CWNP.CWSP-207.by.Jeny.35q

Number: CWSP-207
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: CWSP-207

Exam Name: Certified Wireless Security Professional Exam

Exam A

QUESTION 1
What EAP type supports using MS-CHAPv2, EAP-GTC or EAP-TLS for wireless client authentication?

A. H-REAP
B. EAP-GTC
C. EAP-TTLS
D. PEAP
E. LEAP

Correct Answer: D
Section:

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

Correct Answer: C, D
Section:

QUESTION 3
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: B, E
Section:

QUESTION 4
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
Section:

QUESTION 5
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: A, C, E
Section:

QUESTION 6
Given: Your organization is using EAP as an authentication framework with a specific type that meets the requirements of your corporate policies.
Which one of the following statements is true related to this implementation?

A. The client will be the authenticator in this scenario.

B. The client STAs must use a different, but complementary, EAP type than the AP STAs.

C. The client STAs may communicate over the uncontrolled port in order to authenticate as soon as Open System authentication completes.

D. The client STAs may communicate over the controlled port in order to authenticate as soon as the Open System authentication completes.

Correct Answer: C
Section:

QUESTION 7
Role-Based Access Control (RBAC) allows a WLAN administrator to perform what network function?

A. Minimize traffic load on an AP by requiring mandatory admission control for use of the Voice access category.

B. Allow access to specific files and applications based on the user's WMM access category.

C. Provide two or more user groups connected to the same SSID with different levels of network privileges.

D. Allow simultaneous support for multiple EAP types on a single access point.

Correct Answer: C
Section:

QUESTION 8
Given: ABC Company is deploying an IEEE 802.11-compliant wireless security solution using 802.1X/EAP authentication. According to company policy, the security solution must prevent an eavesdropper from decrypting data frames traversing a wireless connection.
What security characteristics and/or components play a role in preventing data decryption? (Choose 2)

A. Multi-factor authentication
B. 4-Way Handshake
C. PLCP Cyclic Redundancy Check (CRC)
D. Encrypted Passphrase Protocol (EPP)
E. Integrity Check Value (ICV)
F. Group Temporal Keys

Correct Answer: B, F
Section:

QUESTION 9
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
Section:

QUESTION 10
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: C, D, E
Section:

QUESTION 11
Given: A large enterprise is designing a secure, scalable, and manageable 802.11n WLAN that will support thousands of users. The enterprise will support both 802.1X/EAP-TTLS and PEAPv0/MSCHAPv2. Currently, the company is upgrading network servers as well and will replace their existing Microsoft IAS implementation with Microsoft NPS, querying Active Directory for user authentication.
For this organization, as they update their WLAN infrastructure, what WLAN controller feature will likely be least valuable?

A. WPA2-Enterprise authentication/encryption
B. Internal RADIUS server
C. WIPS support and integration
D. 802.1Q VLAN trunking
E. SNMPv3 support

Correct Answer: B
Section:

QUESTION 12
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-to-client 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
Section:

QUESTION 13
Given: When the CCMP cipher suite is used for protection of data frames, 16 bytes of overhead are added to the Layer 2 frame. 8 of these bytes comprise the MIC.
What purpose does the encrypted MIC play in protecting the data frame?

A. The MIC is used as a first layer of validation to ensure that the wireless receiver does not incorrectly process corrupted signals.
B. The MIC provides for a cryptographic integrity check against the data payload to ensure that it matches the original transmitted data.
C. The MIC is a hash computation performed by the receiver against the MAC header to detect replay attacks prior to processing the encrypted payload.
D. The MIC is a random value generated during the 4-way handshake and is used for key mixing to enhance the strength of the derived PTK.

Correct Answer: B
Section:

QUESTION 14
Given: XYZ Company has recently installed an 802.11ac WLAN. The company needs the ability to control access to network services, such as file shares, intranet web servers, and Internet access based on an employee's job responsibilities.
What WLAN security solution meets this requirement?

