CompTIA Security+ (Exam SY0-501)

Course Overview

This course will teach students about identifying security fundamentals and threats, analyzing risk, conducting security assessments, implementing network, operational , host, and software security, managing identity and access, implementing cryptography, addressing security issues, and ensuring business continuity.

Demo - Identifying Basic Authentication and Authorization Concepts
Topic D: Identify Basic Cryptography Concepts
Cryptography
Encryption and Decryption
Encryption and Security Goals
Ciphers
A Key
Symmetric Encryption
Asymmetric Encryption
Hashing
Steganography
Demo - Identifying Basic Cryptography Concepts
Chapter 01 Review

Chapter 02 - Analyzing Risk 46m
Topic A: Analyze Organizational Risk
Risk Management
Components of Risk Analysis
Phases of Risk Analysis
Categories of Threat Types
Risk Analysis Methods
Risk Calculation
Risk Response Techniques
Risk Mitigation and Control Types
Change Management
Guidelines for Analyzing Risk
Demo - Analyzing Risks to the Organization
Topic B: Analyze the Business Impact of Risk
BIA
Impact Scenarios
Privacy Assessments
Critical Systems and Functions
Maximum Tolerable Downtime
Recovery Point Objective
Recovery Time Objective
Mean Time to Failure
Mean Time to Repair
Mean Time Between Failures
Guidelines for Performing a Business Impact Analysis
Demo - Performing a Business Impact Analysis
Chapter 02 Review

Chapter 03 - Identifying Security Threats 2h 49m
Topic A: Identify Types of Attackers
Hackers and Attackers
Threat Actors
Threat Actor Attributes

Open-Source Intelligence
Demo - Identifying Types of Attackers
Topic B: Identify Social Engineering Attacks
Social Engineering
Effectiveness
Impersonation
Phishing and Related Attacks
Hoaxes
Physical Exploits
Watering Hole Attacks
Demo - Identifying Social Engineering Attacks
Topic C: Identify Malware
Malicious Code
Viruses
Worms
Adware
Spyware
Trojan Horses
Keyloggers
Remote Access Trojans
Logic Bombs
Botnets
Ransomware
Advance Persistent Threats
Demo - Identifying Types of Malware
Topic D: Identify Software-Based Threats
Software Attacks
Password Attacks
Types of Password Attacks
Cryptographic Attacks
Types of Cryptographic Attacks
Backdoor Attacks
Application Attacks
Types of Application Attacks
Driver Manipulation
Privilege Escalation
Demo - Identifying Password Attacks
Topic E: Identify Network-Based Threats
TCP/IP Basics
Spoofing Attacks
IP and MAC Address Spoofing
ARP Poisoning
DNS Poisoning
Port Scanning Attacks
Scan Types
Eavesdropping Attacks
Man-in-the-Middle Attacks
Man-in-the-Browser Attacks

Replay Attacks
DoS Attacks
DDoS Attacks
Hijacking Attacks
Amplification Attacks
Pass the Hash Attacks
Demo - Identifying Threats to DNS
Demo - Identifying Port Scanning Threats
Topic F: Identify Wireless Threats
Rogue Access Points
Evil Twins
Jamming
Bluejacking
Bluesnarfing
Near Field Communication Attacks
RFID System Attacks
War Driving, War Walking, and War Chalking
Packet Sniffing
IV Attacks
Wireless Replay Attacks
WEP and WPA Attacks
WPS Attacks
Wireless Disassociation
Demo - Identifying Wireless Threats
Topic G: Identify Physical Threats
Physical Threats and Vulnerabilities
Hardware Attacks
Environmental Threats and Vulnerabilities
Demo - Identifying Physical Threats
Chapter 03 Review

Chapter 04 - Conducting Security Assessments 1h 3m
Topic A: Identify Vulnerabilities
Host Vulnerabilities
Software Vulnerabilities
Encryption Vulnerabilities
Network Architecture Vulnerabilities
Account Vulnerabilities
Operations Vulnerabilities
Demo - Identifying Vulnerabilities
Topic B: Assess Vulnerabilities
Security Assessment
Security Assessment Techniques
Vulnerability Assessment Tools
Types of Vulnerability Scans
False Positives
Guidelines for Assessing Vulnerabilities

