Transition Guide for gtslearning-based *CompTIA® Security+® Certification (Exam SY0-501) Study Guide* to *The Official CompTIA® Security+® Guides (Exam SY0-501): 2019 Update*

This bridge document is written for instructors who have used the *CompTIA Security+ Certification Guides (Exam SY0-501) Study Guide* courseware from gtslearning, and who are looking to come up to speed on the new version quickly and efficiently.

High-Level Overview of Course Design Changes

This edition of the course has been redesigned compared to the order in which lessons and topics were presented in the GTS study guide.

Where GTS contents uses high-level modules mapped to training days, subdivided into units, OCC content is mapped to lessons and topics that are aligned with job functions and tasks. The topics are shorter than the equivalent units in the GTS study guide, providing more opportunities to pause, review, and check understanding of the content. The content sequence is broadly similar, with early Lessons giving students hands-on activity opportunities with cybersecurity tools and software, before proceeding through identity and access management concepts to security infrastructure and design. The course concludes with risk management, software development, and security policy uses.

There are no changes to the exam and exam objectives.

Course Outline Comparison

This table compares the outline of the prior **The Official CompTIA Security+ Guides (Exam SY0-501)** courseware to that of the new **The Official CompTIA Security+ Guides (Exam SY0-501): 2019 Update** courseware.

The Official CompTIA Security+ Guides (Exam SY0-501): 2019 Update	**CompTIA® Security+® Certification (Exam SY0-501) Study Guide**
01A Compare and Contrast Information Security Roles	1.1 Indicators of Compromise
01B Explain Threat Actor Types	1.1 Indicators of Compromise
01C Compare and Contrast Social Engineering Attack Types	1.1 Indicators of Compromise
01D Determine Malware Types	1.1 Indicators of Compromise
02A Compare and Contrast Security Control and Framework Types	1.2 Critical Security Controls
02B Follow Incident Response Procedures	1.4 Incident Response
03A Explain Penetration Testing Concepts	1.2 Critical Security Controls

The Official CompTIA Security+ Guides (Exam SY0-501): 2019 Update	CompTIA® Security+® Certification (Exam SY0-501) Study Guide
03B Assess Security Posture with Topology Discovery Software Tools	1.3 Security Posture Assessment Tools
03C Assess Security Posture with Fingerprinting and Sniffing Software Tools	1.3 Security Posture Assessment Tools
03D Assess Security Posture with Vulnerability Scanning Software Tools	1.2 Critical Security Controls
04A Compare and Contrast Basic Concepts of Cryptography	2.1 Cryptography
04B Explain Hashing and Symmetric Cryptographic Algorithms	2.1 Cryptography
04C Explain Asymmetric Cryptographic Algorithms	2.1 Cryptography
05A Implement Certificates and Certificate Authorities	2.2 Public Key Infrastructure
05B Implement PKI Management	2.2 Public Key Infrastructure
06A Compare and Contrast Identity and Authentication Concepts	2.3 Identification and Authentication
06B Install and Configure Authentication Protocols	2.3 Identification and Authentication
06C Implement Multifactor Authentication	2.3 Identification and Authentication
07A Install and Configure Authorization and Directory Services	2.4 Identity and Access Services
07B Implement Access Management Controls	2.4 Identity and Access Services
07C Differentiate Account Management Practices	2.5 Account Management
07D Implement Account Auditing and Recertification	2.5 Account Management
08A Implement Secure Network Architecture Concepts	3.1 Secure Network Design
08B Install and Configure Secure Switching Infrastructure	3.1 Secure Network Design
08C Install and Configure Network Access Control	3.1 Secure Network Design
08D Install and Configure Secure Routing and NAT Infrastructure	3.1 Secure Network Design
09A Install and Configure Firewalls and Proxies	3.2 Firewalls and Load Balancers
09B Install and Configure Load Balancers	3.2 Firewalls and Load Balancers
09C Install and Configure Intrusion Detection/Prevention Systems	3.3 IDS and SIEM
09D Install and Configure Data Loss Prevention (DLP) Systems	3.3 IDS and SIEM
09E Install and Configure Logging and SIEM Systems	3.3 IDS and SIEM
10A Install and Configure Wireless Infrastructure	3.4 Secure Wireless Access
10B Install and Configure Wireless Security Settings	3.4 Secure Wireless Access
10C Explain the Importance of Physical Security Controls	3.5 Physical Security Controls

