CertBus.com

CERTBUS

CWSP-205 Q&As

Certified Wireless Security Professional (CWSP)

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

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

http://www.CertBus.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
- **80000+** Satisfied Customers

Vendor: CWNP

Exam Code: CWSP-205

Exam Name: Certified Wireless Security Professional (CWSP)

Q&As: Demo

QUESTION 1
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 2
What type of WLAN attack is prevented with the use of a per-MPDU TKIP sequence counter (TSC)?

A. Weak-IV
B. Forgery
C. Replay
D. Bit-flipping
E. Session hijacking

Correct Answer: C

QUESTION 3
What 802.11 WLAN security problem is directly addressed by mutual authentication?

A. Wireless hijacking attacks
B. Weak password policies
C. MAC spoofing
D. Disassociation attacks
E. Offline dictionary attacks
F. Weak Initialization Vectors

Correct Answer: A

QUESTION 4
ABC Company uses the wireless network for highly sensitive network traffic. For that reason, they intend to protect their network in all possible ways. They are continually researching new network threats and new preventative measures. They are interested in the security benefits of 802.11w, but would like to know its limitations.

What types of wireless attacks are protected by 802.11w? (Choose 2)

A. RF DoS attacks
B. Layer 2 Disassociation attacks

C. Robust management frame replay attacks
D. Social engineering attacks

Correct Answer: BC

QUESTION 5
You are configuring seven APs to prevent common security attacks. The APs are to be installed in a small business and to reduce costs, the company decided to install all consumer-grade wireless routers. The wireless routers will connect to a switch, which connects directly to the Internet connection providing 50 Mbps of Internet bandwidth that will be shared among 53 wireless clients and 17 wired clients.

To ensure the wireless network is as secure as possible from common attacks, what security measure can you implement given only the hardware referenced?

A. WPA-Enterprise
B. 802.1X/EAP-PEAP
C. WPA2-Enterprise
D. WPA2-Personal

Correct Answer: D

QUESTION 6
A WLAN is implemented using WPA-Personal and MAC filtering.

To what common wireless network attacks is this network potentially vulnerable? (Choose 3)

A. Offline dictionary attacks
B. MAC Spoofing
C. ASLEAP
D. DoS

Correct Answer: ABD

QUESTION 7
An attack is under way on the network. The attack is preventing users from accessing resources required for business operations, but the attacker has not gained access to any files or data. What kind of attack is described?

A. Man-in-the-middle
B. Hijacking
C. ASLEAP
D. DoS

Correct Answer: D

QUESTION 8
Given: WLAN attacks are typically conducted by hackers to exploit a specific vulnerability within a network.

What statement correctly pairs the type of WLAN attack with the exploited vulnerability? (Choose 3)

A. Management interface exploit attacks are attacks that use social engineering to gain credentials from managers.
B. Zero-day attacks are always authentication or encryption cracking attacks.
C. RF DoS attacks prevent successful wireless communication on a specific frequency or frequency range.
D. Hijacking attacks interrupt a user's legitimate connection and introduce a new connection with an evil twin AP.
E. Social engineering attacks are performed to collect sensitive information from unsuspecting users

F. Association flood attacks are Layer 3 DoS attacks performed against authenticated client stations

Correct Answer: CDE

QUESTION 9
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 10
What is a primary criteria for a network to qualify as a Robust Security Network (RSN)?

A. Token cards must be used for authentication.
B. Dynamic WEP-104 encryption must be enabled.
C. WEP may not be used for encryption.
D. WPA-Personal must be supported for authentication and encryption.
E. WLAN controllers and APs must not support SSHv1.

Correct Answer: C

QUESTION 11
Wireless Intrusion Prevention Systems (WIPS) provide what network security services? (Choose 2)

A. Configuration distribution for autonomous APs
B. Wireless vulnerability assessment
C. Application-layer traffic inspection
D. Analysis and reporting of AP CPU utilization
E. Policy enforcement and compliance management

Correct Answer: BE

QUESTION 12
ABC Company requires the ability to identify and quickly locate rogue devices. ABC has chosen an overlay WIPS solution with sensors that use dipole antennas to perform this task. Use your knowledge of location tracking techniques to answer the question.

In what ways can this 802.11-based WIPS platform determine the location of rogue laptops or APs? (Choose 3)

A. Time Difference of Arrival (TDoA)
B. Angle of Arrival (AoA)
C. Trilateration of RSSI measurements
D. GPS Positioning
E. RF Fingerprinting

Correct Answer: ACE

QUESTION 13
In an effort to optimize WLAN performance, ABC Company has upgraded their WLAN infrastructure from 802.11a/g to 802.11n. 802.11a/g clients are still supported and are used throughout ABC's facility. ABC has always been highly security conscious, but due to budget limitations, they have not yet updated their overlay WIPS solution to 802.11n or 802.11ac.

