CompTIA Security+ (SY0-701) Day 6

Section 4.3: Explain Various Activities Associated with Vulnerability Management

Vulnerability Management Identification Methods

- **Vulnerability Scan** - Examination of a network, system, or application to **identify** and assess potential security weaknesses.
    - Uses automated tools to detect vulnerabilities that could be exploited by cyber attackers.
    - Compares **known vulnerabilities** in a database against the system to determine if it is vulnerable.
- **Application Security** - Involves several methods to identify and mitigate security risks in software applications.
    - **Static Analysis** - Examining the application's source code, byte code, or binaries without executing the program.
    - **Dynamic Analysis** - Testing the application during runtime, simulating attacks to find exploitable vulnerabilities.
    - **Package Monitoring** - Tracking and analyzing the software libraries and packages that the application depends on.
- **Threat Feeds** - A stream of data that provides information about current or emerging cyber threats and vulnerabilities.
    - **Open-source Intelligence (OSINT)** - Threat intelligence gathered from publicly available sources.
    - **Proprietary/Third-Party** - Provided by specialized cybersecurity firms or vendors, usually part of a paid service.
    - **Information-Sharing Organizations (ISACs/ISAOs)** - Collective groups where members share cybersecurity information.
    - **Dark Web** - A part of the internet not indexed by standard search engines, known for illicit activities.
- **Penetration Testing** - Process of simulating cyberattacks on a computer system, network, or web application to identify and exploit vulnerabilities.
- **Responsible Disclosure / Bug Bounty Programs**
    - Organizations provide monetary or other incentives for reported bugs.

- **System/Process Audit**
    - Conduct a thorough inspection to uncover potential security vulnerabilities.
        - Catalog all IT assets, including hardware, software, and data.
        - Compare current system settings against security benchmarks.
        - Verify proper implementation of authentication and authorization mechanisms.
        - Evaluate encryption, backup, and disaster recovery protocols.

Vulnerability Management Analysis

- **Confirmation** - The process of verifying and validating the results obtained from vulnerability scans, assessments, and tests.
    - **True Positive** - The system correctly identifies a real threat or vulnerability.
    - **True Negative** - The system correctly identifies that there is no threat or vulnerability present.
    - **False Positive** - When a system incorrectly identifies a normal or safe activity as a threat or vulnerability.
    - **False Negative** - When a system fails to detect an actual threat or vulnerability.
- **Vulnerability Classification** - The process of categorizing identified vulnerabilities based on various criteria, such as:
    - Severity Rating
    - Type of Vulnerability
    - Affected Components
    - Exploitability
    - Impact
- **Purpose** - Essential for prioritizing remediation efforts, allocating resources effectively, and developing a comprehensive security strategy.
- **Prioritization** - Vulnerabilities should be ranked based on impact and exploitability. Focus on critical vulnerabilities first.

CVE and CVSS

- **Common Vulnerabilities and Exposures (CVE)** - A reference of uniquely identified security issues.
    - Identifiers use CVE-year-number format.
    - Standardization of Vulnerability Identification.
    - Facilitation of Vulnerability Tracking.
    - Enhanced Collaboration and Information Sharing.
    - Prioritization and Risk Assessment.
    - Support for Compliance and Reporting.
    - **Exam Note**: Every CVE has a Unique Identifier.
- **Common Vulnerability Scoring System (CVSS)** - A system for scoring vulnerabilities based on their severity.
    - CVSS assigns a numerical score (ranging from 0 to 10).

Exposure Factor

A metric used to represent the expected percentage of loss that an organization would suffer if a specific asset were compromised in a security incident.

- Quantification of Impact
- Prioritization of Remediation Efforts
- Part of Risk Calculation
- Variable Depending on Asset and Threat
- Risk Management Tool

Environmental Variables

The specific conditions and factors within an organization's operational environment that can influence the impact and severity of security vulnerabilities.

- Network Architecture
- Security Controls in Place
- Regulatory Compliance Requirements

Industry and Organizational Impact

Refers to the specific consequences or effects that security vulnerabilities can have on a particular industry sector or individual organization.

- **Financial Sector**
    - Regulatory fines for data breaches.
    - Impact on customer trust and market value.
- **Healthcare**
    - Risks to patient safety and privacy.
    - Compliance with health information regulations.
- **Retail**
    - Customer data theft leading to reputational damage.
- **Risk Tolerance** - Refers to the level of risk that an organization is willing to accept or retain while pursuing its objectives.
    - Guides Prioritization.
    - Informs Security Strategy.
    - Facilitates Decision-Making.
    - Compliance and Regulatory Alignment.
    - Business Continuity and Resilience.

Vulnerability Management Response, Remediation, and Reporting

Response - Involves the immediate actions taken when a vulnerability is identified.

- Includes assessing the vulnerability, determining its potential impact, and deciding on the appropriate course of action.
- The goal is to quickly contain and control any potential risk posed by the vulnerability.

Remediation

- **Patching** - Process of applying an update to software or firmware to fix vulnerabilities that have been identified.
    - The goal is to protect the system from **known** vulnerabilities that could be exploited by attackers.
- **Insurance** - Refers to policies that provide coverage for losses and liabilities arising from cyber incidents.
    - The goal is to mitigate financial risks associated with cybersecurity incidents.
- **Segmentation** - Dividing a network into smaller parts or segments.
    - The goal is to limit the spread of potential attacks within a network.
- **Compensating Controls**
    - Security measures that are put in place to offset vulnerabilities that cannot be remediated directly.
    - The goal is to provide alternative protection where standard fixes or patches are not feasible.
- **Exceptions and Exemptions** - Cases where specific vulnerabilities are not remediated.
    - The goal is to allow for flexibility in vulnerability management, recognizing that not all vulnerabilities can or should be remediated.

Validating Remediation - Verify the fix has resolved the issue without introducing new problems.

- **Rescanning** - Using vulnerability scanning tools to reassess the system or network after remediation measures have been applied.
- **Auditing** - Examination and review of systems and procedures to ensure that remediation has been carried out according to the policies and standards.
- **Verification** - Process of testing and confirming that the specific remediation actions taken to address vulnerabilities have been successful.

Reporting Vulnerabilities

- Systematic documentation and communication of information about identified vulnerabilities, the status of their remediation, and the overall security posture of an organization.
    - List of Identified Vulnerabilities.
    - Severity Assessment.
    - Remediation Status.
    - Impact Analysis.
    - Recommendations.
    - Trend Analysis.

Section 4.4: Explain Security Alerting and Monitoring Concepts and Tools

Monitoring Activities and Concepts

- Continuous observation, analysis, and response to potential security threats or anomalies.
- **Systems**
    - CPU usage, memory utilization, disk space, and I/O operations.
    - System uptime and performance trends.
    - Detection of malicious activity.
- **Applications**
    - Application response time, error rate.
    - User transaction flows.
    - Resource consumption by applications.
    - Detection of malicious activity.

- **Infrastructure**
    - Network bandwidth and latency.
    - Device health (routers, switches, firewalls).
    - Environmental factors like temperature and humidity in data centers.
    - Detection of malicious activity.

Log Aggregation

- Centralizing log data for improved incident detection and analysis.
    - Example: Combining firewall, server, and application logs.
- **Alerting** - Automated notification for potential security events.
    - Example: Intrusion detection systems flagging unusual traffic.
- **Scanning** - Proactive searches for network and system vulnerabilities.
    - Example: Regular vulnerability assessments and penetration tests.
- **Reporting** - Summarization and communication of monitoring outcomes.
    - Example: Weekly security posture reports, incident briefs.
- **Archiving** - Long-term secure storage of historical monitoring data.
    - Example: Retention of audit logs, transaction logs for compliance.
- **Alert Response and Remediation/Validation** - Actions taken in response to security alerts, followed by the validation of the effectiveness of the actions.
    - **Quarantine** - Isolating a potentially compromised system or network segment to prevent the spread of threats.
    - **Alert Tuning** - Adjusting the alerting system to minimize false positives and prioritize significant security events.

Security Alerting and Monitoring Tools

- **Security Content Automation Protocol (SCAP)**
    - A suite of specifications that standardize how security software communicates and measures configuration settings, vulnerabilities, and patch status.
- **Benchmarks**
    - Recognized standards for optimal security practices.
    - Serve as reference points for audits and compliance.
- **Agents / Agentless**
    - Software installed on monitored devices vs no software being installed.
- **Security Information and Event Management (SIEM)**
    - Collect, correlate, and analyze security-related log data from various sources to detect and respond to security incidents.