The Official CompTIA Security+ Guides (Exam SY0-501): 2019 Update	CompTIA® Security+® Certification (Exam SY0-501) Study Guide
11A Implement Secure Hardware Systems Design	4.3 Secure Systems Design
11B Implement Secure Host Systems Design	4.3 Secure Systems Design
11C Implement Secure Mobile Device Systems Design	4.4 Secure Mobile Device Services
11D Implement Secure Embedded Systems Design	4.3 Secure Systems Design
12A Implement Secure Network Operations Protocols	4.1 Secure Protocols and Services
12B Implement Secure Remote Access Protocols	4.2 Secure Remote Access
12C Implement Secure Remote Administration Protocols	4.2 Secure Remote Access
13A Implement Secure Web Services	4.1 Secure Protocols and Services
13B Implement Secure Communications Services	4.1 Secure Protocols and Services
13C Summarize Secure Virtualization Infrastructure	4.5 Secure Virtualization and Cloud Services
13D Summarize Secure Cloud Services	4.5 Secure Virtualization and Cloud Services
14A Explain Risk Management Processes and Concepts	5.3 Risk Management
14B Explain Resiliency and Automation Strategies	5.2 Disaster Recovery and Resiliency
14C Explain Disaster Recovery and Continuity of Operations Concepts	5.2 Disaster Recovery and Resiliency
14D Summarize Basic Concepts of Forensics	5.1 Forensics
15A Explain the Impact of Vulnerability Types	5.4 Secure Application Development
15B Summarize Secure Application Development Concepts	5.4 Secure Application Development
16A Explain the Importance of Security Policies	5.5 Organizational Security
16B Implement Data Security and Privacy Practices	5.5 Organizational Security
16C Explain the Importance of Personnel Management	5.5 Organizational Security

Course Setup Changes

The OCC course continues the VM-based approach to practical labs. The guest VMs continue to include a Windows Server 2016 domain controller, a Windows Server 2016 web and email server, Ubuntu and CentOS servers, Windows 7 and Windows 10 clients, VyOS routers, pfSense and Security Onion security appliances, and the KALI Linux security testing platform. The lab activities are broadly similar to those in the GTS version of the course, but the environment has been tweaked to streamline and improve some lab tasks, so a new lab setup will have to be performed.

Virtual machine images for all Linux-based guests are provided, as well as the scripts required to implement installations of Windows machines. As always, training providers are responsible for meeting licensing requirements for any software used in the classroom.

A complete and detailed setup guide document is available for download from the CompTIA CHOICE platform.

Other Course Changes

In addition to the course set-up and activity changes, we've also added some additional features to help support your students in their learning.

In the Assessments tile in CompTIA CHOICE, you will find a variety of different assessments that students can take related to the lesson content as well as course-wide final assessment. These assessments can be used for self-study by students or as homework in your course.

In the Video tile in CompTIA CHOICE, you will find access to different videos that can be incorporated into the course. These videos, developed exclusively for CompTIA by ITPro.TV, provide demonstrations of key activities in the course. These are a good alternative to show if you do not have access to all equipment mentioned in the course. Video icons in the course content also alert you and your students to videos that relate to the content covered.

Exam Mapping

This table shows the mapping of the **CompTIA Security+ (Exam SY0-501)** to that of the new **The Official CompTIA Security+ (Exam SY0-501): 2019 Update** courseware.

Domain and Objective	**The Official CompTIA Security+ (Exam SY0-501): 2019 Update**
Domain 1.0 Threats, Attacks, and Vulnerabilities	
1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.	
Viruses	Topic 1D
Crypto-malware	Topic 1D
Ransomware	Topic 1D
Worm	Topic 1D
Trojan	Topic 1D

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Rootkit	Topic 1D
Keylogger	Topic 1D
Adware	Topic 1D
Spyware	Topic 1D
Bots	Topic 1D
RAT	Topic 1D
Logic bomb	Topic 1D
Backdoor	Topic 1D
1.2 Compare and contrast types of attacks.	
Social engineering	Topic 1C
Phishing	Topic 1C
Spear phishing	Topic 1C
Whaling	Topic 1C
Vishing	Topic 1C
Tailgating	Topic 1C
Impersonation	Topic 1C
Dumpster diving	Topic 1C
Shoulder surfing	Topic 1C
Hoax	Topic 1C
Watering hole attack	Topic 1C
Principles (reasons for effectiveness)	Topic 1C
Authority	Topic 1C
Intimidation	Topic 1C
Consensus	Topic 1C
Scarcity	Topic 1C
Familiarity	Topic 1C
Trust	Topic 1C
Urgency	Topic 1C
Application/service attacks	Topics 6B, 8B, 8D, 9B, 12A, 15A
DoS	Topic 9B
DDoS	Topic 9B
Man-in-the-middle	Topic 8B
Buffer overflow	Topic 15A
Injection	Topic 15A
Cross-site scripting	Topic 15A
Cross-site request forgery	Topic 15A
Privilege escalation	Topic 15A
ARP poisoning	Topic 8B
Amplification	Topic 9B
DNS poisoning	Topic 12A

