

Course 753

Operating System and Network Security Foundations (5 days)

Course Description...

This course provides the foundation for Operating System and Network Security. Throughout the course, attendees will cover the security concepts related to securing Computing Environments, from the network cabling right up to the Operating Systems and applications that run on them. Through the use of lecture, and hands-on labs, the key components of Operating System and Network Security will be discussed and demonstrated.

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. This course is also an excellent foundation of knowledge for those studying for the CISSP exam. Since this is a Operating System and Networking course – it is highly recommended that students have an understanding of TCPIP Networking and experience with Operating System Administration (either UNIX or Windows).

Course Outline...

Overview - Security Problems

- Network and Operating System Components
- CIAA – Confidentiality, Integrity, Availability and Authentication
- Knowing the Enemy
- Internal and External Security
- Introduction to Network Security Components
- Introduction to Operating System Security Components

Cryptography Essentials

- Real-World Example: Encryption and Decryption
- Symmetric Encryption
- ASymmetric encryption
- Hashing and Digests
- Public/Private Key Cryptography
- Public Key Infrastructure
- Utilizing Cryptography and Encryption Effectively



Starting with the Network

- Real-World Example: Attacks on the Network
- Denial of Service
- Local Area Network (LAN) Designs
- Firewall Configuration

TCP/IP and Security

- Example: Intercepting TCP/IP Communication
- Understanding TCP/IP communication
- Enhancing TCP/IP Security
- IPSec and Virtual Private Networks
- SSH
- SSL and TLS

Operating System Security

- Example: Attacking an Operating System
- Operating System Fundamentals
- User/Group Management
- Leveraging Operating System Components
- Locking down an Operating System
- Patch Management

Identity within the Network and Operating System

- Example: Attacking Identity
- Understanding Authentication and Authorization
- Windows Specific Authentication Mechanisms (LM/NTLM/AD)
- Open Authentication Mechanisms (Kerberos, RADIUS and TACACS+)
- Two-factor Authentication: Token and Biometric Authentication Mechanisms

Intrusion Detection

- Example: Configure an Intrusion Detection System
- Attack Signatures
- Anomaly Detection
- Host vs Network Detection
- Reacting to Intrusion Detection Reports
- Honey Pots and Traps

Firewalls Revisited

- Example: Defense in Depth
- Packet filter technologies
- Stateful Inspection
- Network Address Translation (NAT)
- Proxy Servers
- Software vs Hardware Firewalls
- Operating System Firewalls



Responsibilities

- Example: Perform a Security Auditing
- Risk Analysis and Evaluation
- Preserving a system after an attack
- Documenting an Attack
- Reporting an attack to Authorities

Disaster Preparation and Business Continuity

- Example: Rebuilding a network
- What are Backups really for?
- Planning for Tomorrow
- Off-Site facilities: Backup Sites and classification

Technology Integration

- Example: Evaluating and adding a Technology to infrastructure
- Wireless LAN
- Wide-Area Wireless LAN
- Remote Users
- VoIP

Security: Additional Case Studies

- Case 1: Operating System Upgrade Vulnerability
- Case 2: Networked Device Attacks
- Case 3: Website Attacks

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