Vendor:CWNP

Exam Code:CWSP-205

Exam Name: Certified Wireless Security Professional

Version: Demo

QUESTION 1

Given: Fred works primarily from home and public wireless hot-spots rather than commuting to the office. He frequently accesses the office network remotely from his Mac laptop using the local 802.11 WLAN.

In this remote scenario, what single wireless security practice will provide the greatest security for Fred?

A. Use an IPSec VPN for connectivity to the office network

B. Use only HTTPS when agreeing to acceptable use terms on public networks

C. Use enterprise WIPS on the corporate office network

D. Use WIPS sensor software on the laptop to monitor for risks and attacks

E. Use 802.1X/PEAPv0 to connect to the corporate office network from public hot-spots

F. Use secure protocols, such as FTP, for remote file transfers.

Correct Answer: A

QUESTION 2

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 3

Given: ABC Company has a WLAN controller using WPA2-Enterprise with PEAPv0/MS- CHAPv2 and AES-CCMP to secure their corporate wireless data. They wish to implement a guest WLAN for guest users to have Internet access, but want to implement some security controls. The security requirements for the hot-spot include:

Cannot access corporate network resources

Network permissions are limited to Internet access

All stations must be authenticated

What security controls would you suggest? (Choose the single best answer.)

A. Implement separate controllers for the corporate and guest WLANs.

B. Use a WIPS to deauthenticate guest users when their station tries to associate with the corporate WLAN.

C. Configure access control lists (ACLs) on the guest WLAN to control data types and destinations.

D. Require guest users to authenticate via a captive portal HTTPS login page and place the guest WLAN and the corporate WLAN on different VLANs.

E. Force all guest users to use a common VPN protocol to connect.

Correct Answer: D

QUESTION 4

Given: XYZ Hospital plans to improve the security and performance of their Voice over Wi-Fi implementation and will be upgrading to 802.11n phones with 802.1X/EAP authentication. XYZ would like to support fast secure roaming for the phones and will require the ability to troubleshoot reassociations that are delayed or dropped during inter-channel roaming.

What portable solution would be recommended for XYZ to troubleshoot roaming problems?

A. WIPS sensor software installed on a laptop computer

B. Spectrum analyzer software installed on a laptop computer

C. An autonomous AP mounted on a mobile cart and configured to operate in monitor mode

D. Laptop-based protocol analyzer with multiple 802.11n adapters

Correct Answer: D

QUESTION 5

Given: ABC Corporation\\'s 802.11 WLAN is comprised of a redundant WLAN controller pair (N+1) and 30 access points implemented in 2004. ABC implemented WEP encryption with IPSec VPN technology to secure their wireless communication because it was the strongest security solution available at the time it was implemented. IT management has decided to upgrade the WLAN infrastructure and implement Voice over Wi-Fi and is concerned with security because most Voice over Wi-Fi phones do not support IPSec.

As the wireless network administrator, what new security solution would be best for protecting ABC\\'s data?

A. Migrate corporate data clients to WPA-Enterprise and segment Voice over Wi-Fi phones by assigning them to a different frequency band.

B. Migrate corporate data and Voice over Wi-Fi devices to WPA2-Enterprise with fast secure roaming support, and segment Voice over Wi-Fi data on a separate VLAN.

C. Migrate to a multi-factor security solution to replace IPSec; use WEP with MAC filtering, SSID hiding, stateful packet inspection, and VLAN segmentation.

D. Migrate all 802.11 data devices to WPA-Personal, and implement a secure DHCP server to allocate addresses from a segmented subnet for the Voice over Wi-Fi phones.

Correct Answer: B

QUESTION 6

Given: Your network implements an 802.1X/EAP-based wireless security solution. A WLAN controller is installed and manages seven APs. FreeRADIUS is used for the RADIUS server and is installed on a dedicated server named SRV21. One example client is a MacBook Pro with 8 GB RAM.

What device functions as the 802.1X/EAP Authenticator?

A. SRV21

B. WLAN Controller/AP

C. MacBook Pro

D. RADIUS server

Correct Answer: B

QUESTION 7

You work as the security administrator for your organization. In relation to the WLAN, you are viewing a dashboard that shows security threat, policy compliance and rogue threat charts. What type of system is in view?

A. Wireshark Protocol Analyzer

B. Wireless VPN Management Systems

C. Wireless Intrusion Prevention System

D. Distributed RF Spectrum Analyzer

E. WLAN Emulation System

Correct Answer: C

QUESTION 8

What WLAN client device behavior is exploited by an attacker during a hijacking attack?

A. When the RF signal between a client and an access point is disrupted for more than a few seconds, the client device will attempt to associate to an access point with better signal quality.

B. When the RF signal between a client and an access point is lost, the client will not seek to reassociate with another access point until the 120 second hold down timer has expired.

C. After the initial association and 4-way handshake, client stations and access points do not need to perform another

4-way handshake, even if connectivity is lost.

D. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client-toclient connections, even in an infrastructure BSS.

E. Client drivers scan for and connect to access points in the 2.4 GHz band before scanning the 5 GHz band.

Correct Answer: A

QUESTION 9

When implementing a WPA2-Enterprise security solution, what protocol must the selected RADIUS server support?

A. LWAPP, GRE, or CAPWAP

B. IPSec/ESP

C. EAP

D. CCMP and TKIP

E. LDAP

Correct Answer: C

QUESTION 10

What is the purpose of the Pairwise Transient Key (PTK) in IEEE 802.11 Authentication and Key Management?

A. The PTK is a type of master key used as an input to the GMK, which is used for encrypting multicast data frames.

B. The PTK contains keys that are used to encrypt unicast data frames that traverse the wireless medium.

C. The PTK is XOR\\'d with the PSK on the Authentication Server to create the AAA key.

D. The PTK is used to encrypt the Pairwise Master Key (PMK) for distribution to the 802.1X Authenticator prior to the 4-Way Handshake.

Correct Answer: B

QUESTION 11

When using the 802.1X/EAP framework for authentication in 802.11 WLANs, why is the 802.1X Controlled Port still blocked after the 802.1X/EAP framework has completed successfully?

A. The 802.1X Controlled Port is always blocked, but the Uncontrolled Port opens after the EAP authentication process completes.

B. The 802.1X Controlled Port remains blocked until an IP address is requested and accepted by the Supplicant.

C. The 4-Way Handshake must be performed before the 802.1X Controlled Port changes to the unblocked state.

D. The 802.1X Controlled Port is blocked until Vender Specific Attributes (VSAs) are exchanged inside a RADIUS packet between the Authenticator and Authentication Server.

Correct Answer: C

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