CompTIA Security+ (701) Study Notes

Contents

Summarize Fundamental Security Concepts

Security Concepts

- **Security Concepts Study Notes:**
    1. **Information Security:**
        - Definition: Protection of data resources from unauthorized access, attack, theft, or damage.
        - CIA Triad:
            - Confidentiality: Data accessible only to authorized individuals.
            - Integrity: Data stored and transferred as intended, with authorized modifications.
            - Availability: Information readily accessible to authorized users.
        - Additional Property: Non-repudiation, preventing denial of actions like creating or modifying data.
    2. **Cybersecurity Framework:**
        - Definition: Provisioning secure processing hardware and software.
        - Five Functions (NIST Framework):
            - Identify: Develop security policies, evaluate risks, recommend controls.
            - Protect: Secure IT assets throughout the lifecycle.
            - Detect: Proactive monitoring for new threats.
            - Respond: Analyze, contain, eradicate threats.
            - Recover: Restore systems and data post-attack.
        - Importance: Guides control selection, aids in risk management and compliance.
    3. **Gap Analysis:**
        - Definition: Process identifying deviations from framework requirements.
        - Purpose: Assess current cybersecurity capabilities, prioritize investments for improvement.
        - Components: Outcome-based, identifies missing/poorly configured controls.
        - Utilization: Initial adoption, compliance fulfillment, periodic validation.
        - Involvement: Can engage third-party consultants for complex assessments.
    4. **Access Control:**
        - Definition: Governs interactions between subjects (users/devices) and objects (resources).
        - Components:
            - Identification: Unique representation of users/devices.
            - Authentication: Proving identity, often via passwords or digital certificates.

        - Authorization: Determining and enforcing resource access rights.
        - Accounting: Tracking authorized resource usage and detecting unauthorized attempts.
    - Implementation: Often through Identity and Access Management (IAM) systems.
    - AAA Framework: Alternative terminology for authentication, authorization, and accounting.
5. **Application of Access Control:**
    - E-commerce Example: Enroll users, manage orders, ensure payment integrity, record customer actions for accountability.

Security Controls

- **Security Controls Study Notes:**
    1. **Introduction to Security Controls:**
        - Definition: Measures to ensure information and cybersecurity assurance.
        - Importance: Selecting and implementing appropriate controls for different scenarios.
        - Responsibility: Often falls under the purview of IT departments within organizations.
    2. **Security Control Categories:**
        - Managerial Controls: Oversight of information systems, including risk identification and control selection.
        - Operational Controls: Implemented by people, such as security training programs.
        - Technical Controls: Implemented as hardware, software, or firmware, like firewalls and antivirus software.
        - Physical Controls: Measures like alarms and security cameras to deter and detect physical access.
    3. **Functional Types of Security Controls:**
        - Preventive Controls: Aim to eliminate or reduce the likelihood of successful attacks.
        - Detective Controls: Identify and record attempted or successful intrusions during an attack.
        - Corrective Controls: Reduce the impact of security policy violations after an attack.
        - Additional Types:
            - Directive Controls: Enforce behavioral rules, often through policies or training.
            - Deterrent Controls: Discourage attackers psychologically, such as warning signs.
            - Compensating Controls: Substitute for principal controls to provide equivalent protection.
    4. **Information Security Roles and Responsibilities:**
        - Chief Information Officer (CIO): Overall responsibility for IT and often security.
        - Chief Security Officer (CSO) or Chief Information Security Officer (CISO): Internal security leadership.
        - Managers: Departmental responsibility for security domains.
        - Technical and Specialist Staff: Implement, maintain, and monitor security policies and controls.
        - Nontechnical Staff: Comply with policies and relevant legislation.
    5. **Information Security Competencies:**
        - Skills required for IT professionals with security responsibilities, including risk assessment, system configuration, incident response, and training.

6. **Information Security Business Units:**
    - Security Operations Center (SOC): Monitors and protects critical information assets, typically in larger corporations.
    - DevSecOps: Integration of security expertise into software development and operations processes.
    - Incident Response: Dedicated teams for handling security incidents, either as part of SOC or standalone units.

Compare Threat Types

Threat Actors

- Threat Actors Study Notes:
  Introduction to Vulnerability, Threat, and Risk:
  - Vulnerability: Weakness in security systems that can be exploited.
  - Threat: Potential for exploitation by a threat actor, intentional or unintentional.
  - Risk: Level of hazard posed by vulnerabilities and threats, calculated based on likelihood and impact.

  Attributes of Threat Actors:
  - Internal/External: Degree of access before initiating an attack, either unauthorized (external) or authorized (internal/insider).
  - Level of Sophistication/Capability: Ability to use advanced exploit techniques and tools.
  - Resources/Funding: Support necessary for sophisticated threat actors, often from nation-states or organized crime.
  - Motivations: Reasons for perpetrating attacks, including financial gain, political agendas, or revenge.

  Threat Actor Types:
  - Hackers:
    - Unauthorized (black hat) or authorized (white hat), with varying levels of skill.
    - Increasingly work in teams or groups, known as hacktivist groups, to promote political agendas.
  - Nation-State Actors:
    - Often pursue espionage and disinformation for strategic advantage, with plausible deniability.
    - Known for sophisticated attacks, such as advanced persistent threats (APTs).
  - Organized Crime and Competitors:
    - Focus on financial fraud, blackmail, and extortion, operating across jurisdictions.
    - Competitors may engage in cyber espionage for theft or disruption.
  - Internal Threat Actors:
    - Can be permanent insiders (employees) or temporary insiders (contractors, guests).
    - Motivated by revenge, financial gain, or unintentional actions like poor security practices.
    - Whistleblowers may release information ethically, while unintentional threats arise from lack of awareness or shadow IT.

Motivations and Strategies of Threat Actors:

- Strategies include service disruption, data exfiltration, and disinformation, affecting confidentiality, integrity, and availability.
- Motivations range from chaotic (e.g., causing chaos) to financial (e.g., fraud, extortion) and political (e.g., promoting change or furthering war aims).
- Threat sources and motivations evolve over time, with shifts from opportunistic to structured attacks associated with organized crime and nation-states.

Attack Surfaces

- **Attack Surface and Threat Vectors**:
  - The attack surface refers to all points where a malicious actor could exploit a vulnerability.
  - It includes network ports, applications, computers, and user interactions.
  - Minimizing the attack surface involves restricting access to known endpoints, protocols, and services.
  - Assessment should cover the overall organization as well as specific scopes like servers, web applications, or user identities.
- **Assessing the Attack Surface**:
  - Organizations should evaluate the attributes of threat actors posing the most risk.
  - External threat actors have a smaller attack surface compared to insider threats.
  - Threat vectors represent paths used by threat actors to execute attacks like data exfiltration or service disruption.
  - Sophisticated actors plan multistage campaigns and may develop novel vectors.
- **Vulnerable Software Vectors**:
  - Vulnerabilities in software allow threat actors to exploit flaws in code or design.
  - Patch management is crucial, as almost no software is free from vulnerabilities.
  - Consolidating to fewer products and ensuring consistent versions help reduce the attack surface.
- **Unsupported Systems and Applications**:
  - Unsupported systems lack vendor updates and patches, making them highly vulnerable.
  - Isolating such systems reduces the likelihood of exploitation.
- **Client-Based versus Agentless Scanning**:
  - Scanning software helps identify vulnerabilities, but threat actors can also use it for reconnaissance.
  - Scans can be client-based, requiring installation, or agentless, scanning without installation.
- **Network Vectors**:
  - Vulnerable software allows threat actors to execute code remotely or locally.
  - Remote exploits occur over a network, while local exploits require authenticated access.
  - Securing networks involves ensuring confidentiality, integrity, and availability.
- **Lure-Based Vectors**:
  - Lures, like malicious files, trick users into facilitating attacks.
  - Common lures include removable devices, executable files, document files, and image files.
- **Message-Based Vectors**:
  - Threat actors use messaging systems like email, SMS, IM, web, and social media to deliver malicious files.
  - Social engineering techniques persuade users to open attachments or links.
- **Supply Chain Attack Surface**:

- Threat actors target supply chains to infiltrate organizations indirectly.
- Procurement management ensures reliable sources of equipment and software.
- Establishing a trusted supply chain involves vetting suppliers, vendors, and partners.

Social Engineering

- **Social Engineering Overview**:
  - People within organizations are part of the attack surface and are collectively referred to as the human vector.
  - Social engineering exploits human psychology to manipulate individuals into divulging information or performing actions for threat actors.
- **Human Vectors**:
  - Employees and contractors possess valuable information about networks and security systems, making them potential targets.
  - Social engineering involves eliciting information or actions from individuals, also known as "hacking the human."
  - Examples include tricking users into providing passwords, obtaining sensitive information from help desks, or infiltrating buildings during emergencies.
- **Impersonation and Pretexting**:
  - Impersonation involves pretending to be someone else to gain trust.
  - Threat actors use persuasive or coercive approaches to deceive targets.
  - Pretexting involves crafting convincing stories to charm or intimidate targets, often relying on privileged information about the organization.
- **Phishing and Pharming**:
  - Phishing combines social engineering with spoofing to trick targets into interacting with malicious resources.
  - Phishing emails or messages persuade users to perform actions like installing malware or revealing credentials.
  - Pharming redirects users from legitimate websites to malicious ones by corrupting name resolution processes.
- **Typosquatting and Business Email Compromise**:
  - Typosquatting involves registering domain names similar to legitimate ones to deceive users.
  - Business Email Compromise targets specific individuals within companies, often executives, using sophisticated techniques to deceive and manipulate.
- **Brand Impersonation and Disinformation**:
  - Brand impersonation involves accurately duplicating company logos and formatting to create visually compelling fakes.
  - Disinformation aims to deceive, while misinformation involves repeating false claims unintentionally.
- **Watering Hole Attack**:
  - This attack targets a group of users who frequent an unsecure third-party website, allowing threat actors to compromise their systems through exploit code.

Explain Cryptographic Solutions

Cryptographic Algorithms

- **Cryptographic Concepts**:
  - Cryptography ensures information security by encoding data.
  - Terms: Plaintext (unencrypted), Ciphertext (encrypted), Algorithm (encryption/decryption process), Cryptanalysis (cracking cryptographic systems).
  - Actors: Alice (sender), Bob (recipient), Mallory (malicious attacker).
- **Symmetric Encryption**:
  - Uses a single secret key for both encryption and decryption.
  - Examples: Substitution and transposition algorithms.
  - Key exchange challenge: securely sharing the key.
  - Fast and efficient for bulk encryption but vulnerable if the key is intercepted.
- **Key Length**:
  - Longer keys increase security by expanding the keyspace.
  - Example: AES-128 vs AES-256, where AES-256 has a significantly larger keyspace.
  - Brute force cryptanalysis: attempting decryption with every possible key value.
- **Asymmetric Encryption**:
  - Uses different but related public and private keys for encryption and decryption.
  - Public key can be freely distributed, while the private key must be kept secret.
  - Involves more computing overhead compared to symmetric encryption.
- **Hashing**:
  - Produces fixed-length digest from plaintext, used for integrity verification.
  - Example: Comparing password hashes or verifying file integrity after download.
  - Algorithms: SHA256 (strong) and MD5 (less secure but still used for compatibility).
- **Digital Signatures**:
  - Combines public key cryptography with hashing for authentication, integrity, and non-repudiation.
  - Sender creates a hash of the message and signs it with their private key.
  - Recipient verifies the signature using sender's public key.
- **Standards**:
  - PKCS#1 defines RSA algorithm for digital signatures.
  - DSA and ECDSA are used for digital signatures and were developed as part of FIPS.

