Web Security Series

Web Security Associate v2.0

Web Security Associate teaches you how to secure your local and cloud network devices and communications from unauthorized activity. This course teaches you network security principles, such as establishing an effective security policy, and about the different types of cyber-attacks activities that you are most likely to encounter.

This course identifies security principles and techniques that enable you to stop a cyber-attacks by understanding how to implement access control lists, operating system hardening and firewall technology. It also teaches you how to personalize 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 cyber-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 cyber-attacks manipulate, and about direct and indirect ways to protect your network operating systems. Finally, you will learn how to respond to and report cyber-attacks activity, engage in proactive detection, and always keep your company's needs in mind. Appendixes are included in the back of this coursebook to provide resources for you as you continue to learn about applying security measures to your network.

Guided, step-by-step labs provide opportunities to practice new skills. You can challenge yourself and review your skills after each lesson with the Lesson Quizzes and Flash cards. Additional skill reinforcement is provided in the online Pre-Assessment, Activities, Lesson Quizzes, Optional Labs, Live Labs, Test Prep, Practice Exams and Post Assessment materials.

Topics

What Is Security?

Network Security Background
What Is Security? Hacker Statistics
Wireless Network Technologies and Security
Wireless Network Security Problems
Wireless Network Security Solutions
Physical and Configuration Solutions
Convergence Networking and Security
Firewall Practices Applied to Virtual LANs (VLANs)
Cyber-attacker Statistics
The Myth of 100-Percent Security
Attributes of an Effective Security Matrix
What You Are Trying to Protect

Security Threats

Who Is the Threat?
Security Threats from Trusted Users
Anonymous Downloads and Indiscriminate Link-Clicking
Security Standards
Wireless Network Modes
Wireless Application Protocol (WAP)
Site Surveys
Web 2.0 Technologies
Greynet Applications
Sensitive Data and Data Classifications
Vulnerabilities with Data at Rest
Data and Drive Sanitizing

Elements of Security

Security Elements and Mechanisms
The Security Policy
Determining Backups
Encryption
Authentication
Specific Authentication Techniques
Access Control
Auditing
Security Tradeoffs
Defense in Depth Strategies

Applied Encryptions

Reasons to Use Encryption
Creating Trust Relationships
Symmetric-Key Encryption
Symmetric Algorithms
One-Way (Hash) Encryption
Asymmetric-Key Encryption
Encryption Review
Certification Authority (CA)
Full/Whole Disk Encryption

Types of Attacks

Network Attack Categories
Brute-Force, Dictionary, and Password Spraying Attacks
Rainbow Tables, Pass-the-Hash, and Birthday Attacks
Password Storage Techniques
System Bugs and Back Doors
Malware (Malicious Software)
TLS Encryption
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
Ransomware
SQL Injection
Cross-Site Scripting (XSS)
Cross-Site Request Forgery (CSRF)
Auditing

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
Domain Name Service (DNS)
Trusted Platform Modules and MicroSoft BitLocker
Secure TCP/IP Services
Change Management

Securing Resources
TCP/IP Security Vulnerabilities
Implementing Security
Resources and Services
Protecting TCP/IP Services
Simple Mail Transfer Protocol (SMTP)
Bring Your Own Device (BYOD)
Internet of Things (IoT)
Communication Systems
Physical Security
Testing Systems
Security Testing Software
Specific tools
Security Assessments
Security and Repetition

Firewalls and Virtual Private Networks
Access Control Overview
Definition and Description of a Firewall
The Role of a Firewall
Firewall Terminology
Operating System and Network Device Hardening
Firewall Configuration Defaults
Packet Filter Rules
Packet Filter Advantages and Disadvantages
Configuring Proxy Servers
URL Filtering
Remote Access and Virtual Private Networks (VPNs)
Public Key Infrastructure (PKI)
Cloud Computing and Virtualization

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

Detecting and Distracting Cyber-attackers
Proactive Detection
Distracting the Cyber-attacker
Deterring the Cyber-attacker

Incident Response
Risk Management, mitigation, and incident response
Creating an Incident Response Policy
Determining If an Attack Has Occurred
Executing the Response Plan
Analyzing and Learning

Target Audience

The CIW *Web Security Associate* courseware teaches you how to secure your local and cloud network devices and communications from unauthorized activity. This course teaches you network security principles, such as establishing an effective security policy, and about the different types of cyber-attacker activities that you are most likely to encounter. Individuals with these security skills can pursue or advance careers in many aspects of online and network security.

Experience level from 0-3 years experience in the following job roles:

- Network server administrators
- Firewall administrators
- Systems administrators
- Application developers
- IT Security Officers

IT security officers Job Responsibilities

Secure your network from unauthorized activity; implement access control lists, operating system hardening and firewall technology; personalize your network security system; ensure proper user authentication; protect network operating systems; and respond to and report hacker activity.

Prerequisites

There are no prerequisites for the Web Security Associate course. However, students should possess Internet and networking knowledge equivalent to what is presented in the CIW Web Foundations series courses. Web Security Associate builds upon this foundational knowledge to give students the skills and knowledge to manage and protect the security of online data, from a single computer to an entire corporate network.