CIW Security Associate

Exam 1D0-671 Objectives

Domain 1: Web Security Associate

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.

1.1.2: Identify the importance of network security, including the CIA triad (Confidentiality, Integrity, and Availability).

1.1.3: Identify the three types of data, at rest, in transit, and in use.

1.1.4: Identify potential risk factors for data security, including improper authentication.

1.1.5: Define Risk management, mitigation, and incident response.

1.1.6: Identify security-related organizations, warning services, and certifications.

1.1.7: Identify key resources that need specialized security measures.

1.1.8: Identify the general types of security threat/attacker.

1.1.9: Identify the tradeoffs made when choosing to increase security posture, decrease cost, or improve performance.

1.1.10: Define the significance of a security policy and necessary sub-policies including AUP, NDA, BYOD policies.

1.1.11: Identify and develop basic components of an effective security policy.

1.1.12: Identify the key user authentication methods.

1.1.13: Define the significance of access control methods.

1.1.14: Define the functions of access control lists (ACLs) and execution control lists (ECLs).

1.1.15: Identify the benefits and proper implementation of a Defense in Depth strategy.

1.1.16: Define the security objectives of Confidentiality, Integrity, and Availability.

1.1.17: Define Operating System and network device hardening.

1.2: Define encryption and the encryption methods used in internetworking.

1.2.1: Identify the three main encryption methods used in internetworking.

1.2.2: Define symmetric (private-key) encryption.

1.2.3: Define asymmetric (public-key) encryption, including distribution schemes, Public Key Infrastructure (PKI).

1.2.4: Define one-way hash encryption.

1.2.5: Identify the importance of auditing.

1.2.6: Select security equipment and software based on ease of use.

1.2.7: Identify security factors related to transmission of unencrypted data across the network.

1.2.8: Identify the function of parallel processing in relation to cryptography.

1.2.9: Identify the significance of encryption in enterprise networks.

1.2.10: Identify the impact of encryption protocols and procedures on system performance.

1.2.11: Create a trust relationship using public-key cryptography.

1.2.12: Identify specific forms of symmetric, asymmetric and hash encryption, including Advanced Encryption Standard (AES).

1.2.13: Define a certification authority (CA) and its role related to trust between systems.

1.2.14: Identify certification authorities that offer certificates at no cost to domain owners.

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.

1.3.2: Define amortization and chargeback issues related to network security architectures.

1.3.3: Use universal guidelines to create effective specific solutions.

1.3.4: Identify potential threats at different layers of the TCP/IP stack.

1.3.5: Consistently apply security principles.

1.3.6: Identify ways to protect operating systems, routers and equipment against physical attacks.

1.3.7: Secure TCP/IP services, including HTTP, HTTPS, FTP, SFTP, DNS, DHCP, SNMP, LDAP, Kerberos.

1.3.8: Identify the significance of testing and evaluating systems and services, in conjunction with change management.

1.3.9: Identify network security management applications, including network scanners, operating system, add-ons, log analysis tools.

1.3.10: Define the nine types of security assessments and identify the strengths and weaknesses of each.

1.3.11: Use of Full/Whole Disk Encryption along with data retention and destruction policies.

1.3.12: Identify Trusted Platform Modules and Microsoft BitLocker.

1.3.13: Demonstrate data and drive sanitizing.

1.3.14: Identify virtualization and cloud computing fundamental concepts, implementation, and security strategies.

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.

1.4.2: Define IPSec concepts.

1.4.3: Identify specific types of security attacks.

1.4.4: Identify Password attacks including Dictionary, Brute Force, Rainbow Tables, Pass the Hash, and Birthday Attacks.

1.4.5: Implementing password storage techniques to include PBKDF2, Bcrypt, salting, and key stretching.

1.4.6: Identify routing issues and security.

1.4.7: Determine the causes and results of a denial-of-service (DOS) attack and Distributed Denial of Service (DDoS).

1.4.8: Recognize attack incidents.

1.4.9: Distinguish between illicit servers and trojans.

1.4.10: Deploy a web server configured to use TLS encryption.

1.5: Identify firewall types and define common firewall terminology.

1.5.1: Define the purpose and function of various firewall types.

1.5.2: Define the role a firewall plays in a company's security policy.

1.5.3: Define common firewall terms.

1.5.4: Identify packet filters and their features.

1.5.5: Identify circuit-level gateways and their features.

1.5.6: Identify application-level gateways and their features.

1.5.7: Identify features of a packet-filtering firewall, including rules, stateful multi-layer inspection.

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.

1.5.9: Define the importance of proxy caching related to performance.

1.5.10: Identify how firewall practices apply to Virtual LANs (VLANs).

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.

1.6.2: Customize your network to manage cyber-attacks activity.

1.6.3: Implement proactive detection.

1.6.4: Distract Cyber-attackers and contain their activity.

1.6.5: Deploy tripwires and other traps on a network host.

1.6.6: Respond appropriately to a security breach.

1.6.7: Identify security organizations that can help in case of system attack.

1.6.8: Subscribe to respected security alerting organizations.

1.6.9: Identify appropriate authorities to contact regarding data theft and other attacks.