Demo - Capturing Network Data with Wireshark
Demo - Scanning for General Vulnerabilities
Topic C: Implement Penetration Testing
Penetration Testing
Penetration Testing Techniques
Box Testing Methods
Penetration Testing Tools
Guidelines for Implementing Penetration Testing
Demo - Implementing Penetration Testing
Chapter 04 Review

Chapter 05 - Implementing Host and Software Security 1h 56m
Topic A: Implement Host Security
Hardening
Operating System Security
Operating System Hardening Techniques
Trusted Computing Base
Hardware and Firmware Security
Security Baselines
Software Updates
Application Blacklisting and Whitelisting
Logging
Auditing
Anti-malware Software
Types of Anti-malware Software
Hardware Peripheral Security
Embedded Systems
Security Implications for Embedded Systems
Guidelines for Securing Hosts
Demo - Implementing Auditing
Demo - Hardening a Server
Topic B: Implement Cloud and Virtualization Security
Virtualization
Hypervisors
Virtual Desktop Infrastructure
Virtualization Security
Cloud Computing
Cloud Deployment Models
Cloud Service Types
Guidelines for Securing Virtualized and Cloud-Based Resources
Demo - Securing Virtual Machine Networking
Topic C: Implement Mobile Device Security
Mobile Device Connection Methods
Mobile Device Management
Mobile Device Security Controls
Mobile Device Monitoring and Enforcement
Mobile Deployment Models

BYOD Security Controls
Guidelines for Implementing Mobile Device Security
Demo - Implementing Mobile Device Security
Topic D: Incorporate Security in the Software Development Lifecycle
Software Development Lifecycle
Software Development Models
DevOps
Versioning
Secure Coding Techniques
Code Testing Methods
Guidelines for Incorporating Security in the Software Development Lifecycle
Demo - Performing Static Code Analysis
Chapter 05 Review

Chapter 06 - Implementing Network Security 2h 15m
Topic A: Configure Network Security Technologies
Network Components
Network Devices
Routers
Switches
Proxies
Firewalls
Load Balancer
Network Scanners and Analysis Tools
Intrusion Detection Systems
Network IDS
Intrusion Prevention Systems
Network IPS
Types of Network Monitoring Systems
Security Information and Event Management
Data Loss/Leak Prevention
Virtual Private Networks
VPN Concentrators
Security Gateways
Unified Threat Management
Guidelines for Configuring Network Security Technologies
Demo - Configuring a Network IDS
Topic B: Secure Network Design Elements
Network Access Control
Demilitarized Zones
Network Isolation
Virtual Local Area Networks
Network Security Device Placement
Network Address Translation
Software-Defined Networking
Guidelines for Securing Network Design Elements
Demo - Securing Network Design Elements

Topic C: Implement Secure Networking Protocols and Services
The Open Systems Interconnection Model
OSI Model and Security
Internet Protocol Suite
Domain Name System
Hypertext Transfer Protocol
Secure Sockets Layer/Transport Layer Security
HTTP Secure
Secure Shell
Simple Network Management Protocol
Real-Time Transport Protocol
Internet Control Message Protocol
Internet Protocol Security
Network Basic Input/Output System
File Transfer Protocols
Email Protocols
Additional Networking Protocols and Services
Ports and Port Ranges
Demo - Installing an Internet Information Services Web Server with Basic Security
Demo - Securing Network Traffic Using IPSec
Topic D: Secure Wireless Traffic
Wireless Networks
Wireless Antenna Types
802.11 Protocols
Wireless Cryptographic Protocols
Wireless Authentication Protocols
VPNs and Open Wireless
Wireless Client Authentication Methods
Wireless Access Point Security
Captive Portals
Site Surveys
Guidelines for Securing Wireless Traffic
Demo - Securing Wireless Traffic
Chapter 06 Review

Chapter 07 - Managing Identity and Access 1h 42m
Topic A: Implement Identity and Access Management
Identity and Access Management
Access Control Models
Physical Access Control Devices
Biometric Devices
Certificate-Based Authentication
File System and Database Access
Guidelines for Implementing IAM
Demo - Implementing DAC for a File Share
Topic B: Configure Directory Services
Directory Services

