The Cyber Codebook (CompTIA Sec+) | Pritam Suryawanshi

🔒Authentication and Access Control

- **CIA (Confidentiality, Integrity, Availability)** – Core principles of cybersecurity.
- **AAA (Authentication, Authorization, Accounting)** – Framework for managing user access and tracking activity.
- **ACL (Access Control List)** – Permissions list for what users can access.
- **PKI (Public Key Infrastructure)** – System for managing encryption keys and certificates.

Security Systems and Tools

- **IDS (Intrusion Detection System)** – Monitors networks for suspicious activity.
- **HIDS (Host-Based IDS)** – Detects threats on individual devices.
- **NIDS (Network IDS)** – Detects threats across the entire network.
- **IPS (Intrusion Prevention System)** – Actively blocks detected threats.

- **IDPs (Intrusion Detection & Prevention System)** – Combines detection and prevention.
- **DLP (Data Loss Prevention)** – Prevents sensitive data from being leaked or lost.

💾 Storage and Hardware

- **RAID (Redundant Array of Independent Disks)** – Combines multiple drives for redundancy/performance.
- **NAS (Network Attached Storage)** – Storage device connected to a network.
- **SAN (Storage Area Network)** – High-speed network of storage devices.
- **SATA (Serial Advanced Technology Attachment)** – Interface for connecting storage devices.
- **eSATA (External SATA)** – External version of SATA for faster data transfer.

🔒 Encryption and Security Standards

- **AES (Advanced Encryption Standard)** – Widely used encryption standard.
- **SSL (Secure Sockets Layer)** – Encrypts data between browser and server (obsolete).
- **TLS (Transport Layer Security)** – Modern replacement for SSL.
- **EFS (Encrypting File System)** – Encrypts files on Windows systems.
- **FDE (Full Disk Encryption)** – Encrypts the entire hard drive.
- **SED (Self-Encrypting Drive)** – A drive that encrypts data automatically.

🖥️ System and Network Components

- **UEFI (Unified Extensible Firmware Interface)** – Modern system firmware interface.
- **MBR (Master Boot Record)** – Legacy boot structure for drives.
- **NTFS (New Technology File System)** – Advanced Windows file system.

- **FAT (File Allocation Table)** – Older file system used on USBs and some drives.
- **DMZ (Demilitarized Zone)** – Isolated network segment for added security.
- **SOHO (Small Office/Home Office)** – Common term for home/small business routers.

📱 Mobile and Device Security

- **MDM (Mobile Device Management)** – Manages and secures mobile devices.
- **IMEI (International Mobile Equipment Identity)** – Unique ID for mobile phones.
- **IMSI (International Mobile Subscriber Identity)** – Identifies a user in the mobile network.
- **PED (Portable Electronic Device)** – Devices like smartphones, tablets, etc.
- **TPM (Trusted Platform Module)** – Hardware chip for storing encryption keys securely.

🌐 Protocols and Services

- **SMTP (Simple Mail Transfer Protocol)** – Sends emails.
- **ICMP (Internet Control Message Protocol)** – Sends error and status messages in networks.
- **ARP (Address Resolution Protocol)** – Maps IP addresses to MAC addresses.
- **URL (Uniform Resource Locator)** – Web address (e.g., https://example.com).

☁️ Virtualization and Cloud

- **VM (Virtual Machine)** – Software-based computer running inside another system.
- **VDE (Virtual Desktop Environment)** – Remote desktop accessed via the cloud.
- **CSP (Cloud Service Provider)** – Company offering cloud computing services.

🏛️ Security Organizations and Standards

- **NSA (National Security Agency)** – U.S. government agency for cybersecurity and surveillance.
- **US-CERT (U.S. Computer Emergency Readiness Team)** – Responds to cyber threats.
- **NCAS (National Cyber Awareness System)** – Educates the public about cyber threats.
- **ISRM (Information Security Risk Management)** – Process for identifying and managing IT security risks.