CompTIA Security+

SY0-701

Complete Study Guide & Cheat Sheet

All 5 Domains • Threats & Attacks • Cryptography • Acronyms

K Taylor Tech

ktaylortech.org

Study Guide Contents

■ *Exam: 90 min | Maximum 90 questions (MCQ + PBQ) | Passing score: 750 / 900*

DOMAIN 1 – General Security Concepts — 12% of exam

1.1 Security Controls

Category	Description	Examples
Technical	Technology-enforced controls	Firewall, IDS/IPS, encryption, MFA, ACL
Managerial	Policy and procedure-based	Security policy, risk assessments, hiring background checks
Operational	Day-to-day human processes	Security awareness training, guard patrols, change mgmt
Physical	Physical access restrictions	Locks, badges, cameras, mantrap, bollards
Type	**Goal**	**Examples**
Preventive	Stop an incident before it occurs	Firewall rules, security awareness, locked doors
Detective	Identify incidents as they happen	IDS, audit logs, CCTV, anomaly detection
Corrective	Minimize impact after incident	Patching, backups, incident response
Deterrent	Discourage attacks	Warning signs, legal notices, login banners
Compensating	Alternative when primary not feasible	MFA where passwords can't be changed
Directive	Direct subjects toward compliance	Policies, procedures, training requirements

1.2 Security Concepts & Frameworks

- CIA Triad: Confidentiality (prevent unauthorized access) | Integrity (prevent unauthorized modification) | Availability (ensure systems are accessible)
- AAA: Authentication | Authorization | Accounting
- Non-repudiation: Cannot deny sending a message — achieved with digital signatures
- Least Privilege: Users get minimum access needed for their job
- Separation of Duties: No single person controls an entire critical process
- Zero Trust: Never trust, always verify — no implicit trust for any user or device
- Defense in Depth: Layered security; multiple controls at multiple levels
- Need to Know: Access only to information required for specific tasks

Framework / Standard	Description
NIST CSF	Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover
NIST SP 800-53	Security & privacy controls catalog for federal systems
ISO 27001	International standard for Information Security Management Systems (ISMS)
ISO 27002	Code of practice — implementation guidance for ISO 27001
PCI DSS	Payment Card Industry Data Security Standard — protects cardholder data
HIPAA	Health Insurance Portability & Accountability Act — protects PHI
SOC 2	Service Organization Control reports — trust service criteria
GDPR	EU General Data Protection Regulation — data privacy rights
CIS Controls	Center for Internet Security — prioritized list of safeguards

1.3 Authentication & Identity

- Authentication factors: Something you know (password/PIN) | Something you have (token/smartcard) | Something you are (biometric) | Somewhere you are (geolocation) | Something you do (behavioral)
- MFA – requires 2+ different factor types
- SSO – Single Sign-On: authenticate once, access multiple systems
- Federation – trust relationship between identity providers (SAML, OIDC)
- SAML – Security Assertion Markup Language: XML-based SSO/federation standard
- OAuth 2.0 – authorization framework (not authentication); grants access tokens
- OpenID Connect (OIDC) – identity layer on top of OAuth 2.0; provides authentication
- PAP – Password Authentication Protocol: plaintext passwords — insecure

- CHAP – Challenge Handshake Authentication Protocol: challenge-response, never sends password
- EAP – Extensible Authentication Protocol: framework used with 802.1X
- Kerberos – ticket-based auth; KDC issues TGTs; used in Active Directory
- RADIUS – UDP 1812/1813; encrypts only password; network device auth
- TACACS+ – TCP 49; encrypts full packet; best for device management

1.4 Cryptography Foundations

- Symmetric encryption: Same key encrypts and decrypts — fast, good for bulk data
- Asymmetric encryption: Public key encrypts, private key decrypts — slower, used for key exchange and signatures
- Hashing: One-way function; produces fixed-length digest; used for integrity
- Digital signature: Hash encrypted with sender's private key — proves integrity + non-repudiation
- PKI: Public Key Infrastructure — CA, certificates (X.509), CRL, OCSP
- Key exchange: Diffie-Hellman (DH/ECDH) — allows secure key agreement over insecure channel
- Perfect Forward Secrecy (PFS): New session key each session; past sessions safe if key compromised

