Hewlett Packard Enterprise

HPE Digital Learner CompTIA - Security+ Content Pack

HPE Content Pack number	CP034
Content Pack length	26 Hours
Content Pack category	Category 2
Learn more	**View now**

Why HPE Education Services?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

The CompTIA Security+ exam will certify that the successful candidate has the knowledge and skills to:

- Install and configure systems to secure applications, networks and devices
- Perform threat analysis and respond with appropriate mitigation techniques
- Participate in risk mitigation activities
- Operate with an awareness of applicable policies, laws and regulations

The successful candidate will perform the above tasks, supporting the principles of CIA (Confidentiality, Integrity and Availability).

Audience

Security professionals working in IT administration with a focus on security who have day-to-day technical information, security experience and a broad knowledge of security concerns and implementations; a minimum of two years experience is recommended

Content Pack Objectives

Passing the associated examination will demonstrate your capability and skills in the areas (domains) that are tested:

- Threats, attacks and vulnerabilities (21%)
- Technologies and tools (22%)
- Architecture and design (15%)
- Identity and access management (16%)
- Risk management (14%)
- Cryptography and PKI (12%)

Examinations

- Exam Reference: SY0-501
- Number of questions: Maximum of 90
- Types of questions: Multiple choice and performance-based
- Time allowed to complete: 90 minutes
- Recommended experience At least two years of experience
- Passing score: 750 (on a scale of 100–900)

Detailed Content Pack outline

CompTIA Security+ SY0-501: The Present Threat Landscape

- Describe the threat landscape
- Describe risks and vulnerabilities
- Define threats, threat agents, exploits, and payloads
- Define countermeasures and mitigation
- Describe IOCs
- Describe script kiddies and hacktivists
- Compare organized crime, states, and APTs
- Describe insider and competitor threats
- Compare internal and external threats
- Compare structured and unstructured threats
- Define levels of sophistication, resources, and funding of threats
- Recognize threat intent and motivation
- Describe different open-source intelligence in threats
- Identify different malware threats
- Define and describe the threat landscape and agents

CompTIA Security+ SY0-501: Types of Malware

- Describe viruses
- Define worms
- Describe Trojans
- Specify RATs
- Identify different vulnerabilities
- Describe ransomware
- Define cryptomalware
- Describe bots and botnets
- Define backdoors
- Define rootkits
- Define logic bombs
- Define keyloggers
- Classify spyware
- Define stegomalware
- Describe polymorphic packers
- Describe and compare malware types

CompTIA Security+ SY0-501: Social Engineering and Related Attacks

- Define impersonation and hoaxing
- Recognize tailgating and piggybacking
- Define shoulder surfing
- Describe dumpster diving
- CompTIA Security+ SY0-501: Social Engineering and Related Attacks
- Compare phishing, spear phishing, and whaling
- Describe watering hole attacks (social networks)
- Compare vishing and smishing
- Specify reasons for effectiveness
- Define clickjacking
- Describe session hijacking
- Describe URL hijacking
- Recognize typosquatting
- Define shimming
- Describe refactoring
- Recognize and classify social engineering and hijacking attacks

CompTIA Security+ SY0-501: Application and Service Attacks

- Describe zero day attacks
- Classify spoofing
- Recognize DoS and DDoS attacks
- Describe man-in-the-middle attacks
- Define ARP poisoning
- Describe buffer overflow attacks
- Recognize injection attacks
- Define privilege escalation
- Compare reflection and amplification
- Describe DNS poisoning
- Recognize domain hijacking
- Define man-in-the-browser
- Compare cross-site scripting and request forgery
- Describe replay attacks
- Define pass the hash attacks
- Recognize application and service attacks

CompTIA Security+ SY0-501: Cryptographic and Wireless Attacks

- Recognize brute-force and dictionary attacks
- Demonstrate brute-force tools
- Describe birthday, known plaintext, and cipher attacks
- Compare online vs. offline attacks
- Define collisions
- Describe downgrade attacks
- Recognize replay attacks
- Specify initialization vector weaknesses
- Compare evil twins and rogue apps
- Describe jamming
- Compare bluejacking and bluesnarfing
- Define WPS attacks
- Recognize disassociation attacks
- Compare RFID and near field communication (NFC)
- Recognize cryptographic and wireless attacks

