Microsoft

CompTIA Security+

Exam SY0-301

David Seidl
Mike Chapple
James Michael Stewart

Training Kit

CompTIA Security+

Your 2-in-1 Self-Paced Training Kit

1 EXAM PREP GUIDE

Ace your preparation for the skills measured by CompTIA Security+ Exam SY0-301. Work at your own pace through a series of lessons and reviews that fully cover each exam objective. Then, reinforce what you've learned by applying your knowledge to real-world case scenarios and practice exercises. This guide is designed to help make the most of your study time.

Maximize your performance on the exam by demonstrating your mastery of:

- Network security
- Compliance and operational security
- Threats and vulnerabilities
- Application, data, and host security
- Access control and identity management
- Cryptography

2 PRACTICE TESTS

Assess your skills with practice tests on CD. You can work through hundreds of questions using multiple testing modes to meet your specific learning needs. You get detailed explanations for right and wrong answers—including a customized learning path that describes how and where to focus your studies.

microsoft.com/mspress

CompTIA Security+

EXAM SY0-301

Your kit includes:

- Self-paced study guide
- Practice tests with multiple, customizable testing options and a learning plan based on your results
- 200 practice and review questions
- Case scenarios, exercises, and best practices
- Fully searchable eBook of this guide

*For **system requirements**, see the introduction.*

About the Authors

David Seidl, Director of Information Security for a major university, leads a team of six information security professionals.

Mike Chapple, CISSP, Ph.D., a senior director for enterprise support systems at a major university, has more than 15 years of information security experience as a practitioner, director, and author.

James Michael Stewart, CISSP, CEH, and CHFI, teaches job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+.

CompTIA Authorized Partner

CompTIA Security+ Certified

9 780735 664265

U.S.A. $49.99
Canada $52.99
[Recommended]

Certification/
CompTIA Security+

Microsoft

CompTIA Security+ (Exam SY0-301) Objective lesson map

	OBJECTIVE	CHAPTER
1.0	**NETWORK SECURITY (21 PERCENT)**	
1.1	Explain the security function and purpose of network devices and technologies: Firewalls; Routers; Switches; Load Balancers; Proxies; Web security gateways; VPN concentrators; NIDS and NIPS (Behavior based, signature based, anomaly based, heuristic); Protocol analyzers; Sniffers; Spam filter, all-in-one security appliances; Web application firewall vs. network firewall; URL filtering, content inspection, malware inspection	2
1.2	Apply and implement secure network administration principles: Rule-based management, Firewall rules, VLAN management, Secure router configuration, Access control lists, Port Security, 802.1x, Flood guards, Loop protection, Implicit deny, Prevent network bridging by network separation, Log analysis	2, 3
1.3	Distinguish and differentiate network design elements and compounds: DMZ, Subnetting, VLAN, NAT, Remote Access, Telephony, NAC, Virtualization, Cloud Computing (Platform as a Service, Software as a Service, Infrastructure as a Service)	3
1.4	Implement and use common protocols: IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SFTP, SCP, ICMP, IPv4 vs. IPv6	3
1.5	Identify commonly used default network ports: FTP, SFTP, FTPS, TFTP, TELNET, HTTP, HTTPS, SCP, SSH, NetBIOS	3
1.6	Implement wireless network in a secure manner: WPA, WPA2, WEP, EAP, PEAP, LEAP, MAC filter, SSID broadcast, TKIP, CCMP, Antenna Placement, Power level controls	3
2.0	**COMPLIANCE AND OPERATIONAL SECURITY (18 PERCENT)**	
2.1	Explain risk related concepts: Control types (Technical, Management, Operational); False positives; Importance of policies in reducing risk (Privacy policy, Acceptable use, Security policy, Mandatory vacations, Job rotation, Separation of duties, Least privilege); Risk calculation (Likelihood, ALE, Impact); Quantitative vs. qualitative; Risk-avoidance, transference, acceptance, mitigation, deterrence; Risks associated to Cloud Computing and Virtualization	1, 4
2.2	Carry out appropriate risk mitigation strategies: Implement security controls based on risk, Change management, Incident management, User rights and permissions reviews, Perform routine audits, Implement policies and procedures to prevent data loss or theft	1, 4
2.3	Execute appropriate incident response procedures: Basic forensic procedures (Order of volatility, Capture system image, Network traffic and logs, Capture video, Record time offset, Take hashes, Screenshots, Witnesses, Track man hours and expense), Damage and loss control, Chain of custody, Incident response: (first responder)	1
2.4	Explain the importance of security related awareness and training: Security policy training and procedures; Personally identifiable information; Information classification: Sensitivity of data (hard or soft); Data labeling, handling and disposal; Compliance with laws, best practices and standards; User habits (Password behaviors, Data handling, Clean desk policies, Prevent tailgating, Personally owned devices); Threat awareness, (New viruses, Phishing attacks, Zero-day exploits); Use of social networking and P2P	4
2.5	Compare and contrast aspects of business continuity: Business impact analysis, Removing single points of failure, Business continuity planning and testing, Continuity of operations, Disaster recovery, IT contingency planning, Succession planning	4