- **Antivirus**
    - Detect, prevent, and remove malicious software or malware from computers and devices.
- **Data Loss Prevention (DLP)**
    - A solution composed of applications, processes, procedures, and technologies that work together to prevent sensitive data from leaving the network without notice.
- **Simple Network Management Protocol (SNMP) Traps**
    - Notifications are sent by network devices to a management system to alert about specific events or conditions
- **NetFlow**
    - Provide traffic metadata for network performance and security monitoring
- **Vulnerability Scanners**
    - Identify weaknesses in systems, applications, and network devices that could be exploited by attackers

Section 4.5: Given a Scenario, Modify Enterprise Capabilities to Enhance Security

Firewall

Rules, Access Lists, Protocols

- Permit (Allow) or Deny rules.
- Access Lists are processed top to bottom.
    - If a deny precedes a permit, the deny takes effect.
    - Implicit deny exists at the end of the list.

Screen Subnet

- Buffer zone between the internet and the internal secure network.
- Ensures security policies are enforced before traffic reaches critical assets.

IDS and IPS

- **Trends and Signatures**
  - Update IDS/IPS settings based on emerging threat trends.
  - Continuously update signature databases.
  - Signatures are patterns associated with known malicious activity.

Web Filter

- **Agent-Based**
  - Installed on end-user devices to filter web traffic.
  - Pros: Prevents accidental clicks on malicious links/sites.
  - Cons: Installation on each device can be bypassed.
- **Centralized Proxy**
  - Filters traffic at a central network point.
  - Pros: Easier management, consistent policy enforcement.
  - Cons: Limited off-network protection, possible latency.
- **URL Scanning**
  - Examines URLs for malicious content or phishing threats.
  - Scans emails, messages, and webpages.
- **Content Categorization**
  - Blocks non-essential or risky sites (e.g., adult, gaming, social media).
- **Block Rules**
  - Sets rules to allow or deny specific websites.
  - Can restrict access based on time or user.
- **Reputation**
  - Evaluates website safety and credibility.

- **Operating System Security**
  - Group Policy: Centralized configuration management in Windows environments.
  - SELinux: Security-Enhanced Linux; implements mandatory access controls to enforce security policies.

Implementation of Secure Protocols

Reasons

- Data protection, trust, compliance, and preventing cyber attacks.

Considerations

- Protocol selection, port selection, transport method.

Examples

- **DNS/DNSSEC (UDP 53)**
  - Resolves domain names to IP addresses.
  - DNSSEC digitally signs DNS information to ensure authenticity and integrity.
- **HTTPS (TCP 443)**
  - Encrypts web traffic using SSL/TLS.
  - Certificates from trusted authorities validate server identity.
- **SSH (TCP 22)**
  - Secure remote command-line access.
  - Replaces Telnet; supports key or password authentication.
  - Use SSHv2 whenever possible.
- **SFTP/FTPS**
  - FTP sends credentials in plaintext; avoid unsecure FTP.
  - SFTP: FTP over SSH (TCP 22).
  - FTPS: FTP over SSL/TLS (TCP 989/990).
- **POP3S/IMAPS (TCP 995 / 993)**
  - Encrypts email in transit, but the server can still read the content.

- **S/MIME**
    - End-to-end encryption for email.
    - Uses digital certificates for signing and encryption.
- **SNMP (UDP 161/162)**
    - Used to gather device information; traps send alerts.
    - SNMPv3 is recommended for authentication and encryption.

DNS Filtering

- Blocks unwanted or harmful internet destinations using DNS queries.

Email Security

- Protects against threats, ensures confidentiality, supports compliance, prevents data breaches, and ensures business continuity.
- **DMARC**: Protects the domain from unauthorized email use.
- **DKIM**: Attaches a digital signature to outgoing email; prevents spoofing.
- **SPF**: Prevents spammers from sending messages on behalf of your domain.
- **Secure Email Gateways (SEGs)**: Filter inbound/outbound email for malware, phishing, and spam.

File Integrity Monitoring

- Monitors files for unexpected changes.
- Alerts administrators of unauthorized modifications.
- Detects potential breaches early.

Data Loss Prevention (DLP)

- Prevents sensitive data from leaving the network.
- Requires a classification system to identify and protect sensitive information.