DOMAIN 2 – Threats, Vulnerabilities & Mitigations — 22% of exam

2.1 Threat Actors & Motivations

Threat Actor	Sophistication	Motivation	Resources
Nation-State (APT)	Very High	Espionage, sabotage, IP theft	Government-funded
Organized Crime	High	Financial gain, ransomware	Well-funded
Hacktivist	Medium	Political/ideological agenda	Variable
Insider Threat	Medium-High	Financial gain, revenge, error	Trusted access
Script Kiddie	Low	Notoriety, curiosity	Pre-made tools
Competitor	Medium	Corporate espionage	Moderate
Shadow IT	Low	Convenience (unintentional)	Internal

2.2 Attack Types & Social Engineering

Attack	Description
Phishing	Mass deceptive email to steal credentials or deliver malware
Spear Phishing	Targeted phishing aimed at specific individual or organization
Whaling	Spear phishing targeting executives (CEO, CFO)
Vishing	Voice phishing — phone calls impersonating legitimate entities
Smishing	SMS phishing — malicious links via text message
Business Email Compromise (BEC)	Impersonate executive via email to authorize fraudulent transactions
Pretexting	Fabricated scenario to manipulate victim into providing information
Baiting	Leave infected USB drive for victim to find and plug in
Quid Pro Quo	Offer something (fake IT help) in exchange for credentials
Tailgating / Piggybacking	Follow authorized person through secured door without badge
Watering Hole	Compromise website frequented by target group
Typosquatting	Register domains with common typos of legitimate sites
Credential Stuffing	Use breached username/password combos on other services
Password Spraying	Try common passwords against many accounts to avoid lockout
Brute Force	Systematically try all possible password combinations
Dictionary Attack	Try words from a wordlist against passwords
Rainbow Table	Pre-computed hash lookups; defeated by salting
Pass-the-Hash	Steal NTLM hash and reuse it to authenticate without plaintext password
Kerberoasting	Request TGS tickets for service accounts; crack offline
Golden Ticket	Forge Kerberos TGTs using compromised KRBTGT hash (full AD control)
Man-in-the-Middle	Intercept and possibly alter communications between two parties
On-Path Attack	Updated term for MitM; attacker positions between communicating parties
Replay Attack	Capture and retransmit valid auth packets to gain access
SQL Injection	Insert SQL commands into input fields to manipulate database
XSS (Cross-Site Scripting)	Inject malicious script into web page viewed by other users
CSRF	Cross-Site Request Forgery: trick authenticated user into performing actions

Attack	Description
Directory Traversal	Access files outside web root using ../sequences
IDOR	Insecure Direct Object Reference: access others' data by changing ID param
Buffer Overflow	Write beyond allocated memory to overwrite adjacent data/code
Race Condition / TOC/TOU	Exploit timing gap between check and use of a resource
DoS / DDoS	Flood target with traffic; DDoS uses botnets/distributed sources
Smurf Attack	Amplified ICMP flood via broadcast address spoofed to victim IP
DNS Amplification	Small DNS queries return large responses; spoofed source = victim
SYN Flood	Half-open TCP connections exhaust server state table
Teardrop	Malformed IP fragments cause crash on reassembly

2.3 Malware Types

Type	Description	Key Trait
Virus	Attaches to legitimate file; spreads when file executed	Requires host file
Worm	Self-replicating; spreads across networks without user	No host file needed
Trojan	Disguised as legitimate software; no self-replication	Deception
Ransomware	Encrypts files; demands ransom for decryption key	Extortion
Spyware	Secretly monitors and exfiltrates user data/keystrokes	Stealth/exfil
Adware	Displays unwanted ads; may track browsing	Revenue generation
Rootkit	Hides presence; gains persistent privileged access	Stealth/persistence
Bootkit	Rootkit infecting MBR/UEFI; loads before OS	Pre-OS persistence
Keylogger	Records keystrokes to capture credentials	Credential theft
Backdoor	Hidden access channel bypassing normal auth	Persistent access
RAT	Remote Access Trojan; full control of victim system	C2 capability
Botnet	Network of compromised systems (bots) under C2 control	Coordinated attacks
Logic Bomb	Malicious code triggered by specific condition/date	Time/trigger based
Fileless Malware	Runs in memory; no files written to disk	AV evasion
Cryptojacker	Uses victim's CPU/GPU to mine cryptocurrency	Resource abuse

2.4 Vulnerability Management

- CVE – Common Vulnerabilities and Exposures: standardized vuln identifier (CVE-YYYY-NNNNN)
- CVSS – Common Vulnerability Scoring System: 0.0–10.0 severity score
- CVSS scores: 0.1–3.9 Low | 4.0–6.9 Medium | 7.0–8.9 High | 9.0–10.0 Critical
- NVD – National Vulnerability Database: NIST-maintained CVE repository
- Zero-day: Vulnerability with no available patch; vendor unaware
- Patch management: Identify → Test → Deploy → Verify → Document
- Vuln scanning: Credentialed (deep, sees more) vs. Non-credentialed (surface-level)
- Penetration testing phases: Recon → Scanning → Exploitation → Post-exploitation → Reporting
- Pen test types: Black box (no info) | Gray box (some info) | White box (full info)
- Bug bounty: Programs rewarding researchers for responsibly disclosing vulnerabilities

DOMAIN 3 – Security Architecture — 18% of exam

3.1 Network Security Architecture

- DMZ – Demilitarized Zone: semi-trusted segment hosting public-facing servers (web, email, DNS)
- Screened subnet: modern term for DMZ — two firewalls create buffer zone
- Segmentation: divide network into zones to limit lateral movement (VLANs, subnets)
- Micro-segmentation: granular segmentation per workload or application (SDN, Zero Trust)
- East-West traffic: server-to-server traffic inside data center (inspect with internal firewall)
- North-South traffic: traffic entering/leaving the network perimeter
- Air gap: physically isolated network with no external connectivity
- Jump server / bastion host: hardened intermediary used to manage devices in secure zones

Firewall Type	Description	OSI Layer
Packet Filter	Filters by IP/port headers; stateless	3-4
Stateful	Tracks connection state; smarter than packet filter	3-4
NGFW	Deep packet inspection, app-awareness, IPS built-in	3-7
WAF	Web Application Firewall; protects HTTP/HTTPS apps	7
Proxy Firewall	Acts as intermediary; breaks connection, inspects	7
UTM	Unified Threat Management; all-in-one appliance	3-7

3.2 Cloud Security

Model	Provider Manages	Customer Manages
IaaS	Physical, hypervisor, networking	OS, middleware, apps, data
PaaS	Infrastructure + OS + runtime	Applications and data
SaaS	Everything	User access and data only

- Shared responsibility model: security obligations split between provider and customer
- CASB – Cloud Access Security Broker: enforces security policies between users and cloud services
- CSPM – Cloud Security Posture Management: detects misconfigurations in cloud environments
- CWPP – Cloud Workload Protection Platform: secures cloud workloads/containers
- Serverless security: secure function code, IAM roles, API gateways, event triggers
- Container security: image scanning, runtime protection, secrets management, namespace isolation
- Infrastructure as Code (IaC): Terraform, CloudFormation — scan templates for misconfigs

3.3 Secure Network Design

- NAC – Network Access Control: verify device posture/compliance before allowing network access
- 802.1X – port-based authentication; uses EAP + RADIUS; required for NAC
- SD-WAN – Software-Defined WAN: centralized policy, encrypted tunnels over internet links
- SASE – Secure Access Service Edge: network + security delivered as cloud service (SD-WAN + SSE)
- SSE – Security Service Edge: CASB + SWG + ZTNA as cloud service
- SWG – Secure Web Gateway: URL filtering, malware inspection, SSL inspection
- ZTNA – Zero Trust Network Access: identity-aware, app-specific access; replaces VPN
- DNS filtering / sinkholing: redirect malicious domains to internal sinkhole IP

3.4 Endpoint Security

- Hardening: disable unused services, close unnecessary ports, remove default accounts
- AV/Anti-malware: signature + heuristic + behavioral detection
- EDR – Endpoint Detection & Response: real-time telemetry, behavioral analysis, automated response
- XDR – Extended Detection & Response: EDR + network + cloud + identity in unified platform
- MDM – Mobile Device Management: enforce policies, remote wipe, containerization
- MAM – Mobile Application Management: manage/secure apps without full device control
- DLP – Data Loss Prevention: prevent unauthorized exfiltration of sensitive data
- FDE – Full Disk Encryption: BitLocker (Windows), FileVault (Mac), LUKS (Linux)
- Secure boot: UEFI verifies bootloader integrity using cryptographic signatures