Public Key Infrastructure

- **Single CA Model:**
  - Root CA directly issues certificates to users and computers.
  - Often used on private networks.
  - Vulnerable because if compromised, the entire PKI collapses.
- **Third-party CAs:**
  - Operate on a hierarchical model.
  - Root CA issues certificates to intermediate CAs, which in turn issue certificates to end entities.
  - Provides clear certificate policies and certification path (chain of trust).
- **Self-signed Certificates:**
  - Used when PKI management is too difficult or expensive.
  - Deployed on machines, web servers, or program code.
  - Often marked as untrusted by operating systems or browsers.
  - Suitable for non-critical environments like development or testing.
- **Certificate Signing Requests (CSR):**
  - Process for requesting certificates.
  - Subject generates a key pair and submits a CSR to the CA.
  - CA reviews and validates the information before issuing the certificate.
  - Private key is not part of the CSR and must be securely stored by the subject.
- **Subject Name Attributes:**
  - CN attribute deprecated; SAN extension field used to represent identifiers.
  - SAN field more secure for representing FQDNs and IP addresses.
  - It's safer to duplicate FQDN information in CN for compatibility.
- **Certificate Revocation:**
  - Certificates can be revoked or suspended by owner or CA for various reasons.
  - Revoked certificates are no longer valid; suspended certificates can be re-enabled.
  - CA maintains a Certificate Revocation List (CRL) accessible to verify certificate status.
- **Key Management:**
  - Lifecycle stages: generation, storage, revocation, expiration/renewal.
  - Decentralized vs. centralized key management models.
  - Cryptoprocessors offer more secure key generation and storage.
  - Trusted Platform Module (TPM) and Hardware Security Modules (HSM) examples.
- **Key Escrow:**
  - Archiving keys with third-party providers.
  - Mitigates risk of key loss or damage.
  - M of N controls ensure multiple authorizations for key operations.

Cryptographic Solutions

1. **Importance of Cryptographic Solutions:**
    - Cryptographic solutions are essential for implementing security controls.
    - They ensure confidentiality, integrity, and authenticity of data.
    - Used to secure data at rest, in transit, and in use.
2. **Encryption for Confidentiality:**
    - Encryption renders data unreadable to unauthorized parties.
    - Protects data even if storage media is stolen or data is intercepted.
    - Data states: at rest, in transit, in use.
3. **Bulk Encryption vs. Asymmetric Encryption:**
    - Bulk encryption (symmetric cipher) used for large data volumes (e.g., AES).
    - Asymmetric encryption (RSA, ECC) less efficient for bulk encryption.
    - Hybrid approach: symmetric for data encryption, asymmetric for key exchange.
4. **Disk and File Encryption:**
    - Full-disk encryption (FDE) encrypts entire storage device, including metadata.
    - Self-encrypting drives (SEDs) have built-in encryption.
    - Partition-based encryption allows selective encryption for different partitions.
5. **Volume and File Encryption:**
    - Volume encryption secures entire storage resource, implemented in software.
    - File encryption encrypts individual files or folders (e.g., Microsoft's EFS).
6. **Database Encryption:**
    - Encryption at database level (TDE) protects entire database.
    - Record/column-level encryption provides granular protection.
    - Enables separation of duties between administrators and data owners.
7. **Transport Encryption and Key Exchange:**
    - Secures data in motion using protocols like TLS, IPsec, WPA.
    - Key exchange enables secure sharing of symmetric session keys.
    - Integrity and authenticity ensured through HMAC or authenticated encryption.
8. **Perfect Forward Secrecy (PFS):**
    - Uses Diffie-Hellman key agreement to generate session keys.
    - Ensures future compromise of server doesn't compromise past sessions.
    - Increases complexity for attackers, enhances security.
9. **Salting and Key Stretching:**
    - Salting prevents precomputed hash attacks by adding random value to passwords.
    - Key stretching (PBKDF2) increases key length through multiple iterations.
    - Mitigates low-entropy password vulnerabilities.
10. **Blockchain:**
    - Blockchain secures transaction records through cryptographic hashing.
    - Decentralized, distributed ledger ensures transparency and integrity.
    - Applications in finance, contracts, voting, identity management, and more.

11. **Obfuscation:**
    - Obfuscation hides data to make it difficult to find.
    - Uses include steganography, data masking, and tokenization.
    - Protects privacy and enhances security in certain contexts.

Implement Identity and Access Management

Authentication

- **Windows Sign-In Screen:**
  - Personal Identification Number (PIN) is a form of something you know.
  - Modern PINs are not limited to numeric sequences and can be of any length and character combination.
  - They are valid for authenticating to a single device only.
- **Password Concepts:**
  - Improper credential management is a major vector for network attacks.
  - Password best practices policy should instruct users on choosing and maintaining passwords.
  - Credential management policy should cover various authentication methods and educate users on social engineering attacks.
- **Password Policies:**
  - Password Length: Enforces minimum and possibly maximum length for passwords.
  - Password Complexity: Requires a combination of uppercase/lowercase alphanumeric and non-alphanumeric characters.
  - Password Age: Forces users to select a new password after a set number of days.
  - Password Reuse and History: Prevents the selection of previously used passwords.
- **Password Aging and Expiration:**
  - Aging allows logging in with the old password after a defined period but mandates choosing a new password immediately.
  - Expiration disables logging in with the outdated password and effectively disables the account.
- **Password Managers:**
  - Users often use poor credential management practices, such as reusing passwords across multiple sites.
  - Password managers generate random passwords and securely store them, reducing the risk of data breaches.
  - Risks include compromise of the master password or vendor's cloud storage, and impersonation attacks.
- **Multifactor Authentication (MFA):**
  - Combines multiple authentication factors for stronger security.

    - Factors include something you have (like a smart card), something you are (biometrics), and somewhere you are (location-based).
- **Biometric Authentication:**
    - Involves physiological or behavioral identifiers like fingerprints or facial scans.
    - Enrollment includes acquiring a biometric sample and creating a template for comparison.
    - Metrics include False Rejection Rate (FRR), False Acceptance Rate (FAR), and Crossover Error Rate (CER).
- **Hard Authentication Tokens:**
    - Generated within a secure cryptoprocessor, avoiding transmission of the token.
    - Types include Certificate-Based Authentication, One-Time Password (OTP), and FIDO Universal 2nd Factor (U2F).
- **Soft Authentication Tokens:**
    - One-time passwords sent via SMS, email, or authenticator apps.
    - Vulnerable to interception, with authenticator apps offering higher security than SMS or email.
- **Passwordless Authentication:**
    - Entirely eliminates knowledge-based factors like passwords.
    - Relies on factors like biometrics or hardware tokens.
    - Utilizes FIDO2 with WebAuthn specifications for secure authentication without passwords.

Authorization

- **Authorization Overview**:
  - Authorization is a crucial aspect of identity and access management (IAM).
  - It involves assigning privileges to network users and services to manage access to resources effectively.
- **Discretionary Access Control (DAC)**:
  - DAC prioritizes the resource owner's authority.
  - Owners have full control over resources and can modify access control lists (ACLs) to grant rights to others.
  - Widely used but vulnerable to insider threats and abuse of compromised accounts.
- **Mandatory Access Control (MAC)**:
  - Based on security clearance levels rather than individual ownership.
  - Each object is assigned a classification label, and each subject is granted a clearance level.
  - Subjects can access objects classified at their own level or below, ensuring confidentiality.
- **Role-Based Access Control (RBAC)**:
  - Defines permissions based on user roles.
  - Each principal is assigned to one or more roles, and permissions are managed by system owners.
  - Offers flexibility and scalability in permission management.
- **Attribute-Based Access Control (ABAC)**:
  - Utilizes subject and object attributes for access decisions.
  - Factors like location, device status, and user behavior influence access control.
  - Provides fine-grained control over access based on contextual information.
- **Rule-Based Access Control**:
  - Access control policies are enforced by system rules rather than user discretion.
  - Examples include RBAC, ABAC, and MAC.
  - Conditional access systems monitor behavior and enforce access rules dynamically.

- **Least Privilege Principle**:
  - Grants the minimum necessary privileges to perform authorized tasks.
  - Reduces the risk of compromised accounts and limits potential damage.
  - Requires careful analysis of business workflows to determine necessary permissions.
- **User Account Provisioning**:
  - Involves setting up user accounts according to standardized procedures.

    - Includes identity proofing, credential issuance, hardware/software allocation, and policy awareness training.
- **Account Restrictions and Policies**:
    - Location-based and time-based policies restrict account access.
    - Policies enforce authorized login hours, session durations, and geographical constraints.
    - Privileged Access Management (PAM) controls and monitors privileged account usage to prevent compromise.
- **Just-in-Time (JIT) Permissions**:
    - Elevates privileges only when needed for a limited duration.
    - Ensures zero standing privileges (ZSP) to minimize attack surface.
    - Implemented through temporary elevation, password vaulting, or ephemeral credentials.

Identity Management

- Identity Management Exam Objectives:
  - Implementing and maintaining identity and access management.
- Authentication Provider:
  - Essential feature of an OS for user authentication.
  - Relies on cryptographic hashes for knowledge-based authentication.
- Windows Authentication:
  - Local sign-in: LSASS compares credentials to hash in SAM database.
  - Network sign-in: LSASS authenticates via Active Directory using Kerberos or NTLM.
  - Remote sign-in: Authentication over VPN, enterprise Wi-Fi, or web portal.
- Linux Authentication:
  - Local user account info in /etc/passwd, password hash in /etc/shadow.
  - Network login via SSH; can use cryptographic keys.
  - Pluggable Authentication Module (PAM) enables different authentication methods.
- Directory Services:
  - Store info about users, computers, security groups, etc.
  - LDAP is a common protocol for interoperability.
  - Distinguished Name (DN) uniquely identifies resources in a directory.
- Single Sign-on (SSO):
  - Authenticates once, access multiple services without re-entering credentials.
  - Kerberos is a common SSO protocol, authenticates users and services.
- Federation:
  - Extends network access to partners, suppliers, customers.
  - Trusts external networks for authentication and authorization.
- SAML (Security Assertion Markup Language):
  - Protocol for exchanging authentication and authorization data.
  - Uses XML for assertions, HTTP/HTTPS for communication.
- OAuth (Open Authorization):
  - Protocol for sharing user attributes between sites.
  - Allows linking identity to consumer sites without sharing passwords.
  - Uses JSON Web Tokens (JWTs) for claims data, supports various grant type

Secure Enterprise Network Architecture

Enterprise Network Architecture

- Network Addressing:
  - IPv4 addresses use a /24 prefix to define a subnet, written as 255.255.255.0.
  - IPv6 addresses are 128-bit and hierarchical, with the last 64 bits representing the host's interface ID.
- Logical Addressing and Access Control:
  - Hierarchical network architecture assigns separate IP subnets to access blocks, facilitating access control.
  - Each access block is allocated a subnet, ensuring logical separation (e.g., guest network vs. enterprise LAN).
- VLANs (Virtual LANs):
  - VLANs segment networks into separate broadcast domains.
  - VLAN IDs (2 to 4,094) are assigned to switches, enabling different ports on the same switch to belong to different VLANs.
- Security Zones:
  - Internal security topology based on network segmentation and access control.
  - Different zones for different levels of trust and access control requirements.
- Attack Surface:
  - Points of vulnerability at different network layers (1/2, 3, 4/7).
  - External and internal attack surfaces require different security controls.
- Port Security:
  - Measures to control physical access to network ports.
  - Methods include MAC filtering, MAC limiting, and IEEE 802.1X authentication.
- Physical Isolation:
  - Critical hosts isolated from networks for security.
  - Challenges include management and restricted access.
- Architecture Considerations:
  - Factors include costs, scalability, availability, resilience, power usage, patch availability, and risk transference.

