CyberGate ACADEMY

CSC

COMPTIA SECURITY+ COURSE

Course Overview

CompTIA Security+ (SY0-601) is a course designed to teach IT professionals the fundamentals of information security. The course covers everything from basic security concepts to advanced topics like identity management and vulnerability management. It provides a solid foundation in the essential security knowledge and skills necessary to develop and maintain a successful security program. The course can be used to prepare for the corresponding CompTIA Security+ certification exam and provide an understanding of security concepts that can be applied in any job.

Course Duration

5 Days (40 Hours).

Target Audience

The CompTIA Security+ SY0-601 training is designed for IT professionals who are looking to gain in-depth knowledge and expertise in the field of cybersecurity. This training is ideal for IT support professionals, system administrators, software developers, hardware engineers, and other individuals working in the security field or performing related IT activities. It is also a great option for those who are looking to gain official recognition of their cybersecurity skillset and become certified in security principles. The training provides an excellent introduction to the important principles and practices within the context of the CompTIA Security+ certification exam, ensuring that all candidates have the proper foundation to fully understand and be able to apply their knowledge when in a work environment.

During this course you should learn

1. Identify threats, attacks and technologies used to mitigate their impact.
2. Understand how to design, implement and manage network security.
3. Comprehend how to use authentication, authorization and access control mechanisms.
4. Gain knowledge of risk mitigation methods and to identify appropriate mitigation techniques.
5. Understand how to secure cloud, virtualization and information technologies.
6. Recognize secure software development principles, policies and procedures.
7. Become familiar with protocols and technologies associated with cryptography.
8. Learn to identify secure networks and systems using monitoring and logging tools.
9. Gain knowledge of organizational security strategies and incident response processes.
10. Understand the different principles, methods and tools used to support operations security.
11. Compare security roles and security controls.
12. Explain threat actors and threat intelligence.
13. Perform security assessments and identify social engineering attacks and malware types.
14. Summarize basic cryptographic concepts and implement public key infrastructure.
15. Implement authentication controls.
16. Implement identity and account management controls.
17. Implement secure network designs, network security appliances, and secure network protocols.
18. Implement host, embedded/Internet of Things, and mobile security solutions.
19. Implement secure cloud solutions.
20. Explain data privacy and protection concepts.
21. Perform incident response and digital forensics.
22. Summarize risk management concepts and implement cybersecurity resilience.
23. Explain physical security.

Course Content

Module1: Comparing Security Roles and Security Controls

- Compare and Contrast Information Security Roles.
- Compare and Contrast Security Control and Framework Types.

Module2: Explaining Threat Actors and Threat Intelligence

- Explain Threat Actor Types and Attack Vectors.
- Explain Threat Intelligence Sources.

Module3: Performing Security Assessments

- Assess Organizational Security with Network.
- Reconnaissance Tools.
- Explain Security Concerns with General Vulnerability Types.
- Summarize Vulnerability Scanning Techniques.
- Explain Penetration Testing Concepts.

Module4: Identifying Social Engineering and Malware

- Compare and Contrast Social Engineering Techniques.
- Analyze Indicators of Malware-Based Attacks.

Module5: Summarizing Basic Cryptographic Concepts

- Compare and Contrast Cryptographic Ciphers.
- Summarize Cryptographic Modes of Operation.
- Summarize Cryptographic Use Cases and Weaknesses.
- Summarize Other Cryptographic Technologies.

Module 6: Implementing Public Key Infrastructure

- Implement Certificates and Certificate Authorities
- Implement PKI Management

Module 7: Implementing Authentication Controls

- Summarize Authentication Design Concepts.
- Implement Knowledge-Based Authentication.
- Implement Authentication Technologies.
- Summarize Biometrics Authentication Concepts.

Module 8: Implementing Identity and Account Management Controls

- Implement Identity and Account Types.
- Implement Account Policies. .
- Implement Authorization Solutions.
- Explain the Importance of Personnel Policies.

Module 9: Implementing Secure Network Designs

- Implement Secure Network Designs.
- Implement Secure Switching and Routing.
- Implement Secure Wireless Infrastructure.
- Implement Load Balancers.

Module 10: Implementing Network Security Appliances

- Implement Firewalls and Proxy Servers.
- Implement Network Security Monitoring.
- Summarize the Use of SIEM.

Module 11: Implementing Secure Network Protocols

- Implement Secure Network Operations Protocols.
- Implement Secure Application Protocols.
- Implement Secure Remote Access Protocols.

Module 12: Implementing Host Security Solutions

- Implement Secure Firmware.
- Implement Endpoint Security.
- Explain Embedded System Security Implications.

Module 13: Implementing Secure Mobile Solutions

- Implement Mobile Device Management.
- Implement Secure Mobile Device Connections.

Module 14: Summarizing Secure Application Concepts

- Analyze Indicators of Application Attacks.
- Analyze Indicators of Web Application Attacks.
- Summarize Secure Coding Practices.
- Implement Secure Script Environments.
- Summarize Deployment and Automation Concepts.

Module 15: Implementing Secure Cloud Solutions

- Summarize Secure Cloud and Virtualization Services.
- Apply Cloud Security Solutions.
- Summarize Infrastructure as Code Concepts.

Module 16: Explaining Data Privacy and Protection Concepts

- Explain Privacy and Data Sensitivity Concepts.
- Explain Privacy and Data Protection Controls.

Module 17: Performing Incident Response

- Summarize Incident Response Procedures.
- Utilize Appropriate Data Sources for Incident Response.
- Apply Mitigation Controls.

Module 18: Explaining Digital Forensics

- Explain Key Aspects of Digital Forensics Documentation.
- Explain Key Aspects of Digital Forensics Evidence Acquisition.

Module 19: Summarizing Risk Management Concepts

- Explain Risk Management Processes and Concepts.
- Explain Business Impact Analysis Concepts.

Module 20: Implementing Cybersecurity Resilience

- Implement Redundancy Strategies
- Implement Backup Strategies
- Implement Cybersecurity Resiliency Strategies

Module 21: Explaining Physical Security

- Explain the Importance of Physical Site Security Controls
- Explain the Importance of Physical Host Security Controls

Labs:

Lab 01: Assisted Lab: Exploring the Lab Environment.
Lab 02: Assisted Lab: Scanning and Identifying Network Nodes.
Lab 03: Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools.
Lab 04: Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan.
Lab 05: Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor.
Lab 06: Applied Lab: Performing Network Reconnaissance and Vulnerability Scanning.
Lab 07: Assisted Lab: Managing the Life Cycle of a Certificate.
Lab 08: Assisted Lab: Managing Certificates with OpenSSL.
Lab 09: Assisted Lab: Auditing Passwords with a Password Cracking Utility.
Lab 10: Assisted Lab: Managing Centralized Authentication.
Lab 11: Assisted Lab: Managing Access Controls in Windows Server.
Lab 12: Assisted Lab: Configuring a System for Auditing Policies.
Lab 13: Assisted Lab: Managing Access Controls in Linux.
Lab 14: Applied Lab: Configuring Identity and Access Management Controls.
Lab 15: Assisted Lab: Implementing a Secure Network Design.
Lab 16: Assisted Lab: Configuring a Firewall.
Lab 17: Assisted Lab: Configuring an Intrusion Detection System.
Lab 18: Assisted Lab: Implementing Secure Network Addressing Services.
Lab 19: Assisted Lab: Implementing a Virtual Private Network.
Lab 20: Assisted Lab: Implementing a Secure SSH Server.
Lab 21: Assisted Lab: Implementing Endpoint Protection.
Lab 22: Applied Lab: Securing the Network Infrastructure.
Lab 23: Assisted Lab: Identifying Application Attack Indicators.
Lab 24: Assisted Lab: Identifying a Browser Attack.
Lab 25: Assisted Lab: Implementing PowerShell Security.
Lab 26: Assisted Lab: Identifying Malicious Code.

Prerequisites

Attendees should meet the following prerequisites:

- Basic Windows and Linux administrator skills
- The ability to implement fundamental networking appliances and IP addressing concepts
- Six to nine months' experience in networking, including configuring security parameters, are strongly recommended.

Course Agenda

Day 1	Module1: Comparing Security Roles and Security Controls Module2: Explaining Threat Actors and Threat Intelligence Module3: Performing Security Assessments Module4: Identifying Social Engineering and Malware Module5: Summarizing Basic Cryptographic Concepts
Day 2	Module 6: Implementing Public Key Infrastructure Module 7: Implementing Authentication Controls Module 8: Implementing Identity and Account Management Controls Module 9: Implementing Secure Network Designs
Day 3	Module 10: Implementing Network Security Appliances Module 11: Implementing Secure Network Protocols Module 12: Implementing Host Security Solutions Module 13: Implementing Secure Mobile Solutions
Day 4	Module 14: Summarizing Secure Application Concepts Module 15: Implementing Secure Cloud Solutions Module 16: Explaining Data Privacy and Protection Concepts
Day 5	Module 17: Performing Incident Response Module 18: Explaining Digital Forensics Module 19: Summarizing Risk Management Concepts Module 20: Implementing Cybersecurity Resilience Module 21: Explaining Physical Security

Technical Requirement

1. Laptop with minimum 8GB Ram.
2. Connected Monitor for iLabs.
3. Hi speed Internet Connection as All the labs it will be accessed through EC-Council Cloud.

Exam Voucher Validity

It will be valid for 12month starting from the last day of the course.

Certification Expiry

It will be valid for 3 years.

YOUR TRUSTED DEFENDERS

ADDRESS

CyberGate Academy
ADPOLY, MBZ City

WEB

academy@cybergate.tech
training@cybergate.tech