CWNP CWSP-206

CWNP Wi-Fi Security Certification Questions & Answers

Exam Summary – Syllabus – Questions

CWSP-206

CWNP Certified Wireless Security Professional

60 Questions Exam –70% Cut Score – Duration of 90 minutes

Table of Contents:

Know Your CWSP-206 Certification Well:

The CWSP-206 is best suitable for candidates who want to gain knowledge in the CWNP Wireless Network. Before you start your CWSP-206 preparation you may struggle to get all the crucial Wi-Fi Security materials like CWSP-206 syllabus, sample questions, study guide.

But don't worry the CWSP-206 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the CWSP-206 syllabus?
- How many questions are there in the CWSP-206 exam?
- Which Practice test would help me to pass the CWSP-206 exam at the first attempt?

Passing the CWSP-206 exam makes you CWNP Certified Wireless Security Professional. Having the Wi-Fi Security certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CWNP CWSP-206 Wi-Fi Security Certification Details:

Exam Name	Wireless Security Professional
Exam Code	CWSP-206
Exam Price	$325 USD
Duration	90 minutes
Number of Questions	60
Passing Score	70%
Recommended Training	**Official Wi-Fi Security Self Study Kit** **Wi-Fi Security eLearning** **Live Network Certification Training Class**
Exam Registration	**PEARSON VUE**
Sample Questions	**CWNP CWSP-206 Sample Questions**
Practice Exam	**CWNP Certified Wireless Security Professional Practice Test**

CWSP-206 Syllabus:

Section	Objectives
Security Policy - 10%	
Define WLAN security Requirements	- Evaluate and incorporate business, technical, and applicable regulatory policies (for example, PCI-DSS, HIPAA, GPDR, etc.) - Involve appropriate stakeholders - Review client devices and applications - Review WLAN infrastructure devices
Develop WLAN security policies	- Translate security requirements to high-level policy statements - Write policies conforming to common practices including definitions of enforcement and constraint specification - Ensure appropriate approval and support for all policies - Implement security policy lifecycle management
Ensure proper training is administered for all stakeholders related to security policies and ongoing security awareness	
Vulnerabilities, Threats, and Attacks - 30%	
Identify potential vulnerabilities and threats to determine the impact on the WLAN and supporting systems and verify, mitigate, and remediate them	- Use information sources to identify the latest vulnerabilities related to a WLAN including online repositories containing CVEs - Determine the risk and impact of identified vulnerabilities - 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

Section	Objectives
	• Examine logs and network traffic where applicable - Describe and detect possible, common WLAN attacks including eavesdropping, man-inthe-middle, cracking, phishing, and social engineering attacks - Implement penetration 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 penetration testing tools including project documentation, scanners, hardware tools, Kali Linux, protocol analyzers, WLAN auditing tools (software and hardware) - 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 WIPS solutions to monitor security events
Describe and perform risk analysis and risk mitigation procedures	- Asset management - Risk Ratings - Loss expectancy calculations - Develop risk management plans for WLANs
WLAN Security Design and Architecture - 45%	
Select the appropriate security solution for a given implementation and ensure it is installed and configured according to policy requirements	- Select and implement appropriate authentication solutions • WPA/WPA2-Personal (Pre-Shared Key) • WPA/WPA2-Enterprise • WPA3-SAE and 192-Bit enterprise security • 802.1X/EAP

Section	Objectives
	• Understand the capabilities of EAP methods including EAP-TLS, EAP-TTLS, PEAP, EAP-FAST, EAP-SIM, and EAP-GTC • Guest access authentication - Select and implement appropriate encryption solutions • Encryption methods and concepts • TKIP/RC4 • CCMP/AES • SAE and 192-bit security • OWE • Virtual Private Network (VPN) - Select and implement wireless monitoring solutions • Wireless Intrusion Prevention System (WIPS) - overlay and integrated • Laptop-based monitoring with protocol and spectrum analyzers - 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) • Pre-shared keys • Pre-RSNA security (WEP and 802.11 Shared Key authentication) • TSN security • RSN security • WPA, WPA2, and WPA3
Implement or recommend appropriate wired security configurations to support the WLAN	- Physical port security in Ethernet switches - Network segmentation, VLANs, and layered security solutions - Tunneling protocols and connections