Network Security Appliances

- **Packet Filtering Firewall**:
  - Stateless firewall: Does not preserve information about network sessions.
  - Analyzes each packet independently without record of previous packets.
  - Vulnerable to attacks spread over multiple packets.
  - Can introduce traffic flow problems, especially with load balancing or dynamically assigned ports.
- **Stateful Inspection Firewall**:
  - Tracks information about established sessions between hosts.
  - Incorporates stateful inspection capability, storing session data in a state table.
  - Checks incoming packets against existing connections in the state table.
  - Once a connection is allowed, traffic usually passes unmonitored to conserve processing effort.
  - Can occur at layer 4 and layer 7.
- **Layer 4 Firewall**:
  - Examines the TCP three-way handshake to distinguish new from established connections.
  - Tracks legitimate TCP connections following SYN > SYN/ACK > ACK sequence.
  - Can detect anomalies like SYN without ACK or sequence number anomalies.
  - Capable of tracking UDP traffic and detecting IP header and ICMP anomalies.
- **Layer 7 Firewall**:
  - Inspects headers and payload of application-layer packets.
  - Verifies application protocol matches the port to prevent malicious data transfer.
  - Can analyze HTTP headers and webpage formatting code to identify threats.
  - Also known as application-aware firewalls or deep packet inspection.
- **Proxy Servers**:
  - Perform application layer filtering and operate on a store-and-forward model.
  - Deconstruct packets, perform analysis, and rebuild packets according to rules.
  - Can be non-transparent (client must be configured) or transparent (intercepts traffic without client reconfiguration).
- **Forward Proxy Servers**:
  - Provide outbound traffic filtering and enable client connections to external resources like websites.
  - Offer traffic management, security, and caching benefits.
- **Reverse Proxy Servers**:
  - Provide inbound traffic filtering and are typically deployed on the network edge.
  - Listen for client requests from the public network, filter, and forward requests to application servers.
- **Intrusion Detection Systems (IDS)**:
  - Perform real-time analysis of network traffic or system/application logs.
  - Utilize sensors to capture traffic data, which is then analyzed by IDS software.
  - Raise alerts or generate log entries for detected threats but do not actively block traffic.

- **Intrusion Prevention Systems (IPS)**:
  - Capable of active response to detected threats, including blocking noncompliant traffic, resetting connections, or redirecting traffic for further analysis.
- **Next-Generation Firewalls (NGFW) and Unified Threat Management (UTM)**:
  - NGFW incorporates intrusion detection functionalities into firewall systems.
  - UTM centralizes various security controls into a single appliance for comprehensive security management.
- **Load Balancers**:
  - Distribute client requests across server nodes to optimize resource usage, provide fault tolerance, and mitigate denial of service attacks.
  - Can be Layer 4 (IP and port-based) or Layer 7 (application-aware) load balancers.
  - Employ scheduling algorithms and health checks to manage traffic distribution effectively.
- **Web Application Firewalls (WAF)**:
  - Designed to protect web servers and back-end databases from code injection and denial of service attacks.
  - Use application-aware processing rules and pattern matching to filter traffic and detect threats.
  - Can be deployed as appliances or plug-in software for web server platforms.

Secure Communications

- **VPN Topologies**:
  - Remote Access VPN: Initiated by the client.
  - Site-to-Site VPN: Configured to operate automatically, connecting two or more private networks.
  - Host-to-Host Tunnel: Securing traffic between two computers on an untrusted private network.
- **VPN Protocols**:
  - Legacy Protocols: Deprecated due to inadequate security (e.g., PPTP).
  - Modern Protocols: TLS and IPsec preferred for VPN access.
- **Transport Layer Security (TLS) Tunneling**:
  - Mutual authentication using digital certificates.
  - TLS creates an encrypted tunnel for user authentication and data transmission.
- **Internet Protocol Security (IPsec) Tunneling**:
  - Operates at OSI layer 3 (network layer).
  - Core Protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP).
  - Modes: Transport mode for host-to-host, tunnel mode for site-to-site VPNs.
- **Internet Key Exchange (IKE)**:
  - Establishes security associations (SA) for IPsec.
  - Negotiations in two phases for key agreement and cipher selection.
- **Remote Desktop**:
  - Remote access to private networks via secure tunnel over public networks.
  - Includes graphical and terminal server access methods.
  - Examples: Microsoft's Remote Desktop Protocol (RDP), TeamViewer, Virtual Network Computing (VNC).
- **Secure Shell (SSH)**:
  - Provides secure remote access to command line terminal.
  - Authentication methods: Username/password, public key, Kerberos.
- **Out-of-Band Management and Jump Servers**:
  - OOB management ensures separate network for administrative access.
  - Jump servers provide controlled access to administrative interfaces on hosts in secure zones.
  - Enhances security by limiting direct access to administrative interfaces.

Secure Cloud Network Architecture

Cloud Infrastructure

- **Containerization:**
  - Enforces resource separation at the operating system level.
  - Defines isolated "cells" for each user instance to run in.
  - Allocated CPU and memory resources for each container.
  - Processes run through the native OS kernel.
  - Containers may run slightly different OS distributions.
  - Docker is a well-known container virtualization product.
  - Supports microservices and serverless architecture.
  - Used in implementing corporate workspaces on mobile devices.

- **Serverless Computing:**
  - Cloud provider manages infrastructure and allocates resources automatically.
  - Charges only for actual usage of the application.
  - Examples include chatbots, mobile backends, IoT services.
  - Major providers include AWS, Microsoft Azure, Google Cloud.
  - Provides scalable, cost-effective infrastructure for event-driven tasks.
- **Microservices:**
  - Collection of small, independent services focusing on specific business capabilities.
  - Modular design with well-defined interfaces.
  - Allows efficient development and deployment of complex applications.
  - Enables teams to work independently on different features.
  - Promises agility, scalability, and resilience.
  - Risks include integration issues and complexity.

- **Infrastructure as Code (IaC):**
  - Manages computing infrastructure using machine-readable definition files.
  - YAML, JSON, and HCL formats are common.
  - Automates deployment and management of infrastructure.
  - Ensures consistency and repeatability across environments.
  - Implemented using tools like Terraform.
- **Load Balancing, Edge Computing, Auto-Scaling:**
  - Load balancing distributes network traffic to improve performance and availability.
  - Edge computing optimizes processing location for reduced latency.
  - Auto-scaling adjusts resources based on demand dynamically.

- **Software Defined Networking (SDN):**
  - Abstract model divides network functions into control, data, and management planes.
  - SDN applications define policy decisions on the control plane.
  - Implemented through APIs interfacing with network devices.
  - Manages both physical and virtual network appliances.
  - Supports rapid deployment of virtual networking using NFV.
- **Cloud Architecture Features:**
  - Data replication, redundancy, and auto-scaling ensure high availability.
  - Disaster recovery, SLAs, and ISAs are critical for data protection.
  - Power efficiency, compute capabilities, and ease of deployment enhance cloud infrastructure.
- **Cloud Security Considerations:**
  - Data protection, patch management, and secure communication are essential.
  - SD-WAN and SASE provide enhanced security features for cloud environments.
  - Zero trust security model and IAM are crucial for secure access.

Embedded Systems and Zero Trust Architecture

- **SCADA Overview**:
  - SCADA replaces control servers in large-scale ICSs.
  - Typically runs as software on ordinary computers.
  - Gathers data from and manages plant devices with embedded PLCs (field devices).
  - Uses WAN communications like cellular or satellite to link to field devices.
- **Applications of ICS/SCADA**:
  - Used in energy (power generation, distribution), industrial (mining, refining), fabrication/manufacturing, logistics, and facilities management.
  - Historically built without strong IT security, but awareness of security importance is increasing.
- **Security Concerns in ICS/SCADA**:
  - Vulnerable to cyberattacks.
  - Example: Stuxnet worm targeting Iran's nuclear program.
  - NIST Special Publication 800-82 provides security control recommendations.
- **Priorities in Industrial Systems**:
  - Safety is paramount.
  - Prioritize availability and integrity over confidentiality (AIC triad instead of CIA triad).
- **Cybersecurity in ICS/SCADA**:
  - Critical for sectors like energy, manufacturing, transportation, and water treatment.
  - Robust cybersecurity measures like network segmentation, access controls, intrusion detection, and encryption are essential.
- **Internet of Things (IoT)**:
  - Refers to networked physical devices with sensors and connectivity.
  - Used in various sectors like smart homes, smart cities, healthcare, agriculture, etc.
  - Factors driving adoption include decreased sensor costs, advances in connectivity tech, and the COVID-19 pandemic.
- **Security Risks Associated with IoT**:
  - Many devices lack adequate security measures.
  - Standardization issues make security implementation challenging.
  - Large volume of data increases the risk of breaches and cyberattacks.
- **Best Practices for IoT Security**:

    - Recommendations from organizations like IoTSF, IIC, CSA, and ETSI.
- **Zero Trust Architecture (ZTA)**:
    - Assumes nothing is trusted by default.
    - Requires continuous authentication and verification for all users, devices, and applications.
    - NIST SP 800-207 defines ZTA and CISA provides a maturity model.
- **Deperimeterization**:
    - Shifts focus from defending network boundaries to protecting individual resources.
    - Essential due to trends like cloud adoption, remote work, mobile devices, outsourcing, and wireless networks.
- **Key Components of Zero Trust Architecture**:
    - Network and endpoint security, IAM, policy-based enforcement, cloud security, network visibility, network segmentation, data protection, and threat detection/prevention.

- **Zero Trust Security Concepts**:
    - Adaptive identity, threat scope reduction, policy-driven access control, and device posture assessment.
- **Control and Data Planes in Zero Trust Models**:
    - Control plane manages policies, while data plane establishes secure sessions.
    - Separation allows for flexibility and scalability.
- **Zero Trust Architecture Examples**:
    - Google BeyondCorp, DoD's JEDI cloud, Cisco Zero Trust Architecture, Palo Alto Networks Prisma Access.

Explain Resiliency and Site Security Concepts

Asset Management

Monitoring and Asset Tracking:

- Inventory and enumeration tasks involve creating and maintaining a comprehensive list of all assets within an organization, including hardware, software, data, and network equipment.
- Regularly updating and verifying asset inventory helps organizations manage assets effectively and ensures accurate information about each asset's location, owner, and status.
- Asset monitoring includes tracking performance, security, and usage to detect potential issues, vulnerabilities, or unauthorized access promptly.
- Proactive asset monitoring helps mitigate risks, optimize resource utilization, and ensure compliance with regulatory requirements.

Ways to Perform Asset Enumeration:

- Manual Inventory: Feasible for smaller organizations or specific asset types, involves physically inspecting assets and recording relevant information.
- Network Scanning: Tools like Nmap, Nessus, or OpenVAS automatically discover and enumerate networked devices, including open ports and services.
- Asset Management Software: Solutions like Lansweeper or ManageEngine automatically discover, track, and catalog various assets, providing a centralized dashboard for management.
- Configuration Management Database (CMDB): Centralized repository for IT infrastructure information, managed by tools like ServiceNow or BMC Remedy.
- Mobile Device Management (MDM) Solutions: Manage mobile assets like smartphones and tablets using solutions like Microsoft Intune or VMware Workspace ONE.
- Cloud Asset Discovery: Cloud-native or third-party tools like AWS Config or CloudAware help discover and catalog assets deployed in the cloud.

Asset Acquisition/Procurement:

- Select hardware and software solutions with strong security features, prioritize reputable vendors providing ongoing support.
- Integrate solutions seamlessly with existing security infrastructure like firewalls, intrusion detection systems, or SIEM platforms.
- Assess total cost of ownership (TCO) considering initial purchase price, ongoing costs, and potential security incidents.
- Prioritize cybersecurity during acquisition to reduce breach risk, enhance compliance, and protect critical data and systems.

Asset Protection Concepts:

- Assets include critical resources, information, and infrastructure components that must be protected from threats and unauthorized access.
- Identify and prioritize assets based on sensitivity and potential impact on core functions if breached.
- Use standard naming conventions and configuration management to ensure consistency and manageability.
- Implement ITIL framework elements for effective configuration management.

Data Backups:

- Essential for ensuring availability and integrity of critical data and systems.
- Regularly test and verify backup data to ensure reliability of recovery process.
- Enterprise backup solutions offer scalability, performance, advanced features like data encryption and ransomware protection, and integration with various environments.

Snapshot, Replication, and Journaling:

- Snapshots capture system state at a specific time, useful for VMs, filesystems, and SANs.
- Replication creates redundant copies of data for availability and recovery.
- Journaling tracks changes to data for recovery and consistency, useful for filesystems.
- Advanced techniques like remote journaling, SAN replication, and VM replication enhance data protection across multiple locations and systems.

Encrypting Backups:

- Adds an extra layer of protection against unauthorized access or theft.
- Ensures compliance with regulations regarding sensitive data protection.
- Essential for safeguarding sensitive customer data, intellectual property, or trade secrets.