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Domain hijacking	Topic 12A
Man-in-the-browser	Topic 15A
Zero day	Topic 15A
Replay	Topic 15A
Pass the hash	Topic 6B
Hijacking and related attacks	Topic 15A
Clickjacking	Topic 15A
Session hijacking	Topic 15A
URL hijacking	Topic 12A
Typo squatting	Topic 12A
Driver manipulation	Topic 15A
Shimming	Topic 15A
Refactoring	Topic 15A
MAC spoofing	Topic 8B
IP spoofing	Topic 8D
Wireless attacks	Topic 10B
Replay	Topic 10B
IV	Topic 10B
Evil twin	Topic 10B
Rogue AP	Topic 10B
Jamming	Topic 10B
WPS	Topic 10B
Bluejacking	Topic 10B
Bluesnarfing	Topic 10B
RFID	Topic 10B
NFC	Topic 10B
Disassociation	Topic 10B
Cryptographic attacks	Topics 4A, 4C, 6B
Birthday	Topic 4C
Known plain text/cipher text	Topic 4A
Rainbow tables	Topic 6B
Dictionary	Topic 6B
Brute force	Topic 6B
Online vs. offline	Topic 6B
Collision	Topic 4C
Downgrade	Topic 4C
Replay	Topic 4C
Weak implementations	Topic 4A
1.3 Explain threat actor types and attributes.	
Types of actors	Topic 1B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Script kiddies	Topic 1B
Hacktivist	Topic 1B
Organized crime	Topic 1B
Nation states/APT	Topic 1B
Insiders	Topic 1B
Competitors	Topic 1B
Attributes of actors	Topic 1B
Internal/external	Topic 1B
Level of sophistication	Topic 1B
Resources/funding	Topic 1B
Intent/motivation	Topic 1B
Use of open-source intelligence	Topic 1B
1.4 Explain penetration testing concepts.	
Active reconnaissance	Topic 3A
Passive reconnaissance	Topic 3A
Pivot	Topic 3A
Initial exploitation	Topic 3A
Persistence	Topic 3A
Escalation of privilege	Topic 3A
Black box	Topic 3A
White box	Topic 3A
Gray box	Topic 3A
Penetration testing vs. vulnerability scanning	Topic 3A
1.5 Explain vulnerability scanning concepts.	
Passively test security controls	Topic 3D
Identify vulnerability	Topic 3D
Identify lack of security controls	Topic 3D
Identify common misconfigurations	Topic 3D
Intrusive vs. non-intrusive	Topic 3D
Credentialed vs. non-credentialed	Topic 3D
False positive	Topic 3D
1.6 Explain the impact associated with types of vulnerabilities.	
Race conditions	Topic 15A
Vulnerabilities due to:	Topic 11B, 11D
End-of-life systems	Topic 11B
Embedded systems	Topic 11D
Lack of vendor support	Topic 11B
Improper input handling	Topic 15A
Improper error handling	Topic 15B
Misconfiguration/weak configuration	Topic 11B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Default configuration	Topic 11B
Resource exhaustion	Topic 9B
Untrained users	Topic 16C
Improperly configured accounts	Topic 7D
Vulnerable business processes	Topic 14A
Weak cipher suites and implementations	Topic 4A
Memory/buffer vulnerability	Topic 15A
Memory leak	Topic 15A
Integer overflow	Topic 15A
Buffer overflow	Topic 15A
Pointer dereference	Topic 15A
DLL injection	Topic 15A
System sprawl/undocumented assets	Topic 13C
Architecture/design weaknesses	Topic 8A
New threats/zero day	Topic 15A
Improper certificate and key management	Topic 5B
Domain 2.0 Technologies and Tools	
2.1 Install and configure network components, both hardware- and software-based, to support organizational security.	
Firewall	Topic 9A
ACL	Topic 9A
Application-based vs. network-based	Topic 9A
Stateful vs. stateless	Topic 9A
Implicit deny	Topic 9A
VPN concentrator	Topic 12B
Remote access vs. site-to-site	Topic 12B
IPSec	Topic 12B
Tunnel mode	Topic 12B
Transport mode	Topic 12B
AH	Topic 12B
ESP	Topic 12B
Split tunnel vs. full tunnel	Topic 12B
TLS	Topic 12B
Always-on VPN	Topic 12B
NIPS/NIDS	Topic 9C
Signature-based	Topic 9C
Heuristic/behavioral	Topic 9C
Anomaly	Topic 9C
Inline vs. passive	Topic 9C
In-band vs. out-of-band	Topic 9C

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Rules	Topic 9C
Analytics	Topic 9C
False positive	Topic 9C
False negative	Topic 9C
Router	Topic 8D
ACLs	Topic 8D
Anti-spoofing	Topic 8D
Switch	Topic 8B
Port security	Topic 8B
Layer 2 vs. Layer 3	Topic 8B
Loop prevention	Topic 8B
Flood guard	Topic 8B
Proxy	Topic 9A
Forward and reverse proxy	Topic 9A
Transparent	Topic 9A
Application/multipurpose	Topic 9A
Load balancer	Topic 9B
Scheduling	Topic 9B
Affinity	Topic 9B
Round robin	Topic 9B
Active–passive	Topic 9B
Active–active	Topic 9B
Virtual IPs	Topic 9B
Access point	Topic 10A
SSID	Topic 10A
MAC filtering	Topic 10A
Signal strength	Topic 10A
Band selection/width	Topic 10A
Antenna types and placement	Topic 10A
Fat vs. thin	Topic 10A
Controller-based vs. standalone	Topic 10A
SIEM	Topic 9E
Aggregation	Topic 9E
Correlation	Topic 9E
Automated alerting and triggers	Topic 9E
Time synchronization	Topic 9E
Event deduplication	Topic 9E
Logs/WORM	Topic 9E
DLP	Topic 9D
USB blocking	Topic 9D

