



## CWNP PW0-200

**Exam Name:** *certified wireless security professional(cwsp)*

**Q & A :** 120 Q&As

**Pdf Demo**

### **Quality and Value for the PW0-200 Exam**

[Just4Exams Practice Exams](#) for CWNP CWNP PW0-200 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

### **100% Guarantee to Pass Your PW0-200 Exam**

If you do not pass the CWNP PW0-200 exam on your first attempt using our Just4Exams **PW0-200 testing engine and pdf study guide**, we will give you a FULL REFUND of your purchasing fee.

### **Downloadable, Interactive PW0-200 Testing engines and PDF Version**

Our Exam Preparation Material provides you everything you will need to take a [CWNP certification](#) examination. Details are researched and produced by [CWNP Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

#### **Free PW0-200 Exams:**

***This is demo only, this pdf do not include the questions and answers picture***

Exam : CENP PW0-200

Title : Certified Wireless Security Professional(CWSP)

1. Joe's new laptop is experiencing difficulty connecting to ABC Company's 802.11 network. The company's wireless network administrator assured Joe that his laptop was authorized in the WIPS for connectivity to all Marketing department APs before it was given to him yesterday. The WIPS termination policy is shown in the exhibit.

What are some possible reasons that Joe cannot connect to the network?

A. Joe disabled his laptop's integrated 802.11 radio and is using a personal PC card radio because of its updated chipsetdriversand client utilities.

B. Joe's integrated 802.11 radio is sending too many Probe Request and EAPoL Start frames due to a corrupted driver.

C. Joe's radio card has associated to an access point belonging to a neighboring 802.11 WLAN because it was configured to connect to any wireless network.

- D. An ASLEAP attack has been detected on APs to which Joe's laptop was trying to associate. The WIPS responded by disabling the APs.
- E. Joe configured his 802.11 radio card to transmit at 100 mW to increase his SNR. The WIPS is detecting this much output power as a DoS attack.
- F. Joe changed the system time on his computer and the WIPS is detecting this as a usage time violation.

Answer: AC

2. Given: A university is installing 10 WLAN controllers and 500 dual-band IEEE 802.11 ERP/OFDM lightweight access points as part of one WLAN domain. The WLAN controllers will work as a cluster and will support users from 20 different departments within the university system.

In this environment how should each WLAN controller connect to the Ethernet infrastructure?

- A. Each WLAN controller should connect between the core layer 3 Ethernet switch and two access-layer Ethernet switches forming 10 distribution segments.
- B. Each WLAN controller should connect to the core layer 3 Ethernet switch via a gigabit (or faster) 802.1Q trunk.
- C. Two WLAN controllers should be connected to the core layer 3 Ethernet switch and the other eight WLAN controllers should be chained in series with those two WLAN controllers forming the cluster.
- D. Each WLAN controller should connect to an access-layer Ethernet switch using a gigabit (or faster) connection.

Answer: B

3. Wireless Intrusion Prevention Systems (WIPS) are used for what purposes?

- A. Performance monitoring and troubleshooting
- B. Enforcing wireless network policy
- C. Detecting and defending against eavesdropping attacks
- D. Security monitoring and notification
- E. Preventing virtual carrier sense attacks by 802.11 transmitters
- F. Physical layer protocol analysis

Answer: ABD

4. What type of WLAN attack is illustrated on the 802.11 protocol analyzer screenshot?

- A. Wideband RF jamming
- B. Bit-flipping
- C. Narrowband RF jamming
- D. Authentication flood
- E. Hijacking

Answer: A

5. Given: ABC Company is planning to implement IPSec VPN technology using the Encapsulating Security Payload (ESP) protocol to secure their wireless connections. You are hired as a security consultant to discuss the security strength of this solution.

What statement about this WLAN security implementation is true?

- A. ESP can only use 3DES encryption which causes high latency on half-duplex networks.
- B. Wireless clients should be configured for NAT transparency so encrypted frames can traverse gateways.
- C. ESP uses public key cryptography which is incompatible with the 802.11 protocol.
- D. The ESP protocol encrypts the entire original frame if implemented in tunnel mode.
- E. When using ESP as a VPN solution the implementation must incorporate SSH2 tunneling as well.

Answer: D

6. During 802.1X/LEAP authentication what authentication credential is passed using clear text across the wireless medium?

- A. Password
- B. x.509 certificate
- C. Username
- D. PAC
- E. Shared secret

Answer: C

7. Given: A network security auditor is assessing an IEEE 802.11 network's exposure to security holes.

What task would save the most time if performed before the audit?

- A. Identify the IP subnet information for each network segment.
- B. Identify the manufacturer of the wireless intrusion prevention system.
- C. Identify the skill level of the wireless network security administrator(s).
- D. Identify the manufacturer of the wireless infrastructure hardware.
- E. Identify the wireless security solution(s) currently in use.

Answer: E

8. What TKIP features prevent attacks against the known weaknesses of WEP?

- A. 32-bit ICV (CRC-32)
- B. Mandatory per-packet keys
- C. RC5 stream cipher
- D. Michael
- E. Increased IV length
- F. 4-Way Handshake

Answer: BDE

9. What happens in a bit flipping attack against an IEEE 802.11 device?

- A. An attacker captures an encrypted frame, modifies the ciphertext, modifies the ICV to hide the change to the ciphertext, and then transmits the frame to appear as if it is from the original source.
- B. An attacker uses a non-linear Message Integrity Check (MIC) on his computer to form a wireless crossover connection with the target computer.
- C. An attacker injects data into a wireless transmission that results in a memory access exception at the target system for the purpose of breaching security.
- D. An attacker sends each frame with the first bit alternating between 0 and 1, causing the target computer to disable encryption synchronization.
- E. An attacker captures an encrypted authentication frame and then executes a cracking algorithm against each 0 and 1 in the frame. After the frame is cracked, it is used to authenticate the attacker's computer.

Answer: A

10. Given: ABC Company has a WLAN controller with three access points, 15 client devices, and uses WPA2-Personal for WLAN security. What statement about ABC Company's WLAN security is true?

- A. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt data traffic.
- B. Traffic injection attacks are possible because the transmitter lacks frame numbering.
- C. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt broadcast traffic.
- D. An authorized WLAN user with a protocol analyzer can decode data frames of other authorized users if he captures that user's 4-Way Handshake.
- E. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.

Answer: D

11. Given: ABC Corporation is selecting a security solution for their new WLAN, and a PPTP VPN is their first consideration because it is included with both server and desktop operating systems. While the 128-bit encryption of Microsoft's MPPE is considered strong enough to adhere to corporate security policy, the company is worried about security holes in MS-CHAPv2 authentication.

As a consultant, what do you tell ABC Corporation about implementing MS-CHAPv2 authentication in a PPTP VPN?

- A. MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.
- B. MS-CHAPv2 is subject to offline dictionary attacks.
- C. MS-CHAPv2 is only secure when combined with WEP.
- D. MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel.
- E. MS-CHAPv2 uses anonymous Diffie-Hellman authentication and is therefore secure.
- F. MS-CHAPv2 can be replaced with EAP-TLS as the authentication mechanism for PPTP.

Answer: BDF

12. What policies would prevent peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hotspots?

- A. Require managed personal firewall software on each laptop.
- B. Require secure applications such as POP3/SFTP and SSH2.
- C. Require VPN software for connectivity to the corporate network.
- D. Require WPA2-Enterprise as the minimal WLAN security solution.
- E. Require Port Address Translation (PAT) on each laptop.
- F. Require a managed wireless endpoint security agent on each laptop.

Answer: ABCF

13. In this diagram illustrating an example of the IEEE 802.11 standard's 4-Way Handshake, what is the purpose of the ANonce and SNonce?

