Introduction

The PW0-204 exam, covering the 2010 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. Exam PW0-204 is one of two exams that are required to earn the CWSP certification:

- Exam PW0-104 – Wireless LAN Administration
- Exam PW0-204 – 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 PW0-204 as to the weight of each section of the exam.

Wireless LAN Security Subject Area	% of Exam
Wireless Network Attacks and Threat Assessment	10%
Monitoring and Management	25%
Security Design and Architecture	50%
Security Policy	5%
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 and Threat Assessment – 10%

1.1   Demonstrate how to recognize, perform, and prevent the following types of attacks, and discuss their impact on the organization:

- Information theft and placement
- Physical device damage or theft
- PHY and MAC Denial of Service (DoS)
- Client hijacking, phishing, and other peer-to-peer attacks
- Protocol analysis (eavesdropping)
- MAC layer protocol attacks
- Social engineering
- Man-in-the-middle
- Authentication and encryption cracking
- Management interface exploits
- Rogue infrastructure hardware placement

1.2   Understand the probability of, demonstrate the methodology of, and execute the preventative measures against the following attacks on wireless infrastructure devices:

- Weak/default passwords on wireless infrastructure equipment
- Misconfiguration of wireless infrastructure devices by administrative staff

1.3   Explain and demonstrate the use of protocol analyzers to capture the following sensitive information:

- Usernames / Passwords / SNMP Community Strings / X.509 certificates
- Encryption keys / Passphrases
- MAC addresses / IP addresses
- Unencrypted data

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   Perform a risk assessment for a WLAN, including:

- Asset risk
- Legal implications
- Regulatory compliance

1.6   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

- Peer-to-peer attack

Monitoring, Management, and Tracking – 25%

2.1 Understand how to use laptop-based protocol and spectrum analyzers to effectively troubleshoot and secure wireless networks.

2.2 Describe the use, configuration, and components of an 802.11 Wireless Intrusion Prevention Systems (WIPS):

- WIPS server software or appliance
- Dedicated sensor hardware/software
- Access points as part-time sensors
- Access points with dedicated sensor radios
- Integration between WLAN controller and WIPS server
- Deployment strategies: overlay and integrated
- Performance and security analysis
- Protocol and spectrum analysis

2.3 Explain 802.11 WIPS baselining and demonstrate the following tasks:

- Measuring performance parameters under normal network conditions
- Understand common reasons for false positives and false negatives
- Configuring the WIPS to recognize all APs and client stations in the area as authorized, external, or rogue

2.4 Describe and understand common security features of 802.11 WIPS:

- Device detection, classification, and behavior analysis
- Rogue Triangulation, RF Fingerprinting, and Time Difference of Arrival (TDoA) 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
- 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 / Guest Access
- Small Office / Home Office
- Small and Medium Enterprise
- Large Enterprise
- Remote Access: Mobile User and Branch Office

3.2   Recognize and understand the following 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
- 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
- Appropriate use and configuration of Per-user Pre-shared Key (PPSK)
- 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
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
  - EAP-TLS
  - EAP-TTLS/MS-CHAPv2
  - EAP-FAST

3.4   Recognize and understand the common uses of VPNs in wireless networks, including:

  - Remote AP
  - VPN client software
  - WLAN Controllers

3.5   Describe, demonstrate, and configure centrally-managed client-side security applications:

- VPN policies
- Personal firewall software
- Wireless client utility 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, importance, and limiting factors of VLANs and network segmentation in an 802.11 WLAN infrastructure.

3.8   Describe, configure, and deploy a AAA server and explain the following concepts related to AAA servers:

- RADIUS server
- Integrated RADIUS services within WLAN infrastructure devices
- RADIUS deployment strategies
- RADIUS proxy services
- LDAP Directory Services integration deployment strategies
- EAP support for 802.11 networks
- Applying user and AAA server credential types (Usernames/Passwords, X.509 Certificates, Protected Access Credentials (PACs), & Biometrics)
- The role of AAA services in wireless client VLAN assignments
- Benefits of mutual authentication between supplicant and authentication server

3.9   Explain frame exchange processes and the purpose of each encryption key within 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
- Passphrase-to-PSK mapping

3.10   Describe and configure major security features in WLAN infrastructure devices:

- Role Based Access Control (RBAC) (per-user or per-group)
- Location Based Access Control (LBAC)
- Fast BSS transition in an RSN
- 802.1Q VLANs and trunking on Ethernet switches and WLAN infrastructure devices
- Hot standby/failover and clustering support
- WPA/WPA2 Personal and Enterprise
- Secure management interfaces (HTTPS, SNMPv3, SSH2)
- Intrusion detection and prevention
- Remote access (branch office and mobile users)

3.11   Explain the benefits of and configure management frame protection (802.11w) in access points and WLAN controllers.

3.12   Explain the purpose, methodology, features, and configuration of guest access networks, including:

- Segmentation
- Captive Portal (Web) Authentication
  - User-based authentication methods

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 marketing campaigns to heighten security 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
- Centralized implementation and management guidelines and procedures
- Inclusion in asset and change management programs

4.2   Describe appropriate installation locations for and remote connectivity to WLAN devices in order to avoid physical theft, tampering, and data theft. Considering the following:

- Physical security implications of infrastructure device placement
- Secure remote connections to WLAN infrastructure devices

4.3   Explain the importance and implementation of client-side security applications:

- VPN client software and policies
- Personal firewall software
- 802.1X/EAP supplicant software

4.4   Explain the importance of on-going WLAN monitoring and documentation:

- Explain the necessary hardware and software for on-going WLAN security monitoring
- Describe and implement WLAN security audits and compliance reports

4.5   Summarize the security policy criteria related to wireless public access network use.

- User risks related to unsecured access
- Provider liability, disclaimers, and acceptable use notifications

4.6   Explain the importance and implementation of a scalable and secure WLAN solution that includes the following security parameters:

- Intrusion detection and prevention
- Role Based Access Control (RBAC) and traffic filtering
- Strong authentication and encryption
- Fast BSS transition

Fast Secure Roaming – 10%

5.1   Describe and implement 802.11 Authentication and Key Management (AKM) including the following:

- Preauthentication
- PMK Caching

5.2 Describe and implement Opportunistic Key Caching (OKC) and explain its enhancements beyond 802.11 AKM.

5.3 Describe and implement 802.11r Authentication and Key Management (AKM) and compare and contrast 802.11r enhancements with 802.11 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 controller-based 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.