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Cloud-based	Topic 9D
Email	Topic 9D
NAC	Topic 8C
Dissolvable vs. permanent	Topic 8C
Host health checks	Topic 8C
Agent vs. agentless	Topic 8C
Mail gateway	Topic 13B
Spam filter	Topic 13B
DLP	Topic 13B
Encryption	Topic 13B
Bridge	Topic 8B
SSL/TLS accelerators	Topic 13A
SSL decryptors	Topic 13A
Media gateway	Topic 13B
Hardware security module	Topic 5B
2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.	
Protocol analyzer	Topic 3C
Network scanners	Topic 3B
Rogue system detection	Topic 3B
Network mapping	Topic 3B
Wireless scanners/cracker	Topic 3C
Password cracker	Topic 6B
Vulnerability scanner	Topic 3D
Configuration compliance scanner	Topic 3D
Exploitation frameworks	Topic 3D
Data sanitization tools	Topic 16B
Steganography tools	Topic 3C
Honeypot	Topic 3D
Backup utilities	Topic 14C
Banner grabbing	Topic 3C
Passive vs. active	Topic 3D
Command-line tools	Topic 3B, 3C
Ping	Topic 3B
Netstat	Topic 3C
Tracert	Topic 3B
nslookup/dig	Topic 3B
arp	Topic 3B
ipconfig/ip/ifconfig	Topic 3B
tcpdump	Topic 3C

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
nmap	Topic 3B, 3C
netcat	Topic 3C
2.3 Given a scenario, troubleshoot common security issues.	
Unencrypted credentials/cleartext	Topic 7D
Logs and event anomalies	Topic 9E
Permission issues	Topic 7D
Access violations	Topic 7D
Certificate issues	Topic 5B
Data exfiltration	Topic 9D
Misconfigured devices	Topic 9A, 10B
Firewall	Topic 9A
Content filter	Topic 9A
Access points	Topic 10B
Weak security configurations	Topic 11B
Personnel issues	Topic 16C
Policy violation	Topic 16C
Insider threat	Topic 16C
Social engineering	Topic 1C
Social media	Topic 16C
Personal email	Topic 16C
Unauthorized software	Topic 11B
Baseline deviation	Topic 11B
License compliance violation (availability/integrity)	Topic 16C
Asset management	Topic 14A
Authentication issues	Topic 7D
2.4 Given a scenario, analyze and interpret output from security technologies.	
HIDS/HIPS	Topic 9C
Antivirus	Topic 9C
File integrity check	Topic 9C
Host-based firewall	Topic 9A
Application whitelisting	Topic 11B
Removable media control	Topic 11B
Advanced malware tools	Topic 9C
Patch management tools	Topic 11B
UTM	Topic 9C
DLP	Topic 9D
Data execution prevention	Topic 11B
Web application firewall	Topic 9A
2.5 Given a scenario, deploy mobile devices securely.	

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Connection methods	Topic 11C
Cellular	Topic 11C
Wi-Fi	Topic 11C
SATCOM	Topic 11C
Bluetooth	Topic 11C
NFC	Topic 11C
ANT	Topic 11C
Infrared	Topic 11C
USB	Topic 11C
Mobile device management concepts	Topic 11C
Application management	Topic 11C
Content management	Topic 11C
Remote wipe	Topic 11C
Geofencing	Topic 11C
Geolocation	Topic 11C
Screen locks	Topic 11C
Push notification services	Topic 11C
Passwords and PINs	Topic 11C
Biometrics	Topic 11C
Context-aware authentication	Topic 11C
Containerization	Topic 11C
Storage segmentation	Topic 11C
Full device encryption	Topic 11C
Enforcement and monitoring for:	Topic 11C
Third-party app stores	Topic 11C
Rooting/jailbreaking	Topic 11C
Sideloading	Topic 11C
Custom firmware	Topic 11C
Carrier unlocking	Topic 11C
Firmware OTA updates	Topic 11C
Camera use	Topic 11C
SMS/MMS	Topic 11C
External media	Topic 11C
USB OTG	Topic 11C
Recording microphone	Topic 11C
GPS tagging	Topic 11C
Wi-Fi Direct/ad hoc	Topic 11C
Tethering	Topic 11C
Payment methods	Topic 11C
Deployment models	Topic 11C

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
BYOD	Topic 11C
COPE	Topic 11C
CYOD	Topic 11C
Corporate-owned	Topic 11C
VDI	Topic 11C
2.6 Given a scenario, implement secure protocols.	
Protocols	
DNSSEC	Topic 12A
SSH	Topic 12C
S/MIME	Topic 13B
SRTP	Topic 13B
LDAPS	Topic 7A
FTPS	Topic 13A
SFTP	Topic 13A
SNMPv3	Topic 12A
SSL/TLS	Topic 13A
HTTPS	Topic 13A
Secure POP/IMAP	Topic 13B
Use cases	Topics 7A, 8B, 8D, 12A, 12C, 13A, 13B
Voice and video	Topic 13B
Time synchronization	Topic 12A
Email and web	Topic 13A, 13B
File transfer	Topic 13A
Directory services	Topic 7A
Remote access	Topic 12C
Domain name resolution	Topic 12A
Routing and switching	Topic 8B, 8D
Network address allocation	Topic 12A
Subscription services	Topic 13A
Domain 3.0 Architecture and Design	
3.1 Explain use cases and purpose for frameworks, best practices, and secure configuration guides.	
Industry-standard frameworks and reference architectures	Topic 2A
Regulatory	Topic 2A
Non-regulatory	Topic 2A
National vs. international	Topic 2A
Industry-specific frameworks	Topic 2A
Benchmarks/secure configuration guides	Topic 2A
Platform/vendor-specific guides	Topic 2A
Web server	Topic 2A