Lightweight Directory Access Protocol
Secure LDAP
Common Directory Services
Demo - Backing Up Active Directory
Topic C: Configure Access Services
Remote Access Methods
Tunneling
Remote Access Protocols
HMAC-Based One-Time Password
Time-Based OTP
Password Authentication Protocol
Challenge-Handshake Authentication Protocol
NT LAN Manager
Authentication, Authorization, and Accounting
Remote Authentication Dial-In User Service
Terminal Access Controller Access-Control System
Kerberos
Demo - Configuring a Remote Access Server
Demo - Setting Up Remote Access Authentication
Topic D: Manage Accounts
Account Management
Account Privileges
Account Types
Account Policy
Password Policy
Multiple Accounts
Shared Accounts
Account Management Security Controls
Credential Management
Group Policy
Identity Federation
Identity Federation Methods
Guidelines for Managing Accounts
Demo - Managing Accounts
Chapter 07 Review

Chapter 08 - Implementing Cryptography 1h 41m
Topic A: Identify Advanced Cryptography Concepts
Cryptography Elements
Hashing Concepts
Data States
Key Exchange
Digital Signatures
Cipher Suites
Session Keys
Key Stretching
Special Considerations for Cryptography

Chapter 09 - Implementing Operational Security 1h 25m

Topic A: Evaluate Security Frameworks and Guidelines
Security Frameworks
Security Framework Examples
Security Configuration Guides
Compliance
Layered Security
Defense in Depth
Demo - Evaluating Security Frameworks and Guidelines
Topic B: Incorporate Documentation in Operational Security
Security Policies
Common Security Policy Types
Personnel Management
Separation of Duties
Job Rotation
Mandatory Vacation
Additional Personnel Management Tasks
Training and Awareness
Business Agreements
Guidelines for Incorporating Documentation in Operational Security
Demo - Incorporating Documentation in Operational Security
Topic C: Implement Security Strategies
Security Automation
Scalability
Elasticity
Redundancy
Fault Tolerance
Redundant Array of Independent Disks
Non-persistence
High Availability
Deployment Environments
Guidelines for Implementing Security Strategies
Demo - Implementing Virtual Machine Snapshots
Topic D: Manage Data Security Processes
Data Security
Data Security Vulnerabilities
Data Storage Methods
Data Encryption Methods
Data Sensitivity
Data Management Roles
Data Retention
Data Disposal
Guidelines for Managing Data Security
Demo - Destroying Data Securely
Demo - Encrypting a Storage Device
Topic E: Implement Physical Controls
Physical Security Controls

Physical Security Control Types
Environmental Exposures
Environmental Controls
Environmental Monitoring
Safety
Guidelines for Implementing Physical Controls
Demo - Implementing Physical Controls
Chapter 09 Review

Chapter 10 - Addressing Security Issues 45m

Topic A: Troubleshoot Common Security Issues
Access Control Issues
Encryption Issues
Data Exfiltration
Anomalies in Event Logs
Security Configuration Issues
Baseline Deviations
Software Issues
Personnel Issues
Asset Management Issues
Demo - Identifying Event Log Anomalies
Topic B: Respond to Security Incidents
Incident Response
Incident Preparation
Incident Detection and Analysis
Incident Containment
Incident Eradication
Incident Recovery
Lessons Learned
Incident Response Plans
First Responders
An Incident Report
Guidelines for Responding to Security Incidents
Demo - Responding to a Security Incident
Topic C: Investigate Security Incidents
Computer Forensics
The Basic Forensic Process
Preservation of Forensic Data
Basic Forensic Response Procedures
Order of Volatility
Chain of Custody
Guidelines for Investigating Security Incidents
Demo - Implementing Forensic Procedures
Chapter 10 Review

Chapter 11 - Ensuring Business Continuity 33m

Topic A: Select Business Continuity and Disaster Recovery Processes
Business Continuity and Disaster Recovery
The Disaster Recovery Process
Recovery Team
Order of Restoration
Recovery Sites
Secure Recovery
Backup Types (Full)
Backup Types (Differential vs. Incremental)
Secure Backups
Geographic Considerations
Guidelines for Selecting Business Continuity and Disaster Recovery Processes
Demo - Selecting Business Continuity and Disaster Recovery Processes
Topic B: Develop a Business Continuity Plan
Business Continuity Plans
Disaster Recovery Plans
IT Contingency Plans
Succession Plans
Failover
Alternate Business Practices
Testing Exercises
After-Action Reports
Guidelines for Developing a BCP
Demo - Developing a BCP
Chapter 11 Review
Course Closure

Total Duration: 16h 19m