

CompTIA Security+ Certification, 2008 Edition + CertBlaster

ISBN-10: 1-4260-0596-2

Duration: Five days

Description:

This ILT Series course, rated 4.9/5.0 in overall quality by ProCert Labs, will prepare students to pass the current CompTIA Security+ 2008 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. Comes with CertBlaster exam prep software (download).

Prerequisites: *CompTIA A+ Certification* and *CompTIA Network+ Certification* or equivalent experience

Topic-Level Outline

Unit 1 : Mitigating threats

*Topic A: * Core system maintenance*

- A-1: Identifying common security threats
- A-2: Updating the operating system
- A-3: Managing software patches
- A-4: Installing service packs
- A-5: Determining whether you need to update your computer's BIOS
- A-6: Configuring Windows Firewall

*Topic B: * Virus and spyware management*

- B-1: Installing antivirus software
- B-2: Scanning your system for spyware
- B-3: Configuring Windows Mail to prevent spam

*Topic C: * Browser security*

- C-1: Managing pop-ups
- C-2: Managing cookies
- C-3: Managing scripting, Java, and ActiveX components
- C-4: Examining input validation, buffer overflows, and XSS

*Topic D: * Social engineering threats*

- D-1: Discussing social engineering
- D-2: Examining phishing

Unit 2 : Cryptography

*Topic A: * Symmetric cryptography*

- A-1: Encrypting and decrypting data
- A-2: Calculating hashes
- A-3: Sharing a secret message with steganography

*Topic B: * Public key cryptography*

- B-1: Exploring public key cryptography
- B-2: Examining certificates
- B-3: Examining certificate trusts
- B-4: Comparing single- and dual-sided certificates
- B-5: Mapping algorithms to applications

Unit 3 : Authentication systems

*Topic A: * Authentication*

- A-1: Identifying the components of authentication
- A-2: Comparing one, two, and three-factor authentication
- A-3: Capturing passwords with a protocol analyzer
- A-4: Installing Active Directory Services
- A-5: Joining a domain

*Topic B: * Hashing*

- B-1: Hashing data
- B-2: Cracking passwords

*Topic C: * Authentication systems*

- C-1: Identifying the requirements of a secure authentication system
- C-2: Examining the components of Kerberos
- C-3: Examining null sessions
- C-4: Comparing authentication systems

Unit 4 : Messaging security

*Topic A: * E-mail security*

- A-1: Identifying the security risks of an e-mail system
- A-2: Configuring security on an e-mail server
- A-3: Digitally signing a message
- A-4: Sending an encrypted message

*Topic B: * Messaging and peer-to-peer security*

- B-1: Identifying the security risks of messaging systems
- B-2: Configuring security on an IM server
- B-3: Configuring IM client security

Unit 5 : User and role based security

*Topic A: * Security policies*

- A-1: Creating a console to manage local security policies
- A-2: Using the GPMC
- A-3: Implementing domain GPOs
- A-4: Analyzing a Windows Vista computer's security

*Topic B: * Securing file and print resources*

- B-1: Creating users and groups based on security needs
- B-2: Securing file resources
- B-3: Securing printer resources

Unit 6 : Public key infrastructure

*Topic A: * Key management and life cycle*

- A-1: Understanding certificate life cycle and management

*Topic B: * Setting up a certificate server*

- B-1: Installing a standalone root certificate authority
- B-2: Installing an enterprise subordinate CA
- B-3: Implementing a file-based certificate request
- B-4: Managing your certificate server
- B-5: Side trip: granting the log on locally right
- B-6: Requesting a user certificate
- B-7: Revoking a certificate
- B-8: Enabling the EFS recovery agent template
- B-9: Enrolling for a recovery agent certificate

B-10: Enabling key archival

B-11: Re-enrolling all certificates

*Topic C: * Web server security with PKI*

- C-1: Requesting and installing a Web server certificate
- C-2: Enabling SSL for the certificate server Web site
- C-3: Making a secure connection
- C-4: Requesting a client certificate via the Web

Unit 7 : Access security

*Topic A: * Biometric systems*

- A-1: Identifying biometric authentication systems
- A-2: Installing a fingerprint reader

*Topic B: * Physical access security*

- B-1: Identifying the risks associated with physical access to systems
- B-2: Examining logging and surveillance best practices

*Topic C: * Peripheral and component security*

- C-1: Identifying the risks associated with common peripherals
- C-2: Mitigating security risks of peripherals

*Topic D: * Storage device security*

- D-1: Enabling file-based encryption
- D-2: Enabling whole disk encryption systems (optional)