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Operating system	Topic 2A
Application server	Topic 2A
Network infrastructure devices	Topic 2A
General purpose guides	Topic 2A
Defense in depth/layered security	Topic 2A
Vendor diversity	Topic 2A
Control diversity	Topic 2A
Administrative	Topic 2A
Technical	Topic 2A
User training	Topic 2A
3.2 Given a scenario, implement secure network architecture concepts.	
Zones/topologies	Topic 8A
DMZ	Topic 8A
Extranet	Topic 8A
Intranet	Topic 8A
Wireless	Topic 8A
Guest	Topic 8A
Honeynets	Topic 8A
NAT	Topic 8D
Ad hoc	Topic 8B
Segregation/segmentation/isolation	Topic 8A
Physical	Topic 8A
Logical (VLAN)	Topic 8A
Virtualization	Topic 8A
Air gaps	Topic 8A
Tunneling/VPN	Topic 12B
Site-to-site	Topic 12B
Remote access	Topic 12B
Security device/technology placement	Topics 8B, 9A, 9B, 9C, 9E, 12B, 13A
Sensors	Topic 9E
Collectors	Topic 9E
Correlation engines	Topic 9E
Filters	Topic 9A
Proxies	Topic 9A
Firewalls	Topic 9A
VPN concentrators	Topic 12B
SSL accelerators	Topic 13A
Load balancers	Topic 9B
DDoS mitigator	Topic 9B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Aggregation switches	Topic 8B
Taps and port mirror	Topic 9C
SDN	Topic 8D
3.3 Given a scenario, implement secure systems design.	
Hardware/firmware security	Topic 11A
FDE/SED	Topic 11A
TPM	Topic 11A
HSM	Topic 11A
UEFI/BIOS	Topic 11A
Secure boot and attestation	Topic 11A
Supply chain	Topic 11A
Hardware root of trust	Topic 11A
EMI/EMP	Topic 11A
Operating systems	Topic 11B
Types	Topic 11B
Network	Topic 11B
Server	Topic 11B
Workstation	Topic 11B
Appliance	Topic 11B
Kiosk	Topic 11B
Mobile OS	Topic 11B
Patch management	Topic 11B
Disabling unnecessary ports and services	Topic 11B
Least functionality	Topic 11B
Secure configurations	Topic 11B
Trusted operating system	Topic 11A
Application whitelisting/blacklisting	Topic 11B
Disable default accounts/passwords	Topic 11B
Peripherals	Topic 11A
Wireless keyboards	Topic 11A
Wireless mice	Topic 11A
Displays	Topic 11A
Wi-Fi-enabled microSD cards	Topic 11A
Printers/MFDs	Topic 11A
External storage devices	Topic 11A
Digital cameras	Topic 11A