- A. They are used to pad Message 1 and Message 2 so there is no empty space in the frame.
- B. The IEEE 802.11 standard requires that all cryptographic frames contain a nonce for security purposes.

- C. They are added together and used as the GMK from which the GTK is derived.
- D. They are values used in the derivation of the Pairwise Transient Key.

Answer: D

14. What WIPS parameter is configured to generate notifications?

- A. Mobile unit density violations
- B. Admission control status
- C. Sensor sensitivity levels
- D. Policy threshold values

Answer: D

15. Given: ABC Company's ERP WLAN has worked perfectly for the last 6 months. One morning none of the company's 10 users can connect to the company's only access point. When the administrator logs into the access point there are hundreds of users associated using Open System authentication.

What is the problem?

- A. The AP has been the victim of an RF DoS attack.
- B. The AP has experienced an AP spoofing attack from a rogue AP.
- C. The AP firmware has been corrupted and is erroneously reporting the number of users.
- D. The AP has experienced an association flood attack.

Answer: D

16. Given: You have a laptop computer with an integrated Wi-Fi compliant MiniPCI card.

What statements describe the limited effectiveness of locating rogue access points using WLAN discovery software such as NetStumbler, Kismet, or MacStumbler?

- A. Discovery tools like those listed cannot determine the authorization status of an access point.
- B. A laptop computer can only be in one location at a time.
- C. Discovery tools like those listed cannot determine if an access point is attached to a wired network.
- D. Rogue access points using non-IEEE 802.11 frequency bands or unpopular modulations are not detected.
- E. When data encryption is used access points cannot be detected using discovery tools like those listed.

Answer: ABCD

17. What four tools are required to hijack a wireless station (at Layer 2 and Layer 3) from the authorized wireless network onto the unauthorized wireless network? (Select two answers that together specify the four necessary tools)

- A. Access point software and a narrowband RF jamming device
- B. A high-gain Yagi antenna and terminal emulation software
- C. A wireless workgroup bridge and a spectrum analyzer
- D. A wireless PC card and DHCP server software
- E. MAC spoofing software and data flooding software

Answer: AD

18. How does a wireless network management system (WNMS) discover EAP usernames?

- A. The WNMS acts as an 802.1X authentication server proxy relaying information between the WLAN controller and the RADIUS server.
- B. The WNMS polls access points or WLAN controllers using SNMP.
- C. The client device sends the username to the WNMS on port 113 (ident service) after successful authentication.
- D. The RADIUS server sends the username to the WNMS after the wireless device successfully authenticates.
- E. The WNMS captures the username by telling APs to sniff the wireless medium during the authentication process.

Answer: B

19. Given: The illustrated WLAN software tool can transmit customized 802.11 frames.

What are two uses for such a tool?

- A. EAPoL flood attacks against access points
- B. Auditing the performance features of a WIPS
- C. Testing Role-Based Access Control features of a WLAN controller
- D. NAV/duration attacks against all stations in a BSA
- E. Altering physical layer frame headers for frame injection attacks
- F. Changing a frame's WEP ICV while it is in transit

Answer: AD

20. Given: John Smith often works from home and wireless hotspots rather than commuting to the office. His laptop connects to the office network over IEEE 802.11 WLANs.

To safeguard his data what wireless security policy items should be implemented?

- A. Use an IPSec VPN for remote connectivity
- B. Use an HTTPS captive portal for authentication at hotspots
- C. Use personal firewall software on his laptop
- D. Use a protocol analyzer on his laptop to monitor for risks
- E. Use 802.1X/PEAPv0 to connect to the corporate office network

Answer: AC

More [PW0-200 Braindumps](#) Information

**Related PW0-200 Exams**

PW0-104 PW0-100 PW0-050 PW0-200 PW0-300  
PW0-205

**Other CWNP Exams**

PW0-050 PW0-070 PW0-100 PW0-104 PW0-200  
PW0-205 PW0-300