CompTIA Security+ Cheat Sheet

CompTIA Security+ Cheat Sheet

You've made a great choice pursuing the CompTIA Security+ certification if you aspire to work in cyber security. It makes you a catch to employers, but the huge amount of study materials can make this a challenging exam.

This CompTIA Security+ Cheat Sheet is a brief roadmap in your preparation for this crucial exam. It gives you a bird's-eye view of key concepts and abbreviations in Security+. Owing to Security+'s overlap with Network+, CCNA, and other networking-related certifications, this cheat sheet excludes material on networking, which we encourage you to review separately.

Download this CompTIA Security+ Cheat Sheet here. When you're ready, let's dive in.

What Is the CompTIA Security+ Certification?

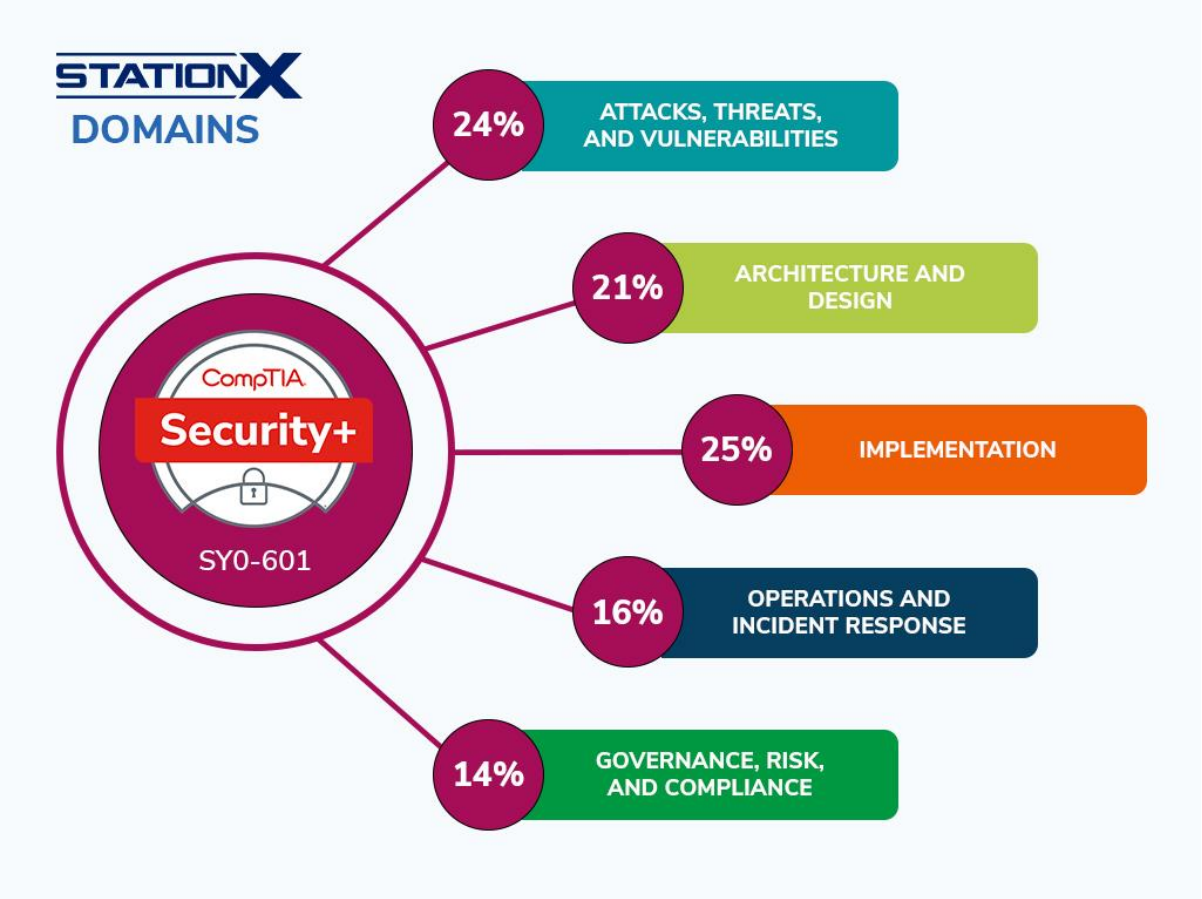
The CompTIA Security+ certification shows employers that you've mastered the fundamental skills to perform essential cyber security functions and pursue a relevant career. Hence, the CompTIA Security+ exam focuses on the day-to-day real-time application of IT security knowledge at work.

You'll need to answer at most 90 questions in this 90-minute examination and complete a survey after it ends. The passing score is 750 on a scale of 100–900.

The latest CompTIA Security+ exam code is SY0-601. The associated exam is available from November 2020 to sometime in 2023–2024. New topics include supply chain management and the Internet of Things (IoT).

Security+ Domains (SY0-601)

The following illustration shows the assessment criteria and the weighting in this examination:



CompTIA Security+ Domains (SY0-601)

This cheat sheet arranges concepts according to the subtopics in our Total Seminars Security+ course, and some topics span several Security+ domains. Hence, we've provided you a key to finding items according to Security+ domain:

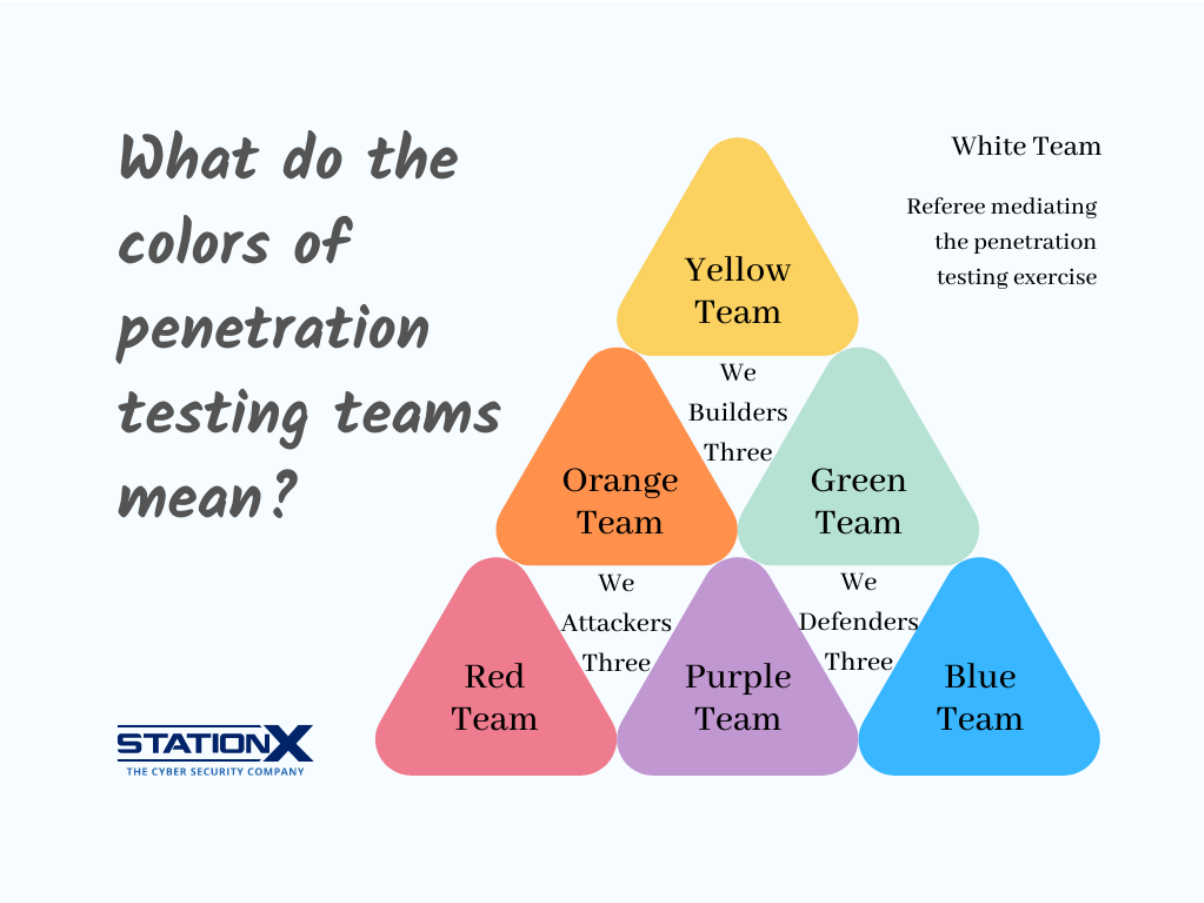
Hashtag (Remember to type the # symbol)	Domain (SY0-601)
#ATV	Attacks, Threats, and Vulnerabilities
#AD	Architecture and Design
#practical	Implementation
#op	Operations and Incident Response
#risk	Governance, Risk, and Compliance

Type these tags into the search bar to find key points related to a specific domain.

Risk Management

The following topics pertain to real-life applications of cyber security. When you review the abbreviations, think: “Do I comprehend the ideas encapsulated by them?”