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
3.4 Explain the importance of secure staging deployment concepts.	
Sandboxing	Topic 15B
Environment	Topic 15B
Development	Topic 15B
Test	Topic 15B
Staging	Topic 15B
Production	Topic 15B
Secure baseline	Topic 15B
Integrity measurement	Topic 15B
3.5 Explain the security implications of embedded systems.	
SCADA/ICS	Topic 11D
Smart devices/IoT	Topic 11D
Wearable technology	Topic 11D
Home automation	Topic 11D
HVAC	Topic 11D
SoC	Topic 11D
RTOS	Topic 11D
Printers/MFDs	Topic 11D
Camera systems	Topic 11D
Special purpose	Topic 11D
Medical devices	Topic 11D
Vehicles	Topic 11D
Aircraft/UAV	Topic 11D
3.6 Summarize secure application development and deployment concepts.	
Development lifecycle models	Topic 15B
Waterfall vs. agile	Topic 15B
Secure DevOps	Topic 15B
Security automation	Topic 15B
Continuous integration	Topic 15B
Baselining	Topic 15B
Immutable systems	Topic 15B
Infrastructure as code	Topic 15B
Version control and change management	Topic 15B
Provisioning and deprovisioning	Topic 15B
Secure coding techniques	Topic 15B
Proper error handling	Topic 15B
Proper input validation	Topic 15B
Normalization	Topic 15B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Stored procedures	Topic 15B
Code signing	Topic 15B
Encryption	Topic 15B
Obfuscation/camouflage	Topic 15B
Code reuse/dead code	Topic 15B
Server-side vs. client-side execution and validation	Topic 15B
Memory management	Topic 15B
Use of third-party libraries and SDKs	Topic 15B
Data exposure	Topic 15B
Code quality and testing	Topic 15B
Static code analyzers	Topic 15B
Dynamic analysis (e.g., fuzzing)	Topic 15B
Stress testing	Topic 15B
Sandboxing	Topic 15B
Model verification	Topic 15B
Compiled vs. runtime code	Topic 15B
3.7 Summarize cloud and virtualization concepts.	
Hypervisor	Topic 13C
Type I	Topic 13C
Type II	Topic 13C
Application cells/containers	Topic 13C
VM sprawl avoidance	Topic 13C
VM escape protection	Topic 13C
Cloud storage	Topic 13D
Cloud deployment models	Topic 13D
SaaS	Topic 13D
PaaS	Topic 13D
IaaS	Topic 13D
Private	Topic 13D
Public	Topic 13D
Hybrid	Topic 13D
Community	Topic 13D
On-premises vs. hosted vs. cloud	Topic 13D
VDI/VDE	Topic 13C
Cloud access security broker	Topic 13D
Security as a Service	Topic 13D
3.8 Explain how resiliency and automation strategies reduce risk.	
Automation/scripting	Topic 14B
Automated courses of action	Topic 14B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Continuous monitoring	Topic 14B
Configuration validation	Topic 14B
Templates	Topic 14B
Master image	Topic 14B
Non-persistence	Topic 14B
Snapshots	Topic 14B
Revert to known state	Topic 14B
Rollback to known configuration	Topic 14B
Live boot media	Topic 14B
Elasticity	Topic 14B
Scalability	Topic 14B
Distributive allocation	Topic 14B
Redundancy	Topic 14B
Fault tolerance	Topic 14B
High availability	Topic 14B
RAID	Topic 14B
3.9 Explain the importance of physical security controls.	
Lighting	Topic 10C
Signs	Topic 10C
Fencing/gate/cage	Topic 10C
Security guards	Topic 10C
Alarms	Topic 10C
Safe	Topic 10C
Secure cabinets/enclosures	Topic 10C
Protected distribution/protected cabling	Topic 10C
Air gap	Topic 10C
Mantrap	Topic 10C
Faraday cage	Topic 10C
Lock types	Topic 10C
Biometrics	Topic 10C
Barricades/bollards	Topic 10C
Tokens/cards	Topic 10C
Environmental controls	Topic 10C
HVAC	Topic 10C
Hot and cold aisles	Topic 10C
Fire suppression	Topic 10C
Cable locks	Topic 10C
Screen filters	Topic 10C
Cameras	Topic 10C
Motion detection	Topic 10C

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Logs	Topic 10C
Infrared detection	Topic 10C
Key management	Topic 10C
Domain 4.0 Identity and Access Management	
4.1 Compare and contrast identity and access management Concepts.	
Identification, authentication, authorization, and accounting (AAA)	Topic 6A
Multi-factor authentication	Topic 6A
Something you are	Topic 6A
Something you have	Topic 6A
Something you know	Topic 6A
Somewhere you are	Topic 6A
Something you do	Topic 6A
Federation	Topic 7A
Single sign-on	Topic 7A
Transitive trust	Topic 7A
4.2 Given a scenario, install and configure identity access services.	
LDAP	Topic 7A
Kerberos	Topic 6B
TACACS+	Topic 7A
CHAP	Topic 6B
PAP	Topic 6B
MSCHAP	Topic 6B
RADIUS	Topic 7A
SAML	Topic 7A
OpenID Connect	Topic 7A
OAuth	Topic 7A
Shibboleth	Topic 7A
Secure token	Topic 7A
NTLM	Topic 6B
4.3 Given a scenario, implement identity and access management controls.	
Access control models	Topic 7B
MAC	Topic 7B
DAC	Topic 7B
ABAC	Topic 7B
Role-based access control	Topic 7B
Rule-based access control	Topic 7B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Physical access control	Topic 6C
Proximity cards	Topic 6C
Smart cards	Topic 6C
Biometric factors	Topic 6C
Fingerprint scanner	Topic 6C
Retinal scanner	Topic 6C
Iris scanner	Topic 6C
Voice recognition	Topic 6C
Facial recognition	Topic 6C
False acceptance rate	Topic 6C
False rejection rate	Topic 6C
Crossover error rate	Topic 6C
Tokens	Topic 6C
Hardware	Topic 6C
Software	Topic 6C
HOTP/TOTP	Topic 6C
Certificate-based authentication	Topic 6C
PIV/CAC/smart card	Topic 6C
IEEE 802.1x	Topic 6C
File system security	Topic 7B
Database security	Topic 7B
4.4 Given a scenario, differentiate common account management practices.	
Account types	Topic 7B
User account	Topic 7B
Shared and generic accounts/credentials	Topic 7B
Guest accounts	Topic 7B
Service accounts	Topic 7B
Privileged accounts	Topic 7B
General concepts	Topic 7C
Least privilege	Topic 7C
Onboarding/offboarding	Topic 7C
Permission auditing and review	Topic 7D
Usage auditing and review	Topic 7D
Time-of-day restrictions	Topic 7C
Recertification	Topic 7D
Standard naming convention	Topic 7C
Account maintenance	Topic 7C
Group-based access control	Topic 7C
Location-based policies	Topic 7C

