encryption currently available

      - **Updated cryptographic protocols**
        - **Enterprise**
          - 192-bit
        - **Personal**

- 192-bit or 128-bit

- Galois Counter Mode Protocol (GCMP)

- **"Enhanced open"**
  - Opportunistic Wireless Encryption (OWE)

- **Management protection frames**

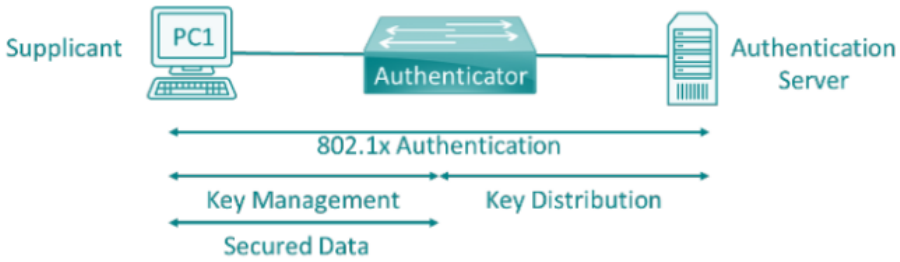
- **Simultaneous authentication of equals (SAE)**
  - A secure password-based authentication and password authenticated key agreement that relies on forward secrecy

- **Forward Secrecy**
  - Assures the session keys will not be compromised even if the long-term secrets used in the session key exchange have

1. AP and client use a public key system to generate a pair of long-term keys
2. AP and client exchange a one-time use session key
3. AP sends client messages and encrypts them using the created session key
4. Client decrypts received messages using the same one-time use session key
5. Process repeats for each message being sent, starting at Step 2

- **Wireless Authentication**
  - **Remote Authentication Dial-In User Service (RADIUS)**
    - Cross-platform protocol that authenticates and authorizes users to services, and accounts for their usage

- Supplicant
- Authenticator
- Authentication server



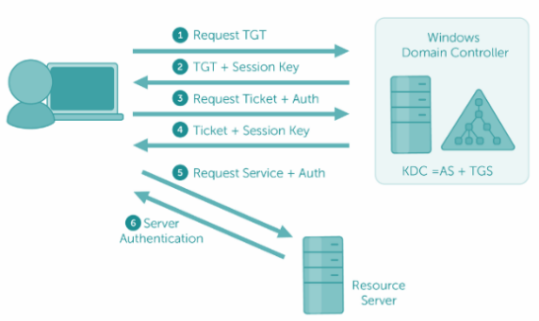
- **Terminal Access Controller Access Control System Plus (TACACS+)**
  - Cisco-proprietary protocol that provides separate authentication, authorization, and accounting services

- **Diameter**
  - Peer-to-peer protocol created as a next-generation version of RADIUS

- **Lightweight Directory Access Protocol (LDAP)**
  - Cross-platform protocol that centralizes info about clients and objects on the network

- **Single Sign-On (SSO)**
  - Enables users to authenticate once and receive authorizations for multiple services across the network

- **Kerberos**
  - Uses symmetric encryption and the Key Distribution Center to conduct authentication and authorization functions



- **802.1x**
  - Used for port-based authentication on both wired and wireless networks
  - Utilize 802.1x as part of your defense

- **Extensible Authentication Protocol (EAP)**
  - Allows for numerous different mechanisms of authentication

    - **EAP-MD5**
      - Utilizes simple passwords and the challenge handshake authentication process to provide remote access authentication
    - **EAP-TLS**
      - Uses public key infrastructure with a digital certificate being installed on both the client and the server
    - **EAP-TTLS**
      - Requires a digital certificate on the server and a password on the client for its authentication
    - **EAP Flexible Authentication via Secure Tunneling (EAP-FAST)**
      - Uses a protected access credential to establish mutual authentication between devices
    - **Protected EAP (PEAP)**
      - Uses server certificates and Microsoft's Active Directory databases to authenticate a client's password
    - **Lightweight EAP (LEAP)**
      - **A proprietary protocol that only works on Cisco-based devices**

- **Wireless Network Security**
  - **Service Set Identifier (SSID)**
    - The name of the wireless network

      1. Name the network after something that is easy to recognize
         - Do not use any personally identifiable information
      2. Random naming scheme
         - Many textbooks recommend to disable the broadcast of the SSID

    - Disabling the broadcast SSID just makes it harder for your authorized users to be able to connect to the network
    - Enabling encryption can give you a lot of security
    - Never use WPA or WEP

- Enable wireless network encryption by configuring your wireless access point
- A strong passphrase will serve as the password or symmetric key for this encryption

- **Guest Access**
  - Allows someone who is visiting your area to connect to your wireless access point and access the Internet
  - Disable guest access

- 2.4 GHz networks are going to operate on channels 1-11
  - The most distance between channels 1-11 are channels 1, 6, and 11
- With 5 GHz and 6 GHz, you can use the auto channel selection

Mobile Device Security

Objective 2.7

- **OBJ 2.7:** Explain common methods for securing mobile and embedded devices

- **Securing Wireless Devices**
  - **Wi-Fi**
    - Used by mobile devices to make a connection to high-speed Internet
    - WPA3 is the highest level of encryption available for mobile Wi-Fi at this time
  - **Bluetooth**
    - Used by mobile devices to connect peripherals to the device
    - Bluetooth requires two devices to make a connection or link
  - Check specifications to see if the device uses at least AES encryption with a strong key
  - Software firewalls are common for larger devices, but not so much for mobile devices
  - The firewall must have root or administrative privileges on the mobile device in order to successfully protect it
  - A VPN connection between a mobile device and a centralized server is safer
  - Remote backups automatically go to places like iCloud for Apple, Google Sync, or OneDrive from Microsoft
  - Always ensure you have secured the wireless connectivity first, then implement a mobile firewall

- **Mobile Device Unlocking**
  - PIN
  - Password
  - Pattern
  - Fingerprint
  - Face ID
  - **Swipe Gesture**
    - Someone can simply take the mobile device and swipe the screen open to unlock it, without using anything to secure it

- **PIN codes and passwords are the simplest types of authentications**

- **Personal Identification Number (PIN Code)**
  - Normally 4-8 digits long, depending on your smartphone or device
  - PIN codes are easy to guess as there are only 10,000 possible codes for a four-digit PIN
  - Shoulder surfing attacks are easy if you use a PIN code as it's just a few digits to remember
  - PIN codes are only numbers, whereas passcodes are numbers, letters, and symbols
  - Passwords can also be easily used by others, due to shoulder surfing and other attacks
  - Wrong passcode entered 10 times can lock you out and make you wait 30 minutes before you're able to try again

- Remote wipe, wipes of all data after 10 failed attempts to login

- **Pattern**
  - The screen shows you nine different dots for you to swipe and make a pattern with
  - Pressing and removing your finger off the touch scanner several times is how you set up Touch ID

- **Facial Recognition**
  - Touch ID has a fail rate of about1 in every 50,000 attempts
  - Face ID has a fail rate of about 1 in every 1,000,000 attempts
  - Both of these are much more secure than a PIN or password
  - Smartphones like to use biometrics first and then PIN or passcode, if you have all of that set up
  - Face ID wasn't helpful in 2020 when everyone was wearing masks, so the PIN or password fallback is very helpful

- **Mobile Malware**
  - Ensure your mobile device is patched and updated
  - Only install apps from the official App Store or Play Store

- **Do not jailbreak/root device**
- **Don't use custom firmware/ROM**
- **Only load official store apps**
- **Always update your software**

- **Mobile Device Theft**
  - Always ensure your device is backed up
  - Don't try to recover your device alone if it is stolen
  - **Remote Lock**
    - Requires a PIN or a password before someone can use the device
  - **Remote Wipe**
    - Allows to remotely erase the contents of the device to ensure that no information can be recovered
- **Mobile App Security**
  - **Only install apps from the official mobile stores**
  - **Transport Layer Security (TLS)**
    - Put an encryption layer and a tunnel between your device and the server to ensure you have confidentiality
  - **Mobile Device Management**
    - Centralized software solution that allows system administrators to create and enforce policies across its mobile devices
    - Turn location services off to ensure privacy
  - **Geotagging**
    - Embedding of the geolocation coordinates into a piece of data, such as a photo
    - Geotagging should be considered when developing your organization's security policies
- **Deployment Options**
  - **Corporate Owned/ Business Only (COBO)**