Secure Data Destruction and Asset Disposal:

- Sanitization and destruction processes remove sensitive information from storage media to prevent unauthorized access.

- Certification provides verification of data destruction process compliance with industry standards and regulations.
- Active methods like overwriting or physical destruction ensure irrecoverability of data from storage devices.
- Proper disposal of assets at the end of lifecycle or when no longer needed minimizes security risks and ensures compliance.

Redundancy Strategies

- **Site Considerations**
  - **Resiliency Provisioning**: Site-level resiliency is common in enterprise environments.
  - **Alternate Processing Site**: Provides similar service levels and can be always available.
  - **Recovery Site**: Used in emergencies, might take longer to set up.
  - **Failover**: Technique ensuring redundancy, quickly taking over functionality from a failed asset.
  - **Site Resiliency Levels**:
    - Hot Site: Immediate failover, fully operational and updated.
    - Warm Site: Similar to hot site but requires loading latest data set.
    - Cold Site: Longer setup time, may be empty building with lease agreement.
  - **Geographic Dispersion**: Distributing recovery sites across different locations to minimize regional disaster impact.
- **Cloud as Disaster Recovery (DR)**
  - **Cost Efficiency**: Cloud providers offer affordable redundancy due to economies of scale.
  - **Scalability**: Cloud services allow redundant capabilities without over-provisioning.
  - **Faster Deployment**: Enables quick setup and deployment of redundant systems.
  - **Simplified Management**: Cloud providers offer tools to reduce redundant infrastructure complexity.
  - **Improved Security and Compliance**: Cloud providers invest heavily in security and compliance.
- **Testing Redundancy and High Availability**
  - **Load Testing**: Validates system performance under expected or peak loads.
  - **Failover Testing**: Validates seamless transition between primary and secondary infrastructure.

    - **Monitoring Systems Testing**: Validates effective detection and response to failures and performance issues.
- **Clustering**
    - **Load Balancing vs. Clustering**: Load balancing distributes traffic, while clustering allows redundant processing nodes to accept connections.
    - **Active/Passive vs. Active/Active Clustering**: Active/passive ensures no performance impact during failover, while active/active utilizes maximum capacity but may degrade performance during failover.
- **Power Redundancy**
    - **Dual Power Supplies**: Provide redundancy, can be replaced without system shutdown.
    - **Managed Power Distribution Units (PDUs)**: Support remote power monitoring and integrate with UPSs.
    - **Battery Backups and UPSs**: Provide temporary power source during outages.
    - **Generators**: Provide backup power for extended periods.
- **Diversity and Defense in Depth**
    - **Platform Diversity**: Reduces risk by using multiple technologies and platforms.
    - **Defense in Depth**: Implements multiple layers of protection against cyber threats.
- **Vendor Diversity**
    - **Cybersecurity Benefits**: Reduces single point of failure and promotes healthy competition.
    - **Business Resilience**: Mitigates risk associated with vendor lock-in and disruptions.
    - **Innovation and Competition**: Encourages innovation and ensures better value for investments.
- **Multi-Cloud Strategies**
    - **Cybersecurity Benefits**: Diversifies risk, improves security posture, and promotes vendor independence.
    - **Business Benefits**: Enhances flexibility, agility, and cost efficiency.
- **Deception Technologies**
    - **Honeypots, Honeynets, Honeyfiles, and Honeytokens**: Cybersecurity tools to detect and defend against attacks by diverting attackers' attention and gathering intelligence.
- **Disruption Strategies**
    - **Active Defense**: Uses tactics like bogus DNS entries, web server decoys, and fake telemetry to raise attack cost and tie up adversary's resources.
- **Testing Resiliency**
    - **Method of Testing**: Tabletop exercises, failover tests, simulations, and parallel processing tests.
    - **Importance of Testing**: Identifies vulnerabilities, evaluates recovery strategies, and improves preparedness for real-life incidents.
- **Documentation**

- **Business Continuity Documentation**: Covers planning, implementation, and evaluation.
- **Test Plans, Scripts, and Results**: Provide structure for testing process and communication with stakeholders.
- **Third-Party Assessments and Certifications**: Offer objective evaluation, compliance verification, and recommendations for improvement.

Physical Security

1. **Fundamental Security Concepts:**
   - Physical security is integral to cybersecurity, protecting physical assets like servers and data centers.
   - Measures include access control, surveillance, and environmental controls.
   - Effective physical security reduces the risk of unauthorized access and insider threats.
2. **Physical Security Controls:**
   - Access control mechanisms include biometric scanners, smart cards, and key fobs.
   - Surveillance systems involve video cameras, motion sensors, and alarms.
   - Environmental controls like backup power and fire suppression are crucial for data centers.
3. **Zone Implementation:**
   - Zones use barriers and security mechanisms to control entry and exit points.
   - Each zone should have increasingly restrictive access.
   - Entry points to secure zones should be discreet to prevent inspection by intruders.
4. **Physical Security through Environmental Design:**
   - Enhances security using non-obvious features in physical spaces.
   - Promotes safety and deters criminal activity in various settings.
5. **Barricades, Fencing, and Lighting:**
   - Barricades channel people through defined entry and exit points.
   - Security fencing needs to be transparent, robust, and secure against climbing.
   - Security lighting improves safety and acts as a deterrent at night.
6. **Bollards and Existing Structures:**
   - Bollards prevent vehicular access to restricted areas.

    - Existing structures can be adjusted for improved site layout and security.
7. **Gateways, Locks, and Access Control:**
    - Gateways require secure locks, which can be physical, electronic, or biometric.
    - Access control vestibules regulate entry to secure areas, preventing tailgating.
    - Access badges replace physical keys and provide access through card readers.
8. **Security Guards and Cameras:**
    - Surveillance enhances resilience, with guards providing visual deterrence.
    - Cameras offer cost-effective monitoring and can use AI for smart security.
    - Alarms supplement other security controls, detecting and deterring threats effectively.

Explain Vulnerability Management

Device and OS Vulnerabilities

1. **Mobile OS Vulnerabilities:**
    - Android and iOS are primary computing platforms, prone to attacks.
    - Android's open-source nature leads to similar benefits and problems as Linux.
    - Fragmentation among manufacturers and versions of Android results in inconsistent patching.
    - iOS, though not open source, faces significant vulnerabilities.
2. **Example OS Vulnerabilities:**
    - Microsoft Windows: MS08-067 and MS17-010 allowed remote code execution, exploited by Conficker and WannaCry.
    - macOS: "Shellshock" vulnerability in Unix-based systems.
    - Android: "Stagefright" vulnerability allowed remote code execution via MMS.
    - iOS: Google's Project Zero discovered vulnerabilities used in "watering hole" attacks.
    - Linux: "Heartbleed" bug compromised OpenSSL cryptographic software.
3. **Legacy and End-of-Life Systems:**
    - EOL systems lack vendor support and critical security patches, posing vulnerabilities.
    - Legacy systems are outdated but may still receive support.
    - Notable examples include Windows 7 and Server 2008.
4. **Firmware Vulnerabilities:**
    - Meltdown and Spectre vulnerabilities impacted computers and mobile devices.
    - "LoJax" exploited UEFI firmware.

    - EOL hardware vulnerabilities arise from discontinued updates.
5. **Virtualization Vulnerabilities:**
    - VM escape allows attackers to access host systems.
    - Examples include "Cloudburst" vulnerability in VMware.
    - Resource reuse can lead to data leakage between virtual machines.
6. **Zero-Day Vulnerabilities:**
    - Previously unknown flaws exploited before developers can fix them.
    - Notable examples include the BEAST and POODLE attacks.
    - Ethical disclosure aims to limit potential harm.
7. **Misconfiguration Vulnerabilities:**
    - Common cause of security vulnerabilities.
    - Default configurations often prioritize usability over security.
    - Proper configuration and change management are crucial.
8. **Cryptographic Vulnerabilities:**
    - Weaknesses in cryptographic systems, algorithms, or protocols.
    - Examples include MD5, SHA-1, and RSA vulnerabilities.
    - Proper key generation and protection are essential.
9. **Sideloading, Rooting, and Jailbreaking:**
    - Methods to gain elevated privileges on mobile devices.
    - Introduces security risks, including malware installation and data breaches.
    - Violates terms of service and voids warranties on some platforms.
10. **Mobile Device Vulnerabilities:**

- Susceptible to common vulnerabilities like insecure Wi-Fi and phishing attacks.
- More likely to be lost or stolen, exposing data if unencrypted.

Application and Cloud Vulnerabilities

- **Malicious Update:**
  - Definition: Update containing harmful code disguised as legitimate.
  - Purpose: Distribution of malware, execution of cyberattacks.
  - Examples: CCleaner compromise (2017), SolarWinds attack (2020).
  - Mitigation: Secure software supply chain management, digital signature verification.
- **Evaluation Scope:**
  - Definition: Analysis of product, system, or service for vulnerabilities.
  - Targets: Software application, network, security service, or IT infrastructure.
  - Goals: Identify weaknesses, ensure compliance with security standards.
- **TOE Practice Description:**
  - Security Testing: Vulnerability assessments, penetration testing.
  - Documentation Review: Ensure implementation according to secure design principles.
  - Source Code Analysis: Identify security vulnerabilities in code.
  - Configuration Assessment: Evaluate security-related configurations.
  - Cryptographic Analysis: Assess encryption mechanisms and key management.
  - Compliance Verification: Ensure compliance with relevant regulations.
  - Security Architecture Review: Evaluate security controls and design.
- **Penetration Tester vs. Attacker:**
  - Scope: Defines objectives for penetration tester or attacker.
  - Penetration Tester: Authorized to evaluate system, report findings, recommend remediation.

- Attacker: Aims to exploit vulnerabilities within target for unauthorized access or other malicious objectives.

- **Web Application Attacks:**
  - Definition: Target applications accessible over the Internet.
  - Characteristics: Exploit poor input validation, misconfigured security settings, outdated software.
  - Examples: XSS, CSRF, improper session management.
- **Cross-Site Scripting (XSS):**
  - Types: Reflected/nonpersistent, stored/persistent, DOM-based.
  - Execution: Injects malicious scripts into trusted sites, executed in client's browser.
- **SQL Injection (SQLi):**
  - Exploits: Unsecure handling of SQL queries.
  - Impact: Unauthorized access to database, data theft, execution of arbitrary code.
- **Cloud-Based Application Attacks:**
  - Targets: Cloud-hosted applications.
  - Exploits: Misconfigurations, weak authentication, insufficient network segmentation.
  - Characteristics: Shared responsibility model, scalability attracts attackers.
- **Cloud Access Security Brokers (CASBs):**
  - Definition: Mediate access to cloud services by users.
  - Functions: Single sign-on authentication, malware scanning, activity monitoring.
  - Implementation: Forward proxy, reverse proxy, API-based.
- **Supply Chain:**
  - Definition: Risks and weaknesses introduced into software products during development, distribution, maintenance.
  - Components: Service providers, hardware suppliers, software providers.
  - Importance: Transparency, visibility, rapid response to vulnerabilities.
  - Tools: OWASP Dependency-Check, SPDX, OWASP CycloneDX standards for SBOM creation.

Vulnerability Identification Methods

- **Network Vulnerability Scanner**
  - Designed to test network hosts such as client PCs, servers, routers, and switches.
  - Compares scan results to configuration templates and lists of known vulnerabilities.
  - Identifies missing patches, deviations from baseline configurations, and related vulnerabilities.
  - Examples include Tenable Nessus and OpenVAS.
- **Credentialed vs. Non-Credentialed Scans**
  - **Non-Credentialed Scans:**
    - Test packets directed at hosts without login access.
    - View obtained is that of an unprivileged user.
    - Useful for external network perimeter assessment or web application scanning.
  - **Credentialed Scans:**
    - Given user account access with appropriate permissions.
    - Allows in-depth analysis, especially for detecting misconfigurations.
    - Mimics insider attacks or compromised user accounts.
- **Application and Web Application Scanners**
  - Specialized for identifying software application weaknesses.
  - Includes static analysis (reviewing code) and dynamic analysis (testing running applications).