CompTIA Security+ SY0-501: Penetration Testing and Vulnerability Scanning

- Compare active vs. passive reconnaissance
- Describe a pivot
- Specify initial exploitation
- Define persistence
- Recognize escalation of privilege
- Compare black vs. gray vs. white box
- Compare pen testing vs. vulnerability scanning
- Passively test security controls
- Identify vulnerability
- Identify lack of security controls
- Identify common misconfigurations
- Compare intrusive vs. non-intrusive
- Compare credentialed vs. non-credentialed
- Describe false positives
- Recognize penetration testing and vulnerability scanning methods

CompTIA Security+ SY0-501: Impacts from Vulnerability Types

- Describe race conditions
- Recognize system vulnerabilities
- Specify improper input and error handling
- Define misconfiguration
- Describe resource exhaustion
- Specify untrained users
- Work with improperly configured accounts
- Recognize vulnerable business processes
- Recognize weak cipher suites and implementations
- Define memory and buffer vulnerability
- Describe system sprawl and undocumented assets
- Describe architecture and design weaknesses
- Recognize new threats and zero-day attacks
- Define improper certificate and key management
- Specify the impact of different types of vulnerabilities

CompTIA Security+ SY0-501: Components Supporting Organizational Security

- Define firewalls
- Describe VPN concentrators
- Compare NIDS and NIPS
- Compare bridges and switches
- Describe routers
- Compare proxies and load balancers
- Recognize wireless access points
- Define SIEM systems
- Describe DLP systems
- Define NAC gateways
- Describe mail gateways
- Define media gateways
- Define encryption gateways
- Recognize specialty appliances
- Describe the various components that support organizational security

CompTIA Security+ SY0-501: Security Assessment Using Software Tools

- Work with protocol analyzers
- Work with network scanners
- Specify wireless scanners/cracker
- Work with password crackers
- Describe vulnerability scanners
- Define configuration compliance scanner
- Describe exploitation frameworks
- Compare data sanitization tools
- Define steganography tools
- Describe honeypots
- Configure backup utilities
- Define banner grabbing
- Compare passive vs. active
- Describe other command line tools
- Work with security assessment using software tools

CompTIA Security+ SY0-501: Cryptography

- Identify the role cryptography plays in maintaining CIA
- Identify the purpose of a cipher
- Identify the properties of a secure cipher
- Describe the function of block ciphers
- Describe the function of stream ciphers
- Describe the purpose of a cryptographic key
- Recognize the various ways to exchange cryptographic keys
- Describe the purpose of encryption
- Describe symmetric algorithms
- Identify various symmetric algorithms
- Describe asymmetric algorithms
- Identify various asymmetric algorithms
- Describe hashing
- Identify various hashing functions
- Describe data integrity
- Describe authentication
- Describe the purpose of digital signatures
- Describe the purpose of key stretching
- Identify additional security considerations such as steganography, obscurity, and weak algorithms
- Identify various cryptographic features and services

CompTIA Security+ SY0-501: Public Key Infrastructure

- Recall the purpose of a PKI and a trusted introducer
- Describe the benefits and uses of the public key infrastructure for an organization
- Recognize the various CA trust models that can be implemented, such as single CA, hierarchical, bridge, peer-to-peer, and mesh
- Describe the concept of certificate chaining
- Identify the purpose and types of pinning
- Describe the benefits of certificate expiration, revocation, and suspension, and distinguish between a CRL and OCSP
- Describe the benefits of key escrow and when you might consider using it
- Recognize the x.509 certificate format and file extensions
- Describe various types certificates and their uses
- Recall various PKI concepts

CompTIA Security+ SY0-501: Wireless Security Settings

- Describe the importance of authentication and encryption for wireless networks
- Identify the differences between the three different types of wireless networks
- Choose the most appropriate wireless standard and mode to secure your wireless communications
- Distinguish between PSK and Enterprise authentication for wireless networks
- Identify the common methods of encrypting communications on wireless networks
- Configure an open wireless network
- Configure a WPA PSK wireless network
- Configure a WPA Enterprise wireless network
- Configure a WPA2 PSK wireless network
- Configure a WPA2 Enterprise wireless network
- Describe and use Wi-Fi Protected Setup
- Describe and use a captive portal
- Recall various wireless security topics and concepts

CompTIA Security+ SY0-501: Analyzing Output from Security Technologies

- Work with Host Intrusion Detection System (HIDS) and Host Intrusion Prevention System (HIPS)
- Describe antivirus
- Define file integrity check
- Describe UTM
- Describe a host-based firewall
- Specify application whitelisting
- Define removable media control
- Compare patch management tools
- Define DLP
- Specify data execution prevention
- Describe web application firewall
- Work with technology output analysis

CompTIA Security+ SY0-501: Deploying Mobile Devices Securely

- Specify connection methods
- Compare deployment models
- Describe passwords, pins, and screen locks
- Define application and content management
- Describe remote wipe
- Compare geofencing and geolocation
- Describe push notification services
- Define biometrics and context-aware authentication
- Classify containerization and storage segmentation
- Describe full device encryption
- Describe enforcement and monitoring
- Describe enforcement and monitoring
- Describe ways to secure mobile devices

CompTIA Security+ SY0-501: Implementing Secure Protocols

- Work with SSH
- Describe Secure Sockets Layer and Transport Layer Security (SSL/TLS)
- Describe HTTPS
- Describe DNSSEC
- Describe SRTP
- Describe FTPS
- Describe SFTP
- Describe LDAPS
- Describe work with SNMPv3
- Describe NTPv3
- Describe Secure POP/IMAP
- Describe S/MIME
- Work with routing protocol authentication
- Recognize various secure versions of common protocols

CompTIA Security+ SY0-501: Troubleshooting Common Security Issues

- Define unencrypted credentials
- Describe logs and events anomalies
- Specify permission issues
- Define access violations
- Specify certificate issues
- Describe data exfiltration
- Describe misconfigured devices
- Recognize weak security configurations
- Classify personnel issues
- Define unauthorized software
- Define baseline deviation
- Recognize license compliance violation
- Describe asset management
- Specify authentication issues
- Specify various security troubleshooting issues

CompTIA Security+ SY0-501: Identity Concepts and Access Services

- Compare identity and access management concepts
- Compare and contrast identity and access management concepts
- Define NTLM
- Compare PAP, CHAP, and MSCHAP
- Describe RADIUS
- Describe Terminal Access Controller Access Control System (TACACS+)
- Recognize Kerberos
- Define LDAP
- Describe secure token
- Define SAML
- Specify OpenID Connect
- Define OAuth
- Describe Shibboleth
- Describe identity concepts and various access services

CompTIA Security+ SY0-501: Identity and Access Management Controls

- Define MAC
- Define DAC
- Define ABAC
- Describe role-based access control
- Describe rule-based access control
- Use a fingerprint scanner
- Work with a retinal and iris scanner
- Use voice recognition
- Describe facial recognition
- Compare FAR, FRR, and CER
- Define tokens
- Describe certificate-based authentication
- Define file system security
- Define database security
- Compare access controls and biometrics

CompTIA Security+ SY0-501: Common Account Management Practices

- Define user accounts
- Compare shared, guest, and generic accounts
- Describe privileged accounts
- Specify service accounts
- Recognize password best practices
- Define credential management and naming conventions
- Recognize group-based access control and Group Policy
- Describe location-based policies
- Define least privilege and time-of-day restrictions
- Compare onboarding and offboarding
- Describe recertification
- Define account maintenance
- Describe auditing and review
- Describe various account management best practices

CompTIA Security+ SY0-501: Frameworks, Guidelines, and Physical Security

- Identify the purpose of various frameworks and architectures
- Specify the reasoning behind following secure configuration guidelines
- Describe the benefits of implementing a layered security approach and the importance of diversity and user training
- Describe the importance of physical security in relation to the success of your organization
- Identify the importance of lighting in relation to security
- Identify the various methods that can be used to control or deter physical access
- Describe the importance of alarms and the difference between false alarms and true alarms
- Identify the benefits of using safes and secure cabinets
- Identify different types of locks and describe the importance of key management
- Describe various authentication options
- Define the importance of HVAC systems and fire suppression systems
- Describe various types of motion detection systems
- Define the concept of a protected system and air gaps
- Describe the purpose of various security controls such as Faraday cages, cable locks, screen filters, cameras, and sign-in and sign-out logs
- Recall the purpose of various security controls