        - Purchased by the company and only used by the employee for work-related purposes
            - Most secure
            - Most restrictive
            - Most expensive

    - **Corporate Owned/ Personally Enabled (COPE)**
        - Company provides a device used for work and/or personal use by employees

    - **Choose Your Own Device (CYOD)**
        - Allows employees to choose device from an approved list of vendors or devices

    - **Bring Your Own Device (BYOD)**
        - Allows employees to bring their own devices, and connect to the corporate network
        - BYOD is the most difficult to secure

    - **Storage Segmentation**
        - Creates a clear separation between work and personal data on a device

    - **Mobile Device Management**
        - Centralized software solution for remote administration and configuration of mobile devices
        - MDM can prevent certain applications from being installed on the device
        - Ensure your organization has a good security policy for mobile devices

- **Hardening Mobile Devices**
    1. Update your device to the latest software
    2. Install Antivirus
    3. Train users on proper security and use of their device
    4. Only install apps from the official app stores
    5. Do not jailbreak or root your devices
    6. Only use Version 2 SIM cards for your devices
    7. Turn off all unnecessary features on your device
    8. Turn on encryption for voice and data

9. Use strong passwords or biometrics
10. Don't allow BYOD

- Ensure your agency has a good security policy for mobile devices

- **Implementing Mobile Device Security**
  - iPadOS will be similar to iOS and similar but not quite the same with Andriod
  - Remember to set up how you want to use your device with locking, unlocking, password, Touch ID, Face ID, and more

- **IoT Vulnerabilities**
  - **S** in IoT stands for security
  - Most IoT devices uses an embedded version of Linux or Android as their OS
  - Many Manufacturers uses outdated or insecure hardware components
    - Insecure defaults
    - Hard-coded configurations
    - Cleartext communication
  - Attackers also monitors Bluetooth frequencies being transmitted and conduct eavesdropping
    - Data modification
    - Data exfiltration
  - Be careful in which exploits you since you can inadvertently cause the device to go offline, crash or malfunction

Windows Security

Objective 2.5

- **OBJ 2.5:** Given a scenario, manage and configure basic security settings in the Microsoft Windows OS

- **Login Options**
  - **Local Sign-in**
    - Uses Local Security Authority (LSA) to compare the submitted credentials
    - Local sign-in is also known as interactive login
  - **Network Sign-in**
    - Uses Kerberos to perform network authentication
  - **Remote Sign-in**
    - Allows users to access the local network by using a VPN or a web portal (SSL/TLS)
  - **Username and Password**
  - **PIN**
  - **Fingerprint**
  - **Facial Recognition**
  - **Single sign-on**
  - **Username and Password**
    - Oldest type of authentication that uses single-factor authentication
    - Knowledge-based factor
  - **Windows Hello**
    - Allows the user to configure an alternate means of authentication
    - Windows Hello PIN can be used to enter the system and authenticate
    - Windows Hello subsystem is considered more secure
    - Windows Hello Fingerprint uses biometric authentication
    - Windows Hello Face uses facial recognition
  - **Single sign-on**

        - Users can authenticate on the device or network to gain access to multiple apps or services
        - Using SSO is considered more secure than having different accounts

- **Users and Groups**
    -
- **Encrypting Windows Devices**
    - **Administrators**
    - **Users**
    - **Guests**
    - **Power users**

    - **Local Account**
        - Account that exists on a single workstation or computer
            - Security Account Manager (SAM)
                - HKEY_LOCAL_MACHINE registry hive
        - Local account cannot be used to log into different computers

    - **Microsoft Account**
        - Created through an online cloud-based portal at account.microsoft.com
        - Microsoft account can be synchronized between devices using the same portal
        - Domain-based users can also create an account as part of the domain environment

    - **User**
        - Able to change their own settings
        - When creating a new user on a system, it should be placed into the standard user group

    - **Administrator**
        - Gives additional security permissions
        - By default, the first user on a system is placed in the Administrator group

    - **Guest**
        - Account is disabled and gives a higher level of security
        - Guest accounts are disabled on Windows 10 and 11

- **Power User**
  - Gives the user an intermediate permission level, but less than an administrator
  - Power user group has the same permission level as the standard user group
  - Administrator mode works at a higher level of permissions that can cause a lot of system damage

- **User Account Control (UAC)**
  - Windows security feature used to protect the system against malicious programs, scripts, and attacks

  - Administrator runs a program using the user credentials, not the administrative credentials

  - Click the Change Account Type button within UAC
  - UAC settings can be configured from "always notify" to "never notify"
  - Change the UAC configuration in the control panel and select "user account control" settings

- **File Permissions**
  - **New Technology File System (NTFS)**
    - Uses file permissions on all files and folders
    - NTFS permissions can be assigned to a file or folder by using a user's account or group
    - Each object has an implicit deny to prevent using a permission
    - Explicit permissions set an allow or deny action
    - Permissions are cumulative

  - **Share Permissions**
    - Applies only to files that were shared using a network connection
    - Share permissions that are used in NTFS permissions will be applied locally and over the network
    - Share permissions are set at the root of the share and its subdirectories
    - The most restrictive will apply to files and folders that are accessed over the network

- **Inheritance**
- Happens with all of the sub folders and files underneath that folder

Securing Workstations

Objective 2.6 and 2.8

- **OBJ 2.6:** Given a scenario, configure a workstation to meet best practices for security
- **OBJ 2.8:** Given a scenario, use common data destruction and disposal methods

- **Account Management**
  - User permissions
  - Admin user account
  - Disable guest accounts
  - Restrict login times
  - Failed login attempts
  - Concurrent logins
  - Timeouts and screen locks

  - Give user the least amount of permissions to be able to do their job

  - File permission control allows to change whether the user can read, modify, or delete data file or folder

  - Set a good, long, and strong password for the administrator account

  - Disable the default admin account and create a new user account for better security

  - Guest accounts represent a significant security vulnerability

  - Disable the guest account and create a regular user account

  - Restrict your login times if you want to have better security

  - Consider this based on your organization and the needs of your employees
    - Account disabled
    - 15-min cool off

  - Account disabled means the user cannot login until they contact help desk

- With the lockout timer, the user has to wait 15 minutes to be able to re-login
- Every Windows user can log into multiple systems using the same account in a domain environment
- You can set the number of concurrent logins allowed
- Limit of only one concurrent login
- Find the right amount of time that makes it work

- **AutoRun and AutoPlay**
  - This can lead to a huge vulnerability
  - Disable autoplay or autorun to increase security

- **Passwords Best Practices**
  - Complexity requirements
  - Expiration requirements
  - Use of passwords

- **Encryption Best Practices**
  - **Unencrypted Data (Cleartext/Plaintext)**
    - Stored, transmitted, or processed in an unprotected format that anyone can view and read
  - **Encrypted Data (Ciphertext)**
    - Scrambled up and unreadable to anyone without the proper encryption or decryption key
    - Encryption is a form of risk mitigation
  - **Data State**
    - Location of data within a processing system
  - **Data at Rest**
    - Any data stored in memory, a hard drive, or a storage device
      - Full disk encryption
      - Folder encryption
      - File encryption
      - Database encryption

- **Data in Transit/Motion**
  - Any data moving from one computer or system to another over the network or within the same computer
    - TLS or SSL
    - IPSec or L2TP
    - WPA2 with AES

- **Data in Use/Processing**
  - Any data read into memory or is currently inside the processor and being worked on or manipulated
    - Data at rest
    - Data in motion
    - Data in processing

- **End-user Best Practices**
  - Anytime you're not using a system, you should log off or lock your computer
  - A screensaver lock will lock your desktop after a period of inactivity
  - Secure personally identifiable information
  - Clean desk policy ensures everything on your desk is put away by end of day
  - Log off if you will be gone for more than a few minutes
  - Critical hardware like laptops must be in your possession or properly secured at all times
  - You want to make sure that data is always protected

- **Data Destruction**
  - Asset disposal occurs whenever a system is no longer needed

  - **Degaussing**
    - Exposes the hard drive to a powerful magnetic field which in turn causes previously-written data to be wiped from the drive

  - **Purging (Sanitizing)**
    - Act of removing data in such a way that it cannot be reconstructed using any known forensic techniques

  - **Clearing**

        - Removal of data with a certain amount of assurance that it cannot be reconstructed

