Certified Wireless Security Professional (CWSP-208) Objectives

Introduction

When you pass the CWSP exam and hold a valid CWNA certification, you earn the CWSP certification and credits towards the CWNE certification should you choose to pursue it.

The Certified Wireless Security Professional (CWSP) is a WLAN subject matter expert (SME) who can assist in the creation and implementation of an organization's enforceable security policy by following applicable regulations, standards, and accepted best practices. This SME can identify and mitigate threats to a wireless network. A CWSP can effectively use appropriate tools and procedures to ensure the ongoing security of the network.

The skills and knowledge measured by this examination are derived from a Job Task Analysis (JTA) involving wireless networking experts (CWNEs) and professionals. The results of this JTA and continued enhancement were used in weighting the subject areas and ensuring that the weighting is representative of the relative importance of the content.

The following table provides the breakdown of the exam as to the distribution of questions within each knowledge domain.

Knowledge Domain	Percentage
Security Policy	10%
Vulnerabilities, Threats, and Attacks	30%
WLAN Security Design and Architecture	50%
Security Lifecycle Management	10%

1.0 Security Policy – 10%

1.1 WLAN security Requirements

1.1.1 Evaluate and incorporate business, technical, and applicable regulatory policies (for example, PCI-DSS, HIPAA, GDPR, etc.)
1.1.2 Identify appropriate stakeholders
1.1.3 Review client devices and applications
1.1.4 Review WLAN infrastructure devices

1.2 WLAN security policies

1.2.1 Translate security requirements to high-level policy statements
1.2.2 Advise on the creation of WLAN security policies based on industry standards
1.2.3 Advise on the implementation of security policy lifecycle management
1.2.4 Ensure appropriate approval and support for all policies

1.3 Ensure proper training is administered for all stakeholders related to security policies and ongoing security awareness

2.0 Vulnerabilities, Threats, and Attacks – 30%

2.1 Identify potential vulnerabilities and threats to determine the impact on the WLAN and supporting systems and verify, mitigate, and remediate them

2.1.1 Use information sources to identify the latest vulnerabilities related to a WLAN including online repositories containing CVEs
2.1.2 Determine the risk and impact of identified vulnerabilities
2.1.3 Select appropriate actions to mitigate threats exposed by vulnerabilities

- Review and adjust device configurations to ensure conformance with security policy
- Implement appropriate code modifications, patches and upgrades
- Quarantine unrepaired/compromised systems
- Examine logs and network traffic where applicable

2.1.4 Explain common WLAN attacks including eavesdropping, man-in-the-middle, cracking, phishing, and other social engineering attacks
2.1.5 Identify methods to detect common WLAN attacks including eavesdropping, man-in-the-middle, cracking, phishing, and other social engineering attacks
2.1.6 Identify methods to mitigate common WLAN attacks including eavesdropping, man-in-the-middle, cracking, phishing, and other social engineering attacks
2.1.7 Identify deprecated 802.11 and Wi-Fi Alliance security solutions (WEP, WPA, TKIP, RC4)
2.1.8 Implement security testing procedures to identify weaknesses in the WLAN

- Use appropriate penetration testing processes including scope definition, information gathering, scanning, attack, and documentation procedures
- Select and use security testing tools including project documentation, scanners, hardware tools, Kali Linux tools, protocol analyzers, and WLAN auditing tools (software and hardware)

2.1.9 Implement network monitoring to identify attacks and potential vulnerabilities

- Use appropriate tools for network monitoring including centralized monitoring, distributed monitoring, and Security Information Event Management (SIEM) systems
- Implement mobile (temporary), integrated and overlay WIDS/WIPS solutions to monitor security events

2.2 Describe and perform risk analysis and risk mitigation procedures

2.2.1 Perform asset management
2.2.2 Calculate risk ratings
2.2.3 Estimate loss expectancy
2.2.4 Develop risk management plans for WLANs

3.0 WLAN Security Design and Architecture – 50%

3.1 Select the appropriate security solution for a given implementation and ensure it is installed and configured according to policy requirements

