

PW0-200 Practice Test

CWNP certified wireless security professional(cwsp)

PW0-200: certified wireless security professional(cwsp)

Practice Exam: PW0-200 Exams

Exam Number/Code: PW0-200

Exam Name: certified wireless security professional(cwsp)

Questions and Answers: 120 Q&As

(CWNP)



Exam : [PW0-200](#)

For candidates making preparation for the CWNP PW0-200 questions and answers, what they most desire is to easily pass the PW0-200 (certified wireless security professional(cwsp)) exam. ItCertHome PW0-200 includes 120 questions and answers, which are collected and collated by experts of CWNP. With our PW0-200 study materials, you can successfully take CWNP certification of PW0-200 exam and go further on CWNP career path.

Free PW0-200 Demo

we provide CWNP PW0-200 demo exam for free (in PDF format) before you decide to purchase it. Thus,you can know better about the quality of our practice exam and then make your right decision.

ItCertHome Test tool's advantages:

High Quality and Value of PW0-200 exam

ItCertHome CWNP CWNP PW0-200 Practice Questions is developed and finished by CWNP technical team , cover every field of the exam . Besides, we have verified PW0-200 answers,almost 100% correct.

100% Guarantee to Pass PW0-200 Exam

We promise to give you FULL REFUND if you fail the CWNP PW0-200 certification(CWNP Certified Network Associate) with the use of our ItCertHome testing engine.

PW0-200 Self Test Mode

ItCertHome provides a simulated and interactive environment where you can test your knowledge and skills about PW0-200 to ensure enough assurance in real testing center.

Periodic Updates of ItCertHome PW0-200

Once there is some change on CWNP PW0-200 exam, we will update it timely, and the product you buy will be updated within 90 days for free.

Professional and Efficient Service

We offer 7*24 customer support via diverse channels: LIVE CHAT,MAIL.Expecting the communication with you about IT certification.

The Questions & Answers cover the latest real test and with all the correct answer.we promise the Q&A for **CWNP CWNP PW0-200** examination of original title complete coverage.ItCertHome **PW0-200 Braindumps** Questions & Answers help you pass the exam. Otherwise,we will give you a full refund.

We promised that use ItCertHome Q&A ensure you pass the exam at your first try.

1. The Q&A are from cooperation exam center of the real original title,summaried by our professional team and collated by senior IT lectured in co-training center to make sure the professional quality of the Q&A.The correctly of the Q&A is 100%, the coverage of PW0-200 Q&A are more than 96%.All you need to study the whole PW0-200 Q&A before you participate the certification exam,it should be possible to easily complete the exam and pass the certification.

2. ItCertHome to all the Q&A, we promised "do not pass the exam give you a full refund". If you buy our PW0-200 Q&A and did not pass the exam at the first try. You can take the examination report card that stamped with PROMETRIC or VUE test centers Seal. we will refund your full cost of PW0-200 Q&A, absolutely guarantee you interests have no losses.(For a full refund details)

3. ItCertHome professional IT Q&A vendors, we provide well after-sale service. To all the customers buy the Q&A, we provide track service. when you buy the Q&A with in one year. you can enjoy the upgrade Q&A service for free. If in this period, the certified test center change the PW0-200 Q&A, we will update the Q&A in the first time, and provide you the download update for free.

[CWNP PW0-200](#) Test belongs to one of the CWNP certified test, if needs to obtain the CWNP certificate, you also need to participate in other related test, the details you may visit the CWNP certified topic, in there, you will see all related CWNP certified subject of examination.

PW0-200

ItCertHome professional provide CWNP PW0-200 the newest Q&A, completely covers PW0-200 test original topic. With our complete CWNP resources, you will minimize your CWNP cost and be ready to pass your PW0-200 tests on Your First Try, 100% Money Back Guarantee included!

This PW0-200 PDF demo do not include the questions and answers's picture:

Exam : CENP PW0-200

Title : Certified Wireless Security Professional(CWSP)

1. 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

2. 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

3. 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

4. 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/SHTTPSand 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

5. 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

6. 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 computerand the WIPS is detecting this as a usage time violation.

Answer: AC

7. 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 NetStumblerKismetor 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 in useaccess points cannot be detected using discovery tools like those listed.

Answer: ABCD

8. 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

9. 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

10. 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

11. 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

12. 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

13. 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

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

A. The WNMS acts as an 802.1X authentication server proxyrelaying 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

15. 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

16. 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

17. 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

18. 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

19. 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

20. 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

More [PW0-200 practice test](#)

Related PW0-200 Exams

[PW0-104](#) *Wireless LAN Administration Exam*

[PW0-100](#) *certified wireless network administrator(cwna)*

[PW0-050](#) *Wireless#*

[PW0-200](#) *certified wireless security professional(cwsp)*

[PW0-300](#) *Certified Wireless Network Expert*

[PW0-205](#) *certified wireless analysis professional(cwap)*

Other CWNP Exams

[PW0-100](#)

[PW0-300](#)

[PW0-050](#)

[PW0-104](#)

[PW0-070](#)

[PW0-200](#)

[PW0-205](#)