

The PW0-200 exam, covering the 2006 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 LAN Discovery	10%
Network Attacks	15%
Network Monitoring	25%
Security Solutions	40%
Security Policy	10%
Total	100%

Wireless LAN Discovery – 10%

- 1.1 Describe and categorize the various methods of target locating and WLAN mapping:
 - Wardriving
 - Freeware discovery applications (Kismet, KisMac, Netstumbler)
 - Integrated Operating System Tools (Microsoft WZC Service)
 - PC card manufacturers' client utilities
 - Public online databases
- 1.2 Describe and apply the following methods of information gathering as they apply to the enterprise:
 - Social Engineering
 - Search engines
 - Public records
 - Garbage collecting (dumpster diving)
- 1.3 Compare, contrast, and demonstrate hardware used to circumvent 802.11 Security:
 - Laptops & tablet PCs
 - Handheld PCs & PDAs
 - Wireless radio cards & antennas
 - Handheld Global Positioning Systems (GPS) devices

Network Attacks – 15%

- 2.1 Demonstrate how to recognize, perform, and prevent the following types of attacks:
 - Physical layer denial-of-service (DoS) attacks
 - MAC layer Denial-of-Service
 - MAC layer protocol attacks
 - Rogue infrastructure hardware placement
 - MAC spoofing
 - Hijacking and peer-to-peer attacks
 - Eavesdropping
- 2.2 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
- 2.3 Explain and demonstrate the use of protocol analysis to capture the following sensitive information:
 - Usernames / Passwords / SNMP Community Strings
 - Encryption keys
 - MAC filter identification
 - Describe and demonstrate preventative measures against protocol analysis

- 2.4 Explain and demonstrate security protocol circumvention against the following types of authentication and/or encryption:
- WEP
 - PSK
 - LEAP
 - PPTP
- 2.5 Explain and demonstrate the following security vulnerabilities associated with public access or other unsecured wireless networks:
- Spamming through the WLAN
 - Viruses / spyware / adware
 - Direct Internet attacks through the WLAN
 - Placement of illegal content
 - Information theft

Network Monitoring – 25%

- 3.1 Understand how to select and use an 802.11 protocol analyzer based on its security features.
- 3.2 Describe and demonstrate the different types of 802.11 Wireless Intrusion Prevention Systems (WIPS):
- Integrated
 - Overlay
 - Integration-enabled
- 3.3 Describe and demonstrate security features of 802.11 WIPS:
- Device identification and categorization
 - Rogue Triangulation vs. Fingerprinting
 - Device tracking
 - Event alerting, notification, and categorization
 - Policy enforcement and violation reporting
 - Wired/Wireless Intrusion mitigation and rogue containment
 - Protocol analysis with filtering
- 3.4 Explain 802.11 WIPS baselining, and describe 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, monitored, or known so that rogues can be easily and quickly identified
- 3.5 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

Security Solutions – 40%

4.1 Recognize and understand the following basic security concepts:

- Functionality and weaknesses of WEP
- Functional parts of TKIP and its differences from WEP
- The role of TKIP in WPA
- Appropriate use and configuration of WPA-Personal and WPA-Enterprise
- Feasibility of WPA-Personal exploitation
- The role of CCMP in WPA2
- Appropriate use and configuration of WPA2-Personal and WPA2-Enterprise

4.2 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, PEAPv1
 - EAP-TLS
 - EAP-TTLS
 - EAP-FAST
- Explain the exploits of specific EAP types:
 - LEAP
 - EAP-MD5

4.3 Explain and describe legacy authentication protocols:

- PAP
- CHAP
- MS-CHAP
- MS-CHAPv2

4.4 Recognize and understand the following concepts about VPNs:

- Common VPN technologies, their appropriate use in wireless networks, and their strengths/weaknesses:
 - PPTP
 - L2TP/IPSec
 - IPSec
 - SSH
- Compare advantages and disadvantages of VPN technology and 802.1X/EAP types in 802.11 WLANs:
 - Protocol overhead
 - Configuration complexity
 - Scalability

- Describe and demonstrate 802.11 WLAN hardware and software that use VPN technology:
 - Access Points
 - Client software
 - WLAN Switches/Controllers

4.5 Describe client-side security software applications:

- VPN policies
- Personal firewall software
- Anti-virus / anti-spyware software

4.6 Describe secure infrastructure management protocols:

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

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

4.8 Describe and demonstrate configuration of 802.1Q VLANs on Ethernet switches and WLAN infrastructure devices.

4.9 Explain the purpose of and features in role-based access control (RBAC), including the configuration of RBAC in WLAN Switches/Controllers.