• TPM – Trusted Platform Module: hardware chip storing encryption keys; supports BitLocker

DOMAIN 4 – Security Operations — 28% of exam

4.1 Identity & Access Management (IAM)

- Provisioning: creating user accounts and assigning access rights
- De-provisioning: revoking access when user leaves or role changes
- RBAC – Role-Based Access Control: permissions assigned to roles, not individuals
- ABAC – Attribute-Based Access Control: policies based on attributes (dept, clearance, time)
- MAC – Mandatory Access Control: system-enforced labels (Top Secret, Secret, Unclassified)
- DAC – Discretionary Access Control: owner sets permissions (standard NTFS/Linux ACLs)
- PAM – Privileged Access Management: secure, audit, and manage admin/privileged accounts
- Just-in-Time access: grant elevated privileges only when needed, for limited time
- Account types: User | Admin | Service | Guest | Shared — each with different risks
- Password policies: complexity, length, history, age, lockout threshold
- Account auditing: review dormant accounts, excessive permissions, privilege creep

4.2 Incident Response

Phase	Key Activities
1. Preparation	IR plan, playbooks, team roles, tools, training, tabletop exercises
2. Detection & Analysis	Alerts, log analysis, SIEM correlation, triage, scoping
3. Containment	Short-term (isolate) + Long-term (patch/change credentials)
4. Eradication	Remove malware, close attack vectors, remediate vulnerabilities
5. Recovery	Restore systems, monitor for re-infection, return to production
6. Lessons Learned	Post-incident review, update procedures, document timeline

- Chain of Custody: documented handling of evidence from collection to court
- Order of Volatility: CPU registers/cache → RAM → Swap → HDD → Logs → Archived media
- Digital forensics: Identify → Preserve → Collect → Examine → Analyze → Report
- Write blocker: hardware/software that prevents modification of forensic media
- Legal hold: preserve all relevant data when litigation is anticipated

4.3 SIEM, SOAR & Logging

- SIEM – Security Information & Event Management: centralized log collection, correlation, alerting
- SOAR – Security Orchestration, Automation & Response: automates repetitive IR tasks
- Log sources: firewall, IDS/IPS, EDR, DNS, DHCP, proxy, AD, cloud audit logs
- Syslog severity: 0 Emergency | 1 Alert | 2 Critical | 3 Error | 4 Warning | 5 Notice | 6 Info | 7 Debug
- NXLog / Rsyslog / Syslog-ng: common log forwarding agents
- NetFlow / IPFIX: network traffic metadata (not full packets); useful for anomaly detection
- Indicators of Compromise (IoC): file hashes, IPs, domains, registry keys, behavioral patterns
- Threat intelligence feeds: STIX/TAXII formats; ISACs; VirusTotal; MISP
- MITRE ATT&CK;: knowledge base of adversary tactics, techniques, and procedures (TTPs)

4.4 Vulnerability & Patch Management

- Scan types: Network scan | Credentialed scan | Web app scan | Container scan | ICS/SCADA scan
- False positive: scanner reports vuln that doesn't exist — verify and tune
- False negative: real vuln not detected — missed; more dangerous than false positive
- Patching priority: CVSS score + exploitability + asset criticality + exposure
- Compensating controls: when patching isn't immediately possible (WAF, isolation, monitoring)
- EOL/EOS software: no more patches — highest risk; isolate or replace

4.5 Data Security & Privacy

Classification	Description	Examples
Public	No harm if disclosed	Marketing materials, press releases
Internal	Internal use only; minor harm	Employee directory, internal procedures

Classification	Description	Examples
Confidential	Significant harm if disclosed	Business plans, client contracts, financials
Restricted/Secret	Severe harm; tightly controlled	Trade secrets, classified government data

