



Network Security and Firewalls

Network Security and Firewalls is a two-day course designed to teach students how to secure networks from unauthorized activity. Students learn about establishing an effective security policy, different types of hacker activities, the hacker's mind-set, and preventing and managing hacker penetration. Students will also learn about authentication procedures, encryption standards and implementations, ports and protocols that hackers manipulate, and how to engage in proactive detection and response/reporting methods.

Topics

What Is Security?

- Network Security Background
- What Is Security?
- Hacker Statistics
- The Myth of 100-Percent Security
- Attributes of an Effective Security Matrix
- What You Are Trying to Protect
- Who Is the Threat?
- Security Standards

Elements of Security

- Security Elements and Mechanisms
- The Security Policy
- Encryption
- Authentication
- Specific Authentication Techniques
- Access Control
- Auditing
- Security Tradeoffs and Drawbacks

Applied Encryption

- Reasons to Use Encryption
- Creating Trust Relationships
- Symmetric-Key Encryption
- Symmetric Algorithms
- Asymmetric-Key Encryption
- One-Way (Hash) Encryption
- Applied Encryption Processes
- Encryption Review

Types of Attacks

- Network Attack Categories
- Brute-Force and Dictionary Attacks
- System Bugs and Back Doors
- Malware (Malicious Software)
- Social Engineering Attacks
- Denial-of-Service (DOS) Attacks
- Distributed Denial-of-Service (DDOS) Attacks
- Spoofing Attacks
- Scanning Attacks
- Man-in-the-Middle Attacks
- Bots and Botnets
- SQL Injection
- Auditing

Recent Networking Vulnerability Considerations

- Networking Vulnerability Considerations
- Wireless Network Technologies and Security
- IEEE 802.11 Wireless Standards
- Wireless Networking Modes
- Wireless Application Protocol (WAP)
- Wireless Network Security Problems
- Wireless Network Security Solutions
- Site Surveys
- Convergence Networking and Security
- Web 2.0 Technologies
- Greynet Applications
- Vulnerabilities with Data at Rest
- Security Threats from Trusted Users
- Anonymous Downloads and Indiscriminate Link-Clicking

General Security Principles

- Common Security Principles
- Be Paranoid
- You Must Have a Security Policy
- No System or Technique Stands Alone
- Minimize the Damage
- Deploy Companywide Enforcement
- Provide Training
- Use an Integrated Security Strategy
- Place Equipment According to Needs
- Identify Security Business Issues
- Consider Physical Security

Protocol Layers and Security

- TCP/IP Security Introduction
- OSI Reference Model Review
- Data Encapsulation
- The TCP/IP Stack and the OSI Reference Model
- Link/Network Access Layer
- Network/Internet Layer
- Transport Layer
- Application Layer

Securing Resources

- TCP/IP Security Vulnerabilities
- Implementing Security Resources and Services
- Protecting TCP/IP Services
- Simple Mail Transfer Protocol (SMTP)
- Physical Security
- Testing Systems
- Security Testing Software
- Security and Repetition

Firewalls and Virtual Private Networks

- Access Control Overview
- Definition and Description of a Firewall
- The Role of a Firewall
- Firewall Terminology
- Firewall Configuration Defaults
- Creating Packet Filter Rules
- Packet Filter Advantages and Disadvantages
- Configuring Proxy Servers
- URL Filtering
- Remote Access and Virtual Private Networks (VPNs)
- Public Key Infrastructure (PKI)

Levels of Firewall Protection

- Designing a Firewall
- Types of Bastion Hosts
- Hardware Issues
- Common Firewall Designs
- Putting It All Together

Detecting and Distracting Hackers

- Proactive Detection
- Distracting the Hacker
- Deterring the Hacker

Incident Response

- Creating an Incident Response Policy
- Determining If an Attack Has Occurred
- Executing the Response Plan
- Analyzing and Learning



Target Audience

Network server administrators, firewall administrators, systems administrators, application developers, and IT security officers.

Course Length

Title of Course is a 12-hour course.

Prerequisites

Students must have passed the CIW Foundations, CIW Server Administrator, and CIW Internetworking Professional exams or have equivalent skills.