CompTIA Security+ (SY0-701) Day 3

Section 2.3: Explain Various Types of Vulnerabilities

Application and Web-based Vulnerability

- Application Vulnerability
    - Memory Injection - A vulnerability in software that allows an attacker to insert and execute malicious code directly in the program's memory space.
    - Buffer Overflow - Occurs when data exceeds buffer capacity, overwriting adjacent memory and potentially allowing arbitrary code execution.
    - Race Conditions - Occur when program behavior depends on the timing of concurrent events, which can lead to unexpected results.
        - Time-of-check (TOC) to Time-of-use (TOU) - A type of race condition where resource state changes between validation and use, creating exploitable opportunities.
    - Malicious Update - Delivery of harmful or unauthorized updates to applications or firmware to compromise system security.
- Web-based Vulnerabilities
    - SQL Injection (SQLi)
        - Malicious SQL queries are inserted into input fields to manipulate databases, bypass security, or corrupt data.
        - Prevented by parameterized queries and input validation.
    - Cross-site Scripting (XSS)
        - Injected scripts executed on user devices to steal data or perform actions.
        - Mitigation includes sanitizing inputs and escaping outputs.

Operating System-based Vulnerabilities

- Buffer Overflow - Excessive input overwrites memory, enabling code execution.
- Privilege Escalation - Exploiting flaws to gain higher access rights than intended.
- Injection Flaws - Untrusted input alters commands or queries, e.g., command or SQL injection.
- Race Conditions - Concurrent processes accessing shared resources can cause unexpected behavior.

- Unpatched Software - Known vulnerabilities remain exploitable due to missing updates.
- Insecure Default Settings - Out-of-the-box configurations that expose security risks.
- Insecure File Permissions - Excessively permissive access can allow unauthorized operations.
- Remote Code Execution - Ability for an attacker to run arbitrary code remotely.

Hardware Vulnerabilities

- Firmware - Vulnerabilities in embedded device software.
- End-of-life - Unsupported hardware lacking security updates.
- Legacy - Outdated hardware that does not meet current security standards.

Virtualization and Cloud Vulnerabilities

Virtualization

- Multiple virtual instances run on a single physical device, sharing resources but requiring isolation.

Virtual Machine (VM) Escape

- Attacker code breaks VM isolation to access host resources.

Resource Reuse

- Inadequately sanitized resources may leak data to other VMs.

Cloud-specific Vulnerabilities

- Misconfigured Security Groups/Firewalls - Overly permissive access allows breaches.
- Inadequate Access Control - Weak identity or permission management.
- Data Exposure/Leakage - Sensitive data disclosed accidentally or maliciously.
- API/Identity Management Flaws - Weak authentication or authorization.
- Shared Technology Vulnerabilities - Infrastructure flaws affecting multiple tenants.
- Lack of Monitoring - Limited visibility reduces incident detection.
- Metadata/IMDS Vulnerabilities - Insecure metadata access can expose instance data.
- Insufficient Encryption - Weak or missing encryption at rest or in transit.

- Vendor-Specific Vulnerabilities - Provider-specific security weaknesses.

Supply Chain Vulnerabilities

- Supplier, manufacturer, or service provider weaknesses can compromise products.

Service Provider

- Risks include service disruptions and data breaches.

Hardware Provider

- Vulnerabilities in firmware, supply chain attacks, and weak hardware security.

Software Provider

- Insecure code, unpatched software, or compromised distribution channels.

Zero-Day Vulnerabilities and More

- Zero-Day Vulnerabilities - Unknown flaws with no vendor patch.
- Cryptographic Vulnerabilities - Weak algorithms or poor implementation (e.g., MD5, TLS misconfigurations, poor key management).
- Misconfiguration Vulnerabilities - Configuration errors that allow breaches or service disruption.

- Mobile Device Vulnerabilities
    - Side loading - Installing unofficial apps, increasing malware risk.
    - Jailbreaking - Removing OS restrictions, exposing device to security threats.

