

NETWORK SERVICES SECURITY THEORY & PRACTICE

Network Services Security Theory and Practice™ is a highly technical and in-depth course in the technical aspects of providing security for primarily IP-based public and private networks, including the Internet, intranets, extranets and IP Virtual Private Networks. This course is designed for technical professionals and is taught by technical professionals.

Audience:

Engineers and operations personnel of Network Services Providers (NSPs), Internet Service Providers (ISPs), Carriers and Network Backbone Providers responsible for operational and information security. This course is also ideal for law enforcement personnel, investigators and government agencies responsible for the investigative and operational aspects of network security. This is a very technical course designed for the practitioner of network security.

Prerequisites:

An in-depth knowledge of network operations and protocols is assumed.

Objectives:

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

- Determine Security Vulnerabilities
- Help Guide Security Policy
- Understand and Implement Security Technologies
- Recommend Better Defensive Measures
- Help Define More Responsive and Effective Security Products and Implementations
- Configure VPN Security
- Perform a Security Audit
- Develop Security Scenarios
- Perform Security Readiness Drills

NETWORK SERVICES SECURITY THEORY & PRACTICE

COURSE OUTLINE

Day 1

1. Introduction: Network Security Philosophy

- The Ideal Security System
- Planning for Internet Security
- Organizational Security Policy
- Hacker Profiles and Motives
- The Financial Impact of Network Security

2. System Security Concepts

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

3. Data Link Layer Security

- Point-to-Point Protocol (PPP)
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Remote Authentication Dial-In User Security (RADIUS)
- Tunneling
 - Layer 2 Forwarding (L2F)
 - Point-to-Point Tunneling Protocol (PPTP)
 - Layer 2 Tunneling Protocol (L2TP)
 - Other

4. Network Layer Security

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

Day 2

5 Transport Layer Security

- Secure Sockets Layer (SSL)
- Kerberos

6 Anatomy of a Firewall

- A Sample Firewall: Checkpoint Systems
- Three Main Operational Areas
 - Security
 - i. Access Control
 - ii. Content Security
 - iii. Intrusion Detection
 - iv. Malicious Activity Detection (MAD)
 - v. Network Address Translation (NAT)
 - vi. User Authentication
 - vii. Virtual Private Networks (VPNs)
 - Performance / Availability
 - i. High Availability
 - ii. Performance Tuning
 - Management
 - i. LDAP Based User Management
 - ii. Reporting Module
 - iii. Third Party Device Management
 - iv. Visual Policy Editor
- Demilitarized Zone (DMZ)

7 Network Services Security Tools & Techniques

- The Insider Threat
- Exploiting Backdoors, Bugs, and Loopholes
- Packet Sniffers
- Social Engineering
- Reverse Social Engineering
- Trespassing, Dumpster Diving, and Shoulder Surfing
- Denial of Service (DoS), Smurfing, and Spam
- Covert Channels and Steganography

continued on the next page

NETWORK SERVICES SECURITY THEORY & PRACTICE

8 Case Study - "Securing the Customer VPN"

- Internet, Intranet, Extranet, VPN
- Risk Assessment
- Network Security Scenarios
- Review and Debrief

9 Conclusion: Toward More Secure Networking