

CompTIA Security+ Course Outline

Duration: 40-50 Hours (Global Standards)

Level: Intermediate

Delivery Mode: Online/Offline

Certification: CompTIA Security+

Global Exam Code: SY0-601 (Latest Version)

Module 1: Introduction to Security Concepts

Duration: 3-5 Hours

- Overview of CompTIA Security+ Certification
 - Understanding Cybersecurity Concepts and Terminology
 - Types of Security Threats and Vulnerabilities
 - Malware, Phishing, Ransomware, Trojans, Worms
 - Social Engineering Techniques
 - Principles of Security: Confidentiality, Integrity, Availability (CIA Triad)
 - Risk Management and Security Policies
 - Importance of Security in Today's Digital World
-

Module 2: Network Security Fundamentals

Duration: 6-8 Hours

- Introduction to Networking Concepts
 - Network Types: LAN, WAN, PAN, VPN
 - OSI and TCP/IP Models
 - Protocols: HTTP/HTTPS, FTP, SSH, ICMP
 - Understanding Firewalls, Routers, and Switches
 - Configuring and Managing Firewalls
 - Types of Firewalls: Packet Filtering, Stateful, Proxy
 - IDS/IPS Systems: Intrusion Detection and Prevention
 - VPNs (Virtual Private Networks) and Remote Access
 - VPN Technologies: SSL, IPsec
 - Remote Access Security: RDP, VNC
 - Network Segmentation and Micro-Segmentation
 - Network Traffic Analysis and Monitoring Tools
-

Module 3: Identity and Access Management (IAM)

Duration: 5-7 Hours

- Understanding Authentication, Authorization, and Accounting (AAA)
 - Types of Authentication:
 - Password-Based, Multifactor Authentication (MFA)
 - Biometrics, Tokens, and Smart Cards
 - Single Sign-On (SSO)
 - Role-Based Access Control (RBAC)
 - Implementing IAM Systems and Techniques
 - Identity Federation, SAML, OAuth, OpenID
 - Access Control Models: Discretionary, Mandatory, and Role-Based Access
 - Managing User Accounts and Access Permissions
 - Understanding Active Directory and Group Policies
-

Module 4: Security Architecture and Design

Duration: 6-8 Hours

- Security Models and Frameworks:
 - Bell-LaPadula, Biba, Clark-Wilson
 - Designing a Secure Network Infrastructure
 - Securing Wired and Wireless Networks
 - Best Practices for Wi-Fi Security: WPA2, WPA3
 - System Hardening Techniques
 - Patching, Configuring Firewalls, and Disabling Unused Services
 - Reducing Attack Surface Area
 - Securing Servers, Endpoints, and Workstations
 - Secure Cloud Computing Architectures
 - Security in the SDLC (Software Development Life Cycle)
-

Module 5: Threats, Vulnerabilities, and Attacks

Duration: 5-7 Hours

- Types of Malware and Their Characteristics
 - Viruses, Worms, Trojans, Spyware, Rootkits
 - Detecting and Mitigating Malware Attacks
- Social Engineering and Phishing Attacks
 - Techniques: Pretexting, Baiting, Spear Phishing

- How to Prevent and Respond to Social Engineering Attacks
 - Types of Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks
 - Tools and Techniques for DoS Attacks
 - Mitigation Strategies
 - Common Attack Vectors:
 - Man-in-the-Middle (MitM), Cross-Site Scripting (XSS), SQL Injection
 - DNS Spoofing, Buffer Overflow
 - Vulnerability Scanning and Penetration Testing
-

Module 6: Cryptography and Public Key Infrastructure (PKI)

Duration: 6-8 Hours

- Basics of Cryptography: Encryption and Decryption Concepts
 - Types of Cryptographic Algorithms
 - Symmetric vs. Asymmetric Cryptography
 - RSA, AES, DES, ECC
 - Key Management: Generation, Storage, and Distribution
 - Public Key Infrastructure (PKI) Concepts
 - Certificates, Certificate Authorities (CA), and Digital Signatures
 - Certificate Revocation Lists (CRLs) and Certificate Expiry
 - Common Cryptographic Protocols
 - SSL/TLS, HTTPS, IPsec
 - Using Encryption for Data Security
 - File, Disk, and Email Encryption
-

Module 7: Security Operations and Incident Response

Duration: 5-7 Hours

- Incident Response Process
 - Identification, Containment, Eradication, and Recovery
 - Documentation and Communication During Incidents
- Disaster Recovery and Business Continuity Planning (BCP)
 - Backup Solutions: Full, Incremental, and Differential
 - Recovery Site Types: Hot, Warm, Cold
- Logging and Monitoring for Security Incidents
 - SIEM (Security Information and Event Management) Systems
 - Monitoring Network Traffic for Suspicious Activity
- Legal and Regulatory Compliance in Security

- GDPR, HIPAA, PCI-DSS, NIST
-

Module 8: Security in the Cloud and Virtualization

Duration: 4-6 Hours

- Introduction to Cloud Computing and Security Challenges
 - Types of Cloud: Public, Private, Hybrid
 - Cloud Service Models: IaaS, PaaS, SaaS
 - Cloud Security Best Practices
 - Data Encryption in the Cloud
 - Multi-Tenant and Shared Responsibility Model
 - Virtualization Security: Hypervisor and Virtual Machines (VMs)
 - Containerization and Securing Docker/Containers
 - Securing Cloud Resources: IAM, Firewalls, and APIs
-

Module 9: Risk Management and Security Controls

Duration: 4-6 Hours

- Risk Management Frameworks and Methodologies
 - Risk Assessment, Risk Mitigation, and Risk Response Strategies
 - Likelihood and Impact in Risk Calculations
 - Types of Security Controls: Preventative, Detective, Corrective
 - Implementing Security Controls in the Network, Systems, and Applications
 - Security Auditing and Compliance Checks
 - Security Standards: ISO/IEC 27001, NIST 800-53, CIS Controls
-

Module 10: CompTIA Security+ Exam Review and Preparation

Duration: 3-4 Hours

- Review of Key Exam Domains
 - Network Security, Threats, Cryptography, Access Management
 - Risk Management, Incident Response, and Security Architecture
- Practice Exam Questions and Scenarios
- Exam Preparation Tips and Strategies

- Time Management During the Exam
 - Post-Exam Guidance and Career Pathways
-

Module 11: CompTIA Security+ Certification Exam

- Final Exam: CompTIA Security+ SY0-601
- Exam Objectives Recap
- Post-Exam: Understanding Certification Results and Career Development