A. An autonomous AP system with MAC filters
B. WPA2-Personal with support for LDAP queries
C. A VPN server with multiple DHCP scopes
D. A WLAN controller with RBAC features
E. A WLAN router with wireless VLAN support

Correct Answer: D
Section:

QUESTION 15
Given: Your network includes a controller-based WLAN architecture with centralized data forwarding. The AP builds an encrypted tunnel to the WLAN controller. The WLAN controller is uplinked to the network via a trunked 1 Gbps Ethernet port supporting all necessary VLANs for management, control, and client traffic.
What processes can be used to force an authenticated WLAN client's data traffic into a specific VLAN as it exits the WLAN controller interface onto the wired uplink? (Choose 3)

A. On the Ethernet switch that connects to the AP, configure the switch port as an access port (not trunking) in the VLAN of supported clients.

B. During 802.1X authentication, RADIUS sends a return list attribute to the WLAN controller assigning the user and all traffic to a specific VLAN.

C. In the WLAN controller's local user database, create a static username-to-VLAN mapping on the WLAN controller to direct data traffic from a specific user to a designated VLAN.

D. Configure the WLAN controller with static SSID-to-VLAN mappings; the user will be assigned to a VLAN according to the SSID being used.

Correct Answer: B, C, D
Section:

QUESTION 16
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
Section:

QUESTION 17
What statements are true about 802.11-2012 Protected Management Frames? (Choose 2)

A. 802.11w frame protection protects against some Layer 2 denial-of-service (DoS) attacks, but it cannot prevent all types of Layer 2 DoS attacks.

B. When frame protection is in use, the PHY preamble and header as well as the MAC header are encrypted with 256- or 512-bit AES.

C. Authentication, association, and acknowledgment frames are protected if management frame protection is enabled, but deauthentication and disassociation frames are not.

D. Management frame protection protects disassociation and deauthentication frames.

Correct Answer: A, D
Section:

QUESTION 18
A single AP is configured with three separate WLAN profiles, as follows:
1. SSID: ABCData -- BSSID: 00:11:22:00:1F:C3 -- VLAN 10 -- Security: PEAPv0/EAP-MSCHAPv2 with AES-CCMP -- 3 current clients
2. SSID: ABCVoice -- BSSID: 00:11:22:00:1F:C4 -- VLAN 60 -- Security: WPA2-Personal with AES-CCMP -- 2 current clients
3. SSID: Guest -- BSSID: 00:11:22:00:1F:C5 -- VLAN 90 -- Security: Open with captive portal authentication -- 3 current clients
Three STAs are connected to ABCData. Three STAs are connected to Guest. Two STAs are connected to ABCVoice.
How many unique GTKs and PTKs are currently in place in this scenario?

A. 1 GTK -- 8 PTKs

B. 2 GTKs -- 5 PTKs

C. 2 GTKs -- 8 PTKs

D. 3 GTKs -- 8 PTKs

Correct Answer: B
Section:

QUESTION 19
Which one of the following is a valid reason to avoid the use of EAP-MD5 in production WLANs?

A. It does not support the outer identity.
B. It is not a valid EAP type.
C. It does not support mutual authentication.
D. It does not support a RADIUS server.

Correct Answer: C
Section:

QUESTION 20
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
Section:

QUESTION 21
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
Section:

QUESTION 22
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
Section:

QUESTION 23
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: B, C
Section:

QUESTION 24
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
Section:

QUESTION 25
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: A, B, D
Section:

QUESTION 26
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.

Correct Answer: C
Section:

QUESTION 27
Given: You have a Windows laptop computer with an integrated, dual-band, Wi-Fi compliant adapter. Your laptop computer has protocol analyzer software installed that is capable of capturing and decoding 802.11ac data.
What statement best describes the likely ability to capture 802.11ac frames for security testing purposes?

A. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.
B. Integrated 802.11ac adapters are not typically compatible with protocol analyzers in Windows laptops. It is often best to use a USB adapter or carefully select a laptop with an integrated adapter that will work.
C. Laptops cannot be used to capture 802.11ac frames because they do not support MU-MIMO.
D. Only Wireshark can be used to capture 802.11ac frames as no other protocol analyzer has implemented the proper frame decodes.
E. The only method available to capture 802.11ac frames is to perform a remote capture with a compatible access point.

