

Web Security Associate

Course Description

CIW Web Security Associate is for students who want to know how to secure networks from unauthorised activities. Individuals with these security skills can pursue or advance careers in many aspects of online and network security including network server administrators, firewall administrators, systems administrators, application developers and IT security officers.

This course identifies security principles and techniques that enable you to stop a hacker by understanding how to implement access control lists, operating system hardening and firewall technology. It also teaches you how to personalise your network security system so you can create a solution that adheres to universal principles, but also conforms to your business needs in responding to specific hacker attacks.

You will learn about authentication procedures, encryption standards and implementations that help ensure proper user authentication. You will also learn about the specific ports and protocols that hackers manipulate, and about direct and indirect ways to protect your network operating systems. Finally, you will learn how to respond to and report hacker activity, engage in proactive detection, and always keep your company's needs in mind.

Topics Covered

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
- Determining Backups
- 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
- Protocol Analyzers

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

Prerequisites

The CIW Web Security Associate course is designed for students with a good understanding of IT, computers and the Internet including knowledge of networks and servers to a level consistent with that found in the [CIW Web Foundations Series](#). Students should also be familiar with the Microsoft Windows

operating system before taking this course as it does not provide entry-level computer literacy. Note: This course is not compatible with Apple computers.

UKWDA Training

You can buy this course online at <http://training.ukwda.org>