CompTIA Security+ SY0-501: Implement Secure Network Architecture Concepts • Describe the reasoning behind implementing different zones and topologies	• Define how physical, logical, virtual, and air gap separation provide security • Describe site-to-site and remote access VPNs	• Define where various devices and technologies should be placed for maximum security benefits • Describe the security concerns surrounding the SDN • Recall the purpose of various secure network architecture concepts
CompTIA Security+ SY0-501: Secure System and Application Design and Deployment • Describe how anchoring the trust of a system within hardware using TPM, SED, and HSM improves security • Describe the benefits of secure system booting and how UEFI plays a role in it • Identify how systems may be protected from EMI and EMP • Identify when security needs to be considered in the supply chain • Recall key considerations of a secure operating system	• Describe the concept of a trusted operating system • Describe the security concerns and considerations when using wireless keyboards and mice, displays, Wi-Fi enabled MicroSD cards, printers, usb storage, and digital cameras • Define secure development concepts • Describe the security concerns of SCADA, IoT, and HVAC • Describe the security concerns of SoC and RTOS • Describe the security concerns of multi-function devices, camera systems, medical devices, vehicles, and aircraft	• Compare waterfall and Agile development life cycle models • Describe the importance of security with DevOps • Define various development concepts • Describe various techniques that are used for secure coding • Define various methods for code quality and testing • Compare compiled code vs. runtime code • Recall various concepts related to secure system design and application development
CompTIA Security+ SY0-501: Cloud, Virtualization, and Resiliency Concepts • Compare different types of hypervisors and the benefits of using application containers • Describe the issues related to VMs • Compare the different types of cloud offerings such as IaaS, PaaS, and SaaS.	• Define the purpose and benefit to using a VDI/VDE • Describe the function of a cloud access security broker and security as a service • Describe how automation and scripting provide resiliency • Describe how templates and master images provide resiliency	• Describe how non-persistence, snapshots, reverting to known states, rolling back configurations all provide resiliency • Describe elasticity, scalability, and distributive allocation • Define how high availability provides resiliency • Describe how RAID can provide resiliency • Recall various virtualization, cloud, and resiliency concepts
CompTIA Security+ SY0-501: Policies, Plans, and Procedures • Describe the benefits of using standard operating procedures • Define various agreements such as BPA, SLA, ISA, and MOU	• Describe the benefits of enforcing mandatory vacations, job rotation, separation of duties, and the principle of least privilege • Describe the benefits of a clean desk policy, a background check policy, exit interviews, NDA, and onboarding • Describe the benefits of security awareness training	• Define the purpose of acceptable use policies • Describe the benefits of social media policies and personal email policies • Recall the purpose of various policies, plans, and procedures
CompTIA Security+ SY0-501: Business Impact Analysis and Risk Management • Describe the purpose of a BCP • Identify the general steps in a BIA • Define concepts related to recovery time such as MTD, RTO, and RPO • Define Mean Time Between Failure (MTBF) and Mean Time to Repair (MTR)	• Describe privacy impact assessment and privacy threshold assessment • Define risk management • Describe risk assessment • Identify risks to an organization • Specify how to and who should be testing for risks	• Define risk analysis • Describe qualitative risk analysis • Describe quantitative risk analysis • Define methods that can be used to respond to risk • Define procedures for implementing change • Recall business impact assessment and risk management concepts

CompTIA Security+ SY0-501: Incident Response, Forensics, and Disaster Recovery • Define incident response and the incident response process • Describe the importance and components of an incident response plan • Describe the purpose of forensic investigation	• Identify the steps required during a forensics investigation • Compare strategic intelligence and strategic counterintelligence • Define disaster recovery and the disaster recovery plan • Describe the different types of recovery sites • Describe the different types of backups • Recognize the geographic implications of disaster recovery	• Identify different security controls • Describe media sanitization and data destruction • Describe the benefits of labeling and handling • Define various data roles • Describe the purpose of data retention • Recall incident response, forensics, disaster recovery, and security concepts
TestPrep SY0-501 CompTIA Security+	• TestPrep SYO-501 is designed to test your knowledge on the skills and competencies being measured by the vendor certification exam. TestPrep can be taken in either Study or Certification mode. Study mode is designed to maximize learning testing your knowledge of the material and also by providing additional information on the topics presented. Certification mode is designed to test your knowledge of the material within a structured testing environment, providing valuable feedback at the end of the test.	
CompTIA Security+	• Practice lab	

Learn more at

www.hpe.com/ww/digitallearner

www.hpe.com/ww/digitallearner-contentpack

Follow us:

CP034, May 2019

Hewlett Packard Enterprise