Web Security Associate Objectives and Locations

The *CIW Web Security Associate-v2.0* course teaches candidates how to secure their network from their unauthorized activity. The CIW Web Security Associate-v2.0 course and this appendix are designed to prepare students for the CIW Web Security Associate certification exam. Students can use this appendix as a study guide to locate content within the coursebook that corresponds to the specific CIW Web Security Associate skills objectives.

You can register for the CIW Web Security Associate certification exam by visiting Prometric at https://securereg3.prometric.com/ or Pearson | VUE at https://home.pearsonvue.com/. You can also contact your participating academic institution. For more information about the CIW Web Security Associate certification exam and CIW certifications, visit https://www.ciwcertified.com/.

Web Security Associate Objective	Lesson(s) and Section(s)
Domain 1.1: Define the significance of network security, and identify various elements of an effective security policy, including risk factors, security-related organizations, key resources to secure, general security threat types, access control.	
1.1.1 Define security.	**Lesson 1: What is Security?** - What Is Security?
1.1.2 Identify the importance of network security, including the CIA triad (Confidentiality, Integrity, and Availability).	**Lesson 1: What is Security?** - Network Security Background - Cyber-attacker Statistics
1.1.3 Identify the three types of data, at rest, in transit, and in use.	**Lesson 2: Security Threats** - Sensitive Data and Data Classifications
1.1.4 Identify potential risk factors for data security, including improper authentication.	**Lesson 1: What Is Security?** - What Is Security? - Lab 1-1: Causing a Darkcomet Trojan infection - The Myth of 100-Percent Security - Wireless Network Security Problems **Lesson 2: Security Threats** - Greynet Applications - Sensitive Data and Data Classifications - Vulnerabilities with Data at Rest - Security Threats from Trusted Users - Anonymous Downloads and Indiscriminate Link-Clicking **Lesson 9: Firewalls and Virtual Private Networks** - URL Filtering **Lesson 12: Incident Response** - Risk Management, Mitigation, and Incident Response
1.1.5 Define Risk management, mitigation, and incident response.	**Lesson 12: Incident Response** - Risk Management, Mitigation, and Incident Response

Web Security Associate Objective	Lesson(s) and Section(s)
1.1.6 Identify security-related organizations, warning services, and certifications.	**Lesson 1: What is Security?** - Cyber-attacker Statistics - IEEE 802.11 Wireless Standards **Lesson 2: Security Threats** - Security Standards
1.1.7 Identify key resources that need specialized security measures.	**Lesson 1: What is Security?** - What You Are Trying to Protect
1.1.8 Identify the general types of security threat/attacker.	**Lesson 2: Security Threats** - Who Is the Threat? - Greynet Applications
1.1.9 Identify the tradeoffs made when choosing to increase security posture, decrease cost, or improve performance.	**Lesson 3: Elements of Security** - Security Tradeoffs
1.1.10 Define the significance of a security policy and necessary sub-policies including AUP, NDA, BYOD policies.	**Lesson 3: Elements of Security** - Security Elements and Mechanisms - Security Policy **Lesson 8: Securing Resources** - Bring Your Own Device (BYOD)
1.1.11 Identify and develop basic components of an effective security policy.	**Lesson 3: Elements of Security** - Security Elements and Mechanisms - Security Policy
1.1.12 Identify the key user authentication methods.	**Lesson 2: Elements of Security** - Authentication - Specific Authentication Techniques
1.1.13 Define the significance of access control methods.	**Lesson 3: Elements of Security** - Access Control - Lab 3-1: Viewing and modifying default access control settings in Windows Server 2016
1.1.14 Define the functions of access control lists (ACLs) and execution control lists (ECLs).	**Lesson 3: Elements of Security** - Access Control - Lab 3-1: Viewing and modifying default access control settings in Windows Server 2016 - Lab 3-2: Viewing the effects of hostile JavaScript in Mozilla Firefox - Lab 3-3: Configuring execution control lists in Windows Server 2016 - Lab 3-4: Creating an execution control list for the su command in Linux
1.1.15 Identify the benefits and proper implementation of a Defense in Depth strategy.	**Lesson 3: Elements of Security** - Defense in Depth Strategy
1.1.16 Define the security objectives of Confidentiality, Integrity, and Availability.	**Lesson 1: What Is Security?** - Network Security Background
1.1.17 Define Operating System and network device hardening.	**Lesson 9: Firewalls and Virtual Private Networks** - Operating System and Network Device Hardening

