ENCOR v1.1 (350-401) Video Training Series
Module 5 – Lesson 3 Quiz

Questions

1. Which native extensible authentication protocol (EAP) type uses certificates for mutual authentication?

   A. EAP-TLS
   B. EAP-MD5
   C. EAP-SSL
   D. EAP-MSCHAPv2

2. Which type of web-based authentication (WebAuth) leverages an external AAA server that works as a centralized RADIUS database, such as Cisco Identity Services Engine (ISE)?

   A. Local WebAuth
   B. Distributed WebAuth
   C. Central WebAuth
   D. Client-Server WebAuth

3. Which encryption standard is leveraged by WPA2 and WPA3 for more advanced encryption and protection?

   A. SSL
   B. TKIP
   C. AES
   D. SHA

4. Identify the component of the EAPOL 4-Way Handshake used to encrypt unicast traffic?

   A. GMK
   B. MIC
   C. ANonce
   D. PTK

Questions and Answers

1. Which native extensible authentication protocol (EAP) type uses certificates for mutual authentication?

   A. EAP-TLS
   B. EAP-MD5
   C. EAP-SSL
   D. EAP-MSCHAPv2

Answer: A
Explanation: EAP-TLS is one of the most commonly used native EAP types. This is considered to be one of the most secure EAP types and is one of the original authentication methods defined by the IEEE 802.1X standard. This requires a certificate authority in order to use X.509 certificates for mutual authentication between the client and server.

Video Reference: Overview of Extensible Authentication Protocols (EAPs)

2. Which type of web-based authentication (WebAuth) leverages an external AAA server that works as a centralized RADIUS database, such as Cisco Identity Services Engine (ISE)?

   A. Local WebAuth
   B. Distributed WebAuth
   C. Central WebAuth
   D. Client-Server WebAuth

Answer: C
Explanation: Central WebAuth redirects network client browsers to a central WebAuth server, which requires the client to login with valid credentials in order to obtain authentication and authorization. This is used in larger deployments that contain a centralized RADIUS database such as Cisco ISE.

Video Reference: Overview of WebAuth

3. Which encryption standard is leveraged by WPA2 and WPA3 for more advanced encryption and protection?

   A. SSL
   B. TKIP
   C. AES
   D. SHA

Answer: C
Explanation: TKIP and AES are two encryption standards leveraged by WPA for securing a wireless network. The temporal key integrity protocol (TKIP) is the original standard used by WPA, combining a key string and SSID in order to generate unique encryption keys. Due to this being susceptible to attacks, WPA2 and WPA3 moved to advanced encryption standard (AES) for improved encryption capabilities with a more advanced algorithm.

Video Reference: Pre-Shared Key (PSK) Theory

4. Identify the component of the EAPOL 4-Way Handshake used to encrypt unicast traffic?

A. GMK
B. MIC
C. ANonce
D. PTK

Answer: D
Explanation: The Groupwise Master Key (GMK) is generated during EAP authentication and is known by both the Supplicant and the Authenticator. The GMK protects multicast and broadcast traffic.

The MIC (Message Integrity Code) is used to confirm a frame has not been modified in transit.

The ANonce is a random number generated by the Authenticator, while the SNonce is a random number generated by the Supplicant.

The PTK (Pairwise Transient Key) encrypts unicast traffic between the Supplicant (i.e., the wireless client) and its Authenticator (i.e., its access point).

Video Reference: Understanding the EAPOL 4-Way Handshake