CompTIA AUTHORIZED PARTNER

COURSE OUTLINE

Course Name: CompTIA Security+

DURATION	SKILLS LEVEL	DILIVERY METHOD	TRAINING CREDITS	TECHNOLOGY
5 Days	Intermediate	Instructor-Led	50	IT Security

Course Description:

The CompTIA Security+ course provides students with the fundamental principles of installing and configuring cybersecurity controls and participating in incident response and risk mitigation.

In addition, this course will teach students with the skills and knowledge required 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 and operate with an awareness of applicable policies, laws and regulations.

This course will prepare you to take the CompTIA Security+ SY0-501 exam by providing 100% coverage of the objectives and content examples listed on the syllabus. Study of the course can also help to build the prerequisites to study more advanced IT security qualifications, such as CompTIA Cybersecurity Analyst (CSA)+, CompTIA Advanced Security Practitioner (CASP), and ISC's CISSP (Certified Information Systems Security Professional).

Prerequisites:

Before attending this course, students should have:

- Attended the CompTIA Network+ and have two years of experience in IT administration with a security focus.

Target Audience:

CompTIA Security+ is aimed at IT professionals with job roles such as security engineer, security consultant, information assurance, junior auditor, penetration tester, security administrator, system and network administrator.

Learning Objectives:

On completion of the course, delegates will be able to:

- Identify strategies developed by cyber adversaries to attack networks and hosts and the countermeasures deployed to defend them.
- Understand the principles of organizational security and the elements of effective security policies.
- Know the technologies and uses of cryptographic standards and products.
- Install and configure network and host-based security technologies.
- Describe how wireless and remote access security is enforced.
- Describe the standards and products used to enforce security on web and communications technologies.
- Identify strategies for ensuring business continuity, fault tolerance and disaster recovery.
- Summarize application and coding vulnerabilities and identify development and deployment methods designed to mitigate them.

Course Outline:

Lesson 1: Threats, Attacks and Vulnerabilities Unit 1: Indicators of Compromise

- Why is Security Important?
- Security Policy
- Threat Actor Types
- The Kill Chain
- Social Engineering
- Phishing
- Malware Types
- Trojans and Spyware
- Open-Source Intelligence

Unit 2: Critical Security Controls

- Security Control Types
- Defence in Depth
- Frameworks and Compliance
- Vulnerability Scanning and PenTest
- Security Assessment Techniques
- Pen Testing Concepts
- Vulnerability Scanning Concepts
- Exploitation Frameworks

Unit 3: Security Posture Assessment Tools

- Topology Discovery
- Service Discovery
- Packet Capture
- Packet Capture Tools
- Remote Access Trojans
- Honeypots and Honeynets

Unit 4: Incident Response

- Incident Response Procedures
- Preparation Phase
- Identification Phase
- Containment Phase
- Eradication and Recovery Phases

Lesson 2: Identity and Access Management

Unit 1: Cryptography

- Uses of Cryptography
- Cryptographic Terminology and Ciphers
- Cryptographic Products
- Hashing Algorithms
- Symmetric Algorithms
- Asymmetric Algorithms
- Diffie-Hellman and Elliptic Curve
- Transport Encryption
- Cryptographic Attacks

Unit 2: Public Key Infrastructure

- PKI Standards
- Digital Certificates
- Certificate Authorities
- Types of Certificate
- Implementing PKI
- Storing and Distributing Keys
- Key Status and Revocation
- PKI Trust Models
- PGP / GPG

Unit 3: Identification and Authentication

- Access Control Systems
- Identification
- Authentication
- LAN Manager / NTLM
- Kerberos
- PAP, CHAP, and MS-CHAP
- Password Attacks
- Token-based Authentication
- Biometric Authentication
- Common Access Card.

Unit 4: Identity and Access Services

- Authorization
- Directory Services
- RADIUS and TACACS+
- Federation and Trusts
- Federated Identity Protocols

Unit 5: Account Management

- Formal Access Control Models
- Account Types
- Windows Active Directory
- Creating and Managing Accounts
- Account Policy Enforcement
- Credential Management Policies
- Account Restrictions and Auditing

Lesson 3: Architecture and Design 1

Unit 1: Secure Network Design

- Network Zones and Segments
- Subnetting
- Switching Infrastructure
- Switching Attacks and Hardening
- Endpoint Security
- Network Access Control
- Routing Infrastructure
- Network Address Translation
- Software Defined Networking

Unit 2: Firewalls and Load Balancers

- Basic Firewall
- Stateful Firewalls
- Implementing a Firewall or Gateway
- Web Application Firewalls
- Proxies and Gateways
- Denial of Service Attacks
- Load Balancers

Unit 3: IDS and SIEM

- Intrusion Detection Systems
- Configuring IDS
- Log Review and SIEM
- Data Loss Prevention
- Malware and Intrusion Response

Unit 4: Secure Wireless Access

- Wireless LANs
- WEP and WPA
- Wi-Fi Authentication
- Extensible Authentication Protocol
- Additional Wi-Fi Security Settings
- Wi-Fi Site Security
- Personal Area Networks

Unit 5: Physical Security Controls

- Site Layout and Access
- Gateways and Locks
- Alarm Systems
- Surveillance
- Hardware Security
- Environmental Controls

Lesson 4: Architecture and Design 2

Unit 1: Secure Protocols and Services

- DHCP Security
- DNS Security
- Network Management Protocols
- HTTP and Web Servers
- SSL / TLS and HTTPS
- Web Security Gateways
- Email Services
- S/MIME
- File Transfer

- Voice and Video Services
- Voice over IP (VoIP)

Unit 2: Secure Remote Access

- Remote Access Architecture
- Virtual Private Networks
- IPsec and IKE
- Remote Access Servers
- Remote Administration Tools
- Hardening Remote Access Infrastructure

Unit 3: Secure Systems Design

- Trusted Computing
- Hardware / Firmware Security
- Peripheral Device Security
- Secure Configurations
- OS Hardening
- Patch Management
- Embedded Systems
- Security for Embedded Systems

Unit 4: Secure Mobile Device Services

- Mobile Device Deployments
- Mobile Connection Methods
- Mobile Access Control Systems
- Enforcement and Monitoring

Unit 5: Secure Virtualization and Cloud Services

- Virtualization Technologies
- Virtualization Security Best Practices
- Cloud Computing
- Cloud Security Best Practices

Lesson 5: Risk Management

Unit 1: Forensics

- Forensic Procedures
- Collecting Evidence
- Capturing System Images Associated Exam and Certification:
- Handling and Analysing Evidence

Unit 2: Disaster Recovery and Resiliency

- Continuity of Operations Planning
- Disaster Recovery Planning
- Resiliency Strategies
- Recovery Sites Backup Plans and Policies
- Resiliency and Automation Strategies

Unit 3: Risk Management

- Business Impact Analysis
- Identification of Critical Systems
- Risk Assessment
- Risk Mitigation

Unit 4: Secure Application Development

- Application Vulnerabilities
- Application Exploits
- Web Browser Exploits
- Secure Application Design
- Secure Coding Concepts
- Auditing Applications
- Secure DevOps

Unit 5: Organizational Security

- Corporate Security Policy
- Personnel Management Policies
- Interoperability Agreements
- Data Roles
- Data Sensitivity Labelling and Handling
- Data Wiping and Disposal
- Privacy and Employee Conduct Policies
- Security Policy Training

Associated Exam and Certification

This course will prepare students to take the **CompTIA Security+ SYO-501 exam.**

Successfully passing this exam will result in the attainment of the **CompTIA Security+ certification.**

After completing this course students will receive a Netcampus course attendance certification.

The CompTIA Security+ certification is valid for three (3) years from the day of your successful completion of the exam.

Exams and Certifications

Notes and Annotations

What is Next