

Introduction

The PW0-200 exam, covering the 2008 objectives, will certify that the successful candidate understands the security weaknesses inherent in wireless LANs, the solutions available to address those weaknesses, and the steps necessary to implement a secure and manageable wireless LAN in an enterprise environment. Exam PW0-200 is one of two exams that are required to earn the CWSP certification:

- Exam PW0-100 – Wireless LAN Administration
- Exam PW0-200 – Wireless LAN Security

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 PW0-200 as to the weight of each section of the exam.

Wireless LAN Security Subject Area	% Of Exam
Wireless Network Attacks	10%
Monitoring, Management, and Tracking	25%
Security Design and Architecture	50%
Threat Assessment and Security Policy	5%
Fast BSS Transition (Fast/Secure Roaming)	10%
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>

Wireless Network Attacks – 10%

- 1.1 Demonstrate how to recognize, perform, and/or prevent the following types of attacks:
 - Physical layer denial-of-service (DoS)
 - MAC layer denial-of-service (DoS)
 - Physical damage or theft
 - MAC layer protocol attacks
 - Rogue infrastructure hardware placement
 - MAC spoofing
 - Hijacking, Phishing, and other peer-to-peer
 - Eavesdropping
 - Authentication and encryption cracking
 - Management interface exploits
 - Social engineering

- 1.2 Explain the commonality and demonstrate the simplicity of the following attacks against wireless infrastructure devices:
 - Weak/default passwords on wireless infrastructure equipment
 - Misconfiguration of wireless infrastructure devices by administrative staff
 - Describe and demonstrate preventative measures against attacks on wireless infrastructure devices

- 1.3 Explain and demonstrate the use of protocol analysis to capture the following sensitive information:
 - Usernames / Passwords / SNMP Community Strings / X.509 certificates
 - Encryption keys / Passphrases
 - MAC addresses / IP addresses
 - Describe and demonstrate preventative measures against protocol analysis

- 1.4 Explain and/or demonstrate security protocol circumvention against the following types of authentication and/or encryption:
 - WEP (Any key length)
 - Shared Key Authentication
 - WPA-Personal / WPA2-Personal
 - LEAP
 - PPTP

- 1.5 Explain and demonstrate the following security vulnerabilities associated with public access or other unsecured wireless networks:
 - Spamming through the WLAN
 - Malware (viruses / spyware / adware / remote control)
 - Direct Internet attacks through the WLAN
 - Placement of illegal content
 - Information theft

Monitoring, Management, and Tracking – 20%

- 2.1 Understand how to select laptop-based protocol and spectrum analyzers based on their security features and how to use each effectively to secure wireless networks.
- 2.2 Describe the different types of 802.11 Wireless Intrusion Prevention Systems (WIPS):
 - WIPS Integrated within a WLAN Controller
 - Overlay WIPS – with dedicated sensors and AP integration
 - WIPS with Integrated Spectrum Analysis
- 2.3 Explain 802.11 WIPS baselining and demonstrate the following tasks:
 - Measuring performance parameters under normal network conditions
 - Understanding common false positives for a specific network configuration
 - Configuring the WIPS to recognize all APs in the area as authorized, external, or rogue so that rogues can be easily and quickly identified
- 2.4 Describe and understand security features of 802.11 WIPS:
 - Device detection, classification, and behavior analysis
 - Rogue Triangulation, RF Fingerprinting, Time Difference of Arrival (TDoA), and Trilateration techniques for real-time device and interference tracking
 - Event alerting, notification, and categorization
 - Policy enforcement and violation reporting
 - Wired/Wireless intrusion mitigation
 - Protocol analysis with filtering
 - Rogue containment and remediation
 - Data forensics
- 2.5 Describe and demonstrate the different types of WLAN management systems and their features:
 - Network discovery
 - Multi-vendor configuration and firmware management
 - Audit management and policy enforcement
 - Network and user monitoring
 - Rogue detection
 - Event alarms and notification
- 2.6 Describe and implement compliance monitoring, enforcement, and reporting
 - Industry requirements (PCI)
 - Government regulations

Security Design and Architecture – 50%

- 3.1 Describe wireless network security models
 - Hotspot / Public Access
 - Small Office / Home Office
 - Small and Medium Business
 - Enterprise
- 3.2 Recognize and understand the following basic security concepts:

- 802.11 Authentication and Key Management (AKM) components and processes
- Robust Security Networks (RSN) and RSN Associations (RSNA)
- Pre-RSNA Security
- Transition Security Networks (TSN)
- RSN Information Elements
- How WPA and WPA2 certifications relate to 802.11 standard terminology and technology
- Functionality and weaknesses of WEP
- Functional parts of TKIP and its differences from WEP
- The role of TKIP/RC4 in WPA implementations
- The role of CCMP/AES in WPA2 implementations
- TKIP compatibility between WPA and WPA2 implementations
- Appropriate use and configuration of WPA-Personal and WPA-Enterprise
- Appropriate use and configuration of WPA2-Personal and WPA2-Enterprise
- Feasibility of WPA-Personal and WPA2-Personal exploitation

3.3 Identify the purpose and characteristics of 802.1X and EAP:

- Supplicant, authenticator, and authentication server roles
- Functions of the authentication framework and controlled/uncontrolled ports
- How EAP is used with 802.1X port-based access control for authentication
- Strong EAP types used with 802.11 WLANs:
 - PEAPv0/EAP-TLS and PEAPv0/EAP-MSCHAPv2
 - PEAPv1/EAP-GTC
 - EAP-TLS
 - EAP-TTLS/MS-CHAPv2
 - EAP-FAST
- Explain the exploits of specific EAP types:
 - LEAP
 - EAP-MD5

3.4 Recognize and understand the following concepts about VPNs:

- Common uses of VPN technology in wireless networks
 - Remote AP
 - VPN client software
 - WLAN Controllers

3.5 Describe and demonstrate configuration of centrally-managed client-side security software applications:

- VPN policies
- Personal firewall software

3.6 Describe and demonstrate the use of secure infrastructure management protocols:

- HTTPS
- SNMPv3
- SFTP (FTP/SSL or FTP/SSH)
- SCP
- SSH2

3.7 Explain the role and importance of VLANs in an 802.11 WLAN infrastructure.

- 3.8 Describe and demonstrate configuration of 802.1Q VLANs on Ethernet switches and WLAN infrastructure devices.
- 3.9 Explain the purpose and features of Role Based Access Control (RBAC), including the configuration of RBAC in WLAN Controllers.
- 3.10 Describe and demonstrate the following types of authentication servers and user databases used with 802.11 WLANs:
- RADIUS Types (external and integrated)
 - RADIUS Deployment Options
 - Directory Services Deployment Options
- 3.11 Explain what an AAA server is and explain the following concepts of AAA servers:
- EAP support for 802.11 networks
 - Proxy services
 - Directory Service Integration
 - Applying user and AAA server credential types (Username/Password, Certificate, Protected Access Credentials (PACs), & Biometrics)
 - The role of AAA services in wireless client VLAN assignments
 - Benefits of mutual authentication between supplicant and authentication server
- 3.12 Explain 802.11 Authentication and Key Management, including:
- Master Session Key (MSK) generation
 - PMK generation and distribution
 - GMK generation
 - PTK / GTK generation & distribution
 - 4-Way Handshake
 - Group Handshake
 - PeerKey Handshake
 - Passphrase-to-PSK mapping
- 3.13 Describe strengths, weaknesses, appropriate applications, and scalability issues of WLAN controllers, access points, WLAN bridges, and WLAN mesh platforms.
- 3.14 Describe and demonstrate configuration of major security features in WLAN controllers, access points, WLAN bridges, and WLAN mesh platforms:
- Layer 2-7 Role Based Access Control (per user or per group)
 - Fast BSS transition in an RSN
 - 802.1Q VLANs and trunking
 - Hot standby/failover and clustering support
 - WPA/WPA2 Personal and Enterprise
 - Secure management interfaces (HTTPS, SNMPv3, SSH2)
 - Intrusion detection and prevention
- 3.15 Explain the benefits of using and demonstrate how to configure management frame protection in access points and WLAN controllers.
- 3.16 Explain where infrastructure devices fit into an enterprise WLAN topology.
- 3.17 Explain the reason for network segmentation and its limiting factors on WLAN network design.