CompTIA Security+ (SY0-701) Day 3

Section 2.3: Explain Various Types of Vulnerabilities

Application and Web-based Vulnerability

- Application Vulnerability
    - Memory Injection - A vulnerability in software that allows an attacker to insert and execute malicious code directly in the program's memory space.
    - Buffer Overflow - Occurs when data exceeds buffer capacity, overwriting adjacent memory and potentially allowing arbitrary code execution.
    - Race Conditions - Occur when program behavior depends on the timing of concurrent events, which can lead to unexpected results.
        - Time-of-check (TOC) to Time-of-use (TOU) - A type of race condition where resource state changes between validation and use, creating exploitable opportunities.
    - Malicious Update - Delivery of harmful or unauthorized updates to applications or firmware to compromise system security.
- Web-based Vulnerabilities
    - SQL Injection (SQLi)
        - Malicious SQL queries inserted into input fields to manipulate databases, bypass security, or corrupt data.
        - Prevented by parameterized queries and input validation.
    - Cross-site Scripting (XSS)
        - Injected scripts executed on user devices to steal data or perform actions.
        - Mitigation includes sanitizing inputs and escaping outputs.

Operating System-based Vulnerabilities

- Buffer Overflow - Excessive input overwrites memory, enabling code execution.
- Privilege Escalation - Exploiting flaws to gain higher access rights than intended.
- Injection Flaws - Untrusted input alters commands or queries, e.g., command or SQL injection.
- Race Conditions - Concurrent processes accessing shared resources can cause unexpected behavior.
- Unpatched Software - Known vulnerabilities remain exploitable due to missing updates.
- Insecure Default Settings - Out-of-the-box configurations that expose security risks.
- Insecure File Permissions - Excessively permissive access can allow unauthorized operations.
- Remote Code Execution - Ability for an attacker to run arbitrary code remotely.

Hardware Vulnerabilities

- Firmware - Vulnerabilities in embedded device software.
- End-of-life - Unsupported hardware lacking security updates.
- Legacy - Outdated hardware that does not meet current security standards.

Virtualization and Cloud Vulnerabilities

Virtualization

- Multiple virtual instances run on a single physical device, sharing resources but requiring isolation.

Virtual Machine (VM) Escape

- Attacker code breaks VM isolation to access host resources.

Resource Reuse

- Inadequately sanitized resources may leak data to other VMs.

Cloud-specific Vulnerabilities

- Misconfigured Security Groups/Firewalls - Overly permissive access allows breaches.
- Inadequate Access Control - Weak identity or permission management.
- Data Exposure/Leakage - Sensitive data disclosed accidentally or maliciously.
- API/Identity Management Flaws - Weak authentication or authorization.
- Shared Technology Vulnerabilities - Infrastructure flaws affecting multiple tenants.
- Lack of Monitoring - Limited visibility reduces incident detection.
- Metadata/IMDS Vulnerabilities - Insecure metadata access can expose instance data.
- Insufficient Encryption - Weak or missing encryption at rest or in transit.
- Vendor-Specific Vulnerabilities - Provider-specific security weaknesses.

Supply Chain Vulnerabilities

- Supplier, manufacturer, or service provider weaknesses can compromise products.

Service Provider

- Risks include service disruptions and data breaches.

Hardware Provider

- Vulnerabilities in firmware, supply chain attacks, and weak hardware security.

Software Provider

- Insecure code, unpatched software, or compromised distribution channels.

Zero-Day Vulnerabilities and More

- Zero-Day Vulnerabilities - Unknown flaws with no vendor patch.
- Cryptographic Vulnerabilities - Weak algorithms or poor implementation (e.g., MD5, TLS misconfigurations, poor key management).
- Misconfiguration Vulnerabilities - Errors in configuration that allow breaches or service disruption.
- Mobile Device Vulnerabilities
    - Side loading - Installing unofficial apps, increasing malware risk.
    - Jailbreaking - Removing OS restrictions, exposing device to security threats.

Section 2.4: Given a Scenario, Analyze Indicators of Malicious Activity

Malware Attacks

(Familiar and key characteristics; be able to pick them out)

Malware – Broad category of malicious software with harmful consequences for users or computers.