3.1.1 Select and implement appropriate authentication solutions

- WPA2/WPA3 Personal/SAE
- WPA2/WPA3-Enterprise
- WPA3-Enterprise 192-Bit
- 802.1X
- RADIUS
- Understand the capabilities of EAP methods including EAP-TLS, EAP-TTLS and PEAP
- Guest access

3.1.2 Select and implement appropriate encryption solutions

- Differentiate encryption methods and concepts
- CCMP, GCMP, and AES
- SAE
- 192-bit modes
- Opportunistic Wireless Encryption (OWE)
- Virtual Private Network (VPN)

3.1.3 Select and implement wireless monitoring solutions

- Wireless Intrusion Prevention System (WIPS) - overlay and integrated

- Laptop-based monitoring with protocol and spectrum analyzers

3.1.4 Understand and explain 802.11 Authentication and Key Management (AKM) components and processes

- Encryption keys and key hierarchies
- Handshakes and exchanges (4-way, SAE, OWE, FT)
- Pre-shared keys
- Enterprise methods
- RSN security
- WPA, WPA2, and WPA3
- RSN Override vs. WPA3 Transition Mode

3.2 Implement or recommend appropriate wired security configurations to support the WLAN

3.2.1 Physical port security in Ethernet switches
3.2.2 Network segmentation, VLANs, and layered security solutions
3.2.3 Tunneling protocols and connections
3.2.4 Access Control Lists (ACLs)
3.2.5 Firewalls

3.3 Implement authentication and security services

3.3.1 Role-Based Access Control (RBAC)
3.3.2 Certificate Authorities (CAs) and Public Key Infrastructure (PKI)
3.3.3 AAA Servers
3.3.4 Client onboarding
3.3.5 Network Access Control (NAC)
3.3.6 BYOD and MDM

3.4 Implement secure transitioning (roaming) solutions

3.4.1 802.11r Fast BSS Transition (FT)
3.4.2 Opportunistic Key Caching (OKC)
3.4.3 Pre-Shared Key (PSK) - standard and per-user

3.5 Secure public access and/or open networks

3.5.1 Guest access
3.5.2 Peer-to-peer connectivity
3.5.3 Captive portals
3.5.4 Wi-Fi Certified Passpoint/Open Roaming
3.5.5 OWE

3.6 Implement preventative measures required for common vulnerabilities associated with wireless infrastructure devices and avoid weak security solutions

3.6.1 Weak/default passwords
3.6.2 Misconfiguration
3.6.3 Firmware/software updates
3.6.4 HTTP-based administration interface access
3.6.5 Telnet-based administration interface access
3.6.6 Older SNMP protocols such as SNMPv1 and SNMPv2

4.0 Security Lifecycle Management – 10%

4.1 Understand and implement management within the security lifecycle of identify, assess, protect, and monitor

4.1.1 Identify technologies being introduced to the WLAN
4.1.2 Assess security requirements for new technologies
4.1.3 Implement appropriate protective measures for new technologies and validate the security of the measures
4.1.4 Monitor and audit the new technologies for security compliance (Security Information Event Management (SIEM), portable audits, infrastructure-based audits, WIPS/WIDS)

4.2 Use effective change management procedures including documentation, approval, and notifications

4.3 Use information from monitoring solutions for load observation and forecasting of future requirements to comply with security policy

4.4 Implement appropriate maintenance procedures including license management, software/code upgrades, and configuration management

4.5 Implement effective auditing procedures to perform audits, analyze results, and generate reports

4.5.1 User interviews
4.5.2 Vulnerability scans
4.5.3 Reviewing access controls
4.5.4 Penetration testing
4.5.5 System log analysis
4.5.6 Report findings to management and support professionals as appropriate

CWSP-208 Exam Acronyms

For the CWSP-208 exam, you must be able to understand and define the following acronyms in relation to 802.11 WLAN operations and analysis. These acronyms may be used on the CWSP-208 exam without definition.