Web Security Associate Objective	Lesson(s) and Section(s)
Domain 1.2: Define encryption and the encryption methods used in internetworking.	
1.2.1 Identify the three main encryption methods used in internetworking.	**Lesson 3: Elements of Security** - Encryption
1.2.2 Define symmetric (private-key) encryption.	**Lesson 4: Applied Encryption** - Symmetric-Key Encryption
1.2.3 Define asymmetric (public-key) encryption, including distribution schemes, Public Key Infrastructure (PKI).	**Lesson 4: Applied Encryption** - Asymmetric-Key Encryption **Lesson 9: Firewalls and Virtual Private Networks** - Public Key Infrastructure (PKI)
1.2.4 Define one-way hash encryption.	**Lesson 4: Applied Encryption** - One-Way (Hash) Encryption
1.2.5 Identify the importance of auditing.	**Lesson 2: Security Threats** - Site Surveys - Lab 2-1: Installing a war-driving application and analyzing a site survey capture - Lab 2-2: Analyzing traffic captured from site survey software **Lesson 3: Elements of Security** - Auditing **Lesson 5: Types of Attacks** - Auditing
1.2.6 Select security equipment and software based on ease of use.	**Lesson 1: What is Security** - Attributes of an Effective Security Matrix **Lesson 3: Elements of Security** - Security Tradeoffs
1.2.7 Identify security factors related to transmission of unencrypted data across the network.	**Lesson 3: Elements of Security** - Encryption
1.2.8 Identify the function of parallel processing in relation to cryptography.	**Lesson 4: Applied Encryption** - Creating Trust Relationships
1.2.9 Identify the significance of encryption in enterprise networks.	**Lesson 3: Elements of Security** - Encryption
1.2.10 Identify the impact of encryption protocols and procedures on system performance.	**Lesson 4: Applied Encryption** - Symmetric-Key Encryption - Symmetric Algorithms - One-Way (Hash) Encryption - Asymmetric-Key Encryption
1.2.11 Create a trust relationship using public-key cryptography.	**Lesson 4: Applied Encryption** - Creating Trust Relationships - Asymmetric-Key Encryption - Applied Encryption Processes

Web Security Associtate Objective	Lesson(s) and Section(s)
1.2.12 Identify specific forms of symmetric, asymmetric and hash encryption, including Advanced Encryption Standard (AES).	**Lesson 4: Applied Encryption** - Symmetric Algorithms - Lab 4-1: Using symmetric encryption algorithms - Asymmetric-Key Encryption - One-Way (Hash) Encryption - Applied Encryption Processes - Lab 4-2: Installing GPG4win 3.0.3 on Windows Server 2016 - Lab 4-3: Generating a key pair using GPG4win 3.0.3 - Lab 4-4: Exporting and signing public keys using GPG4win 3.0.3 - Lab 4-5: Exchanging encrypted messages using GPG4win 3.0.3 - Lab 4-6: Encrypting with GPG4win 3.0.3
1.2.13 Define a certification authority (CA) and its role related to trust between systems.	**Lesson 4: Applied Encryption** - Certification Authority (CA)
1.2.14 Identify certification authorities that offer certificates at no cost to domain owners.	**Lesson 4: Applied Encryption** - Certification Authority (CA)
Domain 1.3: Use universal guidelines and principles of effective network security to create effective specific solutions.	
1.3.1 Identify the universal guidelines and principles of effective network security.	**Lesson 6: General Security Principles** - Common Security Principles
1.3.2 Define amortization and chargeback issues related to network security architectures.	**Lesson 6: General Security Principles** - Identify Security Business Issues
1.3.3 Use universal guidelines to create effective specific solutions.	**Lesson 6: General 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 - Lab 6-1: Conducting a physical attack against a Windows 2016 server
1.3.4 Identify potential threats at different layers of the TCP/IP stack.	**Lesson 7: Protocol Layers and Security** - TCP/IP Security Introduction - The TCP/IP Stack and the OSI Reference Model - Link/Network Access Layer - Network/Internet Layer - Transport Layer - Application Layer

Web Security Associate Objective	Lesson(s) and Section(s)
1.3.5 Consistently apply security principles.	**Lesson 8: Securing Resources** - Implementing Security
1.3.6 Identify ways to protect operating systems, routers and equipment against physical attacks.	**Lesson 8: Securing Resources** - Physical Security
1.3.7 Secure TCP/IP services, including HTTP, HTTPS, FTP, SFTP, DNS, DHCP, SNMP, LDAP, Kerberos.	**Lesson 7: Protocol Layers and Security** - Transport Layer - Application Layer - Lab 7-1: Enabling TCP/IP filtering on Windows Server 2016 - Domain Name Service (DNS) **Lesson 8: Securing Resources** - Protecting TCP/IP Services - Lab 8-1: Securing an Apache2 Web server - Lab 8-2: Securing the FTP service - Simple Mail Transfer Protocol (SMTP)
1.3.8 Identify the significance of testing and evaluating systems and services, in conjunction with change management.	**Lesson 7: Protocol Layers and Security** - Change Management **Lesson 8: Securing Resources** - Testing Systems - Security Testing Software
1.3.9 Identify network security management applications, including network scanners, operating system, add-ons, log analysis tools.	**Lesson 2: Security threats** - Wireless Networking Modes **Lesson 8: Securing Resources** - Simple Mail Transfer Protocol (SMTP) - Security Testing Software
1.3.10 Define the nine types of security assessments and identify the strengths and weaknesses of each.	**Lesson 8: Securing Resources** - Security Assessments
1.3.11 Use of Full/Whole Disk Encryption along with data retention and destruction policies.	**Lesson 4: Applied Encryption** - Full/Whole Disk Encryption
1.3.12 Identify Trusted Platform Modules and Microsoft BitLocker.	**Lesson 7: Protocol Layers and Security** - Trusted Platform Modules and Microsoft BitLocker
1.3.13 Demonstrate data and drive sanitizing.	**Lesson 2: Security Threats** - Data and Drive sanitizing
1.3.14 Identify virtualization and cloud computing fundamental concepts, implementation, and security strategies.	**Lesson 9: Firewalls and Virtual Private Networks** - Cloud computing and virtualization

