Vendor: CWNP

Exam Code: CWSP-207

Exam Name: Certified Wireless Security Professional (CWSP)

Version: DEMO

QUESTION 1
Given: You are using a Wireless Aggregator utility to combine multiple packet captures. One capture exists for each of channels 1, 6 and 11. What kind of troubleshooting are you likely performing with such a tool?

A. Wireless adapter failure analysis.
B. Interference source location.
C. Fast secure roaming problems.
D. Narrowband DoS attack detection.

Answer: C

QUESTION 2
Which of the following security attacks cannot be detected by a WIPS solution of any kind? (Choose 2)

A. Rogue APs
B. DoS
C. Eavesdropping
D. Social engineering

Answer: CD

QUESTION 3
You perform a protocol capture using Wireshark and a compatible 802.11 adapter in Linux. When viewing the capture, you see an auth req frame and an auth rsp frame. Then you see an assoc req frame and an assoc rsp frame. Shortly after, you see DHCP communications and then ISAKMP protocol packets. What security solution is represented?

A. 802.1X/EAP-TTLS
B. Open 802.11 authentication with IPSec
C. 802.1X/PEAPv0/MS-CHAPv2
D. WPA2-Personal with AES-CCMP
E. EAP-MD5

Answer: B

QUESTION 4
Given: In a security penetration exercise, a WLAN consultant obtains the WEP key of XYZ Corporation's wireless network. Demonstrating the vulnerabilities of using WEP, the consultant uses a laptop running a software AP in an attempt to hijack the authorized user's connections. XYZ's legacy network is using 802.11n APs with 802.11b, 11g, and 11n client devices.

With this setup, how can the consultant cause all of the authorized clients to establish Layer 2 connectivity with the software access point?

A. All WLAN clients will reassociate to the consultant's software AP if the consultant's software AP provides the same SSID on any channel with a 10 dB SNR improvement over the authorized AP.
B. A higher SSID priority value configured in the Beacon frames of the consultant's software AP will take priority over the SSID in the authorized AP, causing the clients to reassociate.

C. When the RF signal between the clients and the authorized AP is temporarily disrupted and the consultant's software AP is using the same SSID on a different channel than the authorized AP, the clients will reassociate to the software AP.
D. If the consultant's software AP broadcasts Beacon frames that advertise 802.11g data rates that are faster rates than XYZ's current 802.11b data rates, all WLAN clients will reassociate to the faster AP.

Answer: C

QUESTION 5
What elements should be addressed by a WLAN security policy? (Choose 2)

A. Enabling encryption to prevent MAC addresses from being sent in clear text
B. How to prevent non-IT employees from learning about and reading the user security policy
C. End-user training for password selection and acceptable network use
D. The exact passwords to be used for administration interfaces on infrastructure devices
E. Social engineering recognition and mitigation techniques

Answer: CE

QUESTION 6
As a part of a large organization's security policy, how should a wireless security professional address the problem of rogue access points?

A. Use a WPA2-Enterprise compliant security solution with strong mutual authentication and encryption for network access of corporate devices.
B. Hide the SSID of all legitimate APs on the network so that intruders cannot copy this parameter on rogue APs.
C. Conduct thorough manual facility scans with spectrum analyzers to detect rogue AP RF signatures.
D. A trained employee should install and configure a WIPS for rogue detection and response measures.
E. Enable port security on Ethernet switch ports with a maximum of only 3 MAC addresses on each port.

Answer: D

QUESTION 7
In what deployment scenarios would it be desirable to enable peer-to-peer traffic blocking?

A. In home networks in which file and printer sharing is enabled
B. At public hot-spots in which many clients use diverse applications
C. In corporate Voice over Wi-Fi networks with push-to-talk multicast capabilities
D. In university environments using multicast video training sourced from professor's laptops

Answer: B

QUESTION 8
As the primary security engineer for a large corporate network, you have been asked to author a

new security policy for the wireless network. While most client devices support 802.1X authentication, some legacy devices still only support passphrase/PSK-based security methods.

When writing the 802.11 security policy, what password-related items should be addressed?

A. MSCHAPv2 passwords used with EAP/PEAPv0 should be stronger than typical WPA2-PSK passphrases.
B. Password complexity should be maximized so that weak WEP IV attacks are prevented.
C. Static passwords should be changed on a regular basis to minimize the vulnerabilities of a PSK-based authentication.
D. Certificates should always be recommended instead of passwords for 802.11 client authentication.
E. EAP-TLS must be implemented in such scenarios.

Answer: C

QUESTION 9
Given: ABC Hospital wishes to create a strong security policy as a first step in securing their 802.11 WLAN.

Before creating the WLAN security policy, what should you ensure you possess?

A. Awareness of the exact vendor devices being installed
B. Management support for the process
C. End-user training manuals for the policies to be created
D. Security policy generation software

Answer: B

QUESTION 10
What policy would help mitigate the impact of peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hot-spots?

A. Require Port Address Translation (PAT) on each laptop.
B. Require secure applications such as POP, HTTP, and SSH.
C. Require VPN software for connectivity to the corporate network.
D. Require WPA2-Enterprise as the minimal WLAN security solution.

Answer: C

QUESTION 11
What is one advantage of using EAP-TTLS instead of EAP-TLS as an authentication mechanism in an 802.11 WLAN?

A. EAP-TTLS sends encrypted supplicant credentials to the authentication server, but EAP-TLS uses unencrypted user credentials.
B. EAP-TTLS supports client certificates, but EAP-TLS does not.
C. EAP-TTLS does not require an authentication server, but EAP-TLS does.
D. EAP-TTLS does not require the use of a certificate for each STA as authentication credentials,

but EAP-TLS does.

Answer: D

QUESTION 12
What wireless authentication technologies may build a TLS tunnel between the supplicant and the authentication server before passing client authentication credentials to the authentication server? (Choose 3)

A. EAP-MD5
B. EAP-TLS
C. LEAP
D. PEAPv0/MSCHAPv2
E. EAP-TTLS

Answer: BDE

QUESTION 13
While performing a manual scan of your environment using a spectrum analyzer on a laptop computer, you notice a signal in the real time FFT view. The signal is characterized by having peak power centered on channel 11 with an approximate width of 20 MHz at its peak. The signal widens to approximately 40 MHz after it has weakened by about 30 dB.

What kind of signal is displayed in the spectrum analyzer?

A. A frequency hopping device is being used as a signal jammer in 5 GHz
B. A low-power wideband RF attack is in progress in 2.4 GHz, causing significant 802.11 interference
C. An 802.11g AP operating normally in 2.4 GHz
D. An 802.11a AP operating normally in 5 GHz

Answer: C

QUESTION 14
You are using a protocol analyzer for random checks of activity on the WLAN. In the process, you notice two different EAP authentication processes. One process (STA1) used seven EAP frames (excluding ACK frames) before the 4-way handshake and the other (STA2) used 11 EAP frames (excluding ACK frames) before the 4-way handshake.

Which statement explains why the frame exchange from one STA required more frames than the frame exchange from another STA when both authentications were successful? (Choose the single most probable answer given a stable WLAN.)

A. STA1 and STA2 are using different cipher suites.
B. STA2 has retransmissions of EAP frames.
C. STA1 is a reassociation and STA2 is an initial association.
D. STA1 is a TSN, and STA2 is an RSN.
E. STA1 and STA2 are using different EAP types.

Answer: E

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

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

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**