Exam Objectives The exam objectives listed here are current as of this book's publication date. Exam objectives are subject to change at any time without prior notice and at CompTIA's sole discretion. Please visit the CompTIA Certifications webpage for the most current listing of exam objectives: *http://certification.comptia.org/getCertified/certifications.aspx*.

2.0	**COMPLIANCE AND OPERATIONAL SECURITY (18 PERCENT)**	
2.6	Explain the impact and proper use of environmental controls: HVAC, Fire suppression, EMI shielding, Hot and cold aisles, Environmental monitoring, Temperature and humidity controls, Video monitoring	4
2.7	Execute disaster recovery plans and procedures: Backup / backout contingency plans or policies; Backups, execution and Frequency; Redundancy and fault tolerance (Hardware, RAID, Clustering, Load balancing, Servers); High availability; Cold site, hot site, warm site; Mean time to restore, mean time between failures, recovery time objectives and recovery point objectives	4
2.8	Exemplify the concepts of confidentiality, integrity and availability (CIA)	1
3.0	**THREATS AND VULNERABILITIES (21 PERCENT)**	
3.1	Analyze and differentiate among types of malware: Adware, Virus, Worms, Spyware, Trojan, Rootkits, Backdoors, Logic bomb, Botnets	5
3.2	Analyze and differentiate among types of attacks: Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, Spam, Phishing, Spim, Vishing, Spear phishing, Xmas attack, Pharming, Privilege escalation, Malicious insider threat, DNS poisoning and ARP poisoning, Transitive access, Client-side attacks	5
3.3	Analyze and differentiate among types of social engineering attacks: Shoulder surfing, Dumpster diving, Tailgating, Impersonation, Hoaxes, Whaling, Vishing	5
3.4	Analyze and differentiate among types of wireless attacks: Rogue access points, Interference, Evil twin, War driving, Bluejacking, Bluesnarfing, War chalking, IV attack, Packet sniffing	5
3.5	Analyze and differentiate among types of application attacks: Cross-site scripting, SQL injection, LDAP injection, XML injection, Directory traversal/command injection, Buffer overflow, Zero day, Cookies and attachments, Malicious add-ons, Session hijacking, Header manipulation	5
3.6	Analyze and differentiate among types of mitigation and deterrent techniques: Manual bypassing of electronic controls (Failsafe/secure versus failopen), Monitoring system logs (Event logs, Audit logs, Security logs, Access logs), Physical security (Hardware locks, Mantraps, Video surveillance, Fencing, Proximity readers, Access list), Hardening (Disabling unnecessary services, Protecting management interfaces and applications, Password protection, Disabling unnecessary accounts), Port security (MAC limiting and filtering, 802.1x, Disabling unused ports), Security posture (Initial baseline configuration, Continuous security monitoring, remediation), Reporting (Alarms, Alerts, Trends), Detection Controls vs. prevention controls (IDS vs. IPS, Camera vs. guard)	6
3.7	Implement assessment tools and techniques to discover security threats and vulnerabilities: Vulnerability scanning and interpret results, Tools (Protocol analyzer, Sniffer, Vulnerability scanner, Honeypots, Honeynets, Port scanner), Risk calculations (Threat vs. likelihood), Assessment types (Risk, Threat, Vulnerability), Assessment technique (Baseline reporting, Code review, Determine attack surface, Architecture, Design reviews)	7
3.8	Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning: Penetration testing (Verify a threat exists, Bypass security controls, Actively test security controls, Exploiting vulnerabilities), Vulnerability scanning (Passively testing security controls, Identify vulnerability, Identify lack of security controls, Identify common misconfiguration), Black box, White box, Gray box	7
4.0	**APPLICATION, DATA AND HOST SECURITY (16 PERCENT)**	
4.1	Explain the importance of application security: Fuzzing, Secure coding Concepts (Error and exception handling, Input validation), Cross-site scripting prevention, Cross-site Request Forgery (XSRF) prevention, Application configuration baseline (proper settings), Application hardening, Application patch management	8
4.2	Carry out appropriate procedures to establish host security: Operating system security and settings, Anti-malware (Anti-virus, Anti-spam, Anti-spyware, Pop-up blockers, Host-based firewalls), Patch management, Hardware security (Cable locks, Safe, Locking cabinets), Host software baselining, Mobile devices (Screen lock, Strong password, Device encryption, Remote wipe/sanitation, Voice encryption, GPS tracking), Virtualization	9
4.3	Explain the importance of data security: Data Loss Prevention (DLP), Data encryption (Full disk, Database, Individual files, Removable media, Mobile devices), Hardware based encryption devices (TPM, HSM, USB encryption, Hard drive), Cloud Computing	10

5.0	**ACCESS CONTROL AND IDENTITY MANAGEMENT (13 PERCENT)**	
5.1	Explain the function and purpose of authentication services: RADIUS, TACACS, TACACS+, Kerberos, LDAP, XTACACS	11
5.2	Explain the fundamental concepts and best practices related to authentication, authorization and access control: Identification vs. authentication, Authentication (single factor) and authorization, Multifactor authentication, Biometrics, Tokens, Common access card, Personal identification verification card, Smart card, Least privilege, Separation of duties, Single sign on, ACLs, Access control, Mandatory access control, Discretionary access control, Role/rule-based access control, Implicit deny, Time of day restrictions, Trusted OS, Mandatory vacations, Job rotation	
5.3	Implement appropriate security controls when performing account management: Mitigates issues associated with users with multiple account/roles, Account policy enforcement (Password complexity, Expiration, Recovery, Length, Disablement, Lockout), Group based privileges, User assigned privileges	11
6.0	**CRYPTOGRAPHY (11 PERCENT)**	
6.1	Summarize general cryptography concepts: Symmetric vs. asymmetric, Fundamental differences and encryption methods (Block vs. stream), Transport encryption, Non-repudiation, Hashing, Key escrow, Steganography, Digital signatures, Use of proven technologies, Elliptic curve and quantum cryptography	12
6.2	Use and apply appropriate cryptographic tools and products: WEP vs. WPA/WPA2 and pre-shared key, MD5, SHA, RIPEMD, AES, DES, 3DES, HMAC, RSA, RC4, One-time-pads, CHAP, PAP, NTLM, NTLMv2, Blowfish, PGP/GPG, Whole disk encryption, TwoFish, Comparative strengths of algorithms, Use of algorithms with transport encryption (SSL, TLS, IPSec, SSH, HTTPS)	12
6.3	Explain the core concepts of public key infrastructure: Certificate authorities and digital certificates (CA, CRLs), PKI, Recovery agent, Public key, Private key, Registration, Key escrow, Trust models	12
6.4	Implement PKI, certificate management and associated components: Certificate authorities and digital certificates (CA, CRLs), PKI, Recovery agent, Public key, Private keys, Registration, Key escrow, Trust models	12