Malware Categories

- **Worms**
  - Self-propagating malware which does not require user interaction
  - Frequently spread autonomously across networks
  - May be created with or without an additional payload
- **Viruses**
  - Software which replicates itself when executed
  - Typically modifies other software
  - Dormant until the "host" executable is run
  - May be benign, annoying, or destructive
- **Trojans**
  - Sneak into systems under false pretenses
  - Named after the tactic used by the Greeks to infiltrate Troy
  - Commonly used to drop remote-access malware on a system
    - Gain backdoor access to corporate systems
    - Spy on users' online activity
    - Steal sensitive data
  - Generally, not self-replicating
  - Remote Access Trojans (RATs) sneak in back doors that provide system access and remote control
- **Rootkits**
  - Low-level malware which often avoids detection
  - By establishing total control over a system, rootkits can "lie" to tools designed to detect malware
  - Often operate at the **kernel level**, making them especially difficult to detect or remove
  - Secure Boot offers some protection by cryptographically verifying software loaded at boot time
- **Bloatware**
  - Often bundled with operating systems or software packages and installed alongside them
  - Frequently distributed by third parties
  - May reduce performance or introduce unnecessary vulnerabilities
  - In some cases may function as adware (serving unwanted advertisements) or spyware

- **Spyware**
    - Malicious software which gathers information about users and systems, often without their knowledge
        - May collect:
            - Keystrokes
            - Browsing history
            - Screen captures
            - Webcam or microphone input
- **Keylogger**
    - Software or hardware tool designed to record and monitor keystrokes on a computer or device without the user's knowledge or consent
    - A type of spyware
- **Logic Bomb**
    - A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met
- **Ransomware**
    - Encrypts files and demands payment in return for the decryption key
    - Often imposes a deadline to encourage payment
    - Payment frequently conducted using cryptocurrencies

Physical Attacks

Physical Attack – Unauthorized access or tampering with computer systems, networks, or hardware components.

- Occurs when an attacker gains physical proximity to the target and attempts to compromise its security
- Examples include device theft, USB drops, and tampering with network equipment

Brute Force Attacks

- Repeatedly attempting every possible password, PIN, or encryption key until the correct one is found
- Can be automated using specialized tools

Radio Frequency Identification (RFID) Cloning

- An attacker attempts to create a duplicate or clone of an RFID (Radio Frequency Identification) tag or card
- Used to gain unauthorized access to a secure area, system, or data

Environmental Threats

- Any threat or event that targets a system, infrastructure, or data center by exploiting environmental vulnerabilities
    - **HVAC failures** – may cause overheating and downtime
    - **Fires** – can destroy equipment and data
    - **Floods** – may damage hardware and cause prolonged outages
    - **Earthquakes** – may physically damage systems and infrastructure
    - **Power outages** – can cause unexpected shutdowns and data loss
    - **Equipment failures** – may impact system availability and reliability

Section 2.4: Given a Scenario, Analyze Indicators of Malicious Activity

Network Attacks

Distributed Denial of Service (DDoS)

- A multitude of compromised devices, often part of a botnet, are used to flood a target system or network with an overwhelming amount of traffic or requests.
- **Objective**: Render the targeted system or network unavailable by overwhelming its resources, causing a denial of service to legitimate users.

Types of DDoS:

- **Amplified**
  - Attacker leverages open servers or devices to amplify the volume of traffic directed at the target.
  - Results in a massive traffic surge, overwhelming the target's resources and causing denial of service.
- **Reflected**
  - Attacker sends requests to multiple third-party servers with a spoofed (the target's) source IP address.
  - When the servers respond, the target gets the responses, possibly overwhelming it.

Domain Name System (DNS) Attacks

- **Spoofing/Poisoning** – Corrupting a DNS cache or table to redirect users to malicious sites instead of legitimate destinations.
- **Flooding** – Overwhelming a DNS server with requests, making it unavailable to legitimate users.
- **Amplification** – Exploiting vulnerable DNS servers to send large responses to a target system, amplifying the attack's impact.
- **Hijacking** – Taking control of a DNS server or altering DNS configurations to redirect traffic or intercept communications.