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Account policy enforcement	Topic 7C
Credential management	Topic 7C
Group policy	Topic 7C
Password complexity	Topic 7C
Expiration	Topic 7C
Recovery	Topic 7C
Disablement	Topic 7C
Lockout	Topic 7C
Password history	Topic 7C
Password reuse	Topic 7C
Password length	Topic 7C
Domain 5.0 Risk Management	
5.1 Explain the importance of policies, plans, and procedures related to organizational security.	
Standard operating procedure	Topic 16A
Agreement types	Topic 16A
BPA	Topic 16A
SLA	Topic 16A
ISA	Topic 16A
MOU/MOA	Topic 16A
Personnel management	Topic 16C
Mandatory vacations	Topic 16C
Job rotation	Topic 16C
Separation of duties	Topic 16C
Clean desk	Topic 16C
Background checks	Topic 16C
Exit interviews	Topic 16C
Role-based awareness training	Topic 16C
Data owner	Topic 16C
System administrator	Topic 16C
System owner	Topic 16C
User	Topic 16C
Privileged user	Topic 16C
Executive user	Topic 16C
NDA	Topic 16A, 16C
Onboarding	Topic 16C
Continuing education	Topic 16C
Acceptable use policy/rules of behavior	Topic 16C
Adverse actions	Topic 16C
General security policies	Topic 16C

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Social media networks/applications	Topic 16C
Personal email	Topic 16C
5.2 Summarize business impact analysis concepts.	
RTO/RPO	Topic 14A
MTBF	Topic 14A
MTTR	Topic 14A
Mission-essential functions	Topic 14A
Identification of critical systems	Topic 14A
Single point of failure	Topic 14A
Impact	Topic 14A
Life	Topic 14A
Property	Topic 14A
Safety	Topic 14A
Finance	Topic 14A
Reputation	Topic 14A
Privacy impact assessment	Topic 14A
Privacy threshold assessment	Topic 14A
5.3 Explain risk management processes and concepts.	
Threat assessment	Topic 14A
Environmental	Topic 14A
Man-made	Topic 14A
Internal vs. external	Topic 14A
Risk assessment	Topic 14A
SLE	Topic 14A
ALE	Topic 14A
ARO	Topic 14A
Asset value	Topic 14A
Risk register	Topic 14A
Likelihood of occurrence	Topic 14A
Supply chain assessment	Topic 14A
Impact	Topic 14A
Quantitative	Topic 14A
Qualitative	Topic 14A
Testing	Topic 3A
Penetration testing authorization	Topic 3A
Vulnerability testing authorization	Topic 3A
Risk response techniques	Topic 14A
Accept	Topic 14A
Transfer	Topic 14A
Avoid	Topic 14A

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Mitigate	Topic 14A
Change management	Topic 14A
5.4 Given a scenario, follow incident response procedures.	
Incident response plan	Topic 2B
Documented incident types/category definitions	Topic 2B
Roles and responsibilities	Topic 2B
Reporting requirements/escalation	Topic 2B
Cyber incident response teams	Topic 2B
Exercise	Topic 2B
Incident response process	Topic 2B
Preparation	Topic 2B
Identification	Topic 2B
Containment	Topic 2B
Eradication	Topic 2B
Recovery	Topic 2B
Lessons learned	Topic 2B
5.5 Summarize basic concepts of forensics.	
Order of volatility	Topic 14D
Chain of custody	Topic 14D
Legal hold	Topic 14D
Data acquisition	Topic 14D
Capture system image	Topic 14D
Network traffic and logs	Topic 14D
Capture video	Topic 14D
Record time offset	Topic 14D
Task hashes	Topic 14D
Screenshots	Topic 14D
Witness interviews	Topic 14D
Preservation	Topic 14D
Recovery	Topic 14D
Strategic intelligence/counterintelligence gathering	Topic 14D
Active logging	Topic 14D
Track man-hours	Topic 14D
5.6 Explain disaster recovery and continuity of operations concepts	
Recovery sites	Topic 14C
Hot site	Topic 14C
Warm site	Topic 14C
Cold site	Topic 14C
Order of restoration	Topic 14C

