SY0-701 - CompTIA Security+ NOTES

Root of Trust (Trust Source)

A trusted third party or component that ensures the security and authenticity of a new connection or system.

Examples:

- **HSM (Hardware Security Module)** – External hardware designed for securely storing keys, certificates, and cryptographic credentials on a large scale.

- **TPM (Trusted Platform Module)** – A built-in chip with protection against brute-force attacks. It can work alongside FDE (Full Disk Encryption).

- **Secure Enclave (iOS)** – Isolated from the main processor to provide an additional security layer. It protects sensitive user data even if the Application Processor kernel is compromised. It monitors the boot process, creates true random numbers, stores root cryptographic keys, and more.

- **CA (Certificate Authority)** – Issues SSL/TLS certificates that confirm the authenticity of websites.

Access Control Types:

- **RBAC (Role-Based Access Control)** – IT has different access than Management.

- **Discretionary Access Control** – Access is assigned by the owner. Example: A user creates a file and assigns the level of access.

- **Mandatory Access Control (MAC)** – Different security levels (public, private, secret). Each file and user has different security levels.

- **Rule-Based Access Control** – Access is granted based on conditions (e.g., specific time of day, required browser).

Mail Anti-Spoofing:

- **DMARC** – Uses SPF and DKIM to determine whether an email should be marked as spam.
- **SPF (Sender Policy Framework)** – Checks if the email originates from an authorized server.
- **DKIM (DomainKeys Identified Mail)** – Ensures the message has not been modified. It digitally signs emails to verify their authenticity. The receiver confirms the sender's digital signature using a public key stored in the DNS record.

NAC (Network Access Control):

A security system that checks specific conditions before allowing internet access, such as firewall configuration or OS updates.

Recovery & Incident Response:

- **RPO (Recovery Point Objective)** – Defines how much data loss is acceptable during recovery.
- **RTO (Recovery Time Objective)** – Determines how long it takes to restore service.
- **SIEM (Security Information and Event Management)** – A log aggregation and analysis service.
- **IPSec** – Used for VPN security.
- **Escalation Scripting** – Used for automation and orchestration in Incident Response.

Security Documentation:

- **Statement of Work (SOW)** – Defines tasks.
- **SLA (Service Level Agreement)** – Defines minimum service terms (e.g., 99% uptime guarantee).
- **Data Retention Policy** – Defines how long data must be stored (e.g., EU regulations).
- **Due Care** – Exercising due diligence (e.g., ensuring servers are properly secured, penetration testing).

Risk Management:

- **Accept** – Accepting the risk in business.
- **Transfer** – Outsourcing the risk to another entity.
- **Avoidance** – Disconnecting from the internet to eliminate risk.
- **Risk Tolerance** – Acceptable amount of risk.
- **Mitigation** – Example: Offline backups for ransomware mitigation.

Additional Security Concepts:

- **Shadow IT** – Ignoring IT policies, such as using personal Google Drive for corporate data.
- **Quarantine (Antivirus)** – Isolating files in a safe environment.
- **IPS (Intrusion Prevention System)** – Allows or denies traffic based on known vulnerabilities.
    - **Fail Open** – If IPS fails, network traffic continues to flow.
- **Sideloading** – Manually installing apps outside the official Apple App Store.
- **Vendor Monitoring** – Continuous monitoring of third-party service providers.

- **Regulatory Compliance** – Adhering to legal and industry regulations (e.g., GDPR, HIPAA).
- **Attestation** – Formal confirmation of compliance with standards.

Security & IT Assessments:

- **Self-Assessment** – Company's internal review of security policies.
- **Internal Self-Assessment with Audit** – Verifies that users follow the principle of least privilege.
- **Dependency List** – Helps plan for potential changes.
- **Policy Administrator** – Generates access tokens or credentials.
- **Gap Analysis** – Determines the difference between the current and desired state.

Networking & Infrastructure:

- **Parallel Processing** – Using multiple processors simultaneously.
- **Snapshot** – A type of backup for virtual machines (VMs).
- **Screened Subnet (DMZ)** – A demilitarized zone for security.
- **SCAP (Security Content Automation Protocol)** – Automates vulnerability management.
- **Exposure Factor** – Calculates business loss as a percentage.
    - Example: If 40% of a building is destroyed by fire, the exposure factor = 40%.
- **RAID** – A method of combining hard drives for redundancy (not a backup technology).
- **Right to Audit** – Ensures the ability to conduct periodic audits in contracts with third parties.

Business & Compliance:

- **Due Diligence** – Verifying information before engaging in business transactions.
- **Conflict of Interest** – Personal or family relations affecting business decisions.
- **Data Loss Prevention (DLP)** – Identifies and blocks sensitive data from being sent over the network.
- **Data Sovereignty** – Ensuring data does not leave its country of origin.
- **Geographical Dispersion** – Distributing data centers across multiple locations.

Cybersecurity Measures:

- **Blocking Keyloggers** – Block all unknown outbound network traffic.
- **Invalid Credentials Issue** – Usually caused by missing or improper certificate installation.
- **Chain of Custody** – Documenting evidence handling to ensure integrity.
- **E-Discovery** – Collecting digital documents (e.g., emails) as evidence.
- **Legal Hold** – Preventing data deletion when facing legal proceedings.
- **Non-Repudiation** – Ensures that an action occurred and identifies who performed it.

Network Security Devices:

- **WAF (Web Application Firewall)** – Protects web-based applications by filtering user input in real time.
- **VPN Concentrator** – A central hub for remote VPN connections.
- **UTM (Unified Threat Management)** – An advanced firewall solution.
- **XDR (Extended Detection and Response)** – Identifies malware and cyberattacks.
- **SASE (Secure Access Service Edge)** – A cloud-based VPN alternative.

- **HIPS (Host-Based IPS)** – Monitors and protects an individual device.
- **SNMP (Simple Network Management Protocol)** – Provides alerts and alarms from infrastructure devices.

Hardware & Industrial Security:

- **End of Life (EOL)** – No longer supported by the vendor.
- **Embedded System** – No access to OS or firmware updates (e.g., time clocks).
- **Industrial Control System (ICS)** – Ensures the reliability and security of industrial infrastructure.
- **Enumeration** – Collecting system information.
- **Access Point** – Allows wireless network access.
- **NetFlow Logs** – Summarizes network traffic (e.g., attacker movement across systems).

Key Exchange & Authentication:

- **In-Band Key Exchange** – Sending encryption keys via the same communication channel (e.g., WhatsApp).
- **Out-of-Band Key Exchange** – Using a separate channel (e.g., SMS, in-person meeting).
- **Diffie-Hellman Key Exchange** – A cryptographic protocol for secure key exchange over an insecure channel.

Corporate Device Policies:

- **COPE (Corporate-Owned, Personally Enabled)** – Company-provided devices for work and personal use.
- **CYOD (Choose Your Own Device)** – Employees choose a company-provided device.
- **BYOD (Bring Your Own Device)** – Employees use personal devices for work.

Notes based on the Professor Messer's Practice Exam book https://www.professormesser.com/sy0-701-success-bundle/. Highly recommend as a great source of learning. -KasiaSok