CompTIA Security+ SY0-701 Mnemonics Cheat Sheet

secplusmastery.com

Memory hooks for the hardest acronyms and confusable pairs. A free study resource.

Hooks for the acronyms and pairs that trip people up. A mnemonic gets it into your head; understanding the concept and repeating it keep it there.

AAA and access control

AAA Authentication, Authorization, Accounting, in that order: who are you, what may you do, what did you do.

RADIUS vs TACACS+ RADIUS uses UDP and encrypts only the password. TACACS+ (Cisco) uses TCP and encrypts the whole packet, and splits the three As apart.

MAC / DAC / RBAC MAC = the system (Machine) decides by labels. DAC = the Data owner decides. RBAC = your Role decides.

FAR vs FRR FAR (False Acceptance) lets the wrong person in, a security failure. FRR (False Rejection) keeps the right person out, an annoyance. CER is where the two cross.

Detection and monitoring

IDS vs IPS IDS Detects and alerts (passive, off to the side). IPS Prevents: inline, in the Path, and can drop the traffic.

HIDS vs NIDS HIDS = Host, watches one machine. NIDS = Network, watches a whole segment.

SIEM vs SOAR SIEM spots it (aggregates logs and alerts). SOAR acts on it (runs automated playbooks).

Risk and recovery metrics

RPO vs RTO RPO = recovery POINT = how much DATA you can lose, back to your last backup. RTO = recovery TIME = how long you can be DOWN.

MTBF vs MTTR MTBF = Mean Time Between Failures (reliability; higher is better). MTTR = Mean Time To Repair (how fast you fix it; lower is better).

MTTF Mean Time To Failure, for components you replace rather than repair (one-and-done parts).

SLE, ARO, ALE SLE = Asset Value times Exposure Factor (one event). ARO = times per year. ALE = SLE times ARO (the yearly cost).

Cryptography

CIA triad Confidentiality (keep it secret), Integrity (keep it true), Availability (keep it reachable).

Symmetric vs asymmetric Symmetric = one Shared key, fast, for bulk data. Asymmetric = a pair (public and private), slow, for key exchange and signatures.

Hashing vs encryption Hashing is one-way (integrity and passwords). Encryption is two-way with a key (confidentiality). You can decrypt; you cannot de-hash.

Salt vs pepper A salt is a unique random value stored with each hash to beat rainbow tables. A pepper is a secret value stored separately from the hash.

Wireless security

WEP Wired Equivalent Privacy = Weak, Easily Penetrated. The broken original.

WPA2 vs WPA3 WPA2 uses the crackable 4-way handshake. WPA3 uses SAE, which blocks offline password guessing. Both can use AES-CCMP.

SAE Simultaneous Authentication of Equals, the WPA3 Dragonfly handshake that replaced WPA2's weak one.

Cloud, network, and threat intel

CASB Cloud Access Security Broker, the policy checkpoint between your users and cloud apps.

SASE Say 'sassy': SD-WAN networking plus cloud-delivered security, combined into one edge service.

ZTNA Zero Trust Network Access: verify every request and grant access to one app, never the whole network.

STIX vs TAXII STIX writes the threat intel (the what). TAXII ships it (the how, the transport).

Social engineering and attacks

Phishing family Phishing = email. Spear phishing = a specific person. Whaling = an executive. Vishing = Voice. Smishing = SMS.

Virus vs worm A virus needs a host file and user action. A worm self-replicates and spreads across the network on its own.

DoS vs DDoS DoS = one source floods a target. DDoS = many sources (a botnet) flood it at once.