Microsoft

CompTIA Security+ (Exam SYO-301)

Training Kit

David Seidl
Mike Chapple
James Michael Stewart

Published with the authorization of Microsoft Corporation by:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, California 95472

ISBN: 978-0-7356-6426-5

1 2 3 4 5 6 7 8 9 QG 8 7 6 5 4 3

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

Acquisitions and Developmental Editor: Kenyon Brown

Production Editor: Melanie Yarbrough

Editorial Production: Online Training Solutions, Inc. (OTSI)

Technical Reviewer: Addam Schroll

Copyeditor: Online Training Solutions, Inc. (OTSI)

Indexer: BIM Publishing Services

Cover Design: Twist Creative • Seattle

Cover Composition: Ellie Volkhausen

Illustrator: Online Training Solutions, Inc. (OTSI)

Contents at a glance

Contents

Introduction

This training kit is designed for information technology (IT) professionals who want to earn the CompTIA Security+ certification. It is assumed that you have a basic understanding of computers and operating systems. However, the CompTIA Security+ certification is an entry-level certification, so you are not expected to have any in-depth knowledge to use this training kit.

To become a CompTIA Security+ certified professional, you must take and pass the SY0-301 exam. The primary goal of this training kit is to prepare you with a solid foundation of IT knowledge so that you can successfully pass the exam the first time you take it.

The material covered in this training kit and on exam SY0-301 relates to the technologies, skills, and knowledge a security professional would be expected to understand. These include risk management, infrastructure security, application security, policy, and confidentiality/encryption/availability concepts. You can download the objectives for the SY0-301 exam from the CompTIA website at this URL:

http://certification.comptia.org/Training/testingcenters/examobjectives.aspx

By using this training kit, you will learn how to do the following:

- Conduct risk assessment and risk management activities.
- Respond to a security incident.
- Understand the risks associated with cloud computing and virtualization.
- Explain the various types of network security devices and their purposes.
- Design a network with adequate security controls.
- Administer network security controls on an ongoing basis.
- Secure wireless networks with appropriate encryption.
- Provide appropriate environmental and physical security controls.
- Understand the threats to and security landscape.
- Deploy defenses to prevent and mitigate attacks.
- Conduct vulnerability assessments and manage vulnerabilities.
- Secure applications against attack.
- Secure operating systems using appropriate hardening techniques.
- Use encryption to protect information at rest and in motion.
- Deploy access controls to implement identification, authentication, and authorization.

Refer to the objectives mapping page in the front of this book to see where in the book each exam objective is covered.

About the exam

The SY0-301 exam is focused on skills required to secure systems, applications, and networks. It includes objectives in the following six areas:

- Network security (21 percent of exam)
- Compliance and operational security (18 percent of exam)
- Threats and vulnerabilities (21 percent of exam)
- Application, data, and host security (16 percent of exam)
- Access control and identity management (13 percent of exam)
- Cryptography (11 percent of exam)

The current version of the exam became available in 2011. Over the years, more than 45,000 people around the world have earned the CompTIA Security+ certification. Information security professionals often start with the CompTIA Security+ certification to lay a solid foundation of information security knowledge and later move on to higher-level certifications and better-paying jobs. Among those test takers are those who are working to meet the US Department of Defense's Directive 8570.01-M, which lists the CompTIA Security+ exam as one of the required certifications for employees and contractors who perform information security work.

The CompTIA Security+ exam has a maximum of 100 questions, including both multiple-choice and performance-based questions. You will have 90 minutes in which to take the test, and a score of 750 on a scale of 100-900 is considered a passing score. You can find more information about the exam at:

http://certification.comptia.org/getCertified/certifications/security.aspx

Prerequisites

CompTIA recommends that test takers have the CompTIA Network+ certification as well as two years of technical networking experience with an emphasis on information security work.