AAA	Authentication, Authorization, and Accounting
ACI	Adjacent Channel Interference
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
AP	Access Point
ARM	Adaptive Radio Management
ASK	Amplitude Shift Keying
BPSK	Binary Phase Shift Keying
BSA	Basic Service Area
BSS	Infrastructure Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CCI	Co-Channel Interference
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Protocol
CIA	Confidentiality, Integrity, and Availability
CRC	Cyclic Redundancy Check
CTS	Clear to Send
CVE	Common Vulnerabilities and Exposures
dB	Decibel
dBi	Decibel to Isotropic
dBm	Decibel to Milliwatt
DFS	Dynamic Frequency Selection

DHCP	Dynamic Host Configuration Protocol
DMG	Directional Multi-Gigabit
DMZ	Demilitarized Zone
DNS	Domain Name System
DPSK	Dynamic Pre-Shared Key
DRS	Dynamic Rate Switching
DS	Distribution System
DSM	Distribution System Medium
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EIRP	Equivalent Isotropically Radiated Power
ERP	Extended Rate PHY
ESS	Extended Service Set
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shift Keying
FSR	Fast Secure Roaming
FT	Fast BSS Transition
FTP	File Transfer Protocol
Gbps	Gigabits Per Second
GBps	Gigabytes Per Second
GCMP	Galois Counter Mode Protocol
GDPR	General Data Protection Regulation
GHz	Gigahertz
GI	Guard Interval
GTK	Group Temporal Key

HIPAA	Health Insurance Portability and Accountability Act
HR/DSSS	High Rate DSSS
HT	High Throughput
HTTP	Hypertext Transfer Protocol
Hz	Hertz
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
iPSK	Identify Pre-Shared Key
IR	Intentional Radiator
ISP	Internet Service Provider
KCK	Key Confirmation Key
KDK	Key Derivation Key
KEK	Key Encryption Key
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Medium Access Control
Mbps	Megabits Per Second
MBps	Megabytes Per Second
MBSS	Mesh Basic Service Set
MCA	Multiple Channel Architecture
MCS	Modulation and Coding Scheme

MDM	Mobile Device Management
MHz	Megahertz
MIC	Michael/Message Integrity Check
MIMO	Multiple-Input/Multiple-Output
MOS	Mean Opinion Score
MSK	Master Session Key
MU-MIMO	Multi-User MIMO
mW	Milliwatt
NAC	Network Access Control
NIC	Network Interface Card
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OKC	Opportunistic Key Caching
OTA	Over-the-Air
OWE	Opportunistic Wireless Encryption
PCI-DSS	Payment Card Industry Data Security Standard
PD	Powered Device
PEAP	Protected EAP
PHY	Physical Layer
PIN	Personal identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PPSK	Private Pre-Shared Key
PSE	Power Source Equipment
PSK	Pre-Shared Key or Phase Shift Keying (depending on context)
PTK	Pairwise Transient Key

QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RC4	Rivest Cipher 4
RF	Radio Frequency
RFC	Request for Comments
RRM	Radio Resource Management
RSN	Robust Security Network
RSNA	Robust Security Network Association
RSSI	Received Signal Strength Indicator
RTS	Request to Send
Rx	Receive or Receiver
S1G	Sub-1 GHz
SAE	Simultaneous Authentication of Equals
SCA	Single Channel Architecture
SINR	Signal-to-Interference plus Noise Ratio
SISO	Single-Input/Single-Output
SNR	Signal-to-Noise Ratio
SOHO	Small Office Home Office
SS	Spatial Streams
SSH	Secure Shell
SSID	Service Set Identifier
STA	Station
TCP	Transmission Control Protocol
TK	Temporal Key (sometimes also called TEK for Temporal Encryption Key)

TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
TSN	Transition Security Network
TVHT	Television Very High Throughput
Tx	Transmit or Transmitter
UDP	User Datagram Protocol
VHT	Very High Throughput
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VoWLAN	Voice over WLAN
VPN	Virtual Private Network
W	Watt
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area network
WNMS	Wireless Network Management System
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2
WPA3	Wi-Fi Protected Access version 3
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System