Domain	Concept	Elaboration
#ATV	Threat Actor	Vulnerability exploiter
#ATV	TTP	(Adversary) tactics, techniques, and procedures
#ATV	Hacker	IT infrastructure penetrator
#ATV	Hacktivist	Politically motivated agent
#ATV	Script kiddie	Executor of pre-made programs
#ATV	Insider	Saboteur inside an organization
#ATV	Competitor/Rival	Saboteur outside an organization but in the same industry
#ATV	Shadow IT	IT systems deployed without the central IT department’s oversight
#ATV	Criminal syndicate (organized crime)	Profit-driven agent with intent to blackmail
#ATV	State actor	Foreign government agent
#ATV	APT	Advanced persistent threat: long-term intelligence-mining hacking
#ATV	OSINT	Open-source intelligence • Government reports • Media • Academic papers
#ATV	CVEs	Common Vulnerabilities and Exposures
#ATV	AIS	Automated Indicator Sharing
#ATV	STIX	Structured Threat Information Expression
#ATV	TAXII	Trusted Automated Exchange of Intelligence Information
#risk	GDPR	General Data Protection Regulation
#risk	PCI DSS	Payment Card Industry Data Security Standard
#risk	ISO	International Organization for Standardization
#risk	CSA	Cloud Security Alliance
#risk	AV	Asset Value
#risk	EF	Exposure Factor
#risk	SLE	Single Loss Expectancy = AV × EF
#risk	ARO	Annualized Rate of Occurrence
#risk	ALE	Annualized Loss Expectancy = SLE × ARO
#risk	BIA	Business impact analysis
#risk	MTBF	Mean time between failures
#risk	MTTF	Mean time to failure
#risk	MTTR	Mean time to repair
#risk	RTO	Recovery time objective
#risk	RPO	Recovery point objective
#risk	Residual risk	Remaining risk after mitigation
#ATV #risk	Supply chain attack	Targets insecure elements in the supply chain



What do terms like “red team” and “blue team” mean in penetration testing?

The primary colors red, blue, and yellow refer to attackers, defenders, and builders of a system respectively. The secondary colors are combinations of these roles. For example, purple team members have dual attack/defense roles. The white team supervises the hack.

Cryptography

The following concepts are about obfuscating data from attackers and restoring them once they reach the intended destination.

Domain	Concept	Elaboration
#ATV	Cryptographic attack/cryptanalysis	Finding weaknesses in the cryptosystem
#AD	Data at rest	On computer storage
#AD	Data in use/processing	In RAM being accessed
#AD	Data in transit/motion	Traveling along cables or broadcasting wirelessly
#AD	Symmetric cipher	Streaming: • RC4 Block: • DES • Blowfish • 3DES Considerations: • key length

		• block size • number of rounds
#AD	Asymmetric cipher	Examples: • Diffie-Hellman key exchange • RSA • Elliptic-curve cryptography
#AD	Hashing	One-way, deterministic process of transforming a string of characters into another
#AD	Salting	Characters appended to a string (e.g., password) before hashing
#AD	Steganography	Hide data inside other data
#AD	Quantum	Exploit quantum mechanics
#AD	Post-quantum	Secure against cryptanalysis by quantum computer
#AD	Lightweight cryptography	Small footprint, low computational complexity
#AD	Homomorphic encryption	Makes performing operations on encrypted data possible
#AD #practical	CA	Certificate authority
#AD #practical	CRL	Certificate revocation list
#AD #practical	Stapling	Checks regularly for certificate invalidity
#AD #practical	Pinning	Associates certificate against known copy
#AD #practical	Trust model	• Direct • Third-party • Hierarchical • Distributed
#AD #practical	Key escrow	Third party safeguarding private keys
#AD #practical	Certificate chaining	Top-down CA trust model
#AD #practical	Digital signature	Public key sender verified to own corresponding private key
#practical	P7B	√ certificate √ chain certificates × private key
#practical	P12	√ certificate √ chain certificates √ private key
#practical	PKI	Public Key Infrastructure
#practical	PKCS	Public Key Cryptography Standards
#ATV #AD	Brute-force attack	Trying character combinations Variant: spraying (trying the same password across different accounts)
#ATV #AD	Dictionary attack	Using lists of probable passwords
#ATV #AD	Rainbow tables	Using pre-calculated password hashes
#ATV #AD	Key stretching	Method that strengthens weak passwords

Identity and Account Management

The following concepts deal with methods showing that you are the legitimate owner of an account.

