Course ID

NETSEC

Course Duration

3-4 days

Course Title

Principles of Network Security: CompTIA Security+ and US DoD Directive 8570.1

Aimed At

Computer network administrators, backup operators, security system administrators, corporate and government IT management, IT auditors and staff.

Prerequisites

You should have some prior experience with client-server networks. Two years on-the-job networking experience, with an emphasis on security, will be helpful. CompTIA A+ and Network+ certifications, or equivalent knowledge, are also recommended.

Group Size

5-25

Course In a Nutshell

As more and more businesses use their networks to store and transmit sensitive information, the risk of security breaches continues to rise. A research report of the Computing Technology Industry Association (CompTIA) has identified human errors as the number one cause of such breaches. CompTIA's Security+ certification is an internationally recognized, vendor-neutral standard for validating the network administrators' security competencies. It's also one of the certifications listed in the United States Department of Defense (DoD) Directive 8570 on Information Assurance as part of the requirements for all employees and contractors engaged in work that involves information security sensitivities.

This course, intended to meet the certification requirements of the CompTIA Security+ examination as well as the US DoD Directive 8570.1, will help you properly safeguard the corporate or governmental IT infrastructure entrusted to you. Covered are general security concepts, communication security, infrastructure security, cryptography, and operational security. After completing this course, you will be much better equipped to recognize the various types of threats to network and computer security and employ effective measures to deal with them.

Customize It

Customize this course to your specific background and job requirements at little-to-no additional cost.

- If you have an interest in a particular area, let us know. We can tailor the topics included in the course, emphasis each topic receives, pace of coverage, and the choice of case studies and exercises to suit your needs.
- Are you a less technical professional or manager, primarily interested in the security policy implications? We offer a two-to-three day version of this course aimed at less technical audiences.
- Are you a network professional interested in preventing attacks on your network? We offer a four-day expanded version of this course that includes a comprehensive examination of how hackers may attack your network resources with examples, exercises, and case studies.

Learn How To

- Recognize different types of network resource attacks.
- Implement the latest access methods.
- Establish strong encryption and authentication procedures for your servers.
- Deal with physical security issues.
- Implement a disaster recovery program.
- Develop an effective security training and security awareness program for employees.
- Select the most appropriate security tools for your organization.

Course Outline

- General Security Concepts
    - Access control models
    - Authentication methods
    - Reducing the risks of non-essential protocols
    - Reducing the risks for various types of attacks
    - Mitigating risks from malicious code
    - Understanding authentication, auditing, accounting and identification
- Communications Security
    - Types of remote access technologies
    - R-mail security concepts
    - Internet security concepts
    - Directory security concepts
    - File transfer protocols and concepts
    - Wireless technologies and concepts
- Infrastructure Security
    - Security concerns and concepts of various network devices
    - Security concerns for various types of media
    - Security topologies
    - Intrusion detection
    - Understanding security baselines
- Basics of Cryptography
    - Different types of cryptographic algorithms
    - How cryptography addresses various security concepts
    - Understanding PKI (Public Key Infrastructure)
    - Cryptographic standards and protocols
    - Key Management and Certificate Lifecycles
- Operational/Organizational Security
    - Concepts of physical security
    - Disaster recovery planning
    - Security supplications and business continuity
    - Policies and procedures
    - Concepts of privilege management

  - Understanding forensics
  - Risk identification
  - Education and training of end users, executives and human resources
  - Security documentation concepts

- Wrap-up: Course Recap, Q/A, and Evaluations

How You Will Learn

- You will learn in interactive lecture format from an instructor who's among the most knowledgeable and dynamic in the industry.
- If you already know something about the technology, we will build on that. We'll compare and contrast what's familiar with what's new, making new ideas easier to learn as well as more relevant.
- If your background is less technical, we will use meaningful and ingenious examples and analogies to simplify the complex subject matter.
- The Participant Presentation Material will provide you with a structure to which you can add the information and insight provided in real-time, turning it into a valuable reference resource you can take back to your job.

Revised *Jan. 26, 2007*