Unit 8 : Ports and protocols

*Topic A: * TCP/IP review*

- A-1: Examining protocols in the TCP/IP suite
- A-2: Comparing IPv4 and IPv6 packets

*Topic B: * Protocol-based attacks*

- B-1: Preventing common protocol-based attacks
- B-2: Assessing your vulnerability to DDoS attacks
- B-3: Port scanning
- B-4: Checking ARP cache
- B-5: Examining spoofing attacks
- B-6: Examining replay and hijacking attacks
- B-7: Examining antiquated protocols

Unit 9 : Network security

*Topic A: * Common network devices*

- A-1: Examining switches and bridges
- A-2: Examining routers
- A-3: Examining NAT/PAT devices
- A-4: Examining firewalls and proxy servers
- A-5: Identifying inherent weaknesses in network devices
- A-6: Examining the ways to overcome device threats

*Topic B: * Secure network topologies*

- B-1: Comparing firewall-based secure topologies
- B-2: Identifying the benefits of NAC
- B-3: Examining the security enabled by VPNs

*Topic C: * Browser-related network security*

- C-1: Configuring the Phishing Filter
- C-2: Setting security zones
- C-3: Setting privacy options

*Topic D: * Virtualization*

- D-1: Exploring the benefits of virtualization technologies

Unit 10 : Wireless security

*Topic A: * Wi-Fi network security*

- A-1: Identifying wireless networking vulnerabilities
- A-2: Scanning for insecure access points
- A-3: Installing third-party router firmware
- A-4: Configuring basic router security
- A-5: Enabling transmission encryption

*Topic B: * Non-PC wireless devices*

- B-1: Identifying cell phone and PDA related threats

Unit 11 : Remote access security

*Topic A: * Remote access*

- A-1: Examining RADIUS and Diameter authentication
- A-2: Examining the role of LDAP in a remote access environment
- A-3: Examining TACACS+ authentication
- A-4: Examining how 802.1x adds security to your network
- A-5: Installing Network Policy and Access Services
- A-6: Configuring an NPS network policy
- A-7: Configuring NPS accounting

*Topic B: * Virtual private networks*

- B-1: Comparing VPN protocols
- B-2: Installing Routing and Remote Access Services
- B-3: Enabling a VPN
- B-4: Configuring NPS to provide RADIUS authentication for your VPN
- B-5: Making a VPN connection

Unit 12 : Auditing, logging, and monitoring

*Topic A: * System logging*

- A-1: Viewing event logs
- A-2: Discussing device and application logging

*Topic B: * Server monitoring*

- B-1: Monitoring with Performance Monitor
- B-2: Running a Data Collector Set
- B-3: Viewing a Data Collector Set report
- B-4: Considering auditing policies and practices

Unit 13 : Vulnerability testing

*Topic A: * Risk and vulnerability assessment*

- A-1: Analyzing risks
- A-2: Installing the MBSA
- A-3: Analyzing your system with the MBSA
- A-4: Downloading and installing OVAL
- A-5: Downloading an OVAL XML file
- A-6: Scanning with OVAL
- A-7: Downloading and installing Nessus

A-8: Scanning with Nessus

*Topic B: * IDS and IPS*

B-1: Discussing IDS characteristics

B-2: Installing and monitoring with the Snort IDS

B-3: Comparing HIDS and NIDS

B-4: Examining the role and use of honeypots

*Topic C: * Forensics*

C-1: Examining the forensics process

Unit 14 : Organizational security

*Topic A: * Organizational policies*

A-1: Creating a security policy

A-2: Creating a human resources policy

A-3: Creating an incidence response and reporting policy

A-4: Implementing change management

*Topic B: * Education and training*

B-1: Identifying the need for user education and training

B-2: Identifying education opportunities and methods

*Topic C: * Disposal and destruction*

C-1: Deciding whether to destroy or dispose of IT equipment

Unit 15 : Business continuity

*Topic A: * Redundancy planning*

A-1: Identifying the need for and appropriate use of redundancy

A-2: Creating a disaster recovery plan

*Topic B: * Backups*

B-1: Selecting backup schemes

B-2: Backing up data

B-3: Restoring data

B-4: Identifying appropriate media rotation and storage plans

*Topic C: * Environmental controls*

C-1: Examining environmental controls

Appendix A : CompTIA Security+ objectives map

*Topic A: * Objective map*

Appendix B : CompTIA Security+ acronyms

*Topic A: * Acronym list*