    - **Data remnants** are a big security concern
    - Ensure all data remnants had been removed using overwriting procedures

    - Possible reuse of the device will influence the disposal method

        1. Define which equipment will be disposed of
        2. Determine a storage location until disposal
        3. Analyze equipment to determine disposal method
        4. Sanitize the device and remove all its data
        5. Throw away, recycle, or resell the device

- **Data Destruction Methods**
    - **Sanitizing**
    - **Purging**
    - **Overwriting**
    - **Zeroing**

    - Recycling or repurposing electronics methods: Erasing/wiping (Standard formatting or Low-level formatting)
    - Physical destruction methods: drilling, shredding, incinerating, and degaussing

    - **Erasing or Wiping**
        - The process of destroying old data by writing over the location on the hard drive or solid-state device with new data

    - Forensic experts can recover some hidden data overwritten with a series of ones and zeros
    - Erasing and wiping don't work as well with solid state devices
    - Use Format from the Windows command line to erase the contents of the hard drive
    - Using a standard formatting procedure, you will have better data destruction than you have with a simple erasing or wiping

    - **Low-level Format**

- Procedure provided by the manufacturer which will reset the disk back to its factory condition
  - Secure erase
  - Crypto erase

- **If you don't let this procedure actually finish, you'll have a drive that is no longer functional and no longer usable for anything**

- **Self-Encrypting Drive**
  - A particular type of hardware that will encrypt and decrypt the entire disk
  - By erasing the key, you have now made all the data on it unusable and unreadable

- **Degaussing**
  - Exposing hard disk drives to powerful electromagnets that are going to disrupt the magnetic patterns on those hard disks and cause them to lose their state
  - This does not work if you're using optical media or solid state drives

1. Electronic method: will allow you to reuse or recycle those different drives
2. Physical method: drilling, shredding, incinerating, degaussing

Securing Web Browsers

Objective 2.10

- **OBJ 2.10:** Given a scenario, install and configure browsers and relevant security settings

- **Web Browser Installation**
  - Download from the official app stores either on Windows or Mac, or go to the official websites

- **Extensions and Plug-ins**
  - Extensions and plug-ins are often used interchangeably, but on different web browsers they are used differently
    - Extensions
    - Plug-Ins
    - Apps
    - Search Providers
    - Themes

  - Plug-ins that work in the background to help you do things like video streaming
  - Themes that change your browser's look
  - You can change your default search engine
  - Applications to keep things like document editing in your browser, even for offline use

- **Password Managers**
  - **Password Manager**
    - Helps you secure different passwords and stores them so you can use them easily
    - Memorizing a master passcode while the rest are saved for you is a much better method than using the same password everywhere

- **Encrypted Browsing**
  - You need to ensure that the website is secure before you access it and enter any kind of personal details

- **Private Browsing**
  - **Private Browsing**

    - A special mode in web browsers that ensures the caching features are not being used
    - Even in private browsing, you are still being watched online

- **Pop-up and Ad Blockers**
    - Some fake ads will bring you to fake websites to urge you to buy fake products online
    - Ad blockers aren't for being annoyed with advertising, rather because criminals have been using ads to get to people

- **Cache and History Clearing**
    - Cache allows you to view the same website multiple times without having to redownload images or videos on that site
    - History keeps track of all websites you've been to, unless you clear it
    - All of this is stuff people can use to get an idea of what you do, so it is also a good idea to clear your browser history sometimes

- **Profile Synchronization**
    - **Profile**
        - You make this for different setting preferences, but it doesn't work across all Internet browsers
        - A way to keep your personal and work life separate to avoid problems in the future

Supporting Network Operations

Objective 4.1 and 4.2

- **OBJ 4.1:** Given a scenario, implement best practices associated with documentation and support systems information management
- **OBJ 4.2:** Explain basic change-management best practices

- **Ticketing System**
  - **Ticketing Systems**
    - Used to manage requests, incidents, and problems submitted by users
    - Ticketing system shows user information
      - Phone
      - Email
      - Chat
      - Ticket

    - Newly created tickets show user history

      - Name
      - Contact Details

      - User information
      - Device information

  - **Incidents** happen one time or are isolated issues
  - **Problems** are recurrent and happen to multiple users or devices with the same characteristics

  - **Problem description**
    - Gather more details or information about the problem

  - **Ticket categories**
    - Three basic ticketing types
      - Requests
      - Incidents
      - Problems

- **Problem**
  - A collection of incidents or recurrent issues
  - Every organization configures different categories based on their own business needs

- Assigning severity levels can be done individually or with modern ticketing systems

- **Severity**
  - Classifying tickets in a prioritized order
    - Urgent
    - High
    - Medium
    - Low

    - Tier 3 (1-3%)
    - Tier 2 (20-30%)
    - Tier 1 (70-80%)
    - Tier 0

- **Shifting Left**
  - Gives us more freedom and more ability to solve problems at an earlier level

- What you should be writing in your tickets
  - Problem Description
  - Progress Notes
  - Problem Resolution

- **Knowledge Base Articles**
  - Solution Articles
  - FAQs
  - Product Manuals
  - Tutorials
  - Videos
  - Demonstrations
  - Troubleshooting Guides

- Internal knowledge base for the support agents
  - **Internal/Private**
    - Staff
  - **External/Public**
    - End-user

- Ensure knowledge base is properly tagged, categorized, and searchable

- The kind of information should you include depends on your industry and what you're doing inside of your organization

- Difference between a problem and an incident

1. Knowledge base reduces the support workload
2. Provide good self-service
3. Lower the amount of work
4. Lower the product cost
5. Quick onboarding and training experience

- **Asset Management**
  - **Asset Management**
    - Systematic approach to the governance and realization of value of things over their life cycle
      - Tangible Assets
      - Intangible Assets

      - Development
      - Operation
      - Maintenance
      - Upgrade
      - Disposal

    - A database system allows for the detailed management and configuration of assets
    - Allows the system to associate the user with the workstation that is having the issue

- **Unique Asset Tag and Unique Asset ID**
  - Assigned to that particular device and labeled onto it
  - Having an asset tag with unique ID ensures having a good asset governance
  - Establish good change management practices

- **Procurement Lifecycle**
  - Birth to death of an asset

- **Change management procedures**
  - **Change Request**
    - Verifies the impacts
  - **Procurement**
    - Determines the budget
  - **Deployment**
    - Implements procedures in a secure configuration
  - **Maintenance/Operations**
    - Implements procedures for monitoring and support
  - **Disposal**
    - Implements procedures for sanitizing data remnants

- Warranty
- Licensing

- **Change Management**
  - **Change Management**
    - Maximizes the number of successful IT changes
    - The scope of change management is defined by each organization

  - **Change**
    - Addition, modification, or removal that may have a direct or indirect effect on IT services
  - **Standard changes**
    - Preauthorized and can be implemented without any additional authorization
  - **Normal changes**

        - Changes where the authorization is gained
        - Major changes need a higher level of approval
    - **Emergency changes**
        - Changes that need to be expedited
        - Emergency Change Advisory Board (ECAB)
        - Emergency is when something is broken and needs to get back online quickly

    - **Change Authority** is the person or group that authorizes changes

    - **Pair Programming/Coding**
        - One person codes and the other person reads it and approves it

    - **When working with large system networks, use normal change**

    - **Change Schedule**
        - Helps plan the changes and assists in communicating such changes to the stakeholders to avoid conflicts
        - The change schedule informs everybody what's happening
        - Ensures we have the resources to implement the changes

- **Conducting Change Management**
    - Fault to be fixed
    - New business need/process
    - Planned improvement

    - Write the changes to be made and justify

    - **Change Advisory Board (CAB)**
        - Technical experts
        - Business experts
        - Senior leaders

    - **Back Out/Rollback Plan**
        - Plan of action to take if something goes wrong
        - Always have a rollback plan
        - Use sandbox testing

- **End-user acceptance**
  - Make sure that people understand how to use that new system

- **Documentation Types**
  - **Acceptable use policies**
    - Employees' set of policies for a service or resource
    - Each organization sets up rules based on workflow and company values
    - Acceptable use policy is enforced by the organization to govern its employees and users
    - Regulatory Compliance Requirements
    - A splash screen shows up when someone tries to log into a computer

  - **SOPs**
    - New user set-up checklist and procedures
    - End-user termination checklist and procedures
    - Software installation procedures

  - **Standard Operating Procedure (SOP)**
    - Step-by-step list of actions to comply with the policy
    - SOPs will vary depending on the organization

  - **End-user Termination Checklist and Procedures**
    - Used as part of the employee offboarding process

  - **Follow the SOP checklist for new users and end users**
    - Verify the system requirements
    - Validate the download source
    - Verify files
    - Verify software license
    - Ensure proper installation
    - Provide training and support

  - **Incident Report/After Action Report (AAR)**
    - Gathers the opinions of all involved users, customers, technicians, managers, and stakeholders
    - Figure out the cause

- Incident report is a writeup based on what happened, the cause, and how to prevent it in the future

- **Network topology diagrams**
  - One diagram for logical connections and another one for physical connections

- **Network topology diagram shows network connections in a logical or physical manner**

Backup, Recovery, and Safety

Objective 4.3, 4.4 and 4.5

- **OBJ 4.3:** Given a scenario, implement workstation backup and recovery methods
- **OBJ 4.4:** Given a scenario, use common safety procedures
- **OBJ 4.5:** Summarize environmental impacts and local environmental controls

- **Backup, Recovery, and Safety**
  - **Backup**
    - Process of creating and storing copies of data to protect against data loss
  - **Recovery**
    - Process of restoring data backup during data or system loss

- **Backup and Recovery**
  - **Full backups**
    - The backup job is going to create a file that contains all the data from the source
    - Full backup takes up a lot of space
    - Full backups take a long time
  - **Incremental backups**
    - Will only back up things that have changed since the last backup
  - **Differential backups**
    - Backs up all the data that has been changed since the last full backup
  - **Synthetic backups**
    - An optional type of backup that can create full backups with lower data transfer requirements
    - You're not tying up the server by doing a lot of read/write operations, and to copy everything off of the server
  - **Archive Attribute**
    - Archive attribute flags are set to on anytime you modify a file
  - Anytime we do an incremental backup, we're also going to clear the flag
  - On a differential backup, the flag does not get cleared

- It's going to get cleared when you do a full backup or an incremental backup

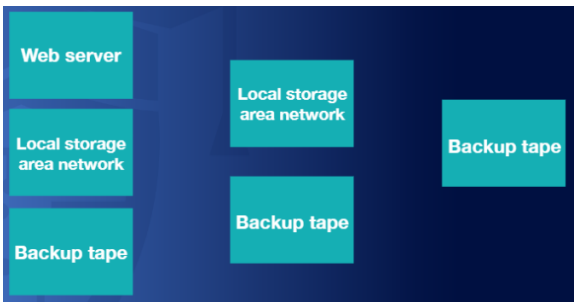
- **Backup Schemes**
  - **Frequency**
    - The period between backup jobs
    - When it comes to determining this frequency, it is all going to depend on how much work you can afford to lose

  - **On-site**
    - The backup storage mechanism is located in the same location as the system they're backing up
  - **Off-site**
    - Backing up to some system not inside the same physical building where your workstations are

  - **Grandfather-Father-Son (GFS)**
    - Tape media rotation scheme that allows some of your backup media to be taken to an offsite storage
    - The **son tapes** will store your most recent data and they have the shortest retention period
    - The **father** is considered the middle generation
    - The **grandfather tapes** will have the longest retention period

- GFS can be modified based on your own needs for retention, as well as for frequency of backups

- **3-2-1 Backup Rule**
  - States that you should have three copies of your data, including your production copy on your servers, two different types of media, and one copy being held offline and off-site



  - You can use GFS in combination with the 3, 2, 1 backup rule
  - A backup can never be called good until you've tested that it actually works

- **Power Continuity**
  - **A redundant power supply mitigates a single point of failure**
  - **Surges**
    - An unexpected increase in the amount of voltage that's being provided
  - **Spikes**
    - A short, transient voltage that can be due to a short circuit, a trip circuit breaker, a power outage, or even a lightning strike
  - **Sags**
    - An unexpected decrease in the amount of voltage provided
  - **Brownouts**
    - Occurs when the voltage drops low enough that it causes the lights to dim and can cause a computer to shut off
  - **Blackouts**
    - Occurs when there is a total loss of power for a long period of time
    - Proper backup power and line conditioning

- **Uninterruptible Power Supply (UPS)**
  - Combines the functionality of a surge suppressor with a battery backup

- **Backup Generator**
  - An emergency power system used when there is an outage of the regular electric grid power
    - Portable gas engine
    - Permanently installed
    - Battery inverter

- **How do you decide which one's right for your organization?**
  - Need
  - Budget
  - Downtime
  - Fuel source

- **Electrical Safety**
  - **Equipment Grounding**
    - Ensures every electrical device has a path to the ground, which is a path that provides the least amount of resistance for electrical current to flow away harmlessly
    - Make sure equipment is properly grounded when installing racks of servers or equipment
    - Never disconnect the ground wire

  - **Proper Power Handling**
    - Keeps the technician safe when working on electrical equipment
    - Never work on a power supply unless you are certified and properly trained to do it
    - Never insert anything into the power supply area of a computer

- **Component Handling and Storage**
  - **Electrostatic Discharge (ESD)**
    - Occurs whenever there's a path that allows electrons to rush from a statically charged body to a component that has no charge
    - To prevent ESD from happening, you need to ensure you take the proper safety precautions

1. **Work in a room that is set up properly to reduce ESD**
2. **Take out anything that can help create static electricity**
3. **Always properly handle components by using ESD safe equipment**

   - Another large cause of ESD is anything that has a mechanical motor
   - Try and reduce static electricity as much as possible

- **HVAC Systems**
  - Make sure HVAC systems are running to protect the servers, workstations, and other equipment
  - Sensitive computer equipment, including servers, computers, and networking gear, releases a lot of heat during their operations
  - HVAC systems also helps with the humidity levels in server rooms and communication closets
  - Humidity level of around 40% to 60% using your HVAC systems
  - Many organizations will connect their HVAC systems to their ICS or SCADA networks
  - Depending on your system's capabilities, you may have to make some choices as to which servers can remain online
  - Place systems and servers in the right location and provide adequate power and cooling

- **Proper Handling and Disposal**
  - Compliance with government regulations

    - **Health and safety laws**
    - **Building codes**
    - **Environmental regulations**

  - This ensures we keep our workplace hazard-free and everything is safe and sound
    - Occupational Safety and Health Administration (OSHA)

  - Building codes are something that are defined at the local, state, and national level

- **Material Safety Data Sheet**
  - Contains all the information about the ingredients, health hazards, precautions, and first aid information

- **How you can properly dispose of those components**
  - Batteries are made up of chemicals that are dangerous to the environment
  - Swollen or leaking batteries should be bagged and properly stored in an appropriate container
  - You need to dispose of it using the proper waste management methods or recycling
  - Most vendors that you buy your toner from will have some sort of recycling program
  - Whenever you're disposing a toner cartridge or recycling it, you should always wrap it up
  - Take them to the proper recycling location or waste management area
  - Make sure you're in compliance with government regulations

- **Personal Safety**
  - One of the most common injuries is caused by lifting things improperly
  - If you do happen to cause an electrical fire, immediately remove the power

  - **PC Vacuum Cleaner**
    - Specialized vacuum cleaner that doesn't create an electrostatic charge

  - **Disconnect the power**
  - **Prevent any kind of trip hazards**
  - **Lift with your legs and not with your back**
  - **Follow proper electrical fire safety**
  - **Use the proper safety equipment**
  - **Use PC safe vacuum**

Policy and Privacy Concepts

Objective 4.6

- **OBJ 4.6:** Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts

- **Incident Response**
  - **Incident Response**
    - A set of procedures an investigator follows when examining a computer security incident
  - **Incident Management Program**
    - Consists of monitoring and detection of security events on a computer network and the use of proper responses to those security events

      - **Preparation**
        - Ensure that it has a well-planned incident response procedure
      - **Identification**
        - Process of recognizing if an event should be classified as an incident
      - **Containment**
        - Focused on isolating the incident
      - **Eradication**
        - Remove the threat or attack
      - **Recovery**
        - Data restoration, system repair, and re-enabling any servers or networks taken down during the incident
      - **Lessons Learned**
        - A process is used to document the instant response process, any changes to the procedures and the processes and make sure we do better next time

- **Chain of Custody**
  - The record of evidence history from collection to court presentation and disposal

  - **Specialized evidence bags** ensure electronic media cannot be damaged or corrupted by electronic discharge (ESD)

- **Faraday Bag**
  - Shields devices from outside signals to prevent data from being altered, deleted, or added to a new device
  - Criminal cases or internal security audits can take months or years to resolve

- **Legal Hold**
  - Preserves all relevant information when litigation is reasonably expected to occur
  - Have spare hardware and good backups of your systems

- **Order of Volatility**
  - **Data Acquisition**
    - Creates a forensically sound copy of the data from a source device

  - **Do I have the right to search or seize this legally?**
    - Any evidence gathered without proper authority or permission can be inadmissible in court

  - **Order of Volatility**
    - Collecting evidence that could be easily tampered or destroyed first

1. **Registers and cache**
2. **Routing tables, ARP caches, process tables and kernel statistics, and memory**
3. **Temporary file systems**
4. **Disks**
5. **Remote logging and monitoring data**
6. **Physical configurations and network topologies**
7. **Archival media**

  - Registers and cache can only be collected when the computer is powered on
  - Contents of the RAM will be lost if the computer is turned off
  - These temporary files are often overwritten during system operation
  - Any data that's persisted on mass storage devices and disc
  - Collect remote logging and monitoring data
  - Data on physical configuration and network topologies helps provide context to an investigation

- Offline and archival media

- **Some key areas (like HKLM\Hardware) are only stored in the memory, so analyze the registry using a memory dump**

- **Data Collection Procedures**
  - Create a forensic disk image of the data as evidence

  - **Capture and hash system images**
  - **Analyze data with tools**
  - **Capture screenshots**
  - **Review network traffic logs**
  - **Capture video**
  - **Consider Order of Volatility**
  - **Take statements**
  - **Review licensing and documentation**
  - **Track man-hours and expenses**

  - **FTK and EnCase** are popular forensic tools

- **Licensing, EULA, and DRM**
  - **Proprietary Software**
    - Original developer retains all rights and ownership of a software code, where you pay them a fee and you receive a license in return
  - **Open-Source License**
    - Makes software free to use, modify, and share
    - There are lots of open-source projects that are not free

  - **Personal License**
    - Allows one individual user to use a piece of software on their given machine
  - **Corporate License**
    - A license for each individual machine or person who is actively using that license

- Active users are people who are actually logged in at this moment using that piece of software
- Licenses provide the legal access to use a software, and also the privilege of getting all the updates and security patches
- Once you lose that valid license, you will no longer be able to get updates to that software or its security patches
- Most software licenses are going to be issued out for a certain period of time
- Use trusted software that comes with a valid license

- **End User License Agreement**
  - Dictates the terms of the license for a software
  - Always understand what is covered inside the EULA

- **Digital Rights Management**
  - Ensures copy protection for music and video that is being used in an online or digital manner
  - DVDs were region-locked and only allowed to be sold in certain regions based on the licensing
  - You may come across issues where some of your users aren't able to play a certain type of file because there's DRM enabled
  - There are many digital formatted files that are protected by DRM

- **Data Classification**
  - Data classification is based on its value to the organization and the sensitivity of the information if it were to be disclosed

    - **Public Data**
      - No impact to the company if released and is often on a company's website
    - **Sensitive Data**
      - Minimal impact if released and includes things like a company's finances
    - **Private Data**
      - Contains information like personnel records, salaries, and other data only used in the organization
    - **Confidential Data**

        - Contains items such as trade secrets, intellectual property data, source code, and things that would harm the company if disclosed

    - **Unclassified**
        - Can be released to the public under the Freedom of Information Act
    - **Controlled Unclassified Information (CUI)**
        - Includes unclassified information that should be protected from public disclosure
    - **Confidential Data**
        - Includes data such as trade secrets that would hurt the government if disclosed
    - **Secret Data**
        - Includes data such as military deployment plans and other things that would damage national security if disclosed
    - **Top Secret Data**
        - Includes blueprints for weapons or other information that could gravely damage national security if known by those unauthorized to know

- **Data Retention**
    - **Data Retention**
        - Maintains and controls certain data to comply with business policies and applicable laws and regulations
    - **Data Preservation**
        - Keeping information for a specific purpose outside of an organization's data retention policy

    - **Short-Term Retention**
        - A term by how often the newest or youngest media sets are overwritten
    - **Long-Term Retention**
        - Any data moved to an archive to prevent being overwritten

    - All of your backups are going to take up valuable storage space
    - Back up everything you're legally required to based on your retention policies
    - Back up what you need based on corporate policies or operations

- **Recovery Point Objective (RPO)**
  - The maximum amount of time that can be lost from a recovery after a disaster, failure, or other event
  - RPO helps drive the recovery window or the redundancy decisions made in your business

- **PII, PHI, and PCI-DSS**
  - **Data Type**
    - A tag or a label to identify a piece of data under a subcategory of a classification
      - **B-I-G-O-T**
        - British Invasion of German Occupied Territory
  - **Health Data**
    - Data related to health conditions, reproductive outcomes, causes of death, or quality of life for individuals or the population
      - **HIPAA**
        - Health Insurance Portability and Accountability Act of 1996
  - **Financial Data**
    - Consists of pieces or sets of information related to the financial health of a business
      - **Payment Card Industry Data Security Standard (PCI DSS)**
        - An agreement that any organization that collects, stores, or processes credit card customer information must abide by
  - **Intellectual Property**
    - A type of data that includes intangible creations of human intellect
      - Copyright
      - Patent
      - Trademark
      - Trade Secret
  - **Personally Identifiable Information (PII)**
    - Any data that could potentially identify a specific individual
      - Microsoft's data loss prevention system (DLP)

- **Data Format**
  - This is the organization of the information into preset structures or specifications
- **Structured Data**
  - Something like a comma separated value list
- **Unstructured Data**
  - Things like PowerPoint slides, emails, text files, chat logs

- Three main types of data you should be aware of as an A+ technician are **PII, PHI, PCI DSS**

- **Security Policies**
  - Privacy policies govern the labeling and handling of data

  - **Acceptable Use Policy (AUP)**
    - Defines the rules that restrict how a computer, network, or other systems may be used

  - **Change Management**
    - Defines the structured way of changing the state of a computer system, network, or IT procedure

  - **Separation of Duties** is a preventative type of administration control

  - **Job Rotation**
    - Different users are trained to perform the tasks of the same position to help prevent and identify fraud that could occur if there was only one user with the job

  - **Mandatory vacations**
    - Require every employee take a vacation at some point during the year

  - **Onboarding and Offboarding Policy**
    - Dictates what type of things need to be done when an employee is hired, fired, or quits

        - Terminated employees are often not cooperative

- **Due Diligence**
    - Ensuring that IT infrastructure risks are known and managed properly
- **Due Care**
    - Mitigation actions that an organization takes to defend against the risks that have been uncovered during due diligence
- **Due Process**
    - A legal term that refers to how an organization must respect and safeguard personnel's rights
    - Due Process protects citizens from their government and companies from lawsuits

Scripting

Objective 4.8

- **OBJ 4.8:** Identify the basics of scripting

- **Scripting**
  - **.bat (Batch File)**
    - Used within Windows inside the command prompt environment
  - **.ps1 (PowerShell)**
    - Used within Windows inside the PowerShell environment
  - **.vbs (Visual Basic)**
    - Used within Windows inside Visual Basic
  - **.sh (Bash Script)**
    - Used within Linux
  - **.js (JavaScript)**
    - Used for automations in webpages and macOS systems
  - **.py (Python)**
    - Generic scripting language used in Windows, Linux, and Mac
  - **Pseudocode**
    - Generic language used to teach new learners how to program a computer

- **Script File Types**
  - **Shell Script**
    - Text-based file that contains commands that can be interpreted and presented to the computer
  - **Batch File (.bat)**
    - Text-based file containing Windows commands and is interpreted from the command line environment
    - Batch files can be used on any Windows-based computer and can be operated from the command line environment
      - **net use**
        - Map drives
      - **Xcopy/Robocopy**
        - Copy
  - **PowerShell (.ps1)**

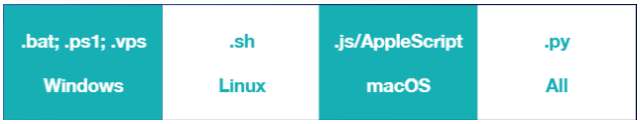
- Allows for more complex scripts
- PowerShell can change and interact with Windows components and features,and also Active Directory
- Commandlets use a basic verb-noun naming scheme

- **Visual Basic Script (.vbs)**
  - Scripting language based on the Visual Basic programming language
  - .vbs runs from other applications, such as MS Word, MS Excel, and other MS Office products

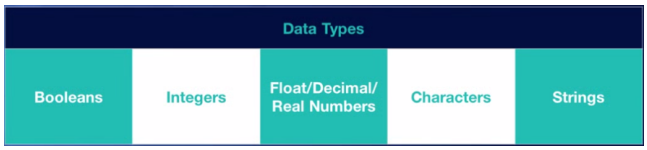
- **Linux Shell Script (.sh)**
  - Works a lot like a batch script inside of Windows

- **JavaScript File (.js)**
  - Scripting language designed to be implemented inside of a web-based interface
  - JavaScript is used on websites and web applications as well as in scripting languages on macOS desktops and servers

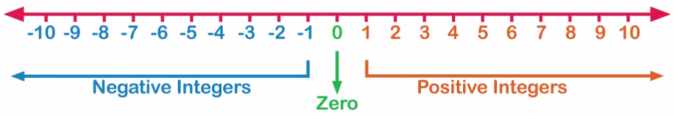
- **Python (.py)**
  - General-purpose scripting and programming language that is used to develop automation scripts and full-fledged software applications
  - Python runs on Windows, Linux, and Mac systems
  - Python is considered an interpreted language because it is cross-platform in nature



- **Variables**
  - Used to store values and data for different data types



- **Boolean**
  - A form of data with only two possible values (True or False)
- **Pseudocode**
  - A made-up language that isn't representative of any singular programming language
- **Integer**
  - A variable that stores an integer or a whole number that may be positive or negative



- **Float/Decimal/Real Number**
  - A variable that stores a decimal number

- **Character**
  - A variable that can only store ASCII character

- **String**
  - A variable that can store multiple characters

- In Pseudocode, no need to define the data type for each variable
- Variables can change throughout the execution of the program

- **Constant**
  - Like a variable, but cannot be changed within the program once defined
  - How do we define the value of variables and constants?

- **Loops**
  - **Loop**
    - A type of flow control that controls which order the code will be executed in a given program
  - **For Loop**
    - Used when the number of times to repeat a block of code is known
  - **While Loop**

        - Used when the number of times to repeat a block of codes is not known and will only stop until something happens
    - **Do Loop**
        - Used when there's an indefinite iteration that need to happen and will only stop until some condition is met at the end of the loop

- **Logic Control**
    - Used to provide conditions based on different logical tests

- **Bash Script Example**
    - Identify the basics of scripting
        - **echo**
            - Printing on screen
        - **if [condition]**
            - Logical construct
        - **$1**
            - Variable

- **Automation Scripting**
    - **Basic Automations**
        - Simple or routine task

    - **Machine Restart**
        - Restart machines using scripts

    - **Network Drive Remapping**
        - Done within normal command line interface using a batch file (.bat) or PowerShell

    - **Application Installation**
        - Can use a batch file or PowerShell in Windows or a shell file in Linux

    - **Update and Security Patch Installation**
        - **PSWindowsUpdate**
            - PowerShell
        - **Wusa.exe file**
            - Batch File

        - **apt or yum**
            - BASH script

    - **Backup Automation**
        - **copy; xcopy; Robocopy**
            - PowerShell or Batch Script
        - **copy (cp)**
            - BASH Script (Linux)

        - **Windows Task Scheduler**
            - Windows
        - **Crontab**
            - Linux

    - **Information Gathering**
        - Use scripts for is to be able to gather information or data from various systems across your network

    - **Using automation and scripting can make life easier**
        - Makes life easier by being able to reach out and touch different assets across your network

- **Scripting Considerations**
    - **Unintentionally introducing malware**
    - **Inadvertently changing system settings**
    - **Causing browser or system crashes due to mishandling resources**

    - Read the scripts and understand what they do before running them
    - Inadvertently changing system settings disables system protection
    - When running a script, use the least permissions needed
    - Depleting hard drive storage space occurs because log files or temporary files are created as part of the scripting process
    - Faulty loops could lose network resources or memory resources
    - Incorrect API calls can cause the web browser's file explorer or command interpreter to crash

Remote Access Support

Objective 4.9

- **OBJ 4.9:** Given a scenario, use remote access technologies

- **Remote Access Protocols**
  - **These different methods allow a client to access a server or a network device remotely over the network**

    - **Telnet Port 23**
      - Sends text-based commands to remote devices and is a very old networking protocol
      - Telnet should never be used to connect to secure devices

    - **Secure Shell (SSH) Port 22**
      - Encrypts everything that is being sent and received between the client and the server

    - **Remote Desktop Protocol (RDP) Port 3389**
      - Provides graphical interface to connect to another computer over a network connection

    - **Remote Desktop Gateway (RDG)**
      - Provides a secure connection using the SSL/TLS protocols to the server via RDP

    - **Create an encryption connection**
      - Control access to network resources based on permissions and group roles
      - Maintain and enforce authorization policies
      - Monitor the status of the gateway and any RDP connections

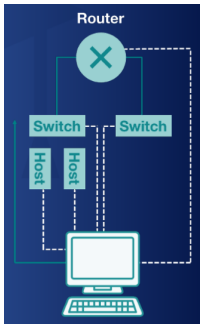
    - **Virtual Private Network (VPN)**
      - Establishes a secure connection between a client and a server over an untrusted public network

    - **Virtual Network Computing (VNC) Port 5900**

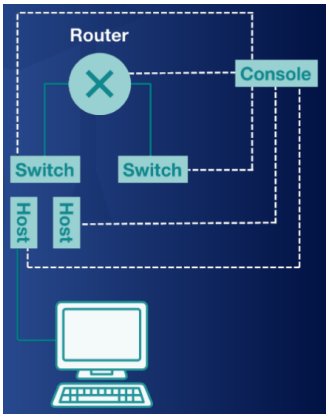
- Designed for thin client architectures and things like Virtual Desktop Infrastructure (VDI)

- **Virtual Desktop Infrastructure (VDI)**
  - Hosts a desktop environment on a centralized server
  - Desktop as a Service (DaaS)

- **In-Band Management**
  - Managing devices through the use of Telnet or SSH protocols over the network



- **Out-of-Band Management**
  - Connecting to and configuring different network devices using an alternate path or management network



  - To prevent a regular user's machine from connecting to the management interfaces of your devices

        - Out-of-band networks add additional costs to the organization

    - **Authentication**
        - Confirms and validates a user's identity

    - **Authorization**
        - Gives the user proper permissions to access a resource

    - **Password Authentication Protocol (PAP)**
        - Sends usernames and passwords in plaintext for authentication
    - **Challenge Handshake Authentication Protocol (CHAP)**
        - Sends the client a string of random text called a challenge which is then encrypted using a password and sent back to the server
    - **Extensible Authentication Protocol (EAP)**
        - Allows for more secure authentication methods to be used instead of just a username and a password

    - Use EAP/TLS in conjunction with a RADIUS or TACACS+ server

- **Remote Monitoring and Management (RMM)**
    - A centralized tool used by managed service providers to manage groups of users and workstations remotely

- **Microsoft Remote Assistance (MSRA)**
    - Will allow a user to ask for help from a technician or a coworker by using a passcorde-protected imitation file

- **Other Remote Access Tools**
    - **Screen-Sharing Software**
        - Type of software that lets you allow somebody else remotely to view what's going on on your screen
        - Screen sharing doesn't have the ability to control what others are seeing on the screen
        - You can use a non-persistent web application in order to be able to do the remote screen-sharing

    - **Video conferencing software do similar functions**

- **File Transfer Software**
  - An important type of software used by technicians to get files to or from a system they're troubleshooting
  - Nearby sharing is Microsoft's version of AirDrop and it works by using Bluetooth and Wi-Fi direct connections between devices
  - For Bluetooth-enabled sharing on Android devices, you'll use a function known as Nearby Share
  - If you're located across the world, you'll have to use a file transfer software like FTP, SFTP, or SSH in order to send those files

- **Desktop Management Software**
  - **Desktop Management Software (Unified Endpoint Management)**
    - Designed for the deployment by an enterprise organization that allows them to understand all the access controls and authorization involved with all of their different systems
    - **UEM** is essentially the desktop or laptop version of MDM
    - Having an agent installed on each and every individual workstation or laptop

  - **Endpoint Detection and Response (EDR)**
    - Allows for the scanning of the desktops and laptops that are being managed by the EDM
    - Gives the ability to use **push deployment techniques** for any upgrades, updates, or security definitions
    - Gives the ability to create **access control rules** that will prevent different workstations from being able to join the network

Troubleshooting Windows

Objective 3.1

- **OBJ 3.1:** Given a scenario, troubleshoot common Windows OS problems

- **Boot Issues**
  - BIOS or UEFI will go through and do a power on self-check to verify that all system components are working properly
    - **BIOS**
      - Master Boot Record
    - **UEFI**
      - GUID Partition Table
  - The firmware will look through the storage device and identify where MBR is, which is always going to be located in the first sector of that disk
  - It will then be able to identify which operating system is supposed to be booted from that master boot record and then turn over control to it
    - bootmgr.exe
    - winload.exe
    - Kernel
    - Hardware abstraction layer
    - Boot device drivers
  - **UEFI boot uses GPT**
    - \EFI\Microsoft\ contains BCD and bootmgfw.efi files
      - Kernel
      - Hardware abstraction layer
      - Boot device drivers
    - Failure to boot
    - No OS found
    - GUI failing to load or a black screen
    - This used to happen because the boot order inside the BIOS or UEFI was set incorrectly
    - Remove any external devices
    - Set the boot order to always go to the internal storage drive first
    - "No OS Found"
    - That disk drive doesn't have an operating system installed

- Use a startup repair tool to open up the recovery command prompt, and then use bootrec in order to be able to repair the drive's boot information
    - bootrec /fixmbr
    - bootrec /fixboot
    - bootrec /rebuildbcd

- **Diskpart Command**
    - A command line disk partitioning tool that can be used to mark the system partition as active
    - It usually indicates that there's some kind of an issue with the graphics driver or the system has some kind of a misconfiguration or corruption
    - Reboot the system into safe mode
    - START+CTRL_SHIFT+B
        - Check Disk command: chkdsk
        - System file checker: sfc
            - Failure to boot
            - No OS found
            - GUI failing to load or a black screen

- **Boot Recovery Tools**
    - Advanced Boot Options
    - Startup Repair
    - WinRE
    - You have a few different options for boot recovery tools, including advanced boot options, startup repair, and the WinRE

- **Update or Driver Rollback**
    - Sometimes system updates may cause problems for your device, and to fix that, we roll back the updates

- **System Restore**
    - System restore allows you to create multiple different points to restore data on your system

- **System Reinstall or Reimage**
  - When you're doing a system restore, you're only restoring the configurations and the files for the system itself
  - In a system reinstall, you're reinstalling a brand new version of Windows, and then you'd have to bring in your files afterwards from a known good backup
  - System Image
    - A snapshot of how a system looks right now, including all personal files, applications, and installations

- **Performance Issues**
  - Your profiles are gonna contain all the information for a particular user on a Windows system

- **System Instability Issues**
  - Memory
  - System files
  - USB devices
  - **System Instability**
    - System freezing, shutting down, failing to respond, rebooting, or powering off without an error message
    - Hardware
      - Overheating, power, processor
    - Software
      - Corrupted kernel files
  - Windows Memory Diagnostic Tool
    - Provides the ability to do memory diagnostics
    - Control panel→Administrative tools
    - Windows recover→Memory diagnostic tool
    - Shut down the computer, take out the memory, and put it back
  - System File Checker (SFC)
    - sfc C:
    - sfc C: /F
    - Use the Windows Update tool or the vendor's website for the latest chipset or system drivers
    - Go to device manager and uninstall the USB host controller device
    - Disable the USB selective suspend power management

        - Powered hub gets its power from the USB, as well as when plugged into a wall outlet
            - Memory
            - System files
            - USB devices

- **Application and Service Issues**
    - Application Crashes
        - Uninstall the program, reboot, and re-install
    - Service Startup Failures
        - Event Viewer
        - Service Tool
            - Manually start the service from the Services Tool
            - Some services are interlinked and work together
            - Two services conflict with each other
            - Core functions inside Windows run as services
            - Use the Registry Server (regsvr32) to register the DLL (dynamic link library)
    - Time drift within the OS
        - CMOS
        - Real-time Clock (RTC)
            - Real-time clock (RTC) is powered by a battery on the motherboard
            - Time drift is an indication that the battery on the motherboard has died
                - Application crashes
                - Service startup failures
                - Time drift within the OS

Troubleshooting Workstation Security

Objective 3.2 and 3.3

- **OBJ 3.2:** Given a scenario, troubleshoot common personal computer (PC) security issues
- **OBJ 3.3:** Given a scenario, use best practice procedures for malware removal

- **Troubleshooting Workstation Security**
  - Software Troubleshooting
    - Investigate and identify malware symptoms
    - Quarantine the infected systems
    - Disable system restore in Windows
    - Remediate the infected system
    - Schedule scans and run updates
    - Enable system restore and create a restore point in Windows
    - Educate the end-user
  - Which is step two in the malware removal process?
    - Schedule scans and run updates

- **Malware Removal Process**
  - **PUA**
    - Potentially Unwanted Application
      - Nmap
      - Netcat
  - Investigate and verify malware symptoms
    - Having a root kit means it has already infected the OS where the anti-malware solution runs
  - Quarantine infected systems
    - Move the system into a logically or physically isolated secure segment of the network
    - Sandbox protects the rest of the systems from getting infected
    - Scan the computer on a trusted system in a sandbox environment
  - Disable system restore in Windows
    - Turn off automated backup systems, such as cloud and external disk backups
  - Remediate infected systems
    - A. Update anti-malware software
    - B. Scanning and removal techniques

- Reboot in safe mode and run the scanning and removal tools
- Run task manager, regedit, and msconfig to turn off different services and background tasks
- Boot the computer using a Windows recovery media disc or a Windows installation disc
- Re-image or re-install the system from a good backup or installation disc

  - Schedule scans and run updates
    - Schedule scans on a daily basis
    - Configuring scanning on access allows to scan downloaded files
  - Enable system restore and create a restore point in Windows
    - Re-enable system restore and create a restore point
      - Restore point after malware removal
      - Restore point clean
    - Turn on automated backups again and validate critical services
  - Educate the end user
    - How to set up and configure a password manager
    - How to verify if a website is actually a website
    - Proper use of social networking and how to tell if something is a scam or trustworthy
    - Educate on the proper use of VPNs
    - Provide anti-phishing training

- **Infected Browser Symptoms**
  - Browser redirection
  - Certificate warnings
    - Redirection happens in conjunction with phishing and pharming
  - Wrong address
    - Manual redirection or typo squatting
  - Automatic redirection
  - Host file infection
    - Host file is what we had before DNS
    - Scan the system, uninstall, and reinstall the browser
    - Check proxy settings and verify no proxy is being used

- **Alerts and Notifications**
  - Stage 1 dropper
  - Stage 2 payload
    - Rogue Antivirus

- **OS Update Failures**
  - Backup
  - System File Checker
    - Turn off the services and run the system file checker to fix it
    - Go through the seven-step malware removal process to remove malware

Troubleshooting Mobile Issues

Objective 3.4

- **OBJ 3.4:** Given a scenario, troubleshoot common mobile OS and application issues

- **Troubleshooting Mobile Issues**
  - Software Troubleshooting

- **Resetting or Rebooting**
  - Many issues can be solved by simply rebooting the device
    - Reboot into safe mode on the Android device
  - Reset
    - Used to remove all of the user's data, applications, and settings
    - After the factory reset is complete, the device will reboot and bring you into a setup menu for you to be able to do an initial configuration
      - Device reset
      - Factory reset

- **Mobile OS Update Failure**
  - Adding new features
  - Fixing vulnerabilities and bugs
    - What can you do to solve this?
      - You may be trying to install an update that isn't available
        - Check what are the minimum requirements for that version of the OS
        - Apple will support devices for about three to five years
        - Always verify the update you're trying to install is compatible with the device model
      - Check if you have enough power to install that update
      - Check your network connectivity
      - The server you're trying to download from can just be really busy
      - You don't have enough storage space available
        - Remove some of your files in order to free up some storage space
        - Make sure you troubleshoot and solve the issue quickly

- **Mobile Performance Issues**
  - The device can either randomly reboot or be slow to respond
    - Overheating
    - Low battery
    - Faulty hardware component
  - The device will actually try to reboot itself
  - The device may just shut itself off and not turn itself back on until the device cools down
  - A faulty piece of hardware can cause the kernel inside of that operating system to panic
  - Use a third-party diagnostic application that can run a report on the hardware to determine if there's any kind of issue
    - Storage space
    - Failed update
    - Faulty app
  - A device that is operating slowly can be caused by different things, including processor throttling
  - The device will slow down first, and then if you don't solve the problem, it will escalate into the device randomly rebooting
  - See how many applications are open, and then close out the ones that are not needed
  - If a code was written in a less efficient way, this can cause applications and programs to run much more slowly
  - Find a different application that does the same function or uninstall that application
  - The device starts to operate slowly, and if it progresses, it can turn into random reboots

- **Mobile App Issues**
  - Applications that fail to launch
  - Applications that fail to close
  - Applications that crash
    - When apps don't launch or operate properly, clear out the cache for those applications
    - Verify the application works on your version of the OS
    - Running out of storage space on your device

        - An application will fail to update if you don't have a valid network connection
        - Delete the application and then re-install it
        - Application issues could sometimes be caused by your company
        - Some mobile device management software can also turn off certain functions or features

- **Mobile Connectivity Issues**
    - Cellular
    - Wi-Fi
    - Bluetooth
    - NFC
    - Wireless file sharing
        - Verify that you have the correct settings for your cellular device
        - Check your network selection
        - Verify that you're not in airplane mode
        - It is important to check that your Wi-Fi is still enabled
        - You'll often get a weaker signal strength when communicating over Wi-Fi on a mobile device
        - Using a thick type of protective case on a smartphone will also reduce the amount of distance that a signal can travel
        - Bluetooth does provide a shorter coverage area
        - Bluetooth can cover between 10 feet and 30 feet of distance
        - Remove the Bluetooth pairing by forgetting that Bluetooth device and then reconnecting to it and re-pairing with it
    - Near-Field Communication (NFC)
        - Very short distance wireless communication technology that only operates within a couple of inches of your device
        - Verify that your airplane mode is not activated
        - Check if airplane mode is enabled
        - Forget that connection and then re-pair with the access point or device that you're trying to communicate with
        - For issues with NFC, simply close the distance and hold the phone there longer
        - Verify that the sender is listed in your recipient's contacts list

- **Mobile Battery Issues**
  - Application configuration is set incorrectly
  - The lower in brightness, the longer the battery lasts
  - Extreme temperature
  - Keep batteries and other electronic devices to 10-38°C
  - Batteries last from 3-5 years
  - Proper charging and discharging of battery
  - Let the battery drain to about 20% before recharging to increase the battery's lifespan
  - Smart charge initiates a slow trickle charge

- **Screen Autorotation Issues**
  - Portrait
  - Landscape
    - Rotation lock is enabled
      - iOS
        - Control center
      - Android
        - Notification drawer
    - User is not touching any other part of the screen
    - Some applications only work in one mode
    - Accelerometer or motion sensor detects which way the phone is held
    - If the sensor stops working, the device will no longer be allowed to autorotate
      - Rotation lock is disabled
      - Check the applications
      - Defective accelerometer or motion sensor

Troubleshooting Mobile Security

Objective 3.5

- **OBJ 3.5:** Given a scenario, troubleshoot common mobile OS and application security issues

- **Rooting and Jailbreaking**
  - **Rooting**
    - Android
  - **Jailbreaking**
    - iOS or iPad OS

  - **Rooting**
    - Allows to get administrative rights on an Android device

    - Android devices are based on Linux
    - Custom firmware gives a new version of the Android OS
    - Custom firmware, or rooting, introduces lots of vulnerabilities
    - Rooting can lead to significant security vulnerabilities

- **Sideloading Apps**
  - **Android**
    - APK
  - **iPhone or iPad**
    - Jailbreaking, Developer tools

  - **APK Sideloading**
    - Installing an application outside of the official store

      - **Settings**
        - Allow third-party applications

    - Sideloading is considered a dangerous practice

  - **Application Spoofing**
    - Occurs when an application passes as a legitimate app

- **Managed Google Play**
  - Android
- **Apple Business Manager**
  - iPhone

  - Third-party app stores have spoofed applications that contain malware
  - Enterprise organizations use sideloading to install applications to access private applications
  - Bootleg application stores have pirated versions of legitimate apps
  - Applications from bootleg app stores usually have malware embedded in them

- **Mobile Malware Symptoms**
  - **High number of ads**
    - Check phone settings and verify that privacy settings are enabled
  - **Fake security warnings**
  - **Slow performance**
    - Crypto Mining
    - Sending Data
  - **Limited network connectivity**
    - Corrupted DNS
    - Redirection attack
    - Proxy installed

  - An on-path attack tries to collect information and see what you see

- **Unexpected Application Behavior**
  - **Bootleg or spoofed application**
  - **High amount of network traffic**
    - DDoS
    - Mass email campaign
    - Cryptomining

- **Leaked Mobile Data**
  - **Leaked Mobile Data**
    - Data from a mobile device going into the public Internet
    - The device is well protected and has an updated OS

- Use long and strong passwords
- Enable two-factor authentication (multifactor authentication)
- Quarantine and investigate as part of an incident response for that data breach
- Check the cloud service and mobile device

Professionalism

Objective 4.7

- **OBJ 4.7:** Given a scenario, use proper communication techniques and professionalism

- **Professionalism**
  - **Learn the best practices for dealing with end-users**
  - **Show up and dress up accordingly**
  - **Avoid distractions**
  - **Based on the rules of the organization**

- **Professional Appearance**
  - **Formal**
    - Gray suit
    - Black suit
    - Navy Blue suit
  - **Business Casual**
    - Khaki pants
    - Polo shirt
    - Button-down shirt
  - **Business formal attire is dressing to impress**
  - **Business professional attire is dressing up but not wearing a full suit**
  - **Business Casual**
    - No need to wear a suit, but you still need to dress up a little bit
  - **Small-business casual is the basic uniform for a tech startup**
    - Small-business casual allows people to be comfortable as long as it is presentable

- **Respect Other's Time**
  1. **Always be on time**
     - Be on time or early to ensure customer is not waiting on you
  2. **Don't waste other people's time**
     - Give customer a timeline and expectation
  3. **Don't get easily distracted**
     - Give customer your full attention

    - Always keep your cellphone in your pocket and do not use it at work unless necessary
4. **Do not interrupt people**
    - When dealing with high-level leaders, work on their schedule
5. **Set expectations and meet those expectations**
    - Set expectations upfront with the customer and give status updates

- **Proper Communication**
    - **Maintain positive attitude and project confidence**
    - **Actively listen and take notes**
    - **Use proper language**
    - **Be culturally sensitive**
    - **Communicate the status**

    - Maintain a positive attitude and make the customer see that you're there to help them
    - Active listening is a skill
        - Open-ended Question
            - Questions that need a valid response
                - "Can you tell me what you saw on your screen before the computer rebooted?"

            - Close-ended Question
                - Questions that are answered with a yes or no, or a simple answer

        - Start with open-ended questions, then follow up with close-ended questions to get final details

    - Use proper language and avoid jargon, acronyms, and slang
        - People from the same country can have different cultural differences
        - Use people's professional titles and treat people with respect and dignity

    - Offer repair or replacement
    - Provide proper documentation
    - Follow up with the customer

        - **Cost**
            - Repair is, what the likely
        - **Timeframe**
            - Repair that option and how long that repair would likely last

    - **Customer Satisfaction (CSAT)**
        - Customer experience metric

- **Dealing with Private Data**
    - **Private Data**
        - End users' confidential and private materials

        - "Is there anything you don't want me to see on this device?"
        - "Is there anything I should stay away from?"

        - Ask if there's anything they don't want you to see
        - Do not open anything that stores confidential or private information
        - Do not use a customer's device for your own personal use
        - Keep the working area clean and tidy

- **Difficult Situations**
    - **Do not personalize the support issues**

    1. **Don't argue with customers**
    2. **Avoid dismissing the customer's problems**
    3. **Avoid being judgmental**
    4. **Clarify customer's statements**
        - Ask open-ended questions
        - Actively listen
    5. **Do not disclose experiences in social media outlets**
        - Do not share experiences on social media