Wireless Attacks

- **Eavesdropping** – Intercepting wireless communications to capture data packets, credentials, or other sensitive information.
- **Rogue Access Points** – Unauthorized wireless access points placed on a network to trick users into connecting.
- **Evil Twin** – A rogue access point configured to mimic a legitimate one, tricking users into connecting and exposing data.
- **Denial of Service (DoS)** – Flooding or interfering with wireless frequencies to make the network unusable.
- **Brute Force** – Attempting repeated password guesses to gain unauthorized access to a wireless network.
- **MAC Address Spoofing** – Attacker alters their device's MAC address to impersonate a legitimate device on the network.

On-Path Attack

- Attackers insert themselves between two parties, posing as the other peer in either direction.
- **Uses**:
    - Eavesdropping (confidentiality)
    - Interference (availability)
    - Modification of communications (integrity)

Credential Replay Attack

- An attacker intercepts and later reuses captured credentials, such as usernames and passwords.
- The attacker doesn't need to decipher or crack the credentials, only replay them as originally captured.

Malicious Code Attack

- Malicious software or code introduced into a computer system, network, or device.
- Intent is to compromise, disrupt, or gain unauthorized access.
- **Examples**: Viruses, Worms, Trojans, Ransomware, Spyware, Adware.

Application Attacks

Injection Application Attack

- An attacker inserts malicious data or commands into an application's input fields or data streams, causing the application to process this input in an unintended and harmful way.
- **Examples**:
    - SQL Injection (SQLi)
    - Cross-Site Scripting (XSS)

Buffer Overflow Application Attack

- Occurs when data exceeds buffer capacity, overwriting adjacent memory and potentially allowing arbitrary code execution.

Replay Attack

- An attacker intercepts and retransmits data packets or messages previously recorded during a legitimate transaction.
- Goal is to repeat the exchange to gain unauthorized access or achieve a malicious outcome.

Privilege Escalation Application Attack

- Attacker exploits vulnerabilities to gain higher access levels than initially granted.
- Elevated access allows unauthorized actions, compromise of security, or control over sensitive resources.

Forgery Application Attack

- Tricks a user into executing unwanted actions on a web application in which they are authenticated.
- **Techniques**:
    - Relies on authentication
    - Uses deceptive links

Directory Traversal Application Attack

- Attacker manipulates input fields or parameters to navigate outside the intended directory structure.
- Goal: Access unauthorized files or directories, potentially exposing sensitive data or executing malicious code.
- **Example**: `www.widget.com/../../../etc/passwd` (%2e%2e%2f represents `../`)

Cryptographic and Password Attacks

Downgrade Cryptographic Attack

- Attacker manipulates the encryption protocol or security settings during client-server communication.
- Forces weaker or outdated cryptographic methods, making interception or manipulation easier.

Collision Cryptographic Attack

- Two different inputs produce the same hash value.
- Attack targets cryptographic hash functions by finding distinct data sets that result in identical hash values.
- **Recall**:
    - Same input → same hash
    - Different input → wildly different results (under normal secure hashing)

Birthday Cryptographic Attack

- Specific type of collision attack based on the **birthday paradox**.
- Seeks different inputs that hash to the same value, exploiting probability of collisions.

Password Attacks

- **Spraying** – Trying a few common passwords across many accounts.

- **Brute Force** – Systematically trying all possible password combinations for a single account.

Indicators of Malicious Activity

- **Account Lockout** – Suggests unauthorized attempts to access an account or system.
- **Concurrent Session Usage** – More active sessions than expected; may indicate compromise.
- **Blocked Content** – Security mechanisms flagging content as harmful, or attackers seizing content to block user access.
- **Impossible Travel** – Logins from geographically distant locations in an unrealistically short time.
- **Resource Consumption** – Resources used abnormally (e.g., high CPU, memory, network traffic).
- **Resource Inaccessibility** – Users unable to access normally available resources.
- **Missing Logs** – Suggests tampering or attempts to cover tracks.
- **Out-of-Cycle Logging** – Logging outside normal patterns may indicate malicious activity.