Domain	Concept	Elaboration
#practical #AD	Multi-factor Authentication (MFA)	Factors: • Something you know • Something you have • Something you are Attributes: • Something you do • Something you exhibit • Someone you know • Somewhere you are
#AD	Efficacy rate	• False acceptance • False rejection • Crossover error rate
#AD #practical	Access control schemes	• Attribute-based access control (ABAC) • Role-based access control • Rule-based access control • MAC • Discretionary access control (DAC) • Conditional access • Privileged access management • Filesystem permissions
#practical	PAP	Password Authentication Protocol
#practical	CHAP	Challenge-Handshake Authentication Protocol Example: MS-CHAP-v2
#practical	Sandboxing	Limiting access privileges of an application to minimize its impact on the rest of the system
#AD #practical	Identity federation	Delegate authentication to trusted third party

Tools of the Trade

We omit terminal commands because practice is more important than rote memorization for performance-based questions on Security+.

Domain	Concept	Key points to review
#op	SPAN	Switch port analyzer
#op	IoC	Indicators of Compromise
#op	SNMP	Simple Network Management Protocol
#op	NXLog	Open-source log collection tool
#op #ATV	SIEM	Security Information and Event Management

Securing Individual Systems

The table below lists vital security concepts.

Domain	Concept	Elaboration
#ATV	Malware	• Virus • Polymorphic virus • Fileless virus • Worm • Trojan • Rootkit • Keylogger • Adware • Spyware • Ransomware • Bots • Remote access Trojan (RAT) • Logic bomb • Cryptomalware • Potentially unwanted programs (PUPs) • Command and control (C2/C&C) • Keyloggers • Backdoor
#ATV	Zero-day attack (ZDI)	Previously unknown vulnerability
#ATV	DNS Sinkholing	Give certain domain names invalid addresses
#ATV	Replay attack	Intercept data and replay later
#ATV	Pointer/object dereference attack	Using a null-value pointer as if its value is valid to bypass security logic
#ATV	Dynamic-link Library (DLL) injection	Force-run code in place of other code
#ATV	Resource exhaustion	Attacks using up bandwidth Examples: DoS, DDoS
#ATV	Race conditions	Trying to perform two or more operations that should follow a proper order—clash
#ATV	Driver attacks	• Driver shimming • Driver refactoring
#ATV	Overflow attacks	• Integer overflow • Buffer overflow
#ATV #AD #practical	Securing hardware	• TPM • Hardware redundancy • UPS • PDU • Cloud redundancy
#practical	Securing endpoints	• Antivirus/Anti-malware • EDR • HIDS • HIPS • NGFW • Allowlist/whitelist • Block/deny lists, blacklist
#AD	Embedded system	Combination of hardware and software for a specific purpose

		Examples: • Raspberry Pi • Field-programmable gate array (FPGA) • Arduino
#AD	Specialized system	Combination of mechanical and digital interfaces for specific purposes Examples: • Medicine • Aviation • Smart meters
#AD	Internet of Things (IoT)	Network of physical devices
#AD	SCADA	Supervisory control and data acquisition
#AD	ICS	Industrial control system

The Basic LAN, Securing Wireless LANs, Securing Public Servers

We omit networking topics such as the above in this cheat sheet, and we encourage you to review them independently.

Physical Security

The best security measures are real-world limitations imposed on digital access. Here are a few concepts worth reviewing:

Domain	Concept	Elaboration
#AD	Air gap	Physical isolation of secure computer network from unsecured networks
#AD	Protected cable distribution (Protected Distribution System)	Wired communications system with sufficient physical protection to carry unencrypted classified information without leakage
#AD	Screened subnet (demilitarized zone)	Five components: • External network • External router • Perimeter network • Internal router • Internal network
#AD	Hot and cold aisles	Draw in cool air to equipment, and draw out hot air from equipment
#AD	Two-person integrity/control	Continuous monitoring by at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures
#AD	Secure data destruction	• Burning • Shredding • Pulping • Pulverizing • Degaussing • Third-party solutions
#AD	Monitoring sensors	• Motion detection • Noise detection

		• Proximity reader • Moisture detection • Cards • Temperature

Secure Protocols and Applications

This table excludes material overlapping with the Network+ exam objectives.

Domain	Concept	Elaboration
#practical	S/MIME	Secure/Multipurpose Internet Mail Extensions
#ATV	Cross-site request forgery (CSRF/XSRF)	Hijack authenticated sessions
#ATV	Server-side request forgery (SSRF)	Cause servers to make outbound HTTP requests
#ATV	Cross-site scripting (XSS) attack	Inject malicious scripts into otherwise benign and trusted websites
#ATV #AD #practical	Injection attack	Affects: • SQL • LDAP • XML
#ATV #AD #practical	Secure coding practices	• Input validation, sanitation • Secure Web browser cookies • HTTP headers • Code signing • Trusted components and APIs
#ATV #AD #practical	Software development life cycle (SDLC)	• Planning • Defining • Designing • Building • Testing • Deployment

Testing Infrastructure

This section is about social engineering and penetration testing. Manipulating perception leads to much damage because humans are the weakest link in cyber security.

Domain	Concept	Elaboration
#ATV	Social engineering	Principles (reasons for effectiveness): • Authority • Intimidation • Consensus • Scarcity • Familiarity • Trust • Urgency
#ATV	Influence campaign	Propaganda:

		• Hybrid warfare • Social media
#ATV	Watering hole attack	Infect a trusted website
#ATV	Spam	Mass mailing of unsolicited messages Variation: Spam over instant messaging (SPIM)
#ATV	Phishing	Attack by email; single target
#ATV	Smishing	Attack by SMS text message
#ATV	Vishing	Attack by telephone or voicemail
#ATV	Spear phishing	Attack by email; multiple targets
#ATV	Whaling	Phishing that targets high-ranking people, such as C-suite executives
#ATV	Invoice scam	Solicit payment from fraudulent invoice, often paired with whaling
#ATV	Dumpster diving	Recover information from trash
#ATV	Shoulder surfing	Look over someone's shoulder, often with a recording device
#ATV	Tailgating	Unauthorized entity follows authorized party into secured premises
#ATV	Piggybacking	Tailgating with the authorized party's consent
#ATV	Credential harvesting (farming)	Attacks to obtain credentials or personal information
#ATV	Pharming	Phishing + farming; making and redirecting users to a fake website
#ATV	Prepending	Adding username mentions to social media posts
#ATV	Pretexting	Digital gunpoint with the ransom being one's private information
#ATV	Impersonation, identity fraud/theft	Attacks using stolen credentials or personal information
#ATV	Eliciting information	Strategic casual conversation without coercion to extract information from targets
#ATV	Reconnaissance	Covert information-gathering
#ATV	Hoax	False alarm
#ATV	Typosquatting	Attacks using mistyped web addresses

#ATV	Vulnerability scanning	Test for weaknesses
		• Passive (monitoring)
		• Active
		  ○ Credentialed
		  ○ Non-credentialed

#ATV	Penetration testing (pentesting)	Actively exploit vulnerabilities
#ATV	Intrusive scan	Damage-causing pentesting
#ATV	Black box	Zero-knowledge pentesting
#ATV	White box	Extensive-knowledge pentesting
#ATV	Gray box	Partial-knowledge pentesting
#ATV #practical	Fuzzing	Input random characters and expect spurious results
#ATV	Pivot	Access network through vulnerable host—then attack
#ATV	Privilege escalation	Get administrator access

Dealing With Incidents

The following is a list of paradigms for handling, preventing, and mitigating cyber security breaches.

Domain	Concept	Elaboration
#op	BCP	Business continuity plan
#op	COOP	Continuity of operations
#op #risk	DRP	Disaster Recovery Plan
#op	IRP	Incident Response Plan
#op	IoC	Indicators of Compromise
#op	Cyber Kill Chain Analysis	Trace steps of a successful hack
#op	MITRE ATT&CK Framework	Identify attacker techniques
#op	Diamond Model of Intrusion Analysis 	Show how threat actors (adversaries) exploit capabilities in infrastructure against victims
#op #ATV	Security Orchestration, Automation, and Response (SOAR)	Automate incident responses, thus reducing response time
#AD #op	Legal hold	Process to preserve all forms of potentially relevant information for potential litigation
#AD #op	Chain of custody (CoC)	Paper trail of physical and electronic evidence
#AD #op	Disaster Recovery Sites	• Hot • Warm • Cold
#AD	RAID	Redundant array of inexpensive disks
#AD	UPS	Uninterruptible power supply
#AD	PDUs	Power distribution units
#AD	NAS	Network-attached storage
#AD	Multipath	Having multiple physical paths between devices
#AD	Network interface card (NIC) teaming	Physical network adapters grouped together
#AD	Load balancer	Distributes traffic across servers
#AD	Scalability	Ease of growing and managing increased demand on infrastructure
#AD	Backup types	• Full • Copy • Differential • Incremental • Snapshot

Conclusion

This CompTIA Security+ Cheat Sheet is a checklist covering the examination syllabus, and we hope it gives you a bird's-eye view of non-networking key topics to remember.

Remember that we offer a complete course to passing the Security+ exam and practice exams to test your abilities. No matter how you prepare for it, we wish you success.