CompTIA Security+ (2011 Objectives)

Course Summary

Description

Students will implement and monitor security on networks, applications, and operating systems, and respond to security breaches.

Objectives
At the end of this course, students will be able to:

- Identify the fundamental concepts of computer security.
- Identify security threats and vulnerabilities.
- Examine network security.
- Manage application, data and host security.
- Identify access control and account management security measures.
- Manage public key infrastructure (PKI).
- Manage certificates.
- Identify compliance and operational security measures.
- Manage risk.
- Establish key components of the security infrastructure.
- Manage security incidents.
- Develop business continuity and disaster recovery plans.

Topics

- Security Fundamentals
- Security Threats and Vulnerabilities
- Network Security
- Managing Application, Data and Host Security
- Access Control, Authentication, and Account Management
- Managing Public Key Infrastructure (PKI)
- Managing Certificates
- Compliance and Operational Security
- Managing Risk
- The Security Infrastructure
- Managing Security Incidents
- Business Continuity and Disaster Recovery

Audience

This course is targeted toward an Information Technology (IT) professional who has networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems, such as OS X, Unix, or Linux, and who wants to further a career in IT by acquiring a foundational knowledge of security topics; prepare for the CompTIA Security+ Certification examination; or use Security+ as the foundation for advanced security certifications or career roles.

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

CompTIA Security+ (2011 Objectives)

Course Summary (cont'd)

Prerequisites

Basic Windows skills and fundamental understanding of computer and networking concepts are required. Students can obtain this level of skill and knowledge by taking the following courses:

- Introduction to Networks and the Internet
- Introduction to Personal Computers: Using Windows 7
- Microsoft Windows 7: Level 1
- Microsoft Windows 7: Level 2

Experience with CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP, are strongly recommended. Students can obtain this level of skill and knowledge by taking any of the following courses:

- CompTIA A+ Certification: A Comprehensive Approach for all 2009 Exam Objectives
- Network+ Certification: Fourth Edition – A CompTIA Certification or CompTIA® Network+® (2009 Objectives)

Additional introductory courses or work experience in application development and programming or in network and operating system administration for any software platform or system are helpful but not required.

Duration

Five days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

CompTIA Security+ (2011 Objectives)

Course Outline (cont'd)

I. Security Fundamentals

A. Information Security Cycle
1. What Is Information Security?
2. What to Protect
3. Goals of Security
4. Vulnerabilities
5. Threats
6. Attacks
7. Intrusions
8. Risk
9. Controls
10. Types of Controls
11. Security Management Objectives
12. How to

B. Information Security Controls
1. The CIA Triad
2. Non-repudiation
3. Authentication
4. Identification
5. The Five As
6. Access Control Methods
7. Implicit Deny
8. Least Privilege
9. Separation of Duties
10. Job Rotation
11. Mandatory Vacation
12. Time of Day Restrictions
13. Privilege Management
14. How to

C. Authentication Methods
1. Authentication Factors
2. User Name/Password Authentication
3. Tokens
4. Trusted OS
5. Biometrics
6. Multi-Factor Authentication
7. Mutual Authentication
8. How to

D. Cryptography Fundamentals
1. Cryptography
2. Encryption
3. Ciphers
4. Cipher Types
5. Encryption and Security Goals
6. Encryption Algorithms
7. Steganography
8. Keys
9. Hashing Encryption
10. Hashing Encryption Algorithms
11. Symmetric Encryption
12. Symmetric Encryption Algorithms
13. Asymmetric Encryption
14. Asymmetric Encryption Algorithms
15. Digital Signatures
16. Quantum Cryptography
17. Hardware-Based Encryption Devices
18. How to

E. Security Policy Fundamentals
1. Security Policies
2. Security Policy Components
3. Security Policy Issues
4. Common Security Policy Types
5. Security Document Categories
6. Change Management
7. Documentation Handling Measures
8. How to

II. Security Threats and Vulnerabilities

A. Social Engineering
1. Social Engineering Attacks
2. Types of Social Engineering
3. Hackers and Attackers
4. Categories of Attackers
5. How to

B. Physical Threats and Vulnerabilities
1. Physical Security
2. Physical Security Threats and Vulnerabilities
3. Hardware Attacks
4. Environmental Threats and Vulnerabilities
5. How to

C. Network-Based Threats
1. TCP/IP Basics
2. Port Scanning Attacks
3. Eavesdropping Attacks
4. Replay Attacks
5. Social Network Attacks
6. Man-in-the-Middle Attacks
7. Denial of Service (DoS) Attacks

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

CompTIA Security+ (2011 Objectives)

Course Outline (cont'd)

8. Distributed Denial of Service (DDoS) Attacks
9. Types of DoS Attacks
10. Session Hijacking
11. P2P Attacks
12. ARP Poisoning
13. DNS Vulnerabilities
14. How to

D. Wireless Threats and Vulnerabilities
1. Wireless Security
2. Wireless Threats and Vulnerabilities
3. How to

E. Software Based Threats
1. Software Attacks
2. Malicious Code Attacks
3. Types of Malicious Code Attacks
4. Password Attacks
5. Types of Password Attacks
6. Backdoor Attacks
7. Application Attacks
8. Types of Application Attacks
9. How to

III. Network Security

A. Network Devices and Technologies
1. Network Components
2. Network Devices
3. Network Technologies
4. Intrusion Detection Systems (IDSs)
5. NIDS
6. NIPS
7. Types of Network Monitoring Systems
8. Virtual Private Networks (VPNs)
9. VPN Concentrator
10. Web Security Gateways
11. How to

B. Network Design Elements and Components
1. NAC
2. VLANs
3. Subnetting
4. NAT
5. Remote Access
6. Remote Access Methods
7. Telephony Components
8. Virtualization
9. Cloud Computing
10. Cloud Computing Service Types
11. How to

C. Implement Networking Protocols
1. Internet Protocols
2. DNS
3. HTTP
4. SSL
5. Transport Layer Security (TLS)
6. HTTPS
7. SSH
8. SNMP
9. ICMP
10. IPSec
11. File Transfer Protocols
12. Ports
13. MMC
14. How to How to Implement Networking Protocols

D. Apply Network Security Administration Principles
1. Rule-Based Management
2. Network Administration Security Methods
3. How to How to Apply Network Security Administration Principles

E. Secure Wireless Traffic
1. The 802.11 Protocol
2. 802.11 Standards
3. The WAP Protocol
4. Wireless Security Protocols
5. Wireless Security Methods
6. How to How to Secure Wireless Traffic

IV. Managing Application, Data and Host Security

A. Establish Device/Host Security
1. Hardening
2. Operating System Security
3. Operating System Security Settings
4. Security Baselines
5. Software Updates
6. Patch Management
7. Logging
8. Auditing
9. Anti-Malware Software
10. Types of Anti-Malware Software

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

CompTIA Security+ (2011 Objectives)

Course Outline (cont'd)

11. Virtualization Security Techniques
12. Hardware Security Controls
13. Strong Passwords
14. How to How to Establish Device/Host Security

B. Application Security
1. What is Application Security?
2. Application Security Methods
3. Input Validation
4. Input Validation Vulnerabilities
5. Error and Exception Handling
6. Cross-Site Scripting
7. Cross-Site Request Forgery (XSRF)
8. Cross-Site Attack Prevention Methods
9. Fuzzing
10. Web Browser Security
11. How to

C. Data Security
1. What is Data Security?
2. Data Security Vulnerabilities
3. Data Encryption Methods
4. Hardware-Based Encryption Devices
5. How to

D. Mobile Security
1. Mobile Device Types
2. Mobile Device Vulnerabilities
3. Mobile Device Security Controls
4. How to

V. Access Control, Authentication, and Account Management

A. Access Control and Authentication Services
1. Directory Services
2. LDAP
3. Common Directory Services
4. Remote Access Methods
5. Tunneling
6. VPN
7. Layer Two Tunneling Protocol (L2TP)
8. Point-to-Point Tunneling Protocol (PPTP)
9. CHAP
10. PAP
11. PGP
12. RADIUS
13. TACACS
14. Kerberos
15. The Kerberos Process
16. How to

B. Implement Account Management Security Controls
1. Identity Management
2. Account Management
3. Account Privileges
4. Account Policy
5. Multiple Accounts
6. Multiple User Account Issues
7. Account Management Security Controls
8. Group Policy
9. How to Implement Account Management Security Controls

VI. Managing Public Key Infrastructure (PKI)

A. Install a Certificate Authority (CA) Hierarchy
1. Digital Certificates
2. Certificate Authentication
3. Single vs. Dual Sided Certificate Authentication
4. Public Key Infrastructure (PKI)
5. PKI Components
6. CA Hierarchies (Trust Models)
7. The Root CA
8. Public and Private Roots
9. Subordinate CAs
10. Offline Root CAs
11. CA Hierarchy Design Options
12. How to How to Install a Certificate Authority (CA) Hierarchy

B. Back Up a CA
1. How to How to Back Up a CA

C. Restore a CA
1. How to How to Restore a CA

VII. Managing Certificates

A. Enroll Certificates
1. The Certificate Enrollment Process
2. The Certificate Life Cycle
3. Certificate Life Cycle Management
4. How to How to Enroll Certificates

B. Secure Network Traffic by Using Certificates
1. SSL Enrollment Process

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

CompTIA Security+ (2011 Objectives)

Course Outline (cont'd)

2. How to How to Secure Network Traffic by Using Certificates

C. Renew Certificates
1. How to How to Renew Certificates

D. Revoke Certificates
1. Certificate Revocation
2. The Certificate Revocation List (CRL)
3. How to How to Revoke Certificates

E. Back Up Certificates and Private Keys
1. Private Key Protection Methods
2. Key Escrow
3. How to How to Back Up Certificates and Private Keys

F. Restore Certificates and Private Keys
1. Private Key Restoration Methods
2. Private Key Replacement
3. How to How to Restore Certificates and Private Keys

VIII. Compliance and Operational Security

A. Physical Security
1. Physical Security Controls
2. Physical Security Control Types
3. Environmental Exposures
4. Environmental Controls
5. Environmental Monitoring
6. How to

B. Legal Compliance
1. Compliance Laws and Regulations
2. Legal Requirements
3. Types of Legal Requirements
4. Due Care
5. Due Diligence
6. Due Process
7. Forensic Requirements
8. How to

C. Security Awareness and Training
1. Security Policy Awareness
2. Employee Education
3. User Security Responsibilities
4. How to

IX. Managing Risk

A. Risk Analysis
1. Risk Management
2. Types of Risk
3. Components of Risk Analysis
4. Phases of Risk Analysis
5. Risk Analysis Methods
6. Risk Calculation
7. Risk Response Strategies
8. How to

B. Implement Risk Mitigation Strategies
1. Risk Control Types
2. Security Incident Management
3. Risk Mitigation Techniques
4. How to Implement Risk Mitigation Strategies

X. The Security Infrastructure

A. Implement Vulnerability Assessment Tools and Techniques
1. Security Assessment Types
2. Security Assessment Techniques
3. Security Assessment Tools
4. Honeypots
5. How to How to Implement Vulnerability Assessment Tools and Techniques

B. Scan for Vulnerabilities
1. The Hacking Process
2. Ethical Hacking
3. Penetration Testing and Vulnerability Scanning
4. Types of Vulnerability Scans
5. Box Testing Methods
6. Security Utilities
7. Vulnerable Port Ranges
8. How to How to Scan for Vulnerabilities

C. Mitigation and Deterrent Techniques
1. Security Posture
2. Detection vs. Prevention Controls
3. Types of Mitigation and Deterrent Techniques
4. How to

XI. Managing Security Incidents

A. Respond to Security Incidents
1. Computer Crime
2. First Responders
3. Chain of Custody
4. Incident Response Policies
5. Computer Forensics

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

CompTIA Security+ (2011 Objectives)

Course Outline (cont'd)

6. Order of Volatility
7. Basic Forensic Response Procedures for IT
8. Basic Forensic Process
9. How to How to Respond to Security Incidents

B. Recover from a Security Incident
1. Damage Assessment and Loss Control Guidelines
2. Organizational Security Reporting Structures
3. Security Incident Reporting Options
4. How to How to Recover from a Security Incident

XII. Business Continuity and Disaster Recovery

A. Business Continuity
1. Business Continuity Plans
2. Business Impact Analysis
3. Continuity of Operations Plan
4. IT Contingency Planning
5. Succession Planning
6. Business Continuity Testing
7. How to

B. Plan for Disaster Recovery
1. Disaster Recovery Plans
2. Fault Tolerance
3. Redundancy Measures
4. High Availability
5. Alternate Sites
6. Disaster Recovery Testing
7. Disaster Recovery Evaluation and Maintenance
8. How to How to Plan for Disaster Recovery

C. Execute Disaster Recovery Plans and Procedures
1. The Recovery Team
2. The Salvage Team
3. The Disaster Recovery Process
4. Secure Recovery
5. Backup Types and Recovery Plans
6. Backout Contingency Plans
7. Secure Backups
8. Backup Storage Locations
9. How to How to Execute Disaster Recovery Plans and Procedures

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically