

## CWSP-205<sup>Q&As</sup>

Certified Wireless Security Professional

**Pass CWNP CWSP-205 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/cwsp-205.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CWNP  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

What software and hardware tools are used together to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network? (Choose 2)

- A. RF jamming device and a wireless radio card
- B. A low-gain patch antenna and terminal emulation software
- C. A wireless workgroup bridge and a protocol analyzer
- D. DHCP server software and access point software
- E. MAC spoofing software and MAC DoS software

Correct Answer: AD

---

**QUESTION 2**

Given: You support a coffee shop and have recently installed a free 802.11ac wireless hot-spot for the benefit of your customers. You want to minimize legal risk in the event that the hot-spot is used for illegal Internet activity.

What option specifies the best approach to minimize legal risk at this public hot-spot while maintaining an open venue for customer Internet access?

- A. Configure WPA2-Enterprise security on the access point
- B. Block TCP port 25 and 80 outbound on the Internet router
- C. Require client STAs to have updated firewall and antivirus software
- D. Allow only trusted patrons to use the WLAN
- E. Use a WIPS to monitor all traffic and deauthenticate malicious stations
- F. Implement a captive portal with an acceptable use disclaimer

Correct Answer: F

---

**QUESTION 3**

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 view the spectrum energy of non-compliant 802.11 devices, which is always different from compliant devices.

D. A protocol analyzer, because it can be used to report on security settings and regulatory or rule compliance

Correct Answer: D

---

**QUESTION 4**

Given: ABC Corporation is evaluating the security solution for their existing WLAN. Two of their supported solutions include a PPTP VPN and 802.1X/LEAP. They have used PPTP VPNs because of their wide support in server and desktop operating systems. While both PPTP and LEAP adhere to the minimum requirements of the corporate security policy, some individuals have raised concerns about MS-CHAPv2 (and similar) authentication and the known fact that MS-CHAPv2 has proven vulnerable in improper implementations.

As a consultant, what do you tell ABC Corporation about implementing MS-CHAPv2 authentication? (Choose 2)

- A. MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.
- B. MS-CHAPv2 is subject to offline dictionary attacks.
- C. LEAP's use of 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 AES authentication, and is therefore secure.
- F. When implemented with AES-CCMP encryption, MS-CHAPv2 is very secure.

Correct Answer: BD

---

**QUESTION 5**

What wireless security protocol provides mutual authentication without using an X.509 certificate?

- A. EAP-FAST
- B. EAP-MD5
- C. EAP-TLS
- D. PEAPv0/EAP-MSCHAPv2
- E. EAP-TTLS
- F. PEAPv1/EAP-GTC

Correct Answer: A