AP Cybersecurity

Revision Sheet · 考前速记

Learn these by heart before the exam. 考试前把这些内容背熟。

Introduction to Security

CIA triad 信息安全三要素: Confidentiality (only the authorised can read), Integrity (data is not altered), Availability (it is there when needed)

Authentication proves WHO you are; authorisation decides WHAT you may do; accounting logs what you did. Do not confuse the first two.

Multi-factor combines something you KNOW (password), HAVE (token), and ARE (biometric). Two of the same factor is not MFA.

Least privilege 最小权限原则: give each user and process only the access it needs, and no more; it limits the damage of any single compromise

Threat is a potential danger; vulnerability is a weakness; risk is the chance a threat exploits a vulnerability. Risk = likelihood times impact.

Defence in depth layers controls so one failure is not fatal. Attackers: script kiddie, hacktivist, insider, organised crime, nation-state.

Securing Spaces (physical + human)

Physical security matters: locks, badges, mantraps, cameras, and secure disposal. Shoulder surfing and dumpster diving are real attacks.

Social engineering 社会工程学: manipulating people rather than machines; the human is usually the weakest link

Phishing (mass email), spear phishing (targeted), whaling (executives), vishing (voice), smishing (SMS), pretexting (a fake scenario).

Tailgating follows an authorised person through a door. Baiting leaves infected media for someone to plug in.

Defence is training and verification: confirm the request through a second channel before acting on it.

Securing Networks

A firewall filters traffic by rules. A DMZ isolates public servers from the internal network. A VPN encrypts traffic across the internet.

IDS detects and alerts; IPS detects and BLOCKS. That one word is the whole difference.

Attacks: DoS/DDoS floods a service, MITM intercepts traffic, spoofing forges an address, packet sniffing reads unencrypted data.

Network segmentation limits lateral movement. Zero trust verifies EVERY request, inside or out.

Encryption in transit 传输中加密: TLS/HTTPS protects data moving across a network so a sniffer sees only ciphertext

Ports and protocols: HTTPS 443, SSH 22, DNS 53. Close the ports you do not need.

Securing Devices

Malware: virus (attaches to a file), worm (self-spreads), trojan (disguised), ransomware (encrypts for money), spyware, rootkit (hides deep).

Harden a device: patch promptly, remove unused software, disable default accounts, enable a host firewall and anti-malware.

Patch management closes known vulnerabilities. A zero-day has no patch yet, so defence in depth is what catches it.

Full-disk encryption protects data AT REST if the device is stolen. Secure boot checks the software has not been tampered with.

Back up on the 3-2-1 rule: three copies, two media, one offsite. It is the real defence against ransomware.

Securing Applications and Data

Validate ALL input. SQL injection and cross-site scripting both come from trusting user input. Never build a query by string concatenation.

Symmetric vs asymmetric 对称与非对称加密: symmetric uses one shared key (fast, AES); asymmetric uses a public/private pair (RSA) to exchange keys and to sign

Hashing is one-way and verifies INTEGRITY (SHA-256). Encryption is reversible with a key. Salt a password hash to beat rainbow tables.

A digital signature = hash the message, encrypt the hash with the PRIVATE key. Anyone can verify with the public key. It proves integrity and authenticity.

Access control models: role-based (by job), rule-based, and mandatory. Log and audit access.

Secure development: threat model early, review code, test, and keep dependencies patched.

Ethics, law, and response

White hat has permission; black hat does not; grey hat acts without permission but discloses. Only test systems you are AUTHORISED to test.

Incident response: prepare, identify, contain, eradicate, recover, learn. Containment comes BEFORE eradication.

Privacy laws protect personal data; report breaches as

required. Collect the minimum data necessary.

Exam technique

Match the control to the CIA goal: encryption serves confidentiality, hashing serves integrity, backups and redundancy serve availability.

For a scenario, name the specific attack AND a specific defence. 'Be careful' is not a control.

Use the exact vocabulary (least privilege, defence in depth, zero trust). The term is the mark.