CompTIA Security+ Study Notes

# CIA Triad

Confidentiality, Integrity, and Availability - The core principles of information security.

# DAD Model

Disclosure, Alteration, and Denial - Reverse of the CIA Triad, representing what we protect against.

# NIST Cybersecurity Framework

A framework for improving cybersecurity practices that includes Identify, Protect, Detect, Respond, and Recover.

# Hashing

A one-way cryptographic function used to ensure data integrity.

# Symmetric Encryption

Encryption method using the same key for both encryption and decryption.

# Asymmetric Encryption

Encryption method using two keys, one public and one private.

# Public Key Infrastructure (PKI)

A framework for managing digital keys and certificates.

# SSL/TLS

Protocols for securing communications, especially for websites (HTTPS).

# Vulnerability

A weakness in a system that can be exploited by attackers.

# Risk

The likelihood of a threat exploiting a vulnerability.

# Exploit

A method used by attackers to take advantage of a vulnerability.

# Attack Surface

All the points where an attacker could potentially gain unauthorized access to a system.

# Social Engineering

Manipulating individuals to reveal confidential information, typically through deception.

# Zero-Day Vulnerability

A vulnerability that is exploited before the vendor is aware of it or has issued a fix.

# Malware

Malicious software designed to harm or exploit a system, including viruses, worms, ransomware, and spyware.

# Phishing

A type of social engineering attack that impersonates legitimate entities to steal information.

# Denial of Service (DoS)

An attack that prevents access to a service or system by overwhelming it with traffic.

# Man-in-the-Middle (MitM) Attack

An attack where the attacker intercepts communication between two parties.

# Botnet

A network of compromised devices controlled by an attacker to perform malicious activities.

# Encryption

The process of converting plaintext into ciphertext to prevent unauthorized access.

# Decryption

The process of converting ciphertext back into readable plaintext.

# Public Key Encryption

An asymmetric encryption method using two keys, one public and one private.

# AES (Advanced Encryption Standard)

A widely-used symmetric encryption algorithm.

# RSA

A public-key encryption algorithm used for secure data transmission.

# Digital Signature

A mathematical scheme for verifying the authenticity and integrity of digital messages.

# Certificate Authority (CA)

A trusted entity that issues digital certificates to authenticate the identity of a user or system.

# SHA (Secure Hash Algorithm)

A cryptographic hash function used to ensure data integrity.

# Authentication

The process of verifying the identity of a user or device.

# Authorization

The process of granting or denying access to resources based on the authenticated identity.

# Single Sign-On (SSO)

A method that allows a user to log in once and access multiple systems without re-authenticating.

# Multi-Factor Authentication (MFA)

A security process that requires two or more authentication factors to verify identity.

# RBAC (Role-Based Access Control)

A system where access is based on the role of the user within an organization.

# LDAP (Lightweight Directory Access Protocol)

A protocol used to access and manage directory services.

# Account Lockout

A security measure that locks user accounts after a certain number of failed login attempts.

# Federation

The process of linking identity management systems across multiple domains to allow single sign-on.

# Load Balancer

A device or software that distributes incoming network traffic across multiple servers to ensure high availability.

# DMZ (Demilitarized Zone)

A physical or logical network area used to separate internal networks from external networks for security.

# DNS Server

A server that resolves domain names to IP addresses, enabling access to websites.

# Firewall

A security system that monitors and controls incoming and outgoing network traffic.

# Intrusion Detection System (IDS)

A system that detects malicious activities or policy violations within a network or system.

# Intrusion Prevention System (IPS)

A system that not only detects but also prevents security threats.

# Virtual Private Network (VPN)

A secure and encrypted connection used to access private networks over the internet.

# Redundancy

The inclusion of extra components or systems to ensure continuous operation in case of failure.

# High Availability (HA)

A design approach that ensures a system is continuously operational, minimizing downtime.

# VPN (Virtual Private Network)

A secure and encrypted connection used to access private networks over the internet.

# Proxy Server

A server that acts as an intermediary between a user's device and the internet for security and privacy.

# NAT (Network Address Translation)

A technique used to translate private IP addresses into public ones to enhance network security.

# WPA2 (Wi-Fi Protected Access 2)

A security protocol for wireless networks that ensures secure data encryption and authentication.

# 802.1X

A network access control protocol used for authenticating devices trying to connect to a network.

# SNMP (Simple Network Management Protocol)

A protocol used for managing and monitoring network devices.

# Incident Response

A structured approach to handling security breaches or attacks to minimize damage.

# Disaster Recovery Plan

A documented process for recovering data and systems after a catastrophic event.

# Business Continuity Plan

A plan to ensure that critical business functions continue during and after a disaster.

# Change Management

A process for managing updates or changes to systems and networks in a controlled manner.

# Data Retention Policy

Guidelines on how long data should be kept and when it should be deleted to minimize security risks.

# Security Information and Event Management (SIEM)

A software solution that provides real-time analysis and alerts based on security events from various network devices.

# Log Management

The practice of collecting, storing, and analyzing logs from different systems to monitor for unusual activities.

# Threat Hunting

The proactive search for potential security threats within a network.

# Vulnerability Scanning

The process of identifying weaknesses in a network or system through automated tools.

# Penetration Testing

A simulated cyberattack to evaluate the security of a system or network.

# GDPR (General Data Protection Regulation)

A regulation in the EU that protects the privacy and personal data of individuals.

# HIPAA (Health Insurance Portability and Accountability Act)

A U.S. law that sets standards for protecting sensitive patient health information.

# PCI DSS (Payment Card Industry Data Security Standard)

A set of standards designed to ensure that companies processing credit card information maintain secure systems.

# SOX (Sarbanes-Oxley Act)

A U.S. law aimed at protecting investors from fraudulent financial reporting by corporations.

# TLS (Transport Layer Security)

A protocol for securing data communications over a computer network.

# Ransomware

A type of malicious software that encrypts a victim's files and demands payment for decryption.

# Trojan Horse

A type of malware that disguises itself as a legitimate program to gain access to a system.

# Worm

A self-replicating program that spreads through networks and systems.

# Spyware

Software that collects information about a user or system without their consent.

# Rootkit

A type of malware that allows an attacker to gain control over a computer without the user's knowledge.

# Keylogger

A program designed to capture keystrokes to steal sensitive information.

# Backdoor

A method of gaining unauthorized access to a system by exploiting vulnerabilities or weaknesses.

# Bot

A network of infected devices used to carry out coordinated malicious activities.

# White Hat

Ethical hackers who test systems for vulnerabilities to improve security.

# Black Hat

Malicious hackers who exploit vulnerabilities for personal gain or to cause harm.

# Gray Hat

Hackers who operate between ethical and malicious activities, sometimes performing unauthorized activities for personal gain or improvement.

# APT (Advanced Persistent Threat)

A type of threat where attackers gain unauthorized access to systems over an extended period.

# Trojans

A malicious program that disguises itself as a legitimate application to trick users.

# Malicious Code

Malicious software designed to damage or disrupt systems, often using code exploits.

# SQL Injection

An attack method where attackers insert harmful code into a web application's database through user input.

# Cross-Site Scripting (XSS)

An attack that injects harmful scripts into trusted websites to compromise users.

# Cross-Site Request Forgery (CSRF)

An attack that tricks users into performing unintended actions through their web browser.

# Buffer Overflow

An attack that exploits a system's memory by sending excess data to overflow the buffer.

# Access Control List (ACL)

A list of rules that defines what traffic is allowed or denied in a network environment.

# Access Control Models

A security model where permissions are based on roles assigned to users.

# Least Privilege

A concept of ensuring that users only have the minimum necessary access to perform their tasks.

# Separation of Duties

A security control to divide tasks and privileges between multiple users to reduce risks.

# Privilege Escalation

The act of gaining higher-level privileges than originally granted by exploiting system weaknesses.

# Tokenization

The process of replacing sensitive data with an equivalent, non-sensitive placeholder.

# Obfuscation

The practice of obscuring data or operations to prevent unauthorized access or understanding.

# Honeypot

A decoy system or resource designed to lure attackers and distract them from real systems.

# Honeynet

A network of decoy systems designed to trap and detect attackers.

# Spoofing

A method of impersonating a legitimate system or service to trick users or devices.

# Flooding

A type of attack where a system is overwhelmed with more requests than it can handle.

# Brute Force Attack

A method of attacking systems by trying many possible combinations to guess passwords.

# Rainbow Tables

A table of precomputed hash values used to quickly reverse a hash function.

# Salting

A method of adding random data to a password before hashing it to increase security.

# Token-based Authentication

An authentication system that generates a token for user access, typically as a second layer of security.

# Public Key

A system that uses both a public and private key pair for secure communication.

# Private Key

A key used in asymmetric encryption that is shared publicly for encryption but kept secret for decryption.

# Digital Certificates

A secret key used in asymmetric encryption to decrypt messages encrypted with the corresponding public key.

# Two-Factor Authentication (2FA)

A certificate issued by a trusted authority to authenticate the identity of users or systems.