4.10 Describe and demonstrate the following types of authentication servers used with 802.11 WLANs:

- RADIUS
- Kerberos
- LDAP

4.11 Explain what an AAA server is and explain the following concepts of AAA servers:

- EAP standards support for 802.11
- Proxy services
- LDAP integration
- Explain AAA's role in RBAC (return list attributes)
- Applying user and AAA server credential types (Username/Password, Certificate, PAC, Biometrics)
- The role of AAA services in VLAN tagging
- Benefits of mutual authentication between supplicant and authentication server

4.12 Explain these authentication design models and their scalability aspects:

- Single site deployment
- Distributed autonomous sites
- Distributed sites, centralized authentication and security
- Distributed sites and security, centralized authentication

- 4.13 Explain 802.11i Authentication and Key Management, including:
- AAA Key generation
 - PMK / GMK generation
 - PTK / GTK generation & distribution
 - 4-Way Handshake
 - Group Handshake
 - STAKey Handshake
 - Pass-phrase-to-PSK mapping
- 4.14 Describe strengths, weaknesses, appropriate applications, and scalability issues of WLAN switches, Access Points, WLAN Bridges, WLAN Routers, and WLAN Mesh Routers.
- 4.15 Describe and demonstrate configuration of major feature sets in WLAN Switches, Access Points, WLAN Bridges, WLAN Routers, and WLAN Mesh Routers:
- 802.11e/WMM QoS support
 - Layer 2-7 Role-Based protocol filtering (per user or per group)
 - 802.11h dynamic frequency and power control
 - Automated site survey with automatic RF power and channel management
 - Fast Layer 2-3 handoff (reassociation)
 - 802.1Q VLANs and trunking
 - Hot standby/failover support
 - 802.3af Power-over-Ethernet
 - WPA/WPA2 Personal and Enterprise security
 - Secure management interfaces (HTTPS, SNMPv3, SSH2)
 - Layer 3-7 VPN termination
 - Intrusion prevention
- 4.16 Describe and demonstrate configuration of major feature sets in Enterprise Encryption Gateways (EEGs)
- 4.17 Explain where infrastructure security devices fit into an enterprise wireless LAN topology.
- 4.18 Explain the reason for network segmentation and its limiting factors on WLAN network design.
- 4.19 Explain the functional differences and advantages of both directly-connected and distributed APs in a WLAN Switch architecture.
- 4.20 Describe and demonstrate layered security solutions.
- 4.21 Explain the impact of L2, L3, and L7 security protocols on client station reassociation.

Security Policy – 10%

- 5.1 Explain and apply the phases of security policy development:
- Define and document
 - Management buy in
 - Communication
 - Monitoring and auditing
 - Response and enforcement
 - Revise and fine tune

- 5.2 Explain the purpose and goals of the following wireless LAN security policies:
- Password policy
 - End-user and administrator training on security solution use and social engineering mitigation
 - Security marketing and propaganda campaigns to heighten awareness
 - On-going review (auditing)
 - Acceptable use & abuse policy
 - Traffic filtering
 - Obtaining the latest security feature sets through firmware and software upgrades
 - Consistent implementation procedure
 - Creation and maintenance of a WLAN security checklist
 - Centralized implementation and management guidelines and procedures
 - Inclusion in asset management program
 - Inclusion in change management program
- 5.3 Perform a risk assessment for a wireless LAN, including asset analysis and legal implications.
- 5.4 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
 - PHY and MAC Denial of Service
 - Client hijacking
 - Protocol analysis (eavesdropping)
 - Social engineering
 - Infrastructure hardware theft
 - Access to unsecured console interfaces
- 5.5 Describe appropriate installation locations for wireless LAN hardware in order to avoid physical theft and tampering, considering the following:
- Security implications of remote placement of devices
 - Physical security for remote infrastructure devices
 - Secure remote connections to wireless LAN infrastructure devices
- 5.6 Explain the importance and implementation of client-side security applications:
- VPN policies
 - Personal firewall software
 - Anti-virus / Anti-spyware software
- 5.7 Explain the importance of layered security solutions.
- 5.8 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
 - Implement & maintain a wireless LAN security checklist

- 5.9 Summarize the security policy criteria related to wireless public-access network use.
- 5.10 Summarize the security implications of using a non-standard security solution.
- 5.11 Given a set of business requirements, design a scalable and secure wireless LAN solution considering the following security parameters:
- Continuous intrusion monitoring and containment
 - Use of Role-Based Access Control and traffic filtering
 - Scalable, segmented network design
 - Use of strong encryption, scalable authentication, and fast reassociation