Note that this is not a requirement to take the exams. Anyone can take the exams after paying for them, and if they pass, they earn the certification. However, you'll have the best chance of success if you have been studying and working with networks and information security professionally and are familiar with the material in the CompTIA Network+ exam.

Performance-based testing

A significant difference in the SY0-301 exam over previous versions is the introduction of performance-based testing. Instead of just using multiple-choice questions, CompTIA is introducing questions that will require you to perform a task. You should expect to see somewhere around three of these questions on the exam, so don't stress over them.

Imagine that you wanted to know if a person could ride a bike. You could ask some multiple-choice questions but you'll find that these questions aren't always reliable. A person might answer questions correctly but not be able to actually ride the bike. Put the person in front of a bike, ask them to ride it, and you'll quickly know whether they can or not. Performance-based testing uses this philosophy to see if the candidate has a skill.

Consider this multiple-choice question:

1. What TCP port is used for SMTP traffic by default?
   - **A.** 21
   - **B.** 23
   - **C.** 25
   - **D.** 80

The correct answer is port 25.

In a performance-based question, you might instead be asked to complete a set of firewall rules by filling in the missing information. This might include selecting the ports corresponding to several services and specifying which rules should be set to allow or deny traffic.

When it's a multiple-choice question, you have a 25-percent chance of getting it correct. In a performance-based question, there are an infinite number of possibilities, and the test designers are able to test you on multiple concepts or facts simultaneously.

Throughout the book, we've included steps and instructions on how to do many tasks with performance-based testing in mind. If you do these tasks as you work through the book, you'll be better prepared to answer these performance-based tests.

Study tips

There's no single study method that works for everyone, but there are some common techniques that many people use to successfully pass these exams. These include:

- **Setting a goal** Pick a date when you expect to take the exam, and set your goal to take it then. The date is dependent on how long it will take you to read the chapters and your current knowledge level. You might set a date two months from now, four months from now, or something else. However, pick a date and set a goal.

- **Taking notes** If concepts aren't familiar to you, take the time to write them down. The process of transferring the words from the book, through your head, and down to your hand really helps to burn the knowledge into your brain.
- **Reading your notes** Go back over your notes periodically to see what has stuck, and what you need to review more. You can't bring notes with you into the testing area, but you can use them to review key material before the exam.
- **Using flash cards** Some people get a lot out of flash cards that provide a quick test of knowledge. These help you realize what you don't know and what you need to brush up on. Many practice test programs include flash cards, so you don't necessarily have to create them yourself.
- **Reviewing the objectives** This is what CompTIA says they'll test you on. Sometimes just understanding the objective will help you predict a test question and answer it correctly.
- **Recording your notes** Many people record their notes in an MP3 player and play them back regularly. You can listen while driving, while exercising, or just about any time. Some people have a partner read the notes, which can give an interesting twist to studying.
- **Taking the practice test questions on the CD** The practice test questions on the CD are designed to test the objectives for the exam but at a deeper level than you'll have on the live exam. Each question includes detailed explanations on why the correct answer is correct, and why the incorrect answers are incorrect. Ideally, you should be able to look at the answers to any question and not just know the correct answer, but also why the incorrect answers are incorrect.

System requirements

The actual system requirements to use this book are minimal. The only requirement is a computer you can use to install the practice tests on the companion CD.

Many of the examples in the book use Windows 7 and Linux or Mac OS X. In most organizations, security staff work with a variety of operating systems, and we have attempted to reflect that in this book. You will find that most Windows commands remain the same whether you are using Windows XP, Windows Vista, Windows 7, or Windows 8, with most differences appearing in the menus used to get to settings. Thus, if you only have a Windows XP–based system to practice Windows commands with, you can still expect to successfully learn the critical practical techniques covered in the book.