- Identifies issues like unvalidated inputs, broken access controls, and SQL injection vulnerabilities.

- **Package Monitoring**
  - Tracks and assesses security of third-party software packages, libraries, and dependencies.
  - Ensures they are up to date and free from known vulnerabilities.
  - Associated with software bill of materials (SBOM) and software supply chain risk management.
- **Threat Feeds**
  - Real-time, continuously updated sources of information about potential threats and vulnerabilities.
  - Integrated into vulnerability management practices for swift response to emerging risks.
  - Gathered from security vendors, cybersecurity organizations, and open-source intelligence.
- **Open-Source Intelligence (OSINT)**
  - Collects and analyzes publicly available information for decision-making.
  - Used in cybersecurity to identify vulnerabilities and threat information.
  - Sources include blogs, forums, social media, and the dark web.
- **Penetration Testing**
  - Aggressive approach to vulnerability management.
  - Involves ethical hacking to breach security and exploit vulnerabilities.
  - Identifies complex vulnerabilities that automated tools may miss.
- **Bug Bounties**
  - Incentivizes external security researchers to discover and report vulnerabilities.
  - Complements penetration testing with a global community of researchers.
  - Encourages responsible disclosure of verified security issues.
- **Auditing**
  - Essential part of vulnerability management.
  - Includes product audits, system/process audits, and security audits.
  - Penetration testing is a critical component of technical and compliance audits.

Vulnerability Analysis and Remediation

Vulnerability Analysis and Remediation

- **Vulnerability Analysis**:
  - Evaluates vulnerabilities for potential impact and exploitability.
  - Considers factors like ease of exploitation, potential damage, asset value, and current threat landscape.
  - Helps prioritize remediation efforts by addressing critical vulnerabilities first.
- **Remediation**:
  - Mitigation techniques include patching, configuration changes, software updates, or system replacement.
  - Compensating controls provide alternative plans when immediate remediation is impossible.
  - Verification of successful remediation via rescanning affected systems.

Common Vulnerabilities and Exposures (CVE)

- **Vulnerability Feeds**:
  - Updated via SCAP, facilitating sharing of intelligence data.
  - Consist of common identifiers for vulnerability descriptions.
- **National Vulnerability Database (NVD)**:
  - Maintained by NIST, provides detailed vulnerability information.

    - Supplements CVE descriptions with additional analysis and CVSS metrics.
- **CVSS (Common Vulnerability Scoring System)**:
    - Generates a score from 0 to 10 based on vulnerability characteristics.
    - Score bands: 0.1+ (Low), 4.0+ (Medium), 7.0+ (High), 9.0+ (Critical).

False Positives, False Negatives, and Log Review

- **False Positives**:
    - Incorrect identification of vulnerabilities by scanners.
    - Can lead to unnecessary time and effort if not addressed.
- **False Negatives**:
    - Undetected vulnerabilities in scans.
    - Risk mitigated by periodic rescanning and using scanners from different vendors.
- **Log Review**:
    - Validates vulnerability reports by examining system and network logs.
    - Confirms vulnerability alerts and ensures accurate remediation.

Vulnerability Analysis

- **Prioritization**:
    - Identifies critical vulnerabilities for focused remediation efforts.
- **Classification**:
    - Categorizes vulnerabilities based on characteristics for clarity.
- **Exposure Factor**:
    - Assesses susceptibility of assets to specific vulnerabilities.
- **Impacts**:
    - Evaluates potential organizational impact for informed decision-making.
- **Environmental Variables**:
    - Includes IT infrastructure, external threat landscape, regulatory environment, and operational practices.

Vulnerability Response and Remediation

- **Remediation Practices**:
    - Patching, cybersecurity insurance, segmentation, compensating controls, exceptions, and exemptions.
- **Validation**:
    - Ensures remediation actions are implemented correctly and do not introduce new vulnerabilities.
- **Reporting**:
    - Highlights existing vulnerabilities, ranks based on severity, provides recommendations, and emphasizes timely reporting for effective remediation.

Evaluate Network Security Capabilities

Network Security Baselines

Hardening Concepts:

- Default settings in network equipment, software, and operating systems balance ease of use with security.
- Default configurations are often targeted by attackers due to well-documented credentials, insecure protocols, etc.
- Hardening involves changing default settings to enhance security, typically following published secure baselines.

Switches and Routers Hardening:

- Change default credentials to mitigate security risks.
- Disable unnecessary services like HTTP or Telnet to reduce attack surface.
- Use secure management protocols like SSH instead of Telnet.
- Implement Access Control Lists (ACLs) to restrict access.
- Enable logging and monitoring to identify security issues.

- Configure port security to limit device connections.
- Implement strong password policies.
- Physically secure equipment to prevent unauthorized access.

Server Hardware and Operating Systems Hardening:

- Change default credentials to prevent unauthorized access.
- Disable unnecessary services to reduce attack surface.
- Apply software security patches and updates regularly.
- Implement the least privilege principle.
- Use firewalls and Intrusion Detection Systems (IDS) to block or alert on malicious activity.
- Secure configurations using baseline configurations like CIS or STIGs.
- Implement strong access controls like strong password policies, MFA, and PAM.
- Enable logging and monitoring for identifying security issues.
- Use antivirus and antimalware solutions to detect and quarantine malware.
- Physically secure server equipment to prevent unauthorized access.

Wireless Network Installation Considerations:

- Ensure good coverage of authorized Wi-Fi access points to prevent rogue and evil twin attacks.
- Use nonoverlapping channels in the 5 GHz band for better performance.
- Conduct site surveys to measure signal strength and interference.
- Use heat maps to optimize WAP placement and configuration.
- Configure wireless encryption settings to secure the network.
- Consider vulnerabilities and limitations of Wi-Fi Protected Setup (WPS).
- Utilize Wi-Fi Protected Access 3 (WPA3) for improved security.

Wi-Fi Authentication Methods:

- Personal, open, and enterprise authentication types.
- WPA2-PSK and WPA3-SAE for personal authentication.
- WPA3 enhances security over WPA2, particularly with SAE protocol.
- Enterprise authentication involves 802.1x, EAP methods, and RADIUS.

Network Access Control (NAC):

- Authenticates users and devices, enforces compliance with security policies.
- Restricts access based on user profile, device type, location, etc.
- Works with VLANs to automate security measures.
- NAC can be agent-based or agentless, each with its advantages and limitations.

Network Security Capability Enhancement

Network Security Capability Enhancement:

- Firewalls, IDS, IPS, and web filters are essential components in network security.
- Firewalls create a barrier between trusted internal networks and untrusted external networks, controlling incoming and outgoing traffic based on rules.
- IDS monitor network traffic for possible incidents and alert administrators.
- IPS not only detect but also prevent threats by taking automated actions like blocking traffic.
- Web filters control access to Internet content, preventing access to malicious websites and monitoring access to restricted sites.

Access Control Lists (ACL):

- ACLs control traffic at a network interface level using packet information like source/destination IP addresses, port numbers, and protocols.
- Firewall rules dictate how firewalls handle inbound/outbound traffic based on IP addresses, port numbers, protocols, or application traffic patterns.

- Rules in a firewall's ACL are processed from top to bottom; specific rules are placed at the top, and a default deny rule is typically at the end.
- Basic principles include blocking internal/private IP addresses, protocols for local network level, penetration testing, and securing hardware.

Screened Subnet:

- Acts as a neutral zone between an organization's internal network and the Internet, separating public-facing servers from sensitive internal resources.
- Hosts web, email, DNS, or FTP services accessible from the Internet but isolated from internal systems to limit damage from breaches.
- Firewalls control traffic to/from the screened subnet, providing an additional layer of protection.

Intrusion Detection and Prevention Systems (IDS/IPS):

- IDS/IPS monitor network traffic for suspicious patterns or activities.
- Host-based (HIDS/HIPS) installed on individual systems detect insider threats, file changes, and local events.
- Network-based (NIDS/NIPS) monitor network traffic for known threats and unusual behavior across multiple systems.

IDS/IPS Tools:

- Snort and Suricata are well-known IDS/IPS tools.
- Security Onion provides intrusion detection, network security monitoring, and log management.
- These tools use signature-based, behavioral/anomaly-based, and trend analysis detection methods.

Web Filtering:

- Web filters block access to malicious or inappropriate websites, preventing malware infections and increasing productivity.
- Agent-based filtering installs software agents on devices, enforcing filtering policies locally.
- Centralized web filtering uses proxy servers to analyze and control web traffic, implementing block rules, content categorization, and reputation-based filtering.
- Issues include overblocking, underblocking, handling of encrypted traffic, and privacy concerns. Proper configuration and management are essential.

Assess Endpoint Security Capabilities

Implement Endpoint Security

ACLs and File System Permissions:

- ACLs manage access control policies for files and directories.
- Each object in the file system has an ACL associated with it.
- ACLs contain a list of allowed accounts and their permissions.
- Permissions include Read (r), Write (w), and Execute (x).
- Permissions are applied based on owner user (u), group (g), and others (o).
- Commands like `chmod` modify permissions using symbolic or absolute mode.

Application Allow Lists and Block Lists:

- Allow lists permit execution only for approved applications.

- Block lists prohibit execution of listed processes.
- Lists need regular updates based on incidents and threat hunting.
- Strategic changes may be necessary based on threat analysis.

Monitoring:

- Monitoring enforces and maintains security measures on endpoints.
- Helps detect changes that weaken security configurations.
- Provides data for compliance and auditing purposes.

Configuration Enforcement:

- Ensures systems adhere to mandatory security configurations.
- Involves standardized configuration baselines, automated management tools, continuous monitoring, and change management processes.

Group Policy:

- Centralized management of Windows OS settings in an Active Directory environment.
- Applies security settings consistently across systems.
- Settings include password policies, firewall settings, software restrictions, etc.

SELinux:

- Security feature in Linux supporting access control security policies.
- Offers granular permission control over processes and system objects.
- Limits resource access to prevent harm from malicious or flawed programs.

Hardening Techniques:

- Protects endpoints against evolving cybersecurity threats.
- Strategies include physical port hardening, logical port security, encryption, and host-based firewalls/IPS.

Installing Endpoint Protection:

- Involves strategic planning, standardized configurations, automated deployments, updates, monitoring, and centralized management.

Changing Defaults and Removing Unnecessary Software:

- Crucial steps in hardening endpoints.
- Changing default passwords and removing unnecessary software reduces vulnerabilities.

Decommissioning:

- Secure process for retiring devices to prevent data exposure.
- Involves data sanitization, resetting to factory settings, and updating inventory records.

Hardening Specialized Devices:

- Unique hardening strategies for industrial control systems, embedded systems, real-time operating systems, and IoT devices.
- Involves network segmentation, authentication, secure coding, and compliance with security standards and certifications.

Mobile Device Hardening

1. **Mobile Device Deployment Models:**
    - Corporate owned, business only (COBO): Device owned by organization, strictly for business use.
    - Corporate owned, personally enabled (COPE): Device provided by organization, allows personal use within policy limits.
    - Choose your own device (CYOD): Employees select devices from a predetermined list.
    - Each model balances control, flexibility, and security differently.
    - COBO offers more control but higher equipment spending; BYOD offers flexibility but security challenges.
2. **Mobile Device Management (MDM):**

    - Crucial for managing, securing, and enforcing policies on smartphones and tablets.
    - Maintains device inventory, ensures authorized access, enforces security policies, and enables remote lock or wipe.
    - Manages device updates, patches, app distributions, and other tasks.
    - Various platforms available: Apple's MDM, Android Enterprise, Microsoft Intune, VMware AirWatch, IBM MaaS360.
3. **Full Device Encryption and External Media:**
    - Most mobile OSes offer full device encryption.
    - iOS offers multiple encryption levels, including Data Protection for sensitive data.
    - Android encrypts user data at the file level by default (since Android 10).
    - Care should be taken with external media (MicroSD cards) to apply encryption where necessary.
4. **Location Services:**
    - Utilizes GPS or Indoor Positioning System (IPS) for device location.
    - Privacy concerns arise due to tracking potential; apps require user permission.
    - Geofencing creates virtual boundaries; can be used for context-aware authentication.
5. **Connection Methods (Cellular, Wi-Fi, Bluetooth):**
    - Cellular connections bypass enterprise network protections; require endpoint controls.
    - Wi-Fi risks from open access points or rogue networks; strong WPA3 security recommended.
    - Bluetooth vulnerabilities include device discovery, authentication issues, malware, and bluejacking/bluesnarfing.
    - NFC for short-range communication and mobile payments; vulnerable to eavesdropping, interception, and data corruption attacks.

