CWSP-205 Q&As

Certified Wireless Security Professional

Pass CWNP CWSP-205 Exam with 100% Guarantee

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

https://www.geekcert.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

Given: Your company has just completed installation of an IEEE 802.11 WLAN controller with 20 controller-based APs. The CSO has specified PEAPv0/EAP-MSCHAPv2 as the only authorized WLAN authentication mechanism. Since an LDAP-compliant user database was already in use, a RADIUS server was installed and is querying authentication requests to the LDAP server.

Where must the X.509 server certificate and private key be installed in this network?

A. Supplicant devices

B. LDAP server

C. Controller-based APs

D. WLAN controller

E. RADIUS server

Correct Answer: E

QUESTION 2

Given: One of the security risks introduced by WPA2-Personal is an attack conducted by an authorized network user who knows the passphrase. In order to decrypt other users\\' traffic, the attacker must obtain certain information from the 4-way handshake of the other users.

In addition to knowing the Pairwise Master Key (PMK) and the supplicant\\'s address (SA), what other three inputs must be collected with a protocol analyzer to recreate encryption keys? (Choose 3)

A. Authenticator nonce

B. Supplicant nonce

C. Authenticator address (BSSID)

D. GTKSA

E. Authentication Server nonce

Correct Answer: ABC

QUESTION 3

Given: John Smith uses a coffee shop\\'s Internet hot-spot (no authentication or encryption) to transfer funds between his checking and savings accounts at his bank\\'s website. The bank\\'s website uses the HTTPS protocol to protect sensitive account information. While John was using the hot-spot, a hacker was able to obtain John\\'s bank account user ID and password and exploit this information.

What likely scenario could have allowed the hacker to obtain John\\'s bank account user ID and password?

A. John\\'s bank is using an expired X.509 certificate on their web server. The certificate is on John\\'s Certificate Revocation List (CRL), causing the user ID and password to be sent unencrypted.

B. John uses the same username and password for banking that he does for email. John used a POP3 email client at the wireless hot-spot to check his email, and the user ID and password were not encrypted.

C. John accessed his corporate network with his IPSec VPN software at the wireless hot-spot. An IPSec VPN only encrypts data, so the user ID and password were sent in clear text. John uses the same username and password for banking that he does for his IPSec VPN software.

D. The bank\\'s web server is using an X.509 certificate that is not signed by a root CA, causing the user ID and password to be sent unencrypted.

E. Before connecting to the bank\\'s website, John\\'s association to the AP was hijacked. The attacker intercepted the HTTPS public encryption key from the bank\\'s web server and has decrypted John\\'s login credentials in near real-time.

Correct Answer: B

QUESTION 4

Given: WLAN protocol analyzers can read and record many wireless frame parameters.

What parameter is needed to physically locate rogue APs with a protocol analyzer?

A. SSID

B. IP Address

C. BSSID

D. Signal strength

E. RSN IE

F. Noise floor

Correct Answer: D

QUESTION 5

Given: Mary has just finished troubleshooting an 802.11g network performance problem using a laptop-based WLAN protocol analyzer. The wireless network implements 802.1X/PEAP and the client devices are authenticating properly. When Mary disables the WLAN protocol analyzer, configures her laptop for PEAP authentication, and then tries to connect to the wireless network, she is unsuccessful. Before using the WLAN protocol analyzer, Mary\\'s laptop connected to the network without any problems.

What statement indicates why Mary cannot access the network from her laptop computer?

A. The nearby WIPS sensor categorized Mary\\'s protocol analyzer adapter as a threat and is performing a deauthentication flood against her computer.

B. The PEAP client\\'s certificate was voided when the protocol analysis software assumed control of the wireless

adapter.

C. The protocol analyzer\\'s network interface card (NIC) drivers are still loaded and do not support the version of PEAP being used.

D. Mary\\'s supplicant software is using PEAPv0/EAP-MSCHAPv2, and the access point is using PEAPv1/ EAP-GTC.

Correct Answer: C