CompTIA Security+

Personal Notes Exam Objectives

Author:
Scott *Skrobel*

May 19, 2024

Table of Contents

1 Threats, Attacks and Vulnerabilities

1.1 Compare and contrast types of attacks

Phishing : Social engineering tactic to acquire personal information from a fake email with a clickable link.
Smishing : (SMS phishing) The use of deceptive text messages into divulging sensitive information.
Vishing : (Voice Phishing) Impersonates a trusted entity, such as a bank to trick into giving information.
Spam : Unsolicited inappropriate messages sent with the purpose of spreading malware, advertising, phishing.
Spear phishing : Targeted type of phishing attack to make the scam convincing, often with insider information.
Dumpster diving : Searching through an organization's or individual's trash to find sensitive information.
Shoulder surfing : Observing a victim's screen or keyboard to obtain sensitive information.
Pharming : Manipulating the DNS system to resolve fake domain names, to lead them to a fake website.
Tailgating : Physical security breach by following authorized person to get access to secure areas.
Eliciting information : Psychological tactics to encourage individuals to share their knowledge willingly.
Whaling : Spear phishing for high-profile executives in an organization.
Prepending : Organizing, manipulating, and structuring data in various applications.
Identity fraud : An individual wrongfully obtains and uses someone else's personal data in a deceptive manner.
Invoice scams : Impersonation of a legit business to deceive individuals into paying fraudulent invoices.
Credential harvesting : Tricking someone into disclosing login credentials to access sensitive info.
Reconnaissance : Initial phase to gather intelligence via passive and active techniques.
Hoax : Fabrication intended to deceive or trick individuals into believing false information or events.
Impersonation : Masquerading as a legitimate user or entity to gain unauthorized access to information.
Watering hole attack : Infecting a commonly visited website of a targeted specific group.
Typosquatting : URL hijacking or domain squatting of fake domains which resemble a legit website.
Pretexting : Fabricated scenario involving direct interaction to obtain sensitive information.
Influence campaigns : Coordinated effort to shape public opinion, influence perceptions, and manipulate.
Hybrid warfare: Blends conventional warfare tactics with unconventional method
Principles (reasons for effectiveness)

- **Authority**: The actor acts as an individual of authority
- **Intimidation**: Frightening or threatening the victim.
- **Consensus**: Convince based on what's normally expected.
- **Scarcity**: Limited resources and time to act.
- **Familiarity**: The victim is well known.
- **Trust**: Gain their confidence, be their friend.
- **Urgency**: Limited time to act, rush the victim.

1.2 Given a scenario, analyze indicators of compromise

Malware

Ransomware: Denies access to a computer system or data until a ransom is paid.

Trojan: A form of malware that pretends to be a harmless application.

Worm: A self-contained infection that can spread itself through networks, emails, and messages.

PUP's: Potentially Unwanted Programs software applications that may exhibit undesirable characteristics.

Memory-resident malware: Operates primarily in a computer's volatile memory (RAM) rather than with files

Command and control: (C2) Centralized server used by attackers to manager compromised devices.

Bots: AI inside an infected machine performs specific actions as a part of a larger entity known as a botnet.

Cryptomalware: A malicious program that encrypts programs and files on the computer to extort money.

Logic Bomb: A malicious program that lies dormant until a specific date or event occurs.

Spyware: Software that installs itself to spy and sends stolen info back to the host machine.

Keyloggers: A malicious program that saves all of the keystrokes of the infected machine.

Remote Access Trojan (RAT) A remotely operated Trojan.

Rootkit: A backdoor program that allows full remote access to a system.

Backdoor: Allows for full access to a system remotely.

Password Attacks

Brute Force: Systematically trying a large number of possible passwords.

- **Offline**: Attempting to crack a password hash without directly interacting with the target system, rather on their own independant computer.
- **Online**: Attempting to guess a user's password by repeatedly trying different combinations.

Sprying: A Type of brute-force attack by attempting to authenticate with commonly used passwords. Small number of passwords against many accounts.

Dictionary: A password attack that creates encrypted versions of common dictionary words and then compares them against those in a stolen password file. Guessing using a list of possible passwords.

Rainbow Table: Large pregenerated data sets of encrypted passwords used in password attacks.

Plaintext/Unencrypted: The attacker has both the plaintext and its encrypted version.

Physical attacks

Malicious Flash Drive: A storage device loaded with malware.

Serial Bus (USB) cable: A USB cable designed to compromise systems upon connection.

Card cloning : Creating a copy of a credit or other card with stolen data.

Skimming: Stealthily capturing and storing all the details stored on your card's magnetic stripe.

Adversarial AI

Tainted Training Data for ML: Modifying the data used to train machine learning models to cause misclassifications or errors.

Security of Machine Learning Algorithms: Ensuring ML algorithms are protected against manipulation and attacks.

Other

Supply-chain Attacks Targeting less-secure elements in the supply network to compromise a primary target.

Cloud-based vs. On-premises Attacks: Security incidents occurring either in a cloud infrastructure or on locally hosted (on-premises) resources.

Cryptographic Attacks

Birthday: Exploiting the probability of two distinct inputs having the same output.

Collision: Finding two different inputs that provide the same output.

Downgrade: Forcing a system to fall back to a less secure version to exploit vulnerabilities.]

1.3 Given a scenario, analyze potential indicators associated with application attacks

Privilege Escalation: An attack that exploits a vulnerability that allows them to gain access to resources that they normally would be restricted from accessing.(imagine logging into a computer as a guest account and having access to admin power)

Cross-site Scripting: (XXS) It's like sneaking a secret note into a bunch of official letters. You insert malicious scripts into websites, which then run on another user's browser, stealing information or performing actions on their behalf without them knowing.

Injections: Occurs when processing invalid data, inserts code into vulnerable program and changes the course of execution.

- **Structured query language (SQL Injection):** Inserting SQL code into a query to manipulate a database (i.e. to view, edit, or delete data).
- **Dynamic-link library(DLL Injection):** Inserting code into a running process by taking advantage of Dynamic Link Libraries used by software.
- **Lightweight Directory Access Protocol (LDAP Injection):** Manipulating Lightweight Directory Access Protocol queries (used for organizing/finding user or device data in networks).
- **Extensible Markup Language (XML Injection):** Inserting elements into an XML document to exploit the structure and logic of an application.

Pointer/object dereference: Imagine forgetting to check who's knocking at the door and just letting them in — failing to validate who or what a pointer is pointing to can allow unauthorized access or crashes.

Directory Traversal: It's like navigating through a building's restricted areas by exploiting weak security, accessing unauthorized files/folders in a system.

Buffer Overflows: Imagine pouring water into a glass until it overflows, only here, excessive data overflows into other memory areas, potentially allowing malicious code execution.

Race Conditions & Time of Check/Time of Use: Two actions racing to utilize a resource and whoever wins could impact the system. If malicious action wins, it can exploit the time gap between checking a condition and using a resource.

Error Handling: How a system responds to unexpected inputs or conditions — poor error handling might expose sensitive information or pathways to attacks.

Input Handling: Not checking or sanitizing input properly could allow harmful data into a system, causing malfunctions or unauthorized activities.

Replay Attack & Session Replays: Replaying is resending data (like login credentials) intercepted earlier to gain unauthorized access. Session replays involve capturing and reusing session identifiers, allowing attackers to impersonate legitimate users.

Integer Overflow: It's like an odometer rolling over to zero after reaching its maximum value, only here, exceeding numerical storage capacity might cause erratic system behavior.

Request Forgeries: Tricking a user or system into performing actions without knowing:

- **Server-Side Request Forgery (SSRF):** Making a server unknowingly perform actions on behalf of an attacker.
- **Cross-Site Request Forgery (CSRF):** Making a user's browser perform an unwanted action on a site where they are authenticated.

API Attacks: Exploiting vulnerabilities in APIs — essentially, pathways that let different software components communicate — to interfere with an application's functionality or steal data.

Resource Exhaustion: Draining a system's resources (like memory or processing power) to slow it down or cause a failure, making it vulnerable to other attacks.

Memory Leak: Continually using up memory without releasing it back, like continually filling a basket with apples and never emptying it, which eventually causes slowdowns or crashes.

Secure Sockets Layer (SSL) stripping: Downgrading a secure HTTPS connection to an unsecured HTTP connection, making data transmission vulnerable to interception.

Driver Manipulation:
- **Shimming**: Using extra code (a shim) to make a driver run in environments it's not compatible with, potentially opening security gaps.
- **Refactoring**: Changing the driver's internal structure without altering its external behavior, potentially introducing vulnerabilities.

Pass the Hash: Using a user's hash (a type of encrypted password) to authenticate with a service without knowing the actual password.

1.4 Given a scenario, analyze potential indicators associated with network attacks

Wireless

Evil Twin: Imagine someone impersonating your Wi-Fi network to trick devices into connecting to it. It's an "evil twin" of your legit Wi-Fi, stealing data and spying on users.

Rogue Access Point: An unauthorized Wi-Fi access point, maybe added by an employee or attacker, which can bypass security settings.

Bluesnarfing: Stealing information from Bluetooth-enabled devices by exploiting vulnerabilities in their Bluetooth connection.

Bluejacking: Sending unsolicited messages to a Bluetooth device, mostly harmless but potentially annoying.

Disassociation: Interrupting the Wi-Fi connection between a device and a network, causing disruptions.