Enhance Application Security Capabilities

Application Protocol Security Baselines

- **Secure Directory Services**:
    - Network directory lists subjects (users, computers, services) and objects (directories, files) with permissions.
    - Most use Lightweight Directory Access Protocol (LDAP) over port 389.
    - Authentication methods:
        - No Authentication: Anonymous access.
        - Simple Bind: Plaintext DN and password.

        - SASL: Negotiates supported authentication mechanisms.
        - LDAPS: Uses digital certificate for secure tunnel on port 636.
    - Limit access: Disable anonymous and simple authentication if secure access is required.
    - Access control policy for read-only and read/write access.
    - Restrict access to private network; block LDAP port from public interface.
- **Simple Network Management Protocol Security (SNMP)**:
    - Framework for management and monitoring.
    - Agent maintains Management Information Base (MIB); communicates over ports 161 (queries) and 162 (traps).
    - SNMP Monitor oversees agents, polls them for info, alerts for traps.
    - Security measures: Disable if not used, use difficult-to-guess community names, restrict management operations, use SNMP v3 for encryption and strong authentication.
- **File Transfer Services**:
    - FTP remains popular despite newer protocols.
    - FTP lacks security mechanisms, vulnerable to interception.
    - SSH FTP (SFTP) and FTP Over SSL (FTPS) provide encryption.
    - SFTP uses SSH over port 22; FTPS uses TLS over ports 21 (explicit) and 990 (implicit).
- **Email Services**:
    - SMTP for sending; mailbox protocol (POP3, IMAP) for storing/accessing.
    - Secure SMTP (SMTPS) and Secure POP (POP3S) use TLS.
    - Secure IMAP (IMAPS) allows permanent connections and folder management.
    - Email Security:
        - SPF, DKIM, DMARC authenticate senders, prevent phishing and spam.
        - Email Gateway scrutinizes emails, utilizes anti-spam filters, antivirus scanners, DMARC, SPF, DKIM.
        - S/MIME encrypts and authenticates email communications.
        - Email Data Loss Prevention (DLP) prevents unauthorized sharing of sensitive information.
- **DNS Filtering**:
    - Blocks or allows access to specific websites by controlling DNS resolution.
    - Proactive defense mechanism against phishing sites, malware, and inappropriate content.
    - Implemented through DNS filtering services, DNS servers, DNS firewalls, or local DNS resolvers.
- **DNS Security**:
    - Configure DNS servers for fault tolerance, restrict recursive queries to local hosts.
    - Patch DNS server software regularly to mitigate vulnerabilities.
    - Prevent DNS footprinting by applying access control lists to prevent unauthorized zone transfers.

    - DNSSEC provides validation process for DNS responses, mitigates spoofing and poisoning attacks.

Cloud and Web Application Security Concepts

Concepts:

- Cloud and web application security involve:
    - Cloud hardening: fortifies cloud infrastructure, reduces attack surface.
    - Application security: ensures secure design, development, deployment.
- Both practices establish a layered defense strategy against various threats.
- Secure coding practices include:
    - Input validation techniques.

        - Principle of least privilege.
        - Secure session management.
        - Encryption enforcement.
        - Patching support.
- Developers should design software with:
    - Comprehensive, structured, meaningful logs.
    - Real-time alerting mechanisms.

Secure Coding Techniques:

- Security considerations for new programming technologies should be understood and tested.
- Modern development practices include security development lifecycle.
- Examples: Microsoft's SDL, OWASP Software Assurance Maturity Model, OWASP Top 10.
- Input validation:
    - Essential for addressing untrusted input issues.
    - Techniques: Allowlisting, Blocklisting, Data Type Checks, Range Checks, Regular Expressions, Encoding.
- Secure Cookies:
    - Principles include 'Secure', 'HttpOnly', 'SameSite' attributes.
    - Protect against session hijacking, cross-site scripting.
- Static Code Analysis:
    - Identifies vulnerabilities, errors, noncompliant coding practices.
    - Tools: SonarQube, Coverity, Fortify.

Code Signing:

- Verifies integrity, authenticity of software code.
- Uses digital signatures, certificates from trusted CAs.
- Assures source, integrity of code, not its safety or security.

Application Protections:

- Data exposure prevention.
- Error handling: Structured exception handling, avoiding default error messages.
- Memory management: Avoiding faulty practices.
- Client-Side vs. Server-Side Validation: Client-side informs users, server-side validates.
- Application Security in the Cloud: Complementary to cloud hardening.

Monitoring Capabilities:

- Enhance logging, monitoring for better threat detection.
- Real-time alerting improves incident response.

Software Sandboxing:

- Isolates processes, prevents access to system.
- Implemented in web browsers, operating systems, virtual machines.

Sandboxing in Security Operations:

- Essential for malware detection, forensic inspection.
- Tools: Cuckoo Sandbox, Joe Sandbox.

These study notes cover the essential concepts and techniques for understanding cloud and web application security, including secure coding practices, input validation, secure cookies, static code analysis, code signing, application protections, monitoring capabilities, and software sandboxing.

Explain Incident Response and Monitoring

Concepts Incident Response

Incident Response and Monitoring Concepts

Incident Response Plan:

- Formal plan listing procedures, contacts, and resources for various incident categories.
- Preparation outcome.

Detection:

- Correlating events from network and system data sources.
- Identifying indicators:
  - Matching events in log files, IDS alerts, etc.
  - Deviations from baseline metrics.
  - Proactive threat hunting.
  - Employee, customer, or supplier notifications.
- Importance of confidential reporting.
- First responder notification crucial for appropriate response.
- Managing alerts through SIEM platform.

Analysis:

- Investigating detected indicators.
- Determining genuine incident and priority level.
- Categorizing true positive incidents.
- Escalating analysis for complex or high-impact events.

Impact:

- Factors affecting impact determination:
  - Data integrity.
  - Downtime.
  - Economic/publicity.
  - Scope.
  - Detection time.
  - Recovery time.

Category:

- Shared understanding of incident terms and concepts.
- Relies on threat intelligence for effective analysis.
- Utilizes frameworks like cyber kill chain for threat research.

Playbooks:

- SOPs for specific cyber threat scenarios.
- Guide for detection and response steps.

Containment:

- Isolation-based and segmentation-based techniques.

- Focus on preserving forensic evidence.

Eradication and Recovery:

- Mitigation and restoration steps post-containment.
- Reconstitution of affected systems.
- Reaudit security controls.
- Notification and remediation for affected parties.

Lessons Learned:

- Root cause analysis.
- Structured inquiry into incident causes.
- Staff meeting and report compilation.
- Focus on improving procedures rather than blaming individuals.

Testing and Training:

- Validate incident response readiness.
- Testing forms: tabletop exercises, walkthroughs, simulations.
- Training on incident detection, reporting, and cross-departmental coordination.

Threat Hunting:

- Proactive discovery of TTPs.
- Utilizes threat intelligence and analytics platforms.
- Considerations for intelligence fusion and adversary maneuvering.

Digital Forensics

1. **Introduction to Digital Forensics**:
    - Digital forensic analysis involves examining evidence gathered from computer systems and networks.

    - Purpose: Uncover relevant information such as deleted files, timestamps, user activity, and unauthorized traffic.
2. **Incident Response Activities**:
    - Importance of digital forensic analysis in incident response.
    - Processes and tools for acquiring digital evidence.
    - Documentation is critical for collecting, preserving, and presenting valid digital proofs.
3. **Due Process and Legal Hold**:
    - Digital forensics for prosecuting crimes, especially insider threats like fraud or misuse of equipment.
    - Importance of due process and procedural safeguards to ensure fairness.
    - Legal hold: Preservation of information relevant to a court case, including electronic records.
4. **Acquisition of Digital Evidence**:
    - Process of obtaining a forensically clean copy of data from seized devices.
    - Impact of legality on acquisition, especially regarding BYOD policies.
    - Order of volatility for evidence collection: CPU cache, system memory, mass storage, remote logging, physical configuration.
5. **System Memory Acquisition**:
    - Importance of volatile data from RAM.
    - Tools and methods for capturing system memory, such as memory dumps.
6. **Disk Image Acquisition**:
    - Acquiring data from nonvolatile storage like hard drives, SSDs, and optical media.
    - Live acquisition vs. static acquisition methods.
    - Imaging tools for bit-level copies of storage media.
7. **Preservation of Digital Evidence**:
    - Ensuring the integrity of evidence by avoiding alterations during acquisition.
    - Use of write blockers to prevent changes to source data or metadata.
8. **Evidence Integrity and Non-Repudiation**:
    - Cryptographic hashing to ensure data integrity.
    - Chain of custody documentation to establish proper handling and integrity of evidence.
9. **Reporting in Digital Forensics**:
    - Ethical principles in analysis: unbiased, repeatable methods, minimal manipulation of evidence.
    - Importance of strong documentation and reporting to withstand legal scrutiny.
10. **E-Discovery**:
    - Filtering relevant evidence from forensic examinations.
    - Functions of e-discovery tools: de-duplication, search, tagging, security, disclosure.

Data Sources

1. **Introduction to Metadata**:

    - Metadata is data about data, including properties like creation time, author, and permissions.
    - It is crucial for establishing timelines and providing evidence in incident investigations.
2. **File Metadata**:
    - Attributes stored by the file system include creation, access, and modification times.
    - Security attributes like read-only or hidden, and permissions represented by ACLs.
    - Extended attributes can include author information, copyright details, or tags for indexing.
3. **Social Media Metadata**:
    - Metadata uploaded to social media can reveal unintended information like location and time.
4. **Web Metadata**:
    - Web servers return resource properties via headers in response to client requests.
    - Headers can include authorization information, data type (text or binary), and may be logged by servers.
5. **Email Metadata**:
    - Email headers contain sender, recipient, and transmission details handled by mail agents.
    - Mail user agents (MUAs) create initial headers, mail delivery agents (MDAs) add or amend headers, and message transfer agents (MTAs) route messages.
    - Headers can contain additional information added by each MTA along the delivery path.
6. **Viewing and Analyzing Metadata**:
    - Headers are not typically exposed to users but can be viewed via message properties or source command.
    - MTAs add detailed information to headers, making it difficult to read in plaintext.
    - Tools like Message Analyzer can parse and display headers in a structured format, showing the delivery path and added headers.

Alerting and Monitoring Tools

Agent-Based and Agentless Collection:

1. **Agent-based Collection**:
    - Involves installing an agent service on each host.
    - Events on the host are logged, filtered, aggregated, and sent to the SIEM server for analysis.
    - Typically used for Windows/Linux/macOS computers.
2. **Listener/Collector**:
    - Hosts push log changes to the SIEM server without installing an agent.
    - Used for devices like switches, routers, and firewalls.
    - Uses Syslog protocol for forwarding logs to SIEM.
3. **Sensor**:
    - Collects packet captures and traffic flow data.
    - Utilizes sniffer tools via mirror port functionality or network tap.

Log Aggregation:

1. **Normalization**:
    - Interprets data from various systems for consistency and searchability.
    - SIEM features connectors or plug-ins for different systems.
    - Requires parsers for each data source to map attributes to standard fields.
2. **Date/Time Normalization**:
    - Ensures consistency across different time zones to establish a single timeline.