Given ABC's deployment strategy, what security risks would not be detected by the 802.11a/g WIPS?

A. Hijacking attack performed by using a rogue 802.11n AP against an 802.11a client
B. Rogue AP operating in Greenfield 40 MHz-only mode
C. 802.11a STA performing a deauthentication attack against 802.11n APs
D. 802.11n client spoofing the MAC address of an authorized 802.11n client

Correct Answer: B

QUESTION 14
Your organization required compliance reporting and forensics features in relation to the 802.11ac WLAN they have recently installed. These features are not built into the management system provided by the WLAN vendor. The existing WLAN is managed through a centralized management console provided by the AP vendor with distributed APs and multiple WLAN controllers configured through this console.

What kind of system should be installed to provide the required compliance reporting and forensics features?

A. WNMS
B. WIPS overlay
C. WIPS integrated
D. Cloud management platform

Correct Answer: B

QUESTION 15
You are implementing an 802.11ac WLAN and a WIPS at the same time. You must choose between integrated and overlay WIPS solutions. Which of the following statements is true regarding integrated WIPS solutions?

A. Integrated WIPS always perform better from a client throughput perspective because the same radio that performs the threat scanning also services the clients.
B. Integrated WIPS use special sensors installed alongside the APs to scan for threats.
C. Many integrated WIPS solutions that detect Voice over Wi-Fi traffic will cease scanning altogether to accommodate the latency sensitive client traffic.
D. Integrated WIPS is always more expensive than overlay WIPS.

Correct Answer: C

QUESTION 16
You have been recently hired as the wireless network administrator for an organization spread across seven locations. They have deployed more than 100 APs, but they have not been managed in either an automated or manual process for more than 18 months. Given this length of time, what is one of the first things you should evaluate from a security perspective?

A. The channel widths configured
B. The channels in use
C. The VLANs in use
D. The firmware revision

Correct Answer: D

QUESTION 17
ABC Company has deployed a Single Channel Architecture (SCA) solution to help overcome some of the common problems with client roaming. In such a network, all APs are configured with the same channel and BSSID. PEAPv0/EAP-MSCHAPv2 is the only supported authentication mechanism.

As the Voice over Wi-Fi (STA-1) client moves throughout this network, what events are occurring?

A. STA-1 initiates open authentication and 802.11 association with each AP prior to roaming.
B. The WLAN controller is querying the RADIUS server for authentication before the association of STA-1 is moved from one AP to the next.
C. STA-1 controls when and where to roam by using signal and performance metrics in accordance with the chipset drivers and 802.11k.
D. The WLAN controller controls the AP to which STA-1 is associated and transparently moves this association in accordance with the physical location of STA-1.

Correct Answer: D

QUESTION 18
Select the answer option that arranges the numbered events in the correct time sequence (first to last) for a client associating to a BSS using EAP-PEAPv0/MSCHAPv2.
1. Installation of PTK
2. Initiation of 4-way handshake
3. Open system authentication
4. 802.11 association
5. 802.1X controlled port is opened for data traffic
6. Client validates server certificate
7. AS validates client credentials

A. 3--4--6--7--2--1--5
B. 4--3--5--2--7--6--1
C. 5--3--4--2--6--7--1
D. 6--1--3--4--2--7--5
E. 4--3--2--7--6--1--5
F. 3--4--7--6--5--2--1

Correct Answer: A

QUESTION 19
Given: You have implemented strong authentication and encryption mechanisms for your enterprise 802.11 WLAN using 802.1X/EAP with AES-CCMP.
For users connecting within the headquarters office, what other security solution will provide continuous monitoring of both clients and APs with 802.11-specific tracking?

A. IPSec VPN client and server software
B. Internet firewall software
C. Wireless intrusion prevention system
D. WLAN endpoint agent software
E. RADIUS proxy server

Correct Answer: C

QUESTION 20
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

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

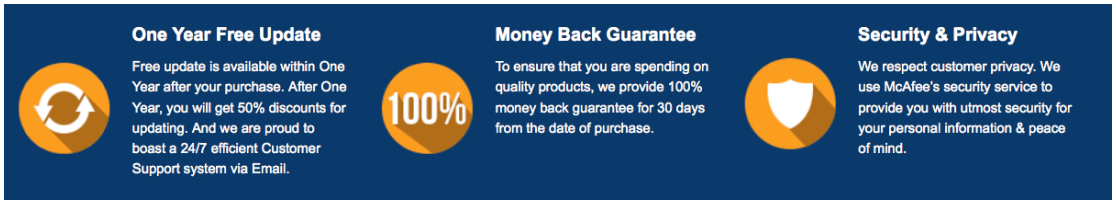
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions