

INFRASTRUCTURE AND NETWORK SECURITY THEORY & PRACTICE

Infrastructure and Network Security Theory and Practice™ is an introductory level course covering a wide range of areas related to the security of network and operational infrastructure. This is an ideal course to use as a stepping stone to other, more advanced topics, or as a general introduction for organizational security or law enforcement personnel.

Audience:

This class is designed specifically for the needs of individuals dealing in the operational areas of network, systems and infrastructure security. This includes operational personnel, law enforcement authorities, carrier personnel who deal with law enforcement authorities and issues, including the Carrier Assistance of Law Enforcement Act (CALEA), consultants, managers, supervisors and product planners and designers.

Prerequisites:

There are no prerequisites for this course other than a need to know about network, systems and infrastructure security.

Objectives:

At the conclusion of this course the student will be able to:

- Better Understand Terrorist's Tactics, Tools and Objectives
- Perform a Security Audit
- Identify and Correct Security Vulnerabilities
- Develop Security Scenarios
- Do Role-Plays with Your Security Team
- Perform Readiness Drills
- Identify False Documents
- Understand Document Forgery Processes
- Understand and Counter Terrorist Information Gathering Techniques
- Do Internal Security Awareness Training
- Understand The Implementation of Security Technologies
- Recommend Better Defensive Measures
- Secure an Electronic Crime Scene for Forensics

INFRASTRUCTURE AND NETWORK SECURITY THEORY & PRACTICE

COURSE OUTLINE

Day 1

1. Introduction: Network Security Philosophy

- The Ideal Security System
- Protecting Proprietary Information
- Planning for Security
- Organizational Security Policy
- The Impact of Terrorism and Hacker Activity
- Understanding the Enemy: A Rogue's Gallery

2. Network Building Blocks

- Internet Overview
- PCs / Terminals
- Servers
- Routers / Switches
- Layered Communications

3. System Security Concepts

- Physical Security Measures
- Encryption
- Cryptography
- Key Systems
- Authentication and Authorization
- Digital Signatures and Certificates
- Policy-Based Security Enforcement
- Malicious Software

4. Network Services and Infrastructure Security

- Physical Security
- Issues
 - False Positives
 - False Negatives
 - Impact on Operations
- Document Authentication and Forgery
- Security Awareness, Readiness and Training
 - Polite Challenges
 - Media Security
 - Bulk Encryption

● Data Link Security

- Point-to-Point Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Remote Authentication Dial-In Service (RADIUS)
- Tunneling
 - i. Layer 2 Forwarding (L2F)
 - ii. Point-to-Point Tunneling Protocol (PPTP)
 - iii. Layer 2 Tunneling Protocol (L2TP)
 - iv. Other

● Network Layer Security

- Internet Protocol Security (IPsec)
- IP Proxy Agents / Proxy Servers

Day 2

5. Higher Layer Services Security

- Transport Layer Security
 - Secure Sockets Layer (SSL)
 - Kerberos
- Session Layer Security
 - Passwords
 - Encrypted Passwords
 - One-Time Use Passwords
 - Biometric Authentication
 - Cookies
- Presentation Layer Security
 - Encryption
 - Encrypting File System (EFS)

continued on the next page

INFRASTRUCTURE AND NETWORK SECURITY THEORY & PRACTICE

6. Application Layer and Application Security

- Application Layer Security
 - Secure Shell (SSH)
 - Secure HTML (SHTML)
 - Secure HTTP (SHTTP)
 - Secure Electronic Transactions (SETs)
 - Java, Active-X, Visual Basic
- Above the OSI Stack
 - Application Encryption
 - Air Gap Technology (AGT)
 - Other Technologies

7. Hackers, Terrorists and Law Enforcement

- Hacker and Terrorist Tools
 - The Insider Threat
 - Exploiting Backdoors, Bugs, and Loopholes
 - Social Engineering
 - Reverse Social Engineering
 - Trespassing, Dumpster Diving, and Shoulder Surfing
 - Denial of Service, Smurfing, and Spam
 - Covert Channels and Steganography
- Law Enforcement
 - Privacy Issues
 - Tools
 - i. CALEA
 - ii. CARNIVORE
 - iii. ECHELON
 - iv. Monitoring and Surveillance
 - Cooperation/Coordination Between Agencies
 - i. Jurisdictional Issues
 - ii. Cross-Border / International Coordination
 - iii. Extradition
- Forensics 101

8. Exploit Gallery: Anatomy of 4 Common Attacks

- The Rolex (Social Engineering)
- Inside I Love You (A Classic Worm)
- Trinoo Attack (Distributed Resource Re-allocation)
- rootkits and IRC (Script Kiddies in Action)

9. Conclusion: Toward More Secure Networking