Alerting and Monitoring Activities:

1. **Alerting**:
    - SIEM runs correlation rules on extracted indicators to detect potential incidents.
    - Correlation involves interpreting relationships between data points.
    - Correlation rules use logical expressions and operators to define conditions.
    - Threat intelligence feeds associate collected data with known threat indicators.
2. **Incident Response**:
    - Includes analysis, containment, eradication, and recovery steps.
    - Validation during analysis confirms true positives.
    - Quarantine isolates the source of indicators.
3. **Reporting**:
    - Provides insight into security system status.
    - Formats tailored for different audiences like executives, managers, and compliance regulators.
    - Metrics include authentication data, patch status, incident statistics, and trend reporting.
4. **Archiving**:
    - Retains historical log and network traffic data.

- Supports retrospective incident and threat hunting and compliance requirements.
- Requires a retention policy to manage data volume and SIEM performance.

Alert Tuning and Monitoring Infrastructure:

1. **Alert Tuning**:
   - Reduces false positives to avoid alert fatigue.
   - Techniques include refining detection rules, redirecting alerts, and continuous monitoring.
   - False negatives are also addressed to prevent overlooking threats.
2. **Monitoring Infrastructure**:
   - Uses managerial reports for day-to-day monitoring of computer resources and network infrastructure.
   - Network monitors collect data about network infrastructure appliances for status monitoring.
   - NetFlow provides flow data analysis for network traffic metadata.

Monitoring Systems and Applications:

1. **System Monitors and Logs**:
   - System monitors assess host health status using SNMP traps.
   - Logs are critical for security information, audit trails, and intrusion detection.
2. **Application and Cloud Monitors**:
   - Monitor application/service status, bandwidth consumption, and cloud services.
   - Vulnerability scanners assess host vulnerabilities and misconfigurations.
   - Antivirus software detects malware and integrates with SIEM for alerting.
3. **Data Loss Prevention (DLP)**:
   - Controls data copying to restrict it to authorized media and services.
   - Monitoring statistics for DLP policy violations help identify trends.
4. **Benchmarks and Compliance Scans**:
   - Compare system configurations to established benchmarks for compliance.
   - Compliance scans ensure conformity to regulatory standards and best practices.

Analyze Indicators of Malicious Activity

Malware Attack Indicators

Spyware and Keyloggers:

- Viruses and worms evolved from destructive replication to facilitating intrusion, fraud, and data theft.
- Tracking cookies record web activity, IP addresses, search queries, etc., while supercookies and beacons track covertly.
- Adware alters browser settings, inserts ads, and changes search providers.
- Spyware monitors application activity, captures screenshots, and activates recording devices like microphones.
- Keyloggers record keystrokes to steal confidential information like passwords and credit card data.
- Metasploit Meterpreter tool can be used to dump keystrokes from victim machines.

Backdoors and Remote Access Trojans:

- Backdoors provide unauthorized access, while Remote Access Trojans (RATs) operate covertly for administrative control.
- Compromised hosts may have bots, forming botnets used for DDoS attacks, spam, or cryptomining.
- RATs connect to a command and control (C&C) host for remote control, often using covert channels like IRC or HTTPS/DNS.

Rootkits:

- Trojans requiring user execution inherit user privileges; gaining admin privileges needs UAC confirmation.
- Rootkits operate at the system level, concealing themselves as legitimate processes, files, or services.
- Some rootkits exploit vulnerabilities to gain SYSTEM privileges or reside in firmware for persistence.

Ransomware, Crypto-Malware, and Logic Bombs:

- Ransomware encrypts files, demanding payment for decryption; crypto-ransomware encrypts data and demands ransom in cryptocurrency.
- Cryptojacking hijacks resources for cryptocurrency mining, often across botnets.
- Logic bombs execute after a set time or event, triggering malicious actions.

TTPs and IoCs:

- Tactics, Techniques, and Procedures (TTPs) describe threat behaviors, methods, and detailed procedures used by threat actors.
- Indicators of Compromise (IoCs) are residual signs of successful or ongoing attacks, including compromised processes, connections to C&C networks, and altered system settings.

Malicious Activity Indicators:

- Sandboxes isolate and analyze suspicious code; resource consumption, file system changes, and account compromise indicate malicious activity.
- Access denial, resource inaccessibility, and suspicious account behavior like lockouts or impossible travel suggest a security breach.
- Threat actors may attempt to cover their tracks by deleting or altering logs, leading to missing or manipulated log entries.

Physical and Network Attack Indicators

- **ARP Poisoning Attack:**
  - Targets subnet's default gateway.
  - If successful, attacker intercepts traffic destined for remote networks.
  - Implemented through ARP poisoning to perform on-path attack.
- **DNS Attacks:**
  - Exploit weaknesses in Domain Name System (DNS).
  - Various types: typosquatting, DRDoS, DoS against public DNS services, DNS server hijacking.
  - DNS poisoning compromises name resolution process.
  - Methods: on-path attacks, DNS client cache poisoning, DNS server cache poisoning.
- **Wireless Attacks:**
  - Rogue Access Points:
    - Unauthorized access points installed on the network.
    - Can be malicious or accidental.
    - Evil twin mimics legitimate access point to deceive users.
  - Wireless Denial of Service:
    - Disrupts wireless networks using interference or spoofed frames.
  - Wireless Replay and Key Recovery:
    - Exploits lack of encryption in management frame traffic.
    - Disassociation attacks disconnect clients.
    - Aimed at recovering network keys.

- **Password Attacks:**
  - Online Attacks:
    - Interact directly with authentication service.
    - Mitigated by limiting login attempts.
  - Offline Attacks:
    - Exploit obtained password hashes.
    - Utilize packet sniffers or access to password databases.
  - Brute Force, Dictionary, Hybrid Attacks:
    - Attempt every combination or use dictionary words.
  - Password Spraying:
    - Tries common passwords with multiple usernames.

- **Credential Replay Attacks:**
  - Target Windows Active Directory networks.
  - Exploit cached credentials to gain access to other hosts.
  - Types: pass the hash, golden ticket, silver ticket attacks.
- **Cryptographic Attacks:**
  - Downgrade Attacks:
    - Forces use of weaker protocols or ciphers.
  - Collision Attacks:
    - Exploits weak hashing functions to create same hash for different inputs.

- Birthday Attacks: ■ Exploits collisions in hash functions through brute force.

- **Malicious Code Indicators:**
  - Types of malicious activity: shellcode, credential dumping, pivoting/lateral movement, persistence.
  - Indicators found in endpoint protection software or network logs.
  - Malware interacts with network, file system, and registry.

Application Attack Indicators

1. **Application Attacks Overview**:
    - Application attacks target vulnerabilities in OS or application software.
    - Vulnerabilities can lead to compromised security systems or application crashes.
    - Main scenarios: compromising OS or third-party apps, compromising website or web application security.
2. **Indicators of Application Attacks**:
    - Increased application crashes/errors can indicate exploitation attempts.
    - Anomalous CPU, memory, storage, or network utilization can also be indicators.
    - Indicators may be found in system logs or application-specific logs.
3. **Privilege Escalation**:
    - Goal: Allow threat actors to run their own code on the system.
    - Types: Vertical (elevation) and horizontal privilege escalation.
    - Indicators: Process logging, audit logs, incident response, and endpoint protection agents.
4. **Buffer Overflow**:
    - Exploits vulnerabilities by overwriting data in a buffer.
    - Common vulnerability: stack overflow.
    - Mitigation: Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP).
5. **Replay Attacks**:
    - Exploit session mechanisms like cookies.
    - Session token identification and exploitation.
6. **Forgery Attacks**:
    - CSRF: Exploits cookies for unauthorized actions.
    - SSRF: Causes server to process arbitrary requests targeting other services.
7. **Injection Attacks**:
    - Exploits unsecure application request processing.
    - Types include XML Injection, LDAP Injection, Directory Traversal, and Command Injection.
8. **URL Analysis**:
    - HTTP request structure and methods.
    - Percent encoding and its misuse for obfuscation.
    - Web server logs as indicators of attacks, including status codes and HTTP header information.

Summarize Security Governance Concepts

Policies, Standards, and Procedures

Security Governance Concepts

1. **Importance of Standards**
    - Stakeholders influence standards choice.
    - Standards reflect dedication to quality, security, reliability.
    - Strategic selection based on legal, business, risk management, and stakeholder needs.
    - Adoption impacts operations; appropriate selection enhances effectiveness.
2. **Industry Standards**
    - ISO/IEC 27001, 27002, 27017, 27018.
    - NIST Special Publication 800-63.
    - PCI DSS.
    - FIPS.
    - Audit compliance and security practices; assess adherence and identify gaps.
3. **Internal Standards**
    - Password standards: hashing, salting, transmission, reset, managers.
    - Access control standards: models, verification, privilege management, authentication, session management, audit trails.
4. **Physical Security Standards**
    - Building, workstation, datacenter security.
    - Equipment disposal, visitor management.
5. **Encryption Standards**
    - Algorithms, key length, management.
6. **Legal Environment**
    - Governance committees ensure compliance with laws and regulations.
    - Legislation examples: Sarbanes-Oxley Act, Computer Security Act, Federal Information Security Management Act.
    - International laws like GDPR and CCPA protect privacy globally.
7. **Global Law**
    - Laws like GDPR and CCPA have international reach.
    - GDPR emphasizes informed consent, data subject rights.
    - CCPA empowers California residents with data control rights.
8. **Regulations and Laws**
    - National, local, regional laws vary; compliance essential.
    - Examples: HIPAA, GLBA, FISMA, Data Protection Act, PIPEDA, IT Act.
9. **Industry-Specific Regulations**
    - Examples across healthcare, finance, telecommunications, energy, education, government sectors.
    - Compliance ensures industry-specific data protection.

10. **Governance and Accountability**
    - Ensures compliance with laws and regulations.
    - Continuous monitoring, evaluation, and updating essential.
    - Governance boards, committees crucial for oversight.
11. **Centralized vs. Decentralized Governance**
    - Centralized: unified decision-making; standardized practices.
    - Decentralized: localized decision-making; adaptability.
    - Hybrid models combine elements for flexibility and standardization.
12. **Government Entities and Groups**
    - Regulatory, intelligence, law enforcement, defense agencies involved.
    - Data protection authorities enforce regulations.
    - National cybersecurity agencies focus on critical infrastructure protection.
13. **Data Governance Roles**
    - Owner: strategic guidance.
    - Controller: legal and regulatory compliance.
    - Processor: secure data handling.
    - Custodian: implementation and enforcement of security controls.

Change Management

Study Notes on Change Management:

1. Importance of Change Management:

- Systematic approach to managing changes in IT infrastructure.
- Goal: Minimize risk and disruption, maximize value and efficiency of changes.
- Relies on planning, testing, approval, and implementation.
- Considers impacts, dependencies, and develops contingency plans.
- Requires proper documentation and communication.

2. Change Management Programs:

- Ensure efficient and effective handling of changes.
- Minimize risks associated with changes.
- Manage various changes including software deployments, updates, hardware replacements, etc.
- Prevent introduction of vulnerabilities, service disruptions, or compliance issues.

3. Change Management Approval Process:

- Begins with submitting a Request for Change (RFC).
- Reviewed by designated change manager or committee.
- Formal approval involving stakeholders.
- Documentation and communication throughout the process.

4. Factors Driving Change Management:

- Involvement of stakeholders from various parts of the organization.
- Ensures comprehensive review of proposed changes.
- Promotes acceptance and adoption of changes.
- Facilitates ownership and responsibility.

5. Change Management Concepts:

- Impact Analysis: Identifying and assessing potential implications of proposed changes.
- Test Results: Evaluation of changes in a test environment before implementation.
- Backout Plans: Contingency plans for reversing changes if implementation fails.
- Maintenance Windows: Predefined time frames for implementing changes.
- Standard Operating Procedures (SOPs): Detailed instructions for implementing changes consistently.

6. Allowed and Blocked Changes:

- Allow lists: Approved changes exempt from full change management process.

- Deny lists: Explicitly blocked changes requiring full change management process.
- Ensure control over authorized and unauthorized changes.

7. Restarts, Dependencies, and Downtime:

- Considerations for minimizing disruptions during change implementation.
- Scheduled maintenance windows and minimizing impacts on business operations.
- Understanding dependencies to mitigate unintended outages.

8. Legacy Systems and Applications:

- Unique challenges in managing changes due to outdated technology and lack of support.
- Requires specialized solutions and extensive testing.