Web Security Associate Objective	Lesson(s) and Section(s)
Domain 1.4: Apply security principles and identify security attacks.	
1.4.1 Deploy Pretty Good Privacy (PGP)/Gnu Privacy Guard (GPG) in Windows and Linux/UNIX systems.	**Lesson 4: Applied Encryption** - Applied Encryption Processes - Lab 4-2: Installing GPG4win 3.0.3 on Windows Server 2016 - Lab 4-3: Generating a key pair using GPG4win 3.0.3 - Lab 4-4: Exporting and signing public keys using GPG4win 3.0.3 - Lab 4-5: Exchanging encrypted messages using GPG4win 3.0.3 - Lab 4-6: Encrypting files with GPG4win 3.0.3
1.4.2 Define IPSec concepts.	**Lesson 9: Firewalls and Virtual Private Networks** - Remote Access and Virtual Private Networks (VPNs)
1.4.3 Identify specific types of security attacks.	**Lesson 1: What is Security?** - Wireless Network Security Problems - Convergence Networking and Security **Lesson 2: Security Threats** - Greynet Applications - Anonymous Downloads and Indiscriminate Link-Clicking **Lesson 5: Types of Attacks** - Network Attack Categories - Brute-Force and Dictionary Attacks - Lab 5-1: Using John the Ripper in Windows Server 2016 - System Bugs and Back Doors - Malware (Malicious Software) - Lab5-2: Conducting a virus scan in Windows to help thwart attacks - Social Engineering Attacks - Lab 5-3: Sending fake email messages - Denial-of-Service (DoS) Attacks - Distributed Denial-of-Service (DDoS) Attacks - Lab 5-4: Analyzing a SYN flood in a packet sniffer - Lab 5-5: Identifying network-based attacks - Spoofing Attacks - Scanning Attacks - Lab 5-6: Using Nmap to scan a system in Windows Server 2016 - Man-in-the-Middle Attacks - Lab 5-7: Conducting a man-in-the-middle attack - Bots and Botnets - SQL Injection
1.4.4 Identify Password attacks including Dictionary, Brute Force, Rainbow Tables, Pass the Hash, and Birthday Attacks.	**Lesson 5: Types of Attacks** - Brute-Force and Dictionary Attacks
1.4.5 Implementing password storage techniques to include PBKDF2, Bcrypt, salting, and key stretching.	**Lesson 5: Types of Attacks** - Password storage techniques

Web Security Associate Objective	Lesson(s) and Section(s)
1.4.6 Identify routing issues and security.	**Lesson 5: Types of Attacks** - Man-in-the-Middle Attacks **Lesson 7: Protocol Layers and Security** - Network/Internet Layer - Application Layer **Lesson 9: Firewalls and Virtual Private Networks** - Firewall Terminology **Lesson 10: Levels of Firewall Protection** - Hardware Issues
1.4.7 Determine the causes and results of a denial-of-service (DOS) attack and Distributed Denial of Service (DDoS).	**Lesson 5: Types of Attacks** - Distributed Denial-of-Service (DDOS) Attacks - Lab 5-4: Analyzing a SYN flood in a packet sniffer **Lesson 7: Protocol Layers and Security** - Network/Internet Layer - Application Layer **Lesson 8: Securing Resources** - Protecting TCP/IP Services - Simple Mail Transfer Protocol (SMTP)
1.4.8 Recognize attack incidents.	**Lesson 1: What is Security?** - Convergence Networking and Security **Lesson 5: Types of Attacks** - System Bugs and Back Doors - Distributed Denial-of-Service (DDoS) Attacks - Lab 5-4: Analyzing a SYN flood in a packet sniffer - Lab 5-5: Identifying network-based attacks
1.4.9 Distinguish between illicit servers and trojans.	**Lesson 5: Types of Attacks** - Malware (Malicious Software)
1.4.10 Deploy a web server configured to use TLS encryption.	**Lesson 5: Types of Attacks** - TLS encryption
Subdomain 1.5: Identify firewall types and define common firewall terminology.	
1.5.1 Define the purpose and function of various firewall types.	**Lesson 9: Firewalls and Virtual Private Networks** - Definition and Description of a Firewall **Lesson 10: Levels of Firewall Protection** - Designing a Firewall - Types of Bastion Hosts - Common Firewall Designs
1.5.2 Define the role a firewall plays in a company's security policy.	**Lesson 9: Firewalls and Virtual Private Networks** - The Role of a Firewall
1.5.3 Define common firewall terms.	**Lesson 9: Firewalls and Virtual Private Networks** - Firewall Terminology **Lesson 10: Levels of Firewall Protection** - Designing a Firewall
1.5.4 Identify packet filters and their features.	**Lesson 9: Firewalls and Virtual Private Networks** - Firewall Terminology

Web Security Associate Objective	Lesson(s) and Section(s)
1.5.5 Identify circuit-level gateways and their features.	**Lesson 9: Firewalls and Virtual Private Networks** - Firewall Terminology
1.5.6 Identify application-level gateways and their features.	**Lesson 9: Firewalls and Virtual Private Networks** - Firewall Terminology
1.5.7 Identify features of a packet-filtering firewall, including rules, stateful multi-layer inspection.	**Lesson 9: Firewalls and Virtual Private Networks** - Packet Filter Rules - Packet Filter Advantages and Disadvantages
1.5.8 Identify fundamental features of a proxy-based firewall (e.g.; service redirection, service passing, gateway daemons), and implement proxy-level firewall security.	**Lesson 9: Firewalls and Virtual Private Networks** - Firewall Terminology - Configuring Proxy Servers - Lab 9-3: Configuring a proxy server in Windows Server 2016 - URL Filtering
1.5.9 Define the importance of proxy caching related to performance.	**Lesson 9: Firewalls and Virtual Private Networks** - Firewall Terminology - Configuring Proxy Servers
1.5.10 Identify how firewall practices apply to Virtual LANs (VLANs).	**Lesson 1: What is Security?** - Firewall Practices Applied to Virtual LANs (VLANs)
Subdomain 1.6: Plan a firewall system that incorporates multiple levels of protection, including firewall system design, proactive detection, setting traps, security breach response, security alerting organizations.	
1.6.1 Implement a packet-filtering firewall.	**Lesson 9: Firewalls and Virtual Private Networks** - Packet Filter Rules - Packet Filter Advantages and Disadvantages - Lab 9-1: Installing WinRoute Firewall in Windows Server 2016 - Lab 9-2: Configuring packet filtering rules **Lesson 10: Levels of Firewall Protection** - Putting It All Together - Lab 10-1: Creating an internal network with WinRoute Firewall (*instructor-led*) - Lab 10-2: Denying HTTP access (*instructor-led*) - Lab 10-3: Configuring an FTP packet-filtering rule for a specific host (*instructor-led*)
1.6.2 Customize your network to manage cyber-attacks activity.	**Lesson 3: Elements of Security** - Determining Backups **Lesson 9: Firewalls and Virtual Private Networks** - Configuring Proxy Servers - Lab 9-3: Configuring a proxy server in Windows Server 2016 - Remote Access and Virtual Private Networks (VPNs) **Lesson 10: Levels of Firewall Protection** - Hardware Issues - Common Firewall Designs **Lesson 11: Detecting and Distracting Cyber-Attackers** - Proactive Detection - Distracting the Cyber-attacker

Web Security Associate Objective	Lesson(s) and Section(s)
1.6.3 Implement proactive detection.	**Lesson 11: Detecting and Distracting Cyber-Attackers** - Proactive Detection
1.6.4 Distract Cyber-attackers and contain their activity.	**Lesson 11: Detecting and Distracting Cyber-Attackers** - Distracting the Cyber-Attacker - Deterring the Cyber-Attacker
1.6.5 Deploy tripwires and other traps on a network host.	**Lesson 11: Detecting and Distracting Cyber-Attackers** - Distracting the Cyber-Attacker - Lab 11-1: Setting a logon tripwire script in Windows Server 2016 - Lab 11-2: Using Tripwire for Linux
1.6.6 Respond appropriately to a security breach.	**Lesson 12: Incident Response** - Creating an Incident Response Policy - Determining if an Attack Has Occurred - Executing the Response Plan - Analyzing and Learning
1.6.7 Identify security organizations that can help in case of system attack.	**Lesson 12: Incident Response** - Executing the Response Plan
1.6.8 Subscribe to respected security alerting organizations.	**Lesson 12: Incident Response** - Executing the Response Plan - Lab 12-1: Subscribing to security mailing lists
1.6.9 Identify appropriate authorities to contact regarding data theft and other attacks.	**Lesson 12: Incident Response** - Executing the Response Plan