- 3.18 Explain the functional differences and advantages of both directly-connected and distributed APs in a Split-MAC (WLAN controllers with lightweight APs) WLAN architecture.
- 3.19 Explain the impact of L2, L3, and L7 security protocols on client roaming.
- 3.20 Explain the purpose, features, advantages, disadvantages, and configuration of Captive Portal (Web) Authentication implementations using WLAN controllers.
 - Use of user-based authentication methods
 - Use of secure authentication protocols
 - Use as guest access in corporate deployments

Threat Assessment and Security Policy – 5%

- 4.1 Explain the purpose and goals of the following WLAN security policies:
 - Password policy
 - End-user and administrator training on security solution use and social engineering mitigation
 - Internal security marketing campaigns to heighten awareness
 - Periodic network security audits
 - Acceptable network use & abuse policy
 - Use of Role Based Access Control (RBAC) and traffic filtering
 - Obtaining the latest security feature sets through firmware and software upgrades
 - Consistent implementation procedure through creation and maintenance of a WLAN security checklist
 - Centralized implementation and management guidelines and procedures
 - Inclusion in asset and change management programs
- 4.2 Perform a risk assessment for a WLAN, including asset risk assessment and legal implication assessment.
- 4.3 Perform a baseline analysis of a series of WLAN attack scenarios and discuss their impact on the organization. Attacks include the following:
 - Information theft and placement
 - Physical device damage or theft
 - PHY and MAC Denial of Service (DoS)
 - Client hijacking
 - Protocol analysis (eavesdropping)
 - MAC layer protocol attacks
 - Social engineering
 - Man-in-the-middle
 - Authentication and encryption cracking
 - Infrastructure hardware theft
 - Management interface exploits
 - Rogue infrastructure hardware placement
- 4.4 Describe appropriate installation locations for and remote connectivity to WLAN devices in order to avoid physical theft, tampering, and eavesdropping. Considering the following:
 - Physical security implications of infrastructure device placement
 - Secure remote connections to WLAN infrastructure devices
- 4.5 Explain the importance and implementation of client-side security applications:
 - VPN client software and policies
 - Personal firewall software

- 802.1X/EAP supplicant software
- 4.6 Explain the importance of on-going WLAN monitoring and documentation:
- Explain the necessary hardware and software for on-going WLAN security monitoring
 - Explain the necessary criteria for on-going WLAN security audits and reporting
 - Implement and conduct timely and consistent reporting procedures
- 4.7 Summarize the security policy criteria related to wireless public-access network use.
- 4.8 Given a set of business requirements, design a scalable and secure WLAN solution considering the following security parameters:
- Continuous intrusion monitoring and containment
 - Use of Role Based Access Control (RBAC) and traffic filtering
 - Scalable network design
 - Use of strong encryption, scalable authentication, and fast BSS transition

Fast BSS Transition (Fast/Secure Roaming) – 10%

- 5.1 Describe and implement 802.11i Authentication and Key Management (AKM) including the following:
- Preauthentication
 - PMK Caching
- 5.2 Describe and implement Opportunistic Key Caching and explain the enhancements beyond 802.11i AKM.
- Key Architecture
- 5.3 Describe and implement 802.11r Authentication and Key Management (AKM) and compare and contrast 802.11r enhancements beyond 802.11i AKM and Opportunistic Key Caching.
- Fast BSS Transition (FT) Key Architecture
 - Key Nomenclature
 - Initial Mobility Domain Association
 - Over-the-Air Transition
 - Over-the-DS Transition
- 5.4 Describe applications of Fast BSS transition.
- 5.5 Describe and implement non-traditional roaming mechanisms.
- Single Channel Architecture (SCA) WLAN controllers with lightweight APs
 - Infrastructure-controlled handoff
- 5.6 Describe how 802.11k Radio Resource Measurement factors into fast BSS transition.
- Neighbor Reports
 - Contrasting SCA and MCA Architectures
- 5.7 Describe the importance, application, and functionality of Wi-Fi Voice-Personal product certification.