

CIW Security Professional Series – Course 1: Network Security and Firewalls (November 2002)

Network Security and Firewalls teaches you how to secure your network from unauthorized activity. This course teaches you about security principles, such as establishing an effective security policy, and about the different types of hacker activities that you are most likely to encounter.

Topics

What Is Security?

- Network Security Background
- What Is Security?
- Hacker Statistics
- What Is the Risk?
- 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 Concepts and Mechanisms

Elements of Security

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

Applied Encryption

- Reasons to Use Encryption
- Creating Trust Relationships
- Rounds, Parallelization and Strong Encryption
- Symmetric-Key Encryption
- Symmetric Algorithms
- Asymmetric Encryption
- Hash Encryption
- Applied Encryption Processes
- Encryption Review

Types of Attacks

- Attack Categories
- Brute-Force and Dictionary Attacks
- System Bugs and Back Doors
- Social Engineering and Non-Direct Attacks

General Security Principles

- Common Security Principles: Introduction
- 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
- TCP/IP and Network Security
- The TCP/IP Suite and the OSI Reference Model
- Physical Layer
- Network 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)
- Testing and Evaluating
- Implementing New Systems and Settings
- 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
- 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

- Preparing for the Inevitable
- Proactive Detection
- Distracting the Hacker
- Deterring the Hacker

Incident Response

- Planning for Response
- Create a Response Policy
- Decide Ahead of Time
- Do Not Panic
- Document Everything
- Assess the Situation
- Stop or Contain Activity
- Execute the Response Plan
- Analyze and Learn

Target Audience

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

Job Responsibilities

Implement e-business solutions security policies; identify security threats and develop countermeasures using firewall systems and attack-recognition technologies; and manage the deployment of security solutions.

Prerequisites

Students must have completed the CIW Foundations and CIW Internetworking Professional series or be able to demonstrate equivalent Internet knowledge.

Duration

12 hours

CIW Security Professional Series – Course 2: Operating System Security (October 2002)

Operating System Security is a course designed to teach students the latest security industry recommendations and how to properly protect Windows 2000 and Linux servers in a variety of settings. Students will learn how to protect Windows 2000 and Linux systems from attacks, reconfigure the operating system to fully protect it, and scan hosts for known security problems. By the end of the course, students will have a solid understanding of the security architectures used by Windows 2000 and Linux.

Topics

Security Principles

- Overview of Security Principles
- Definition of Security
- Evaluation Criteria
- Security Levels
- Security Mechanisms
- Security Management
- Windows 2000 Security
- Windows 2000 Security Architecture
- Linux Security
- Pluggable Authentication Modules (PAMs)

Account Security

- Securing Accounts: An Overview
- Passwords
- Verifying System State
- Password Aging in Linux

File System Security

- File System Security Overview
- Windows 2000 File System Security
- Remote File Access Control
- Linux File System Security

Assessing Risk

- Risk Assessment Basics
- Security Threats
- Windows 2000 Security Risks
- General UNIX Security Vulnerabilities
- Keyloggers
- System Port Scanning
- UNIX Security Risks
- NIS Security Concerns
- NFS Security Concerns

Reducing Risk

- Reducing Risk through Simplification
- Patches and Fixes
- Windows 2000 Registry Security
- Disabling and Removing Unnecessary Services in Windows 2000
- Reducing Risk in Linux Systems

Target Audience

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

Job Responsibilities

Implement e-business solutions security policies; identify security threats and develop countermeasures using firewall systems and attack recognition technologies; and manage the deployment of security solutions.

Prerequisites

Students must have completed Network Security and Firewalls or be able to demonstrate equivalent knowledge.

Duration

6 hours

CIW Security Professional Series – Course 3: Security Auditing, Attacks, and Threat Analysis (November 2002)

Security Auditing, Attacks, and Threat Analysis teaches you how to conduct a security audit. It teaches you how to perform the different phases of an audit, including discovery and penetration. You will also learn how to prevent hackers from controlling your network, and how to generate effective audit reports that can help organizations improve their security and become current with industry security standards. Finally, you will learn about how to recommend industry-standard security solutions for your enterprise. As you examine different threats and learn more about how network hosts participate on a network, you will determine how to assess and manage the risk posed to each system. This course introduces various tools to help you in the auditing process; you will use some of these tools in the labs. You will also study international standards, along with time-tested methods for auditing a network efficiently. After completing this course, you will have in-depth training and experience in analyzing the hacker process and associated methodologies. You will be able to counteract attacks using specific, practical tools, including enterprise-grade security-scanning and intrusion-detection programs. You will also learn how to analyze your findings and make recommendations for establishing the best security possible in a given scenario.

Topics

Security Auditing

- Introduction to Auditing
- What Is an Auditor?
- What Does an Auditor Do?
- Auditor Roles and Perspectives
- Conducting a Risk Assessment
- Risk Assessment Stages

Discovery Methods

- Discovery
- Security Scans
- Enterprise-grade Auditing Applications
- Social Engineering
- What Information Can You Obtain?

Auditing Server Penetration and Attack Techniques

- Network Penetration
- Attack Signatures and Auditing
- Compromising Services
- Common Targets
- Routers
- Databases
- Web and FTP Servers
- E-mail Servers
- Naming Services
- Auditing for System Bugs
- Auditing Trap Doors and Root Kits
- Auditing Denial-Of-Service Attacks
- Combining Attack Strategies
- Denial of Service and the TCP/IP Stack

Security Auditing and the Control Phase

- Network Control
- Control Phase Goals
- UNIX Password File Locations
- Control Methods
- Auditing and the Control Phase

Intrusion Detection

- What Is Intrusion Detection?
- IDS Applications and Auditing
- Intrusion Detection Architecture
- IDS Rules
- IDS Actions
- False Positives
- Intrusion-Detection Software
- Purchasing an IDS
- Auditing with an IDS

Auditing and Log Analysis

- Log Analysis
- Baseline Creation
- Firewall and Router Logs
- Operating System Logs
- Filtering Logs
- Suspicious Activity
- Additional Logs
- Log Storage
- Auditing and Performance Degradation

Audit Results

- Auditing Recommendations
- Creating the Audit Report
- Improving Compliance
- Improving Router Security
- Enabling Proactive Detection
- Host Auditing Solutions
- Replacing and Updating Services
- Secure Shell (SSH)
- SSH and DNS

Target Audience

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

Prerequisites

Students must have completed *Network Security and Firewalls* or be able to demonstrate equivalent Internet knowledge.

Duration

12 hours

Job Responsibilities

Implement e-business solutions security policies; identify security threats and develop countermeasures using firewall systems and attack-recognition technologies; and manage the deployment of security solutions.