Correct Answer: B
Section:

QUESTION 28
In order to acquire credentials of a valid user on a public hot-spot network, what attacks may be conducted? Choose the single completely correct answer.

A. Social engineering and/or eavesdropping
B. RF DoS and/or physical theft
C. MAC denial of service and/or physical theft
D. Authentication cracking and/or RF DoS
E. Code injection and/or XSS

Correct Answer: A
Section:

QUESTION 29
Given: AAA is an architectural framework used to provide three separate security components in a network. Listed below are three phrases that each describe one aspect of the AAA framework.
Option-1 --- This AAA function is performed first and validates user identify prior to determining the network resources to which they will be granted access.
Option-2 --- This function is used for monitoring and auditing purposes and includes the collection of data that identifies what a user has done while connected.
Option-3 --- This function is used to designate permissions to a particular user.
What answer correctly pairs the AAA component with the descriptions provided above?

A. Option-1 -- Access Control Option-2 -- Authorization Option-3 -- Accounting
B. Option-1 -- Authentication Option-2 -- Accounting Option-3 -- Association
C. Option-1 -- Authorization Option-2 -- Access Control Option-3 -- Association
D. Option-1 -- Authentication Option-2 -- Accounting Option-3 -- Authorization

Correct Answer: D
Section:

QUESTION 30
You have an AP implemented that functions only using 802.11-2012 standard methods for the WLAN communications on the RF side and implementing multiple SSIDs and profiles on the management side configured as

follows:
1. SSID: Guest -- VLAN 90 -- Security: Open with captive portal authentication -- 2 current clients
2. SSID: ABCData -- VLAN 10 -- Security: PEAPv0/EAP-MSCHAPv2 with AES-CCMP -- 5 current clients
3. SSID: ABCVoice -- VLAN 60 -- Security: WPA2-Personal -- 2 current clients
Two client STAs are connected to ABCData and can access a media server that requires authentication at the Application Layer and is used to stream multicast video streams to the clients.
What client stations possess the keys that are necessary to decrypt the multicast data packets carrying these videos?

A. Only the members of the executive team that are part of the multicast group configured on the media server
B. All clients that are associated to the AP using the ABCData SSID
C. All clients that are associated to the AP using any SSID
D. All clients that are associated to the AP with a shared GTK, which includes ABCData and ABCVoice.

Correct Answer: B
Section:

QUESTION 31
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
Section:

QUESTION 32
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
Section:

QUESTION 33
When used as part of a WLAN authentication solution, what is the role of LDAP?

A. A data retrieval protocol used by an authentication service such as RADIUS
B. An IEEE X.500 standard compliant database that participates in the 802.1X port-based access control process
C. A SQL compliant authentication service capable of dynamic key generation and distribution
D. A role-based access control protocol for filtering data to/from authenticated stations.
E. An Authentication Server (AS) that communicates directly with, and provides authentication for, the Supplicant.

Correct Answer: A
Section:

QUESTION 34
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
Section:

QUESTION 35
Given: ABC Company is implementing a secure 802.11 WLAN at their headquarters (HQ) building in New York and at each of the 10 small, remote branch offices around the United States. 802.1X/EAP is ABC's preferred security solution, where possible. All access points (at the HQ building and all branch offices) connect to a single WLAN controller located at HQ. Each branch office has only a single AP and minimal IT resources.
What security best practices should be followed in this deployment scenario?

A. An encrypted VPN should connect the WLAN controller and each remote controller-based AP, or each remote site should provide an encrypted VPN tunnel to HQ.
B. APs at HQ and at each branch office should not broadcast the same SSID; instead each branch should have a unique ID for user accounting purposes.
C. RADIUS services should be provided at branch offices so that authentication server and supplicant credentials are not sent over the Internet.
D. Remote management of the WLAN controller via Telnet, SSH, HTTP, and HTTPS should be prohibited across the WAN link.

Correct Answer: A
Section: