

Course 755

Network Security: Problems, Solutions and Responsibilities

(3 days)

Course Description...

This unique course leads students through the types of Network Security Problems, Solutions and Responsibilities. Throughout the course, attendees will examine several different types of Network Security problems by experiencing real-world exploits that take advantage of the problems, and discuss solution and prevention methods. In addition, responsibilities of network & security personnel will be discussed, including preparing for, preserving, documenting and reporting Network Security issues.

Who Should Attend...

Attendees should include Managers, Network and System Administrators, Developers, Programmers, Developers, and others with a need to know and understand Network Security related problems. Since this is a networking course – it is highly recommended that students have an understanding of TCPIP Networking and experience with System Administration (either UNIX or Windows).

Course Outline...

Overview - Network Security Problems

- CIAA – Confidentiality, Integrity, Availability and Authentication
- Comparing Internet vs. Intranet Network Security Issues
- Review of Network Security Components
- Types of Attacks and Exploits

Network Security: Confidentiality Problems

- Real-World Example: Attacks on Network Confidentiality
- Utilizing Cryptography and Encryption Effectively
- Exchanging and Protecting Encryption Keys
- Evaluating a Confidentiality Solution
- What about Privacy?

Network Security: Authentication Problems

- Example: Attacking Authentication
- Authentication Methods: Something you know, have or are
- Addressing Password Vulnerabilities
- Open vs. Proprietary Authentication Protocols
- Operating System Privileges



Network Security: Integrity Problems

- Real-World Examples: Attacks on Information and Communication Integrity
- Methods to preserve Integrity
- Input and Data Modification
- Utilizing backups to verify integrity
- Returning to previous versions of data

Network Security: Availability Problems

- Real-World Example: Attacks on Network Availability
- Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- Prediction and Preventative Measures
- Understanding the limitations of Network Administration

Network Security: Responsibilities

- Performing a Security Audit to Identify Vulnerabilities
- Preserving a system after an attack
- Documenting an Attack
- Reporting an attack to Authorities
- Taking Measures

Network Security: Additional Case Studies

- Case 1: Wireless Network Attack
- Case 2: Internet Registration Attack
- Case 3: Internal/Trusted Attacks

Please contact your ROI representative to discuss course tailoring!!!