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