CompTIA Security+ Certification Exam SY0-301

Course Introduction 4m

Course Introduction

Unit 01 - Mitigating Threats 2h 32m

Topic A: System Maintenance

Causes of Compromised Security
Technology Weaknesses
Configuration Weaknesses
Policy Weaknesses
Human Error and Malice
Securing the Operating System
Microsoft Update
Windows Update Categories
Demo - A-2: Updating the Operating System
Patch Management
Demo - A-3: Managing Software Patches
Service Packs
Demo - A-4: Checking for and Installing Service Packs
BIOS Version
BIOS Update
Demo - A-5: Determining Whether you Need to Update your Computer's BIOS
Windows Firewall
User Account Control
Demo - A-6: Configuring Windows Firewall

Topic B: Application Security

Application Vulnerabilities
Countermeasures
Demo - B-1: Managing Application Security

Topic C: Physical Security

Physical Access Control
Smart Card and Reader
Fingerprint Scanner
Biometric Devices
Plant Security
Cipher Lock
Man-trap

Topic D: Malware

Malware Varieties
Malware Effects
Anti-malware
Antivirus Software
Anti-malware Products
Demo - D-2: Installing Antivirus Software
Windows Defender
Demo - D-3: Scanning your System for Spyware

Topic E: Social Engineering

Social Engineering
Types of Social Engineering
Social Engineering Countermeasures
Phishing

Demo - E-2: Examining Phishing
Spam
Social Networking
Unit 01 Review

Unit 02 - Cryptography 1h 24m

Topic A: Symmetric Cryptography
Cryptography
Alice, Bob, and Eve
ROT13 Cipher
Keys
Symmetric Encryption in Action
Common Symmetric Ciphers
Hashes
Uses for Hashes
MD5 Hash Algorithm
SHA
Hash Vulnerabilities
Demo - A-2: Calculating Hashes
Steganography
Demo - A-3: Sharing a Secret Message with Steganography
Topic B: Public Key Cryptography
Public Key Cryptography
Asymmetric Encryption in Action
Common Asymmetric Ciphers
Demo - B-1: Exploring Public Key Cryptography
Digital Signatures
Signature Process
Features of Signatures
Digital Certificates
Certificate Types
Demo - B-2: Examining Certificates
Public Key Infrastructure
Certificate Policy
Certificate Practice Statement
Trust Models
Single-authority Trust Model
Hierarchical Trust Model
Web of Trust Model
Demo - B-3: Examining Certificate Trusts
Single- and Dual-key Certificates
Quantum Cryptography
Unit 02 Review

Unit 03 - Authentication 1h 32m

Topic A: Authentication Factors and Requirements
Three Steps to Secure Resources
Authentication Factors
One-factor Authentication
Two-factor Authentication
Three-factor Authentication
Considerations
Identification and Authentication
Identity Proofing
Single Sign-on
Topic B: Authentication Systems

Authentication Protocols
NTLM
NTLM Challenge-response
NTLM Vulnerabilities
Kerberos
Kerberos System Composed of:
Kerberos Data Types:
Kerberos Authentication Process
Cross-realm Authentication
Kerberos Security Weaknesses
Null Sessions
Topic C: Authentication System Vulnerabilities
Authentication Vulnerabilities
Secure Passwords
Password Realities
Least Privilege
Demo - C-1: Identifying Authentication Vulnerabilities
Wireshark
Demo - C-2: Capturing Passwords with a Protocol Analyzer
Password Cracking
Password Guessing
SAM and SYSTEM Files
Demo - C-3: Cracking Passwords
Unit 03 Review

Unit 04 - User- and Role-based Security **1h 2m**

Topic A: Baseline Security Policies
Security Baselines
Demo - A-1: Using MBSA to Analyze Security
Group Policy Settings
Local GPO Types
GPO Editor
Local Computer GPO Nodes
Demo - A-2: Creating a Console to Manage Local Security Policies
Policy Properties Dialog Box
Container Types
Types of Domain GPOs
GPOs Applied in this Order
Demo - A-3: Using the GPMC
Topic B: Resource Access
Groups
Demo - B-1: Creating Users and Groups Based on Security Needs
Permissions
File System Security
Access Control Models
Demo - B-2: Securing File Resources
Unit 04 Review

Unit 05 - Peripheral Security **1h 1m**

Topic A: File and Disk Encryption
File and Disk Encryption
File-level Encryption
Demo - A-1: Enabling File-based Encryption
Whole Disk Encryption
Windows BitLocker
BitLocker Life Cycle

Recovery
Other Disk Encryption Tools
Demo - A-2: Creating an Encrypted Volume
Demo - A-3: Mounting, Using, and Dismounting an Encrypted Volume

Topic B: Peripheral and Component Security

Peripherals and Components
USB Drives
Laptops
Shredding Standards
Demo - B-2: Using Windows Policies to Mitigate the Risks of Peripherals

Topic C: Mobile Device Security

Mobile Device Risks
Additional Concerns
Mitigating Risks
Screen Lock
Android Security Settings
WaveSecure
Risks and Threats
Unit 05 Review

Unit 06 - Public Key Infrastructure 1h 12m

Topic A: Public Key Cryptography

Management
Setup and Initialization Phase
Administration Phase
Cancellation and Key History
Administrative Responsibilities

Topic B: Implementing Public Key Infrastructure

Microsoft Certificate Services
AD Integration Options
CA Role
Demo - B-1: Installing a Standalone Root Certificate Authority
Demo - B-2: Installing an Enterprise Subordinate CA
Demo - B-3: Implementing a File-based Certificate Request
Demo - B-4: Managing your Certificate Server
User Certificates
Demo - B-5: Requesting a User Certificate
Certificate Revocation
Demo - B-6: Revoking a Certificate
Key Escrow and Recovery
Key Recovery Agent
Demo - B-7: Enabling the EFS Recovery Agent Template
Demo - B-8: Enrolling for a Recovery Agent Certificate
Demo - B-9: Enabling Key Archival
Demo - B-10: Re-enrolling All Certificates

Topic C: Web Server Security with PKI

Securing Web Servers
Commercial Certificate
Demo - C-1: Requesting and Installing a Web Server Certificate
Demo - C-2: Enabling SSL for the Certificate Server Website
HTTPS Connections
Demo - C-3: Making a Secure Connection
Demo - C-4: Requesting a Client Certificate via the Web
Unit 06 Review

Unit 07 - Application and Messaging Security 1h 11m

Topic A: Application Security

Application Security
Programmer’s Perspective
Administrator’s Perspective
User’s Perspective
Application Attacks

Topic B: E-mail Security

E-mail Security
E-mail Application Security
Demo - B-2: Configuring an E-mail Client to Use Secure Authentication
Signed and Encrypted Mail
PGP
PGP Certificates
S/MIME
X.509 Certificates
PGP vs. S/MIME
Demo - B-3: Examining S/MIME Features
Using PGP
Demo - B-4: Installing Gnu Privacy Guard and Enigmail
Demo - B-5: Creating an OpenPGP Certificate and Key Pair
Signed Message
Demo - B-6: Sending a Signed Message

Topic C: Social Networking and Messaging

Social Networking
Instant Messaging
IM Ports
Unit 07 Review

Unit 08 - Ports and Protocols 1h 51m

Topic A: TCP/IP Basics

TCP/IP Architecture
Application-layer Protocols
HTTP
HTTPS Connections
FTP
Trivial File Transfer Protocol
SFTP
Telnet
DNS
Additional Protocols
Transport-layer Protocols
Port Numbers
Service Port Numbers
Demo - A-3: Using Port Numbers
IPv4 Classes
IPv4 Header
CIDR and NAT
IPv6 Header
IPv6 Scopes
IPv6 Address Types
Demo - A-4: Comparing IPv4 and IPv6 Packets

Topic B: Protocol-based Attacks

DoS Attacks
TCP Three-way Handshake
Smurf Attack

Ping-of-Death Attacks
Xmas Attacks
Demo - B-1: Preventing Common Protocol-based Attacks
DDoS Attacks
DDoS Attack Protection
Demo - B-2: Assessing your Vulnerability to DDoS Attacks
Man-in-the-Middle Attacks
Spoofing
IP Address Spoofing
Demo - B-3: Scanning Ports
ARP Poisoning
Demo - B-4: Checking the ARP Cache
Spoofing Attacks
Replay Attacks
TCP/IP Hijacking
Unit 08 Review

Unit 09 - Network Security 2h 2m

Topic A: Network Devices
OSI Reference Model
Networking Devices
Repeaters, Hubs, Switches
Switch Security
Routers
Router State Management
NAT and PAT
Port Address Translation
Firewalls and Proxies
Firewall Categories
Security Issues
Overcoming Weaknesses
Topic B: Secure Network Topologies
Security Zones
Intranet Zone
Perimeter Network
DMZ Options
Screened Host
Bastion Host
Three-homed Firewall
Back-to-back Firewalls
Dead Zone
Traffic Filtering
Network Bridging
VLAN
Network Access Control
VPN
IPSec Encryption
Topic C: Secure Networking
Firewall Administration
Rule Planning
Demo - C-1: Configuring Firewall Rules
Port Security
Demo - C-2: Blocking Ports with the Windows Firewall
VLAN Security
Secure Router Configuration
Topic D: Virtualization and Cloud Computing

Virtual Computers
Citrix XenServer
Virtualization Concerns and Risks
Cloud Computing
Cloud Deployment
Cloud Categories
Risks and Concerns
Unit 09 Review

Unit 10 - Wireless Security 57m

Topic A: Wireless Network Security
802.11 Standard
802.11 Family
802.11 Networking
Wireless Security Threats
Wireless Security
Transmission Encryption
Configuration Options
Demo - A-2: Configuring a Wireless Access Point
Configuring Wireless Clients
RADIUS
Demo - A-3: Configuring a Wireless Client
Wireless Network Vulnerabilities
Wi-Fi Scanners
War Chalking Symbols
Topic B: Mobile Device Security
Mobile Device Security
Infrastructure Issues
Protecting Against Attacks
Unit 10 Review

Unit 11 - Remote Access Security 1h 1m

Topic A: Remote Access
AAA
RADIUS
RADIUS Authentication
Realms
RADIUS Security
RADIUS Benefits
LDAP and Remote Access
LDAP Security
LDAP Authentication/Authorization
TACACS+
TACACS+ versus RADIUS
802.1X
Network Policy Server (NPS)
Demo - A-5: Installing Network Policy and Access Services
Demo - A-6: Configuring an NPS Network Policy
Demo - A-7: Configuring NPS Accounting
Topic B: Virtual Private Networks
Virtual Private Networks
VPN Technologies
VPN Security Models
VPN Protocols
PPTP versus L2TP
IPSec Protocols

Encryption Modes
Secure Shell (SSH)
VPN Solutions
Service Provider Tunneling
Demo - B-2: Installing Routing and Remote Access Services
Demo - B-3: Enabling a VPN
Demo - B-4: Configuring NPS to Provide RADIUS Authentication for your VPN
Unit 11 Review

Unit 12 - Vulnerability Testing and Monitoring 58m

Topic A: Risk and Vulnerability Assessment
Assessment Types
Vulnerability Assessments
Vulnerability Testing Tools
Penetration Testing
Penetration vs. Vulnerability
Demo - A-2: Scanning the Network
Topic B: Auditing and Logging
Event Viewer
Windows Server 2008 Event Viewer
Events
Event Types
Event Details
Demo - B-1: Viewing Event Logs
Device and Application Logging
Topic C: Intrusion Detection and Prevention Systems
Intrusion Detection
Events
NIDS
IDScenter for Snort
Example Snort Rule
HIDS
HIDS Advantages Over NIDS
Honeypots and Honeynets
Honeypot Examples
Honeypot Deployment
Topic D: Incident Response
Computer Forensics
Evidence-Gathering Principles
Chain of Custody
Remediation
Unit 12 Review

Unit 13 - Organizational Security 49m

Topic A: Organizational Policies
CIA Triad
Control Types
Risk Assessment
Security Policy Contents
Acceptable-Use Policy
Due Care
Privacy
Separation of Duties
Need to Know
Password Management
Service-level Agreement

Disposal and Destruction
Human Resources Policies
Incident Response Policy
Incident Response Policy Contents
Preparation
Detection
Containment
Eradication
Recovery
Follow-up
Hiring
Employee Review and Maintenance
Post-employment
Code of Ethics
Change Management
Change Documentation

Topic B: Education and Training

Education
Communication
User Awareness
Types of Training

Topic C: Disposal and Destruction

Disposal
Data Security and Destruction
Disposal of Electronics
Disposal of Computer Equipment
Unit 13 Review

Unit 14 - Business Continuity 1h 8m

Topic A: Business Continuity Planning

Business Impact Assessment
Threats
Business Continuity Teams
Contingency Plan
Documentation
Disaster or Service Failure
Utility Services
Redundant Locations
Disaster Recovery Exercises

Topic B: Disaster Recovery

Fault Tolerance
RAID Level 0
RAID Level 1
RAID Level 3
RAID Level 5
RAID 0+1 (or RAID 01)
RAID 1+0 (or RAID 10)
RAID Considerations
Level-specific Considerations
Software vs. Hardware RAID
Backup Tools
Backup Types
Backup Media
Backup Storage
Grandfather Method
Tower of Hanoi

Incremented Media Backup
Backup Storage (Cont.)
Data Restoration
Demo - B-4: RAID Configuration (Software)
Topic C: Environmental Controls
Fire Suppression Systems
Fire Extinguisher Classes
Fire Extinguisher Contents
Extinguisher Label
Safety Guidelines
HVAC
Shielding
Unit 14 Review
Course Closure

Total Duration: 18hrs 45m