Wireless LAN Security Exam (CWSP-205) Objectives

Introduction

The CWSP-205 exam, covering the 2015 objectives, will certify that the successful candidate understands the security weaknesses inherent in WLANs, the solutions available to address those weaknesses, and the steps necessary to implement a secure and manageable WLAN in an enterprise environment. With a valid CWNA certification, Exam CWSP-205 is required to earn the CWSP certification:

The skills and knowledge measured by this examination are derived from a survey of wireless networking experts from around the world. The results of this survey were used in weighing the subject areas and ensuring that the weighting is representative of the relative importance of the content.

The following chart provides the breakdown of exam as to the weight of each section of the exam.

Wireless LAN Security Subject Area	**% of Exam**
Wireless Network Attacks and Threat Assessment	20%
Security Policy	5%
Wireless LAN Security Design and Architecture	50%
Monitoring and Management	25%
Total	**100%**

CWNP Authorized Materials Use Policy

CWNP does not condone the use of unauthorized 'training materials', aka 'brain dumps'. Individuals who utilize such materials to pass CWNP exams will have their certifications revoked. In an effort to more clearly communicate CWNP's policy on use of unauthorized study materials, CWNP directs all certification candidates to the CWNP Candidate Conduct Policy at:

http://www.cwnp.com/exams/CWNPCandidateConductPolicy.pdf

Please review this policy before beginning the study process for any CWNP exam. Candidates will be required to state that they understand and have abided by this policy at the time of exam delivery. If a candidate has a question as to whether study materials are considered "brain dumps", he/she should perform a search using CertGuard's engine, found here: http://www.certguard.com/search.asp

1.0 Wireless Network Attacks and Threat Assessment – 20%

1.1 Describe general network attacks common to wired and wireless networks, including DoS, phishing, protocol weaknesses and configuration error exploits.

1.2 Recognize common attacks and describe their impact on WLANs, including PHY and MAC DoS, hijacking, unauthorized protocol analysis and eavesdropping, social engineering, man-in-the-middle, authentication and encryption cracks and rogue hardware.

1.3 Execute the preventative measures required for common vulnerabilities on wireless infrastructure devices, including weak/default passwords on wireless infrastructure equipment and misconfiguration of wireless infrastructure devices by administrative staff.

1.4 Describe and perform risk analysis and risk mitigation procedures, including asset management, risk ratings, loss expectancy calculations and risk management planning.

1.5 Explain and demonstrate the security vulnerabilities associated with public access or other unsecured wireless networks, including the use of a WLAN for spam transmission, malware injection, information theft, peer-to-peer attacks and Internet attacks.

2.0 Security Policy – 5%

2.1 Explain the purpose and goals of security policies including password policies, acceptable use policies, WLAN access policies, personal device policies, device management (APs, infrastructure devices and clients) and security awareness training for users and administrators.

2.2 Summarize the security policy criteria related to wireless public access network use including user risks related to unsecured access and provider liability.

2.3 Describe how devices and technology used from outside an organization can impact the security of the corporate network including topics like BYOD, social networking and general MDM practices.

3.0 Wireless LAN Security Design and Architecture – 50%

3.1 Describe how wireless network security solutions may vary for different wireless network implementations including small businesses, home offices, large enterprises, public networks and remote access.

3.2 Understand and explain 802.11 Authentication and Key Management (AKM) components and processes including encryption keys, handshakes and pre-shared key management.

3.3 Define and differentiate among the 802.11-defined secure networks, including pre-RSNA security, Transition Security Networks (TSN) and Robust Security Networks (RSN) and explain the relationship of these networks to terms including RSNA, WPA and WPA2.

3.4 Identify the purpose and characteristics of IEEE 802.1X and EAP and the processes used including EAP types (PEAP, EAP-TLS, EAP-TTLS, EAP-FAST and EAP-SIM), AAA servers (RADIUS) and certificate management.

3.5 Recognize and understand the common uses of VPNs in wireless networks, including remote APs, VPN client access, WLAN controllers and cloud architectures.

3.6 Describe centrally-managed client-side security applications, including VPN client software and policies, personal firewall software, mobile device management (MDM) and wireless client utility software.

3.7 Describe and demonstrate the use of secure infrastructure management protocols, including HTTPS, SNMP, secure FTP protocols, SCP and SSH.

3.8 Explain the role, importance, and limiting factors of VLANs and network segmentation in an 802.11 WLAN infrastructure.

3.9 Understand additional security features in WLAN infrastructure and access devices, including management frame protection, Role-Based Access Control (RBAC), Fast BSS transition (pre-authentication and OKC), physical security methods and Network Access Control (NAC).

3.10 Explain the purpose, methodology, features, and configuration of guest access networks and BYOD support, including segmentation, guest management, captive portal authentication and device management.

4.0 Monitoring, Management, and Tracking – 25%

4.1 Explain the importance of ongoing WLAN monitoring and the necessary tools and processes used as well as the importance of WLAN security audits and compliance reports.

4.2 Understand how to use protocol and spectrum analyzers to effectively evaluate secure wireless networks including 802.1X authentication troubleshooting, location of rogue security devices and identification of non-compliant devices.

4.3 Understand the common features and components of a Wireless Intrusion Prevention Systems (WIPS) and how they are used in relation to performance, protocol, spectrum and security analysis.

4.4 Describe the different types of WLAN management systems and their features, including network discovery, configuration management, firmware management, audit management, policy enforcement, rogue detection, network monitoring, user monitoring, event alarms and event notifications.

4.5 Describe and implement compliance monitoring, enforcement, and reporting. Topics include industry requirements, such as PCI-DSS and HIPAA, and general government regulations.

CWSP Terminology

In addition to the preceding objectives, the following security specialty terms should be clearly understood by CWSP-205 exam candidates:

802.11r
802.11w
802.1X
Access Control List (ACL)
Access Point (AP)
Advanced Encryption Standard (AES)
Alarms
Asymmetric Encryption
Authentication
Authentication and Key Management (AKM)
Authentication Header (AH)
Authentication Server

Authentication, Authorization and Accounting (AAA)
Authenticator
Authorization
Availability
Bring Your Own Device (BYOD)
Certificate Authority (CA)
Compliance
Confidentiality
Counter-Mode/CBC Mac Protocol (CCMP)
Denial of Service (DoS)
Discovery
Distributed DoS (DDoS)
EAP Flexible Authentication via Secure Tunneling (EAP-FAST)
EAP Subscriber Identity Module (EAP-SIM)
EAP Transport Layer Security (EAP-TLS)
EAP Tunneled TLS (EAP-TTLS)
Eavesdropping
Encapsulated Security Payload (ESP)
Encryption
Evil Twin
Extensible Authentication Protocol (EAP)
Fast Basic Service Set (BSS) Transition
File Transfer Protocol (FTP)
Firewall
Firmware
Hashing
Health Insurance Portability and Accountability Act (HIPAA)
Hijacking
Hypertext Transfer Protocol over SSL (HTTPS)
Infrastructure
Integrity
Interference
Internet Protocol (IP)
Intrusion Detection System (IDS)
IP Security (IPSec)
Lightweight EAP (LEAP)
Location-Based Access Control (LBAC)
MAC Filter
Malware
Man-in-the-middle
Medium Access Control (MAC)
Mobile Device Management (MDM)
Network Access Control (NAC)
Notifications
Opportunistic Key Caching (OKC)
Payment Card Industry (PCI) Data Security Standard (DSS)
Peer-to-Peer
Phishing
Physical Layer (PHY)
Policy
Pre-authentication
Private Key
Protected EAP (PEAP)
Protocol analysis
Public Key
Public Key Infrastructure (PKI)

RADIUS (Remote Authentication Dial-In User Service)
Risk
Rivest Cipher 4 (RC4)
Robust Security Network (RSN)
Rogue
Role-Based Access Control (RBAC)
Secure Copy (SCP)
Secure FTP (SFTP)
Secure Shell (SSH)
Secure Sockets Layer (SSL)
Service Level Agreement (SLA)
Simple Network Management Protocol (SNMP)
Social Engineering
Spam
Spectrum analysis
Supplicant
Symmetric Encryption
Temporal Key Integrity Protocol (TKIP)
TACACS/TACACS+
Threat
Transition Security Network (TSN)
Virtual Local Area Network (VLAN)
Virtual Private Network (VPN)
Vulnerability
War Driving
Wi-Fi Protected Access (WPA)
Wi-Fi Protected Access v2 (WPA2)
Wi-Fi Protected Setup (WPS)
Wired Equivalent Privacy (WEP)
Wireless Intrusion Prevention System (WISP)
Wireless Local Area Network (WLAN)