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Backup concepts	Topic 14C
Differential	Topic 14C
Incremental	Topic 14C
Snapshots	Topic 14C
Full	Topic 14C
Geographic considerations	Topic 14C
Off-site backups	Topic 14C
Distance	Topic 14C
Location selection	Topic 14C
Legal implications	Topic 14C
Data sovereignty	Topic 14C
Continuity of operation planning	Topic 14C
Exercises/tabletop	Topic 14C
After-action reports	Topic 14C
Failover	Topic 14C
Alternate processing sites	Topic 14C
Alternate business practices	Topic 14C
5.7 Compare and contrast various types of controls.	
Deterrent	Topic 2A
Preventive	Topic 2A
Detective	Topic 2A
Compensating	Topic 2A
Technical	Topic 2A
Administrative	Topic 2A
Physical	Topic 2A
5.8 Given a scenario, carry out data security and privacy practices.	
Data destruction and media sanitization	Topic 16B
Burning	Topic 16B
Shredding	Topic 16B
Pulping	Topic 16B
Pulverizing	Topic 16B
Degaussing	Topic 16B
Purging	Topic 16B
Wiping	Topic 16B
Data sensitivity labeling and handling	Topic 16B
Confidential	Topic 16B
Private	Topic 16B
Public	Topic 16B
Proprietary	Topic 16B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
PII	Topic 16B
PHI	Topic 16B
Data roles	Topic 16B
Owner	Topic 16B
Steward/custodian	Topic 16B
Privacy officer	Topic 16B
Data retention	Topic 16B
Legal and compliance	Topic 16B
Domain 6.0 Cryptography and PKI	
6.1 Compare and contrast basic concepts of cryptography.	
Symmetric algorithms	Topic 4B
Modes of operation	Topic 4B
Asymmetric algorithms	Topic 4C
Hashing	Topic 4B
Salt, IV, nonce	Topic 4A
Elliptic curve	Topic 4C
Weak/deprecated algorithms	Topic 4A
Key exchange	Topic 4C
Digital signatures	Topic 4C
Diffusion	Topic 4A
Confusion	Topic 4A
Collision	Topic 4C
Steganography	Topic 4A
Obfuscation	Topic 4A
Stream vs. block	Topic 4B
Key strength	Topic 4A
Session keys	Topic 4C
Ephemeral key	Topic 4C
Secret algorithm	Topic 4A
Data in transit	Topic 4B
Data at rest	Topic 4B
Data in use	Topic 4B
Random/pseudorandom number generation	Topic 4A
Key stretching	Topic 6B
Implementation vs. algorithm selection	Topic 4B
Crypto service provider	Topic 4B
Crypto modules	Topic 4B
Perfect forward secrecy	Topic 4C
Security through obscurity	Topic 4A
Common use cases	Topic 4A, 4B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Low power devices	Topic 4B
Low latency	Topic 4B
High resiliency	Topic 4A
Supporting confidentiality	Topic 4A
Supporting integrity	Topic 4A
Supporting obfuscation	Topic 4A
Supporting authentication	Topic 4A
Supporting non-repudiation	Topic 4A
Resource vs. security constraints	Topic 4B
6.2 Explain cryptography algorithms and their basic characteristics.	
Symmetric algorithms	Topic 4B
AES	Topic 4B
DES	Topic 4B
3DES	Topic 4B
RC4	Topic 4B
Blowfish/Twofish	Topic 4B
Cipher modes	Topic 4B
CBC	Topic 4B
GCM	Topic 4B
ECB	Topic 4B
CTM	Topic 4B
Stream vs. block	Topic 4B
Asymmetric algorithms	Topic 4C, 5B
RSA	Topic 4C
DSA	Topic 4C
Diffie-Hellman	Topic 4C
Groups	Topic 4C
DHE	Topic 4C
ECDHE	Topic 4C
Elliptic curve	Topic 4C
PGP/GPG	Topic 5B
Hashing algorithms	Topic 4B
MD5	Topic 4B
SHA	Topic 4B
HMAC	Topic 4B
RIPEMD	Topic 4B
Key stretching algorithms	Topic 6B
bcrypt	Topic 6B
PBKDF2	Topic 6B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Obfuscation	Topic 4A
XOR	Topic 4
ROT13	Topic 4A
Substitution ciphers	Topic 4A
6.3 Given a scenario, install and configure wireless security settings.	
Cryptographic protocols	Topic 10B
WPA	Topic 10B
WPA2	Topic 10B
CCMP	Topic 10B
TKIP	Topic 10B
Authentication protocols	Topic 10B
EAP	Topic 10B
PEAP	Topic 10B
EAP-FAST	Topic 10B
EAP-TLS	Topic 10B
EAP-TTLS	Topic 10B
IEEE 802.1x	Topic 10B
RADIUS federation	Topic 10B
Methods	Topic 10B
PSK vs. Enterprise vs. open	Topic 10B
WPS	Topic 10B
Captive portals	Topic 10B
6.4 Given a scenario, implement public key infrastructure.	
Components	Topic 5A, 5B
CA	Topic 5A
Intermediate CA	Topic 5B
CRL	Topic 5B
OCSP	Topic 5B
CSR	Topic 5A
Certificate	Topic 5A
Public key	Topic 5A
Private key	Topic 5A
Object identifiers (OID)	Topic 5A
Concepts	Topic 5B
Online vs. offline CA	Topic 5B
Stapling	Topic 5B
Pinning	Topic 5B
Trust model	Topic 5B
Key escrow	Topic 5B

Domain and Objective	The Official CompTIA Security+ (Exam SY0-501): 2019 Update
Certificate chaining	Topic 5B
Types of certificates	Topic 5A
Wildcard	Topic 5A
SAN	Topic 5A
Code signing	Topic 5A
Self-signed	Topic 5A
Machine/computer	Topic 5A
Email	Topic 5A
User	Topic 5A
Root	Topic 5A
Domain validation	Topic 5A
Extended validation	Topic 5A
Certificate formats	Topic 5A
DER	Topic 5A
PEM	Topic 5A
PFX	Topic 5A
CER	Topic 5A
P12	Topic 5A
P7B	Topic 5A

In Closing

This course is still designed for learners who have experience as IT professionals with experience in TCP/IP networking and Windows administration, and who want to gain additional knowledge of security topics or use this course as the foundation for advanced security certifications and career roles. To obtain CompTIA Security+ certification, learners will need to pass the SY0-501 exam. Enjoy the course!