9. Documentation and Version Control:

- Tracking and controlling changes to documents, code, or data.
- Ensures historical record of changes, consistency, and quick reversion to previous versions.
- Impacts various documentation including change requests, policies, system documentation, etc.

Automation and Orchestration

Study Notes on Automation and Orchestration:

1. Importance of Automation and Orchestration:

- Tools for managing security operations efficiently.
- Automation: Performs repetitive, rule-based tasks to reduce human error.
- Orchestration: Coordinates interactions between automated processes and systems.
- Enhances efficiency, reduces errors, and provides clear audit trails.

2. Automation and Scripting:

- Critical tools in modern IT operations for streamlining processes and enhancing security.
- Enhances security governance by enforcing policies consistently.
- Aids in change management by reducing implementation time and providing audit trails.

3. Capabilities of Automation:

- Provisioning: Automating user and resource provisioning tasks to reduce manual effort and errors.
- Guardrails and Security Groups: Automating monitoring and enforcement of security policies.
- Ticketing: Automating incident detection, ticket generation, routing, and escalation procedures.
- Service Management: Automating routine tasks to free up time for strategic analysis.
- Continuous Integration and Testing: Automation improves code quality and accelerates development cycles.
- Application Programming Interfaces (APIs): Automation orchestrates interactions between software systems.

4. Benefits of Automation and Orchestration:

- Enhances efficiency by reducing repetitive tasks and human error.
- Combats operator fatigue in security operations.
- Improves security posture by enforcing standardized baselines and automating security tasks.
- Supports staff retention initiatives by reducing fatigue from repetitive tasks.

5. Challenges of Automation and Orchestration:

- Complexity: Requires deep understanding of systems and processes.
- Cost: Initial investment in tools, integration, and training can be high.

- Single Point of Failure: Critical automated systems failing could cause widespread problems.
- Technical Debt: Hasty implementation leading to poorly documented code or system instability.
- Ongoing Support: Requires continuous updates, patches, and maintenance for effectiveness.

6. Benefits of Infrastructure Management Automation:

- Ensures consistency and accuracy throughout the infrastructure.
- Saves time and resources by quickly deploying configurations.
- Enhances scalability, flexibility, standardization, compliance, and change management.
- Strengthens security and governance by enforcing security controls and applying patches consistently.

Explain Risk Management Processes

Risk Management Processes and Concepts

1. Risk Management Overview:

- Proactive and systematic approaches to identify, assess, prioritize, and mitigate risks.
- Risk mitigation involves reducing exposure to or the effects of risk factors.

2. Risk Management Strategies:

- Risk Deterrence/Reduction: Controls to make risk incidents less likely or less costly.
- Avoidance: Stopping activities causing risk, although infrequently a credible option.
- Risk Transference: Assigning risk to a third party, such as through insurance.
- Risk Acceptance/Tolerance: No countermeasures put in place due to risk level justification.
- Risk Exceptions/Exemptions: Formal recognition of risks that cannot be mitigated within specified conditions.

3. Residual Risk and Risk Appetite:

- Residual Risk: Likelihood and impact after mitigation measures.
- Risk Appetite: Strategic assessment of tolerable residual risk levels.

4. Risk Management Processes:

- Identification of Mission Essential Functions (MEFs) and vulnerabilities.
- Analysis of threats, business impacts, and risk responses.
- Assessing likelihood and impact of risks using qualitative and quantitative methods.
- Risk management frameworks like NIST RMF or ISO 31K guide processes.
- Risk Registers: Documents results of risk assessments, including severity, mitigation strategies, and ownership.

5. Risk Threshold and Key Risk Indicators (KRIs):

- Risk Threshold: Defines acceptable risk levels based on various factors.
- KRIs: Predictive indicators to monitor and predict potential risks, supporting proactive risk management.

6. Business Impact Analysis (BIA) and Mission Essential Functions (MEFs):

- BIA: Identifying and assessing impact of disruptions on business operations.
- MEFs: Functions critical for business continuity that cannot be deferred.

7. Key Metrics in Risk Management:

- Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), Work Recovery Time (WRT), Recovery Point Objective (RPO).
- Mean Time to Repair (MTTR) and Mean Time Between Failures (MTBF) as KPIs for system reliability and efficiency.

Vendor Management Concepts

- **Vendor Management Concepts:**
    - Third-party risk assessment involves:
        - Vendor due diligence.
        - Risk identification and assessment.
        - Ongoing monitoring.
        - Incident response planning.
    - Vendor due diligence includes evaluating:
        - Security practices.
        - Financial stability.
        - Regulatory compliance.
        - Reputation.
    - Risk identification and assessment involve:
        - Identifying potential risks.
        - Assessing impact on operations, data, and reputation.
    - Ongoing monitoring ensures:
        - Vendors maintain security controls.
        - Adhere to contractual obligations.
        - Promptly address identified risks or vulnerabilities.
    - Critical in risk management to:
        - Identify, assess, and mitigate risks.
        - Implement robust assessment processes.
        - Maintain regulatory compliance.
        - Foster a safe operational environment.

- **Vendor Selection:**
    - Systematically evaluate potential vendors.
    - Steps include:
        - Identifying risk criteria.
        - Conducting due diligence.
        - Selecting vendors based on risk profile.
    - Aims to identify and mitigate risks related to:
        - Financial stability.
        - Operational reliability.
        - Data security.
        - Regulatory compliance.
        - Reputation.
    - Select vendors aligning with:

        - Organization's risk tolerance.
        - Effective risk management capability.

- **Third-Party Vendor Assessment:**
    - External entities providing goods, services, or technology.
    - Offer specialized expertise and support.
    - Range from technology providers to suppliers.
    - Bring efficiency, cost-effectiveness, and innovation.
    - Introduce potential risks:
        - Access to sensitive data.
        - Infrastructure.
        - Critical processes.
    - Proper assessment ensures adherence to security standards, compliance, and fulfillment of obligations.

Audits and Assessments

1. **Purpose of Audits and Assessments:**
    - Ensure operations align with standards, policies, and regulations.
    - Identify gaps and provide recommendations for improvement.
    - Enhance security measures by assessing effectiveness and efficiency.
2. **Attestation and Assessments:**
    - Attestation verifies security controls' accuracy and compliance.
    - Independent examination assures stakeholders of security measures.
3. **Internal vs. External Assessments:**
    - Internal assessments by employees ensure continuous improvement.
    - External assessments by third-party providers offer impartial evaluation.
    - Both methods complement each other for comprehensive evaluation.
4. **Internal Assessment Approaches:**
    - Compliance Assessment: Ensures alignment with laws, regulations, and policies.
    - Audit Committee: Provides oversight and assurance on financial practices.
    - Self-Assessment: Allows for internal evaluation of performance and practices.
5. **External Assessment Approaches:**
    - Regulatory Assessments: Ensure compliance with laws and industry standards.
    - Examination: Independent evaluation of financial statements and controls.
    - Assessment: Broad evaluation of performance, practices, and capabilities.
    - Third-Party Audit: Objective assessment by external entities for compliance.

Study Notes on Penetration Testing:

1. **Purpose of Penetration Testing:**
    - Simulate real-world attacks to identify vulnerabilities and weaknesses.
    - Test specific systems, incident response capabilities, and physical controls.
2. **Types of Penetration Testing:**
    - Offensive Penetration Testing (Red Teaming): Mimics potential attackers' tactics.
    - Defensive Penetration Testing (Blue Teaming): Evaluates defensive measures.
    - Physical Penetration Testing: Assesses physical security practices and controls.
    - Integrated Penetration Testing: Holistic approach combining different methodologies.
3. **Active and Passive Reconnaissance:**
    - Active: Probing and interacting with target systems to gather information.

- Passive: Gathering information without directly interacting, focusing on publicly available data.

4. **Known, Partially Known, and Unknown Testing Methods:**
   - Known Environment: Detailed knowledge about the target system or network.
   - Partially Known Environment: Limited knowledge requiring reconnaissance.
   - Unknown Environment: Little prior knowledge to simulate real-world scenarios.

Summarize Data Protection and Compliance Concepts

Data Classification and Compliance

- **Definition of Data Breach:**
  - Occurs when information is read, modified, or deleted without authorization.
  - Includes loss of any type of data, especially corporate and intellectual property.
  - Privacy breach specifically refers to loss or disclosure of personal and sensitive data.
- **Organizational Consequences of Breaches:**
  - Reputation damage: Leads to negative publicity and loss of customer trust.
  - Identity theft: Can result in lawsuits for damages.
  - Fines: Regulators may impose fixed sums or a percentage of turnover.
  - IP theft: Loss of revenue due to theft of copyrighted material or corporate data.
- **Notifications of Breaches:**
  - Requirements set by law or regulations dictate who must be notified.
  - Breach can include loss, theft, or accidental disclosure of information.
  - Accidental breaches pose substantial risks if effective procedures are lacking.
  - Breach may be considered even with potential for unauthorized access.
- **Escalation:**
  - Even minor breaches should be escalated to senior decision-makers.
  - Impact from legislation and regulation should be considered.
- **Public Notification and Disclosure:**
  - Notification to law enforcement, affected individuals, third-party companies, and the public may be required.
  - Legislation sets out requirements and timescales for notifications.
  - Disclosure includes description of breached information, contact details, consequences, and mitigation measures.
- **Compliance:**
  - Refers to adherence to security standards, regulations, and best practices.

    - Requires establishment of policies, procedures, controls, and technical measures.
    - Noncompliance can result in legal sanctions, financial penalties, reputational damage, and loss of customer trust.
- **Data Protection Methods:**
    - Geographic restrictions, encryption, hashing, masking, tokenization, obfuscation, segmentation, permission restrictions.
- **Data Loss Prevention (DLP):**
    - Automates discovery, classification, and enforcement of data protection rules.
    - Components include policy server, endpoint agents, and network agents.
    - Remediation actions include alerting, blocking, quarantining, and tombstoning.

Personnel Policies

- **Personally Owned Devices in the Workplace:**
    - Portable devices like smartphones, USB sticks, etc., pose security threats due to easy file copying and potential camera/voice recording functions.
    - Solutions like network access control, endpoint management, and data loss prevention can help prevent attachment of such devices to corporate networks.
    - Companies may struggle to enforce policies against bringing personal devices onsite.
    - Unauthorized use of personal software (shadow IT) can lead to security vulnerabilities and legal liabilities for the organization.
- **Clean Desk Policy:**
    - Requires employees to keep their work areas free from documents to prevent unauthorized access to sensitive information.
- **User and Role-Based Training:**
    - Essential for ensuring users understand security policies, incident reporting, site security procedures, data handling, password/account management, social engineering threats, etc.
    - Training should be tailored to different job roles' security requirements and levels of expertise.
- **Training Topics and Techniques:**
    - Use a variety of techniques like workshops, one-on-one instruction, computer-based training, videos, etc., to improve engagement and retention.
    - Computer-based training can include simulations and branching scenarios to practice cybersecurity tasks.
- **Critical Elements for Security Awareness Training:**
    - Includes policy training, situational awareness, insider threat education, password management, and training on handling removable media and cables.
    - Also covers social engineering tactics, operational security, and training for hybrid/remote work environments.
- **Phishing Campaigns:**

    - Simulated phishing attacks are used to raise awareness about phishing risks among employees.
    - Training helps employees recognize and respond effectively to phishing attempts, reducing the likelihood of data breaches.
- **Anomalous Behavior and Recognizing Risky Behaviors:**
    - Training focuses on identifying unusual actions or patterns that could indicate security threats.
    - Employees learn to recognize and report risky, unexpected, and unintentional behaviors that could lead to security incidents.
- **Security Awareness Training Lifecycle:**
    - Follows stages of assessing security needs, planning, development, delivery, evaluation, reinforcement, and monitoring/adaptation to ensure effectiveness.
- **Development and Execution of Training:**
    - Emphasizes creating engaging materials, incorporating real-world examples, and facilitating discussions to enhance learning.
- **Reporting and Monitoring:**
    - Methods include assessments, incident reporting analysis, phishing simulations, observations/feedback, and tracking metrics like training completion rates.