CompTIA Security+ (Exam SY0-401)

Course Overview

This course will prepare students to pass the current CompTIA Security+ SY0-401 certification exam. After taking this course, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

Course Introduction 3m
Course Introduction

Lesson 01 - Security Fundamentals 2h 29m
Topic A: The Information Security Cycle
What Is Information Security?
What to Protect
Goals of Security
Risk
Threats
A Vulnerability
Intrusions
Attacks
Controls
Types of Controls
The Security Management Process
Topic B: Information Security Controls
The CIA Triad
Non-repudiation
Identification
Authentication
Authentication Factors
Authorization
Access Control
Access Control Models
Accounting and Auditing
Common Security Practices
Implicit Deny
Least Privilege
Separation of Duties
Job Rotation
Mandatory Vacation
Time of Day Restrictions
Privilege Management

Topic C: Authentication Methods
User Name/Password Authentication
Tokens
Biometrics
Geolocation
Keystroke Authentication
Multi-factor Authentication
Mutual Authentication
Topic D: Cryptography Fundamentals
Cryptography
Encryption and Decryption
Ciphers
Cipher Types
Encryption and Security Goals
Demo - Exploring Public Key Cryptography
Steganography
Demo - Sharing a Secret Message with Steganography
A Key
Hashing Encryption
Hashing Encryption Algorithms
Demo - Calculating Hashes
Symmetric Encryption
Symmetric Encryption Algorithms
Asymmetric Encryption
Asymmetric Encryption Techniques
Key Exchange
Digital Signatures
Cipher Suites
Session Keys
Key Stretching
Topic E: Security Policy Fundamentals
A Security Policy
Security Policy Components
Common Security Policy Types
Group Policy
Security Document Categories
Change Management
Documentation Handling Measures
Lesson 01 Review

Lesson 02 - Identifying Security Threats and Vulnerabilities 2h 38m

Topic A: Social Engineering
Social Engineering Attacks
Social Engineering Effectiveness
Types of Social Engineering
Hackers and Attackers
Categories of Attackers
Topic B: Malware
Malicious Code Attacks
Viruses

Demo - Installing Antivirus Software
Worms
Adware
Spyware
Demo - Scanning Your System for Spyware
Trojan Horses
Rootkits
Logic Bombs
Botnets
Ransomware
Polymorphic Malware
Armored Viruses
Topic C: Software-Based Threats
Software Attacks
Password Attacks
Types of Password Attacks
Backdoor Attacks
Application Attacks
Types of Application Attacks
Demo - Managing Application Security
Topic D: Network-Based Threats
TCP/IP Basics
Port Scanning Attacks
Eavesdropping Attacks
Man-in-the-Middle Attacks
Replay Attacks
Social Network Attacks
DoS Attacks
DDoS Attacks
Types of DoS Attacks
Session Hijacking
P2P Attacks
ARP Poisoning
Transitive Access Attacks
DNS Vulnerabilities
Topic E: Wireless Threats and Vulnerabilities
Wireless Security
Demo - Configuring a Wireless Access Point
Demo - Configuring a Wireless Client
Rogue Access Points
Evil Twins
Jamming
Bluejacking
Bluesnarfing
Near Field Communication
War Driving and War Chalking
IV Attacks
Packet Sniffing
Wireless Replay Attacks
Sinkhole Attacks

WEP and WPA Attacks
WPS Attacks
Topic F: Physical Threats and Vulnerabilities
Physical Security
Physical Security Threats and Vulnerabilities
Hardware Attacks
Environmental Threats and Vulnerabilities
Lesson 02 Review

Lesson 03 - Managing Data, Application, and Host Security 3h 4m
Topic A: Manage Data Security
Layered Security
Defense in Depth
What Is Data Security?
Data Security Vulnerabilities
Data Storage Methods
Data Encryption Methods
Hardware-Based Encryption Devices
Types of Hardware-Based Encryption Devices
Data States
Permissions and Access Control Lists
Handling Big Data
Data Policies
Guidelines for Managing Data Security
Demo - Managing Data Security
Topic B: Manage Application Security
What Is Application Security?
Patch Management
Application Security Methods
Input Validation
Input Validation Vulnerabilities
Client-Side and Server-Side Validation
Error and Exception Handling
XSS
XSRF
Cross-Site Attack Prevention Methods
Fuzzing
Web Browser Security
Demo - Configuring a Web Browser
Guidelines for Establishing Web Browser Security
NoSQL Databases
Database Security
Guidelines for Managing Application Security
Topic C: Manage Device and Host Security
Hardening
Demo - Hardening a Server
Operating System Security
Operating System Security Settings
TCB
Security Baselines

Software Updates
Application Blacklisting and Whitelisting
Logging
Auditing
Demo - Implementing Auditing
Anti-malware Software
Types of Anti-malware Software
Virtualization Security Techniques
Hardware Security Controls
Non-standard Hosts
Security Controls for Non-standard Hosts
Strong Passwords
Guidelines for Establishing Device and Host Security
Topic D: Manage Mobile Security
Mobile Device Types
Mobile Device Vulnerabilities
Mobile Device Security Controls
Mobile Application Security Controls
BYOD Controls
Guidelines for Managing Mobile Security
Lesson 03 Review

Lesson 04 - Implementing Network Security 3h 9m
Topic A: Configure Security Parameters on Network Devices and Technologies
Network Components
Network Devices
Demo - Configuring Firewall Parameters
Network Analysis Tools
IDS
NIDS
Demo - Configuring a Network Intrusion Detection System
Wireless IDS
IPS
NIPS
WIPS
Types of Network Monitoring Systems
VPN
VPN Concentrator
Web Security Gateways
Topic B: Network Design Elements and Components
NAC
DMZ
VLAN
Subnet
NAT
Remote Access
Telephony Components
Virtualization
Cloud Computing
Cloud Computing Deployment Models

Cloud Computing Service Types
Topic C: Implement Networking Protocols and Services
OSI Model
OSI Model and Security
TCP/IP
DNS
HTTP
SSL/TLS
HTTPS
SSH
SNMP
ICMP
IPSec
Demo - Securing Network Traffic Using IP Security
iSCSI
Fibre Channel
FCoE
Telnet
NetBIOS
File Transfer Protocols
Ports and Port Ranges
Demo - Installing an IIS Web Server
Topic D: Apply Secure Network Administration Principles
Rule-Based Management
Network Administration Security Methods
Unified Threat Management
Guidelines for Applying Network Security Administration Principles
Topic E: Secure Wireless Traffic
Wireless Networks
Wireless Antenna Types
802.11 Standards
Wireless Security Protocols
VPNs and Open Wireless
Wireless Security Methods
Captive Portals
Site Surveys
Guidelines for Securing Wireless Traffic
Demo - Securing Wireless Traffic
Lesson 04 Review

Lesson 05 - Implementing Access Control, Authentication, and Account Management 1h 17m
Topic A: Access Control and Authentication Services
Directory Services
LDAP
LDAPS
Common Directory Services
Demo - Backing Up Active Directory
Remote Access Methods
Tunneling
Remote Access Protocols

HOTP
TOTP
PAP
CHAP
Guidelines for Securing Remote Access
PGP
RADIUS
TACACS
Kerberos
SAML
Topic B: Implement Account Management Security Controls
Identity Management
Account Management
Account Privileges
Account Policy
Multiple Accounts
Shared Accounts
Account Federation
Account Management Security Controls
Demo - Account Management Security Controls
Credential Management
Group Policy
Guidelines for Implementing Account Management Security Controls
Lesson 05 Review

Lesson 06 - Managing Certificates 57m
Topic A: Install a CA Hierarchy
Digital Certificates
Certificate Authentication
PKI
PKI Components
CA Hierarchies
The Root CA
Public and Private Roots
Subordinate CAs
Offline Root CAs
CA Hierarchy Design Options
Demo - Installing a Certificate Authority
Topic B: Enroll Certificates
The Certificate Enrollment Process
Demo - Enrolling for Certificates
The Certificate Life Cycle
Certificate Life Cycle Management
Topic C: Secure Network Traffic by Using Certificates
The SSL Enrollment Process
Topic D: Renew Certificates
Certificate Renewal
Topic E: Back Up and Restore Certificates and Private Keys
Private Key Protection Methods
Key Escrow

Private Key Restoration Methods
The Private Key Replacement Process
Topic F: Revoke Certificates
Certificate Revocation
Demo - Revoking Certificates
A CRL
OCSP
Lesson 06 Review

Lesson 07 - Implementing Compliance and Operational Security 50m
Topic A: Physical Security
Physical Security Controls
Physical Security Control Types
Environmental Exposures
Environmental Controls
Environmental Monitoring
Safety
Topic B: Legal Compliance
Compliance Laws and Regulations
Legal Requirements
Types of Legal Requirements
Forensic Requirements
Topic C: Security Awareness and Training
Security Policy Awareness
Role-Based Training
PII
Classification of Information
The Employee Education Process
User Security Responsibilities
Validation of Training Effectiveness
Topic D: Integrate Systems and Data with Third Parties
Business Partners
Social Media Networks and Applications
Interoperability Agreements
Risk Awareness
Data Sharing and Backups
Guidelines for Securely Integrating Systems and Data with Third Parties
Lesson 07 Review

Lesson 08 - Risk Management 50m
Topic A: Risk Analysis
Risk Management
Security Assessment Types
Risk Types
Components of Risk Analysis
Phases of Risk Analysis
Risk Analysis Methods
Risk Calculation
Risk Response Strategies
Risk Mitigation and Control Types

Topic B: Implement Vulnerability Assessment Tools and Techniques
Vulnerability Assessment Techniques
Vulnerability Assessment Tools
Topic C: Scan for Vulnerabilities
The Hacking Process
Ethical Hacking
Vulnerability Scanning and Penetration Testing
Types of Vulnerability Scans
Demo - Scanning for Port Vulnerabilities
Demo - Scanning for Password Vulnerabilities
Box Testing Methods
Security Utilities
Topic D: Mitigation and Deterrent Techniques
Security Posture
DLP
Demo - Capturing Network Data
Detection Controls and Prevention Controls
Risk Mitigation Strategies
Types of Mitigation and Deterrent Techniques
Failsafe, Failsecure, and Failopen
Lesson 08 Review

Lesson 09 - Troubleshooting and Managing Security Incidents 33m
Topic A: Respond to Security Incidents
Security Incident Management
Computer Crime
An IRP
First Responders
Chain of Custody
Computer Forensics
Order of Volatility
Basic Forensic Process
Basic Forensic Response Procedures for IT
Big Data Analysis
Guidelines for Responding to Security Incidents
Topic B: Recover from a Security Incident
Basic Incident Recovery Process
Damage Assessment
Recovery Methods
An Incident Report
Guidelines for Recovering from a Security Incident
Lesson 09 Review

Lesson 10 - Business Continuity and Disaster Recovery Planning 50m
Topic A: Business Continuity
A BCP
BIA
MTD
RPO
RTO

Continuity of Operations Plan
Alternate Sites
IT Contingency Planning
Succession Planning
Business Continuity Testing Methods
Topic B: Plan for Disaster Recovery
A DRP
Fault Tolerance
Redundancy Measures
Demo - Creating a RAID Array Through Software
High Availability
Disaster Recovery Testing and Maintenance
Guidelines for Planning for Disaster Recovery
Topic C: Execute DRPs and Procedures
The Disaster Recovery Process
Recovery Team
Secure Recovery
Backup Types and Recovery Plans
A Backout Contingency Plan
Secure Backups
Backup Storage Locations
Guidelines for Executing DRPs and Procedures
Lesson 10 Review
Course Closure

Total Duration: 16h 39m