- PII – Personally Identifiable Information: name, SSN, address, DOB, etc.
- PHI – Protected Health Information: medical records, diagnoses, treatment info
- PCI DSS – Payment Card Industry: protects cardholder data (credit card numbers)
- Data at rest: encrypted on storage media (AES-256, FDE, database encryption)
- Data in transit: encrypted over network (TLS 1.2+, VPN, SFTP, HTTPS)
- Data in use: protected with DLP, memory encryption, access controls
- Data retention: define how long data is kept; securely destroy per policy (DoD 5220.22-M, Gutmann)
- Tokenization: replace sensitive data with non-sensitive token; common in PCI
- Data masking: obscure data for non-production use; original data unchanged

DOMAIN 5 – Security Program Management & Oversight — 20% of exam

5.1 Risk Management

Term	Definition
Risk	Likelihood × Impact of a threat exploiting a vulnerability
Threat	Any potential event that could cause harm
Vulnerability	Weakness that could be exploited by a threat
Asset	Something of value that needs protection
Likelihood	Probability that a threat event will occur
Impact	Magnitude of harm if a threat event occurs
Inherent Risk	Risk before any controls are applied
Residual Risk	Remaining risk after controls are in place
Risk Appetite	Amount of risk an organization is willing to accept
Risk Tolerance	Acceptable variance around risk appetite
Control Risk	Risk that a control will fail to function properly

Risk Response Strategies

Strategy	Description	Example
Avoid	Eliminate the activity causing the risk	Don't collect unnecessary customer data
Transfer	Shift risk to a third party	Cyber insurance, outsourcing
Mitigate	Reduce likelihood or impact with controls	Patch vuln, add firewall rule
Accept	Acknowledge risk and take no action (documented)	Low-risk/low-likelihood issue

- Qualitative risk: subjective ratings (High/Medium/Low) — faster, good for initial assessment
- Quantitative risk: numeric values — ALE = ARO x SLE (Annual Loss Expectancy = Rate x Single Loss)
- SLE – Single Loss Expectancy: asset value x exposure factor
- ARO – Annual Rate of Occurrence: how often event expected per year
- ALE – Annual Loss Expectancy: SLE x ARO

5.2 Compliance, Auditing & Assessments

- Internal audit: conducted by organization's own team; identifies control gaps
- External audit: independent third party; required for many regulations
- Penetration test: simulated attack to find exploitable weaknesses
- Vulnerability assessment: scan + analyze weaknesses; does NOT exploit
- Risk assessment: identify and evaluate risks to the organization
- Compliance monitoring: continuous checks against regulatory requirements
- Right to audit clause: contractual right to audit third-party vendors
- SOC 1: financial reporting controls | SOC 2: security/availability/confidentiality | SOC 3: public version of SOC 2

5.3 Business Continuity & Disaster Recovery

Term	Definition
BCP	Business Continuity Plan: maintain operations during and after disruption
DRP	Disaster Recovery Plan: restore IT systems after disaster
RTO	Recovery Time Objective: max acceptable downtime
RPO	Recovery Point Objective: max acceptable data loss (time-based)
MTBF	Mean Time Between Failures: avg time between system failures
MTTR	Mean Time To Repair: avg time to restore a failed component

Term	Definition
BIA	Business Impact Analysis: identify critical processes and their dependencies
Failover	Automatic switch to backup system when primary fails
Redundancy	Duplicate critical components to eliminate single points of failure

- Backup types: Full (all data) | Incremental (changes since last backup) | Differential (changes since last FULL)
- 3-2-1 rule: 3 copies, 2 different media, 1 offsite
- Recovery sites: Hot (ready immediately) | Warm (hours) | Cold (days/weeks)
- Tabletop exercise: discussion-based IR/BCP walkthrough — no actual systems
- Functional exercise: tests specific functions (e.g., notification, evacuation)
- Full-scale exercise: comprehensive, realistic simulation involving all teams

5.4 Third-Party Risk & Supply Chain

- SLA – Service Level Agreement: contractual performance guarantees
- MOU – Memorandum of Understanding: informal agreement between parties
- MOA – Memorandum of Agreement: more formal than MOU
- MSA – Master Service Agreement: governs ongoing vendor relationship
- NDA – Non-Disclosure Agreement: protects confidential information shared with third parties
- Vendor risk assessment: evaluate third-party security posture before onboarding
- Supply chain attacks: compromise vendor/software to attack downstream customers (SolarWinds)
- Hardware security: Trusted Platform Module (TPM), Hardware Security Module (HSM), secure boot
- SBOM – Software Bill of Materials: inventory of all components in software/firmware