Jamming: Flooding a frequency (like Wi-Fi or cell frequencies) to block communications.

Radio frequency identification (RFID): A tech that uses radio waves for tracking and identification but can be exploited to illicitly read information.

Near-field communication (NFC): A way to wirelessly share data over short distances, like payment info, which can be exploited for unauthorized data access.

Initialization Vector (IV): A random number used in cryptography for preventing predictability in encrypted data, but if not handled properly, can be a vulnerability.

Layer 2 Attacks

ARP Poisoning: Confusing network devices by sending fake Address Resolution Protocol messages, redirecting traffic through an attacker's device.

Media access control (MAC) Flooding: Overflowing the network switch with too many Media Access Control addresses, forcing it into acting like a basic hub and revealing internal data traffic.

MAC Cloning: Copying a legit MAC address to impersonate a network device.

Domain Name System (DNS)

Domain Hijacking: Taking control of a domain away from the rightful owner, often for malicious activities.

DNS Poisoning: Providing false DNS responses to redirect a user's traffic to malicious sites.

URL Redirection: Manipulating URLs to direct users to unintended pages, often for phishing.

Domain Reputation: How trustworthy a domain is, based on its past actions and security posture.

Distributed denial-of-service (DDoS): Overwhelming a target, such as a website, with a flood of internet traffic, making it unavailable to users. Variants include targeting network, application, or operational technology layers.

On-Path Attack (Man-in-the-Middle): This is like eavesdropping, where the attacker intercepts and possibly alters the communication between two parties without them knowing.

Malicious code or script execution

PowerShell, Python, Bash: Different scripting languages that can be used to automate tasks or exploit vulnerabilities.

Macros, VBA: Automated scripts, often in Office documents, that can be exploited to run malicious code.

1.5 Different threat actors, vectors, and intelligence sources

Actors and Threats

dvanced Persistent Threat (APT): Highly skilled attackers, often funded by governments, who aim to stealthily infiltrate and stay in networks for a long time, usually for espionage.

Insider Threats: People inside an organization (like employees or contractors) who pose security risks, either maliciously or inadvertently.

State Actors: Hackers sponsored by national governments to engage in cyber espionage, warfare, or sabotage.

Hacktivists: Individuals or groups hacking for political or social reasons rather than financial gain.

Script Kiddies: Inexperienced hackers who use pre-written scripts or tools to perform attacks, without much understanding of how they work.

Criminal Syndicates: Organized crime groups engaging in cybercrime for financial gain.

Hackers: People who find and exploit vulnerabilities in systems. They can be:

- **Authorized:** Have permission to access.
- **Unauthorized:** No permission to access.
- **Semi-authorized:** Somewhere in between; maybe they had permission at one point or for certain tasks.

Shadow IT: Unauthorized tech solutions used inside an organization without the IT department's knowledge or approval.

Competitors: Business rivals who might engage in cyber tactics to gain a competitive edge.

Attributes of Actors

- **Internal/External:** Are they inside or outside the organization?
- **Level of Sophistication:** How skilled are they?
- **Resources:** What tools, money, or people do they have at their disposal?
- **Intent/Motivation:** Why are they doing what they're doing?

Vectors

- **Direct Access:** Physically accessing systems.
- **Wireless:** Via Wi-Fi, Bluetooth, etc.
- **Email:** Think phishing or malware attachments.
- **Supply Chain:** Targeting suppliers or service providers.
- **Social Media:** Spreading malware or misinformation.
- **Removable Media:** USB drives, DVDs, etc.
- **Cloud:** Exploiting vulnerabilities in cloud services.

Threat Intelligence Sources

- **Open-Source Intelligence (OSINT):** Publicly available info.
- **Vulnerability Databases:** Listings of known security vulnerabilities.
- **Public/Private Information-Sharing Centers:** Organizations that share threat data.
- **Dark Web:** A part of the internet not indexed by search engines, often hosting illegal activities.
- **Indicators of Compromise:** Signs that a breach has occurred.
- **Automated Indicator Sharing (AIS), STIX/TAXII:** Tools and formats for sharing threat intelligence.
- **Predictive Analysis:** Forecasting future threats.

- **Threat Maps:** Visual representation of ongoing cyber attacks globally.
- **File/Code Repositories:** Places where software code is stored, which can sometimes contain vulnerabilities.

Research Sources

- **Vendor Websites:** Companies that make software/hardware often provide updates or alerts.
- **Conferences:** Where experts discuss the latest in cybersecurity.
- **Academic Journals:** Peer-reviewed publications on new findings.
- **Request for Comments (RFC):** Official documentations and standards.
- **Local Industry Groups:** Local or regional groups focusing on security.
- **Social Media:** Real-time info, but needs verification.
- **Threat Feeds:** Live data streams about potential threats.
- **Adversary Tactics, Techniques, and Procedures (TTP):** Documented strategies used by attackers.

1.6 Explain the security concerns associated with various types of vulnerabilities

Actors and Threats

Cloud-based vs. On-premises Vulnerabilities: Cloud-based vulnerabilities: Relate to the weaknesses within cloud services and platforms that can be exploited by attackers, such as misconfigured cloud storage or inadequate identity and access management. On-premises vulnerabilities: Concern issues in your own physical environment (like a server room in your building), like outdated firewalls or servers with unpatched software.

Zero-day: A Zero-day vulnerability refers to a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the vulnerability. It's called "zero-day" because the developers have "zero days" to fix the problem that has just been exposed — and perhaps already exploited by hackers.

Weak Configurations

- **Open Permissions:** Allowing too much access to too many people/users.
- **Unsecure Root Accounts:** Not protecting high-level administrative accounts properly.
- **Errors:** Mistakes in coding or system setup.
- **Weak Encryption:** Not using strong methods to protect data.
- **Unsecure Protocols:** Using outdated or insecure communication protocols.
- **Default Settings:** Not changing the settings that the system or application came with.
- **Open Ports and Services:** Leaving too many openings for attackers to potentially exploit.

Third-party Risks

- **Vendor Management:** Not properly overseeing or managing the organizations you buy products or services from.
- **System Integration:** Problems that might arise when trying to get different systems to work together.
- **Lack of Vendor Support:** Vendors not providing sufficient help or updates for their products.
- **Supply Chain:** The process of creating and delivering a product, which can be disrupted or exploited at various stages.
- **Outsourced Code Development:** Getting external parties to write software for you, which might not be as secure.
- **Data Storage:** Where and how you store data, and the vulnerabilities there.

Legacy Platforms: Using outdated systems or software that no longer receive updates and therefore, might be full of vulnerabilities.]

Improper or Weak Patch Management

- **Firmware:** The foundational software for hardware, often neglected in the patching process.
- **Operating System (OS):** The main software that runs a computer, which might be left outdated.
- **Applications:** Programs used for various purposes that might not be kept up-to-date with security patches.

Impacts

- **Firmware:** The foundational software for hardware, often neglected in the patching process.
- **Data Loss:** Losing data due to an incident.
- **Data Breaches:** Unauthorized access to data.

- **Data Exfiltration:** The unauthorized copying, transfer, or retrieval of data.
- **Identity Theft:** Unauthorized use of someone's personal data.
- **Financial:** Monetary losses from an incident.
- **Reputation:** Damage to the organization's standing.
- **Availability Loss:** Losing access to systems, data, or networks.

1.7 Summarize the techniques used in security assessments

Threat Hunting

- **Intelligence Fusion:** Combining various sources of information to generate actionable intelligence about threats.
- **Threat Feeds:** Streams of data related to potential threats, like IP addresses known to be malicious.
- **Advisories and Bulletins:** Alerts and notifications regarding new threats or vulnerabilities.
- **Maneuver:** Adapting to or moving against a threat to neutralize it.

Vulnerability Scans

- **False Positives:** Alerts on vulnerabilities that aren't actually present (false alarms).
- **False Negatives:** Failing to detect an actual vulnerability (missing a real threat).
- **Log Reviews:** Analyzing logs to identify suspicious activity.
- **Credentialed vs. Non-credentialed:** Scans with login credentials vs. those without to see system vulnerabilities from different viewpoints.
- **Intrusive vs. Non-intrusive:** Scans that might impact system performance vs. those that don't.
- **Application/Web Application/Network:** Scans targeting different elements: software applications, web platforms, or network infrastructure.
- **CVE/CVSS:** Standardized identifiers and scorings for vulnerabilities.
- **Configuration Review:** Checking system setups for vulnerabilities.

Syslog/Security Information and Event Management (SIEM)

- **Review Reports:** Analyzing compiled data and insights.
- **Packet Capture:** Collecting data packets transmitted over networks for analysis.
- **Data Inputs:** Different types of data fed into the SIEM for analysis.
- **User Behavior Analysis:** Studying how users interact with systems to identify anomalies.
- **Sentiment Analysis:** Utilizing data analysis to understand sentiments or attitudes expressed in source data.
- **Security Monitoring**: Continuously observing systems to detect and respond to security incidents.
- **Log Aggregation:** Collecting log data from different sources into a single location.
- **Log Collectors:** Systems or applications that gather log data.

Security Orchestration, Automation, and Response (SOAR)

- **Security Orchestration:** Coordinating and structuring how different security solutions work together.
- **Automation:** Utilizing technology to perform tasks without human intervention.
- **Response:** Actions taken to mitigate, prevent, or remediate security incidents.

2 Architecture and Design