Preparing for the CompTIA Security+™ Certification Exam - 5 Days

Course 446 Overview

You Will Learn How To

- Successfully prepare for the CompTIA Security+ Certification Exam
- Confidently explain and define an array of security terminologies
- Navigate the complexity of secure communication protection
- Explore the concepts of network protection with firewalls and IDS
- Investigate privacy and integrity issues such as cryptography, PKI and digital signatures

Who Should Attend

Security professionals, government and military personnel seeking IAT-2 or IAM-1 certification to fulfill the 8570.1 Directive, network security personnel and managers with previous technical skills or background.

Workshop Activities

- Practicing exams daily for the six domains
- Analyzing protocols and security issues with Wireshark
- Employing an IDS to detect and deflect attacks
- Protecting communication with encryption and digital signatures
- Validating certificates using public keys
- Scanning for vulnerabilities

Preparing for the CompTIA Security+™ Certification Exam - 5 Days

Course 446 Outline

Introduction to the CompTIA Security+ Exam

- The six domains of knowledge
- Expected level of expertise
- Assessing initial readiness

Securing the Network

Communication security goals

- Evaluating network design and components
- Examining ports, protocols and threats
- Implementing wireless security

Secure administration principles

- Designing for security
- Managing VLANs and firewall rules
- Implementing port security
- Leveraging flood guards

Compliance and Operational Security

Risk-related concepts

- Inspecting methods of control
- Conducting risk reduction
- Formulating risk models
- Evaluating risk

Mitigation strategies

- Deterrence, avoidance and transference
- Incident response
- Preparing security awareness training

Business continuity measures

- Assessing environmental controls
- Planning for disaster recovery
- Analyzing continuity of business plans
- Implementing high-availability

Access Controls

Infrastructure principles

- Assessing MAC, DAC and RBAC
- Comparing logical and physical access controls

Strengthening the infrastructure

- Utilizing authentication systems
- Implementing multifactor authentication
- Kerberos and CHAP

Threats and Vulnerabilities

Identifying vulnerabilities and threats

- Isolating botnets, viruses and worms
- Preventing man-in-the-middle attacks
- Stopping social engineering ploys
- Malicious insiders
- Spamming, phishing and vishing

Application attacks

- Detecting buffer overflows
- Rejecting injection attacks
- Preventing cookie misuse
- Halting cross-site scripting (XSS)

Application, Data and Host Security

Security assessment tools

- Fuzzers
- Patch management
- Application hardening

Host security tools and techniques

- Anti-malware
- Physical security
- Mobile devices

Fundamentals of Cryptography

Assuring privacy with encryption

- The CIA model and beyond
- Cryptographic standards and protocols
- Deploying symmetric encryption
- Implementing Public Key cryptography

Establishing cryptographic security

- Performing digital signatures
- Exploring the role of certificate authorities
- Managing keys and the CRL
- Analyzing X.509 certificates

Final Review

Preparing for the examination

- Priming for the exam
- Handling out-of-date questions
- Utilizing additional study guides

Assessing readiness

- Final review and assessment
- Taking a complete practice exam