Cryptography Quick Reference

Symmetric Algorithms

Algorithm	Key Size	Block Size	Mode Notes	Status
AES	128/192/256-bit	128-bit	CBC, CTR, GCM (authenticated)	Current standard
3DES	112/168-bit	64-bit	Legacy triple DES	Deprecated 2023
DES	56-bit	64-bit	Broken — easily cracked	Do not use
RC4	40–2048-bit	Stream	Stream cipher; found in WEP	Broken
Blowfish	32–448-bit	64-bit	Old but still used in bcrypt	Legacy
ChaCha20	256-bit	Stream	Modern stream cipher; TLS 1.3	Current

Asymmetric Algorithms

Algorithm	Key Size	Use	Notes
RSA	2048–4096-bit	Encryption, signatures, KX	Widely used; slow for bulk data
ECC	256-bit ≈ RSA 3072	Encryption, signatures	Smaller keys; efficient; TLS 1.3
DSA	1024–3072-bit	Digital signatures only	Used in FIPS 186
ECDSA	256-bit	Digital signatures	ECC version of DSA; efficient
EdDSA/Ed25519	256-bit	Digital signatures	Modern, fast, high security
DH	2048–4096-bit	Key exchange	Foundation of secure key agreement
ECDH	256-bit	Key exchange	ECC version of DH; used in TLS 1.3
ElGamal	Variable	Encryption, key exchange	Used in PGP/GPG

Hashing Algorithms

Algorithm	Output Size	Status	Common Use
MD5	128-bit	Broken	Non-security checksums only; file verification
SHA-1	160-bit	Deprecated	Avoid; collision attacks known
SHA-256	256-bit	Current	TLS certificates, code signing, HMAC
SHA-384	384-bit	Current	Higher-security certs and protocols
SHA-512	512-bit	Current	Highest SHA-2 security
SHA-3	224–512-bit	Current	NIST standard; different design from SHA-2
RIPEMD-160	160-bit	Acceptable	Used in Bitcoin addresses
bcrypt	60-char	Current	Password hashing; includes salt + cost factor
PBKDF2	Variable	Current	Password-based key derivation; NIST approved
Argon2	Variable	Current (Best)	Winner of Password Hashing Competition 2015
HMAC	Varies	Current	Keyed hash for message authentication

PKI & Certificate Types

Term	Description
CA	Certificate Authority: issues and signs digital certificates
Root CA	Top of PKI hierarchy; ultimate trust anchor; kept offline
Intermediate CA	Subordinate CA that issues end-entity certificates; online
CRL	Certificate Revocation List: list of revoked serial numbers

Term	Description
OCSP	Online Certificate Status Protocol: real-time revocation check
OCSP Stapling	Server pre-fetches OCSP response to reduce client latency
X.509	Standard format for digital certificates
CSR	Certificate Signing Request: sent to CA to obtain signed cert
DV Cert	Domain Validation: only verifies domain ownership
OV Cert	Organization Validation: verifies org identity
EV Cert	Extended Validation: highest assurance; green bar (legacy)
Wildcard Cert	*.domain.com — covers all subdomains of one domain
SAN Cert	Subject Alternative Name: covers multiple specific FQDNs
Self-signed Cert	Signed by its own private key; not trusted by default
Certificate Pinning	App accepts only specific cert/key; prevents substitution attacks

Ports & Protocols Quick Reference

Port	Protocol	Transport	Security Notes
20/21	FTP	TCP	Cleartext — replace with SFTP (22) or FTPS (990)
22	SSH / SFTP / SCP	TCP	Encrypted remote access and file transfer
23	Telnet	TCP	Cleartext — never use; replace with SSH
25	SMTP	TCP	Cleartext server-to-server mail; use STARTTLS
53	DNS	UDP/TCP	UDP queries; TCP zone transfer; consider DNSSEC / DoH / DoT
67/68	DHCP	UDP	Protect with DHCP snooping; watch for rogue DHCP
80	HTTP	TCP	Cleartext web — enforce HTTPS redirect
88	Kerberos	TCP/UDP	AD authentication; protect KDC; watch for golden ticket attacks
110	POP3	TCP	Cleartext email retrieval; use POP3S (995)
119	NNTP	TCP	Usenet newsgroups
123	NTP	UDP	Time sync; stratum 0=atomic; NTP amplification attack vector
135	RPC	TCP	Windows RPC; often exploited; restrict at firewall
137-139	NetBIOS	TCP/UDP	Legacy Windows naming; disable if not needed
143	IMAP	TCP	Cleartext; use IMAPS (993)
161/162	SNMP	UDP	v1/v2c insecure (community string); use SNMPv3
389	LDAP	TCP	Cleartext directory; use LDAPS (636) or StartTLS
443	HTTPS	TCP	TLS-encrypted web; require TLS 1.2+
445	SMB	TCP	File sharing; EternalBlue exploit; block at perimeter
465/587	SMTPS/Submit	TCP	Encrypted email submission; prefer 587 with STARTTLS
514	Syslog	UDP	Cleartext logs; use syslog TLS (6514) for security
636	LDAPS	TCP	LDAP over TLS — preferred over port 389
993	IMAPS	TCP	IMAP over TLS
995	POP3S	TCP	POP3 over TLS
1194	OpenVPN	UDP	Open-source VPN; UDP preferred over TCP
1433	MS SQL Server	TCP	Restrict to app servers only; high-value target
1723	PPTP	TCP	Legacy VPN; weak encryption — avoid
3306	MySQL	TCP	DB port; restrict access; patch regularly
3389	RDP	TCP	Remote Desktop; common attack surface; use NLA + MFA
5060/5061	SIP/SIPS	UDP/TCP	VoIP signaling; 5061 = TLS-encrypted
6514	Syslog TLS	TCP	Encrypted syslog forwarding
8080/8443	HTTP/HTTPS Alt	TCP	Alternate web ports; often used by proxies/dev servers

SY0-701 Acronym Glossary

Acronym	Expansion
AAA	Authentication, Authorization, Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
ALE	Annual Loss Expectancy
APT	Advanced Persistent Threat
ARO	Annual Rate of Occurrence
AV	Asset Value / Antivirus
ABAC	Attribute-Based Access Control
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CA	Certificate Authority
CASB	Cloud Access Security Broker
CIA	Confidentiality, Integrity, Availability
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoS	Denial of Service
DRP	Disaster Recovery Plan
EAP	Extensible Authentication Protocol
EDR	Endpoint Detection & Response
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standard
FIM	File Integrity Monitoring
GDPR	General Data Protection Regulation
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
IAM	Identity and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IoC	Indicator of Compromise
IR	Incident Response
ISMS	Information Security Management System
KDC	Key Distribution Center (Kerberos)
MAC	Mandatory Access Control / Message Auth Code
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair

Acronym	Expansion
NGFW	Next-Generation Firewall
NIST	National Institute of Standards & Technology
NVD	National Vulnerability Database
OCSP	Online Certificate Status Protocol
OIDC	OpenID Connect
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standard
PFS	Perfect Forward Secrecy
PHI	Protected Health Information
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAML	Security Assertion Markup Language
SASE	Secure Access Service Edge
SBOM	Software Bill of Materials
SIEM	Security Information & Event Management
SLA	Service Level Agreement
SLE	Single Loss Expectancy
SMB	Server Message Block
SOAR	Security Orchestration Automation & Response
SOC	Security Operations Center
SQL	Structured Query Language
SSE	Security Service Edge
SSO	Single Sign-On
STIX	Structured Threat Information Expression
SWG	Secure Web Gateway
TAXII	Trusted Automated eXchange of Indicator Information
TGT	Ticket Granting Ticket (Kerberos)
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTPs	Tactics, Techniques, and Procedures
UAT	User Acceptance Testing
UTM	Unified Threat Management
VPN	Virtual Private Network
WAF	Web Application Firewall
XDR	Extended Detection & Response
XSS	Cross-Site Scripting
ZTNA	Zero Trust Network Access
Zero Trust	Security model: never trust, always verify
DoH	DNS over HTTPS

NAC	Network Access Control	DoT	DNS over TLS
		NLA	Network Level Authentication (RDP)

■ *Study tip: You scored 10/15 on a Security+ diagnostic cold — strong base! Focus extra time on Security Operations (Domain 4, 28%) and Security Program Management (Domain 5, 20%).*