CompTIA Security+ (SY0-601)

Course Overview

This course will prepare students for the CompTIA Security+ SY0-601 exam. Topics covered include understanding threats, analyzing attacks, cryptography, implementing secure networks, operational procedures, forensics, and more.

Chapter 2 - Analyzing Attacks 1h

Analyzing Attacks
Topic A: Security Assessment Tools and Techniques
Understanding Assessments
Threat Hunting
Vulnerability Scanning
Syslog and SIEM
SIEM Components
Topic B: Application Attacks
Application Attacks
Privilege Escalation
Cross-Site Scripting
Injections
Application Attack Issues
Session Attacks
Additional Attacks
Topic C: Network Attacks
Introduction to Network Attacks
Wireless Network Attacks
Layer 2 Attacks
Service Attacks
Demo - DNS Poisoning
Malicious Code
Topic D: Penetration Testing
Penetration Testing
Environment Types
Pentesting Concepts
Network Reconnaissance
Exercise Types
Chapter 2 Review

Chapter 3 - Architecture and Design 1h 28m

Architecture and Design
Topic A: Enterprise Security Architecture
Enterprise Standardization Needs
Configuration Management
Data Protection
Additional Security Concepts
Disaster Recovery
Deception and Disruption
Topic B: Designing Authentication and Authorization
Authentication and Authorization
Authentication Methods
Authentication Technologies
Biometrics
Multifactor Authentication
Demo - Multifactor Authentication
Topic C: Designing Resiliency
Resiliency and Cybersecurity
Redundancy Concepts

Replication Concepts
Backup Concepts
Additional Resiliency Options
Topic D: Cloud and Virtualization Concepts
Cloud Models
Cloud Types
Cloud Service Providers
Additional Cloud Concepts
Additional Cloud Concepts (cont.)
Demo - Cloud Computing Security
Topic E: Securing Application Development and Deployment
Application Development Environments
Secure Coding Techniques
Automation Techniques
Application Design Concepts
Chapter 3 Review

Chapter 4 - Physical and System Security 29m
Physical and System Security
Topic A: Physical Security Controls
Importance of Physical Controls
Standard Controls
Security Monitoring
Security Personnel
Secure Areas
Secure Data Destruction
Demo - Data Destruction Software
Topic B: Securing Embedded and Specialized Systems
Embedded Systems
Specialized Systems
Additional System Types
Communication Considerations
Constraints
Chapter 4 Review

Chapter 5 – Cryptography 57m
Cryptography
Topic A: Cryptographic Concepts
Introduction to Cryptography
Common Use Cases
Integrity Verification
Understanding Keys
Crypto Limitations
Quantum
Additional Cryptographic Types
Topic B: Public Key Infrastructures
Introduction to PKIs
Certificate Authorities
Certificates
Certificate Verification

Certificate Formats
Demo - Implementing PKI
Additional Concepts
Chapter 5 Review

Chapter 6 - Implementing Secure Networks 1h 41m
Implementing Secure Networks
Topic A: Implement Secure Protocols
Network Protocols
Use Cases
Application Layer Protocols
IP Security
Topic B: Implement Secure Network Designs
Network Segmentation
High Availability
Virtual Private Networks
Secure Network Appliances
Firewalls
Demo - Configuring a Host-Based Firewall
Additional Network Security Concepts
Topic C: Implementing Security in the Cloud
Cloud Security Controls
Cloud Storage Security
Cloud Network Security
Compute Security
Additional Cloud Solutions
Topic D: Implement Wireless Security
Cryptographic Protocols
Authentication Protocols
Authentication Methods
Installation Considerations
Topic E: Implement Secure Mobile Solutions
Deployment Models
Connection Methods and Receivers
Mobile Device Management (MDM)
Mobile Devices
Enforcement and Monitoring
Additional Controls
Chapter 6 Review

Chapter 7 - Implementing Secure Hosts and Identities 1h
Implementing Secure Hosts and Identities
Topic A: Implement Authentication and Authorization Systems
Understanding Identity
Access Control Methods
Demo - Role-Based Access Control
Authentication Management
Remote Access Authentication
Authentication and Authorization Protocols
Topic B: Implement Identity and Account Management Controls

Account Types
Account Policies
Demo - Configuring Account Policies
Additional Identity Terms
Topic C: Implement Host and Application Security Solutions
Endpoint Protection
Client Level Protections
Network Level Protections
Boot Integrity
Database Security
System Hardening
Application Security
Chapter 7 Review

Chapter 8 - Operational Procedures 55m
Operational Procedures
Topic A: Using Tools to Assess Security
Network Reconnaissance and Discovery
Network Tools
Network Tools (cont.)
Demo - Using Network Tools
File Manipulation Tools
Packet Capture and Relay
Shell and Script Environments
Forensics Tools
Topic B: Utilizing Data Sources for Investigation
Vulnerability Scan Output
SIEM Dashboards
Log Files
Additional Monitoring
Topic C: Applying Mitigation Techniques
Reconfiguring Endpoint Solutions
Configuration Changes
Additional Mitigation Techniques
Chapter 8 Review

Chapter 9 - Incident Response and Forensics 38m
Incident Response and Forensics
Topic A: Incident Response Policies and Procedures
Incident Response Plans
Incident Response Process
Exercises
Attack Frameworks
Additional Plans
Demo - Examining IRPs
Topic B: Understanding Digital Forensics
Introduction to Forensics
Evidence Categories
Documentation and Evidence
Acquisition Concepts

Integrity
Additional Concepts
Chapter 9 Review

Chapter 10 - Governance, Risk, and Compliance 1h 9m
Governance, Risk, and Compliance
Topic A: Introduction to Control Types
Security Controls
Control Categories
Control Types
Topic B: Understanding Governance
Introduction to Governance
Regulations and Standards
Key Frameworks
Benchmarks
Demo - Data Loss Prevention (DLP)
Topic C: Implementing Security Policies
Personnel-Based Policies
Personnel-Based Policies (cont.)
Third-Party Risk Management
Data
Credential Policies
Topic D: Implementing Risk Management
Risk Types
Risk Management Strategies
Risk Analysis
Risk Analysis (cont.)
Disasters
Business Impact Analysis
Topic E: Compliance with Privacy and Sensitive Data
Organizational Consequences
Data Types
Privacy Enhancing Technologies
Roles and Responsibilities
Chapter 10 Review
Course Closure

Total Duration: 10h 45m