Section	Objectives
	- Access Control Lists (ACLs) - Firewalls
Implement authentication and security services	- Role-Based Access Control (RBAC) - Certificate Authorities (CAs) - AAA Servers - Client onboarding - Network Access Control (NAC) - BYOD and MDM
Implement secure transitioning (roaming) solutions	- 802.11r Fast BSS Transition (FT) - Opportunistic Key Caching (OKC) - Pre-Shared Key (PSK) - standard and per-user
Secure public access and/or open networks	- Guest access - Peer-to-peer connectivity - Captive portals - Hotspot 2.0/Passpoint
Implement preventative measures required for common vulnerabilities associated with wireless infrastructure devices and avoid weak security solutions	- Weak/default passwords - Misconfiguration - Firmware/software updates - HTTP-based administration interface access - Telnet-based administration interface access - Older SNMP protocols such as SNMPv1 and SNMPv2
Security Lifecycle Management - 15%	
Understand and implement management within the security lifecycle of identify, assess, protect, and monitor	- Identify technologies being introduced to the WLAN - Assess security requirements for new technologies - Implement appropriate protective measures for new technologies and validate the security of the measures - Monitor and audit the new technologies for security compliance (Security Information Event Management (SIEM), portable audits, intrastructure-based audits, WIPS/WIDS)
Use effective change management procedures including	

Section	Objectives
documentation, approval, and notifications	
Use information from monitoring solutions for load observation and forecasting of future requirements to comply with security policy	
Implement appropriate maintenance procedures including license management, sofware/code upgrades, and configuration management	
Implement effective auditing procedures to perform audits, analyze results, and generate reports	- User interviews - Vulnerability scans - Reviewing access controls - Penetration testing - System log analysis - Report findings to management and support professionals as appropriate

CWNP CWSP-206 Sample Questions:

Question: 1

Which of these types of EAP use three phases of operation?

a) EAP-TTLS
b) EAP-PEAPv0 (EAP-MSCHAPv2)
c) EAP-PEAPv0 (EAP-TLS)
d) EAP-FAST
e) EAP-TLS (privacy mode)
f) EAP-TLS (nonprivacy mode)

Answer: d

Question: 2

You must locate non-compliant 802.11 devices. Which one of the following tools will you use and why?

a) A spectrum analyzer, because it can show the energy footprint of a device using WPA differently from a device using WPA2.
b) A spectrum analyzer, because it can decode the PHY preamble of a non-compliant device.
c) A protocol analyzer, because it can be used to report on security settings and regulatory or rule compliance.
d) A protocol analyzer, because it can be used to view the spectrum energy of non-compliant 802.11 devices, which is always different from compliant devices.

Answer: c

Question: 3

How are IPsec VPNs used to provide security in combination with 802.11 WLANs?

a) Client-based security on public access WLANs
b) Point-to-point wireless bridge links
c) Connectivity across WAN links
d) All of the above

Answer: d

Question: 4

When deploying a corporate 802.11 WLAN, what password-related items should always be included in a security policy? (Choose two.)

a) The password policy should mandate a procedure on how passphrases are created for handheld devices that use WPA2-Personal.
b) End-user WPA2-Enterprise passwords should contain numbers, special characters, and upper- and lowercase letters.
c) Client-side certificates should always be used instead of passwords when securing a WLAN.
d) Machine authentication should always be mandated.

Answer: a, b

Question: 5

What would be the intended purpose of using a third-party AP as part of a WLAN audit?

a) Audit the WIPS.
b) Audit the wired infrastructure.
c) Audit Layer 2.
d) Audit Layer 1.

Answer: a

Question: 6

With a WLAN infrastructure, where can the guest captive web portal operate?

a) AP
b) WLAN controller
c) Third-party server
d) All of the above

Answer: d

Question: 7

At which layer of the OSI model does 802.11 technology operate?

a) Session
b) Network
c) Physical
d) Presentation
e) Transport

Answer: c

Question: 8

The CCMP header is made up of which of the following pieces? (Choose two.)

a) PN
b) TTAK
c) TSC
d) Key ID
e) MIC

Answer: a, d

Question: 9

What are some the components within an MDM architecture? (Choose all that apply.)

a) AP
b) RADIUS
c) BYOD
d) APNs
e) GCM

Answer: a, d, e

Question: 10

Which of these attacks are considered denial-of-service attacks? (Choose two.)

a) Man-in-the-middle
b) Jamming
c) Deauthentication spoofing
d) MAC spoofing
e) Peer-to-peer

Answer: b, c

Study Guide to Crack CWNP Wi-Fi Security CWSP-206 Exam:

- Getting details of the CWSP-206 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CWSP-206 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CWNP provided training for CWSP-206 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CWSP-206 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.

- Practicing on CWSP-206 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CWSP-206 Certification

Make NWExam.com your best friend during your Wireless Security Professional exam preparation. We provide authentic practice tests for the CWSP-206 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CWSP-206 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CWSP-206 exam.

Start Online practice of CWSP-206 Exam by visiting URL
https://www.nwexam.com/cwnp/cwsp-206-cwnp-wireless-security-professional-cwsp