Network Access Control

- **Guest Network**: Separate network with a portal.
- **Posture Assessment**: Ensures client compliance; quarantines non-compliant devices.
- **Agents**: Persistent or non-persistent endpoint checks.

Endpoint Security Controls

- **EDR**: Tracks, analyzes, and responds to endpoint events.
- **XDR**: Extends EDR to include email, cloud, and network telemetry.

User Behavior Analytics (UBA)

- Establishes normal activity baselines.
- Detects deviations signaling potential threats.
- Identifies insider misuse.
- Assigns risk levels based on activity patterns.

Section 4.6: Given a Scenario, Implement and Maintain Identity and Access Management

Identity and Access Management

Provisioning/De-provisioning User Accounts

- Set up a user account with the necessary access rights, tailored to each user's role and requirements.
    - Prioritize authorization procedures, including management approval and identity verification, before account creation.
    - **Principle of Least Privilege**
- Revoke access and remove user accounts when no longer needed or upon role changes.
    - Ensure timely action to prevent unauthorized access.
    - Conduct periodic audits to maintain security.

Permission Assignments and Implications

Permission Assignment – The process of granting specific rights to users or groups.

- Considerations:
    - **Principle of Least Privilege**
    - Segregation of Duties
    - Role-Based Access Control (RBAC)
- Implications:
    - Security Risks
    - Compliance Issues
    - Operational Efficiency

Identity Proofing – Verifying that a person is who they claim to be.

- Methods:
    - Paper Documentation
        - Passport
        - Driver's License
        - Birth Certificate
        - Credit Report
    - Knowledge-Based Verification

Single Sign-On (SSO) and Federation

SSO – A user authentication service that permits a user to use one set of login credentials to access multiple applications.

- The primary goal of SSO is to simplify the management of multiple usernames and passwords.

Federation – Establishing agreements and using technologies that enable the sharing and acceptance of identities across **different systems or organizations**.

- Allows users to use a single set of credentials to access multiple applications or services, even if those resources are spread across different domains or organizations.

LDAP (Lightweight Directory Access Protocol)

- Centralizes user credentials for enterprise-wide identity management.
- Maintains organizational structure and user roles for access control.
- Acts as a backbone for quick and secure user verification across systems.

SAML (Security Assertion Markup Language)

- XML-based SSO solution for web browsers.
- Transfers identity data between two parties for authentication and authorization:
    - Identity Provider (IdP)
    - Service Provider (SP)

OAuth (Open Authorization)

- Access delegation framework.
- Allows a website or application to access resources hosted by other web apps on behalf of a user.

OpenID Connect

- JSON-based SSO solution for modern web apps and services, including mobile and smart devices.
- Data structured in JSON format.
- Transported using simple HTTPS flows.
- Security with JSON Web Tokens (JWT).
    - Created for federated authentication, enabling third parties to authenticate users.
    - Examples: “Login with Google,” “Login with Facebook,” “Login with AWS.”

Interoperability

- The ability of different systems, networks, or applications to work together seamlessly, regardless of their underlying architecture, platform, or design.
    - In the context of IAM, interoperability ensures that diverse identity management systems can exchange, understand, and use information effectively across various domains and environments.
    - Achieved by adhering to industry standards (such as SAML, OAuth, OpenID Connect, LDAP).

Attestation

- The process of verifying and certifying that access rights and privileges assigned to users are appropriate and necessary for their roles.
    - Regular reviews
    - Audits
    - Compliance and verification

Access Controls

Security measures in IAM that define how users can interact with resources and data within a system.

- **Mandatory Access Control (MAC)** – Access based on centralized policies; often used in environments where confidentiality and classification of data are paramount.
- **Discretionary Access Control (DAC)** – Access is determined by the owner or administrator of the protected system; common in less stringent environments.
- **Role-Based Access Control (RBAC)** – Access is grouped by role, and access to resources is determined by the roles assigned to users.
- **Rule-Based Access Control (RuBAC)** – Access to resources is based on a set of rules defined by the system administrator.
- **Attribute-Based Access Control (ABAC)** – Decisions to grant or deny access are based on user attributes, resource attributes, environmental factors, and other contextual data.
- **Time-of-Day Restriction** – Access to resources is restricted based on the time of day or week.
- **Principle of Least Privilege** – Ensures that users only have the minimum level of access required to perform their job functions.