Certified Wireless Security Professional (CWSP)

1. Given: Mary has just finished troubleshooting an 802.11g network performance problem using a laptop-based WLAN protocol analyzer. The wireless network implements 802.1X/PEAP and the client devices are authenticating properly. When Mary disables the WLAN protocol analyzer, configures her laptop for PEAP authentication, and then tries to connect to the wireless network, she is unsuccessful. Before using the WLAN protocol analyzer, Mary's laptop connected to the network without any problems.

A. Mary's supplicant software is using PEAPv0/EAP-MSCHAPv2, and the access point is using PEAPv1/EAP-GTC.

B. The PEAP client's certificate was voided when the protocol analysis software assumed control of the wireless adapter.

C. The nearby WIPS sensor categorized Mary's protocol analyzer adapter as a threat and is performing a deauthentication flood against her computer.

D. The protocol analyzer's network interface card (NIC) drivers are still loaded and do not support the version of PEAP being used.

Answer(s): D

---

2. Wireless Intrusion Prevention Systems (WIPS) are used for what purposes? (Choose 3)

A. Performance monitoring and troubleshooting

B. Security monitoring and notification

C. Preventing physical carrier sense attacks

D. Enforcing wireless network security policy

E. Detecting and defending against eavesdropping attacks

F. Classifying wired client devices

Answer(s): A,B,D

---

3. 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.

A. 802.11n client spoofing the MAC address of an authorized 802.11n client

B. Hijacking attack performed by using a rogue 802.11n AP against an 802.11a client

C. Rogue AP operating in Greenfield 40 MHz-only mode

D. 802.11a STA performing a deauthentication attack against 802.11n APs

Answer(s): C

---

4. 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. Wireless Intrusion Prevention System

B. Wireshark Protocol Analyzer

C. Wireless VPN Management Systems

D. Distributed RF Spectrum Analyzer

E. WLAN Emulation System

Answer(s): A

---

5. 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.

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

B. Use enterprise WIPS on the corporate office network

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

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

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

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

Answer(s): C

---

6. 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

Answer(s): D

---

7. Given: WLAN protocol analyzers can read and record many wireless frame parameters.

A. BSSID

B. Signal strength

C. RSN IE

D. SSID

E. Noise floor

F. IP Address

Answer(s): B

---

8. You are implementing a wireless LAN that will be used by point-of-sale (PoS) systems in a retail environment. Thirteen PoS computers will be installed. To what industry requirement should you ensure you adhere?

A. HIPAA

B. Directive 8500.01

C. ISA99

D. PCI-DSS

Answer(s): D

---

9. Given: A WLAN protocol analyzer trace reveals the following sequence of frames (excluding the ACK frames): 1) 802.11 Probe Req and 802.11 Probe Rsp 2) 802.11 Auth and then another 802.11 Auth 3) 802.11 Assoc Req and 802.11 Assoc Rsp 4) EAPOL-KEY 5) EAPOL-KEY 6) EAPOL-KEY 7) EAPOL-KEY

A. EAP-TLS

B. 802.1X/LEAP

C. WEP-128

D. WPA2-Personal

E. WPA-Enterprise

Answer(s): D

---

10. 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.

A. Layer 2 Disassociation attacks

B. Robust management frame replay attacks

C. Social engineering attacks

D. RF DoS attacks

Answer(s): A,B

---

11. 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 is always more expensive than overlay WIPS.

B. Integrated WIPS always perform better from a client throughput perspective because the same radio that performs the threat scanning also services the clients.

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 use special sensors installed alongside the APs to scan for threats.

Answer(s): C

---

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

A. Hijacking attacks interrupt a user's legitimate connection and introduce a new connection with an evil twin AP.

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

C. RF DoS attacks prevent successful wireless communication on a specific frequency or frequency range.

D. Management interface exploit attacks are attacks that use social engineering to gain credentials from managers.

E. Social engineering attacks are performed to collect sensitive information from unsuspecting users

F. Zero-day attacks are always authentication or encryption cracking attacks.

Answer(s): A,C,E

---

13. Given: ABC Company has 20 employees and only needs one access point to cover their entire facility. Ten of ABC Company's employees have laptops with radio cards capable of only WPA security. The other ten employees have laptops with radio cards capable of WPA2 security. The network administrator wishes to secure all wireless communications (broadcast and unicast) for each laptop with its strongest supported security mechanism, but does not wish to implement a RADIUS/AAA server due to complexity.

A. Implement two separate SSIDs on the AP-one for WPA-Personal using TKIP and one for WPA2-Personal using AES-CCMP.

B. Implement an SSID with WPA-Personal that allows both AES-CCMP and TKIP clients to connect.

C. Implement an SSID with WPA2-Personal that sends all broadcast traffic using AESCCMP and unicast traffic using either TKIP or AES-CCMP.

D. Implement an SSID with WPA2-Personal that allows both AES-CCMP and TKIP clients to connect.

Answer(s): A

---

14. 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.

A. The only method available to capture 802.11ac frames is to perform a remote capture with a compatible access point.

B. Laptops cannot be used to capture 802.11ac frames because they do not support MUMIMO.

C. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.

D. Only Wireshark can be used to capture 802.11ac frames as no other protocol analyzer has implemented the proper frame decodes.

E. 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.

Answer(s): E

---

15. The following numbered items show some of the contents of each of the four frames exchanged during the 4-way handshake:

A. 1, 2, 3, 4

B. 2, 3, 4, 1

C. 4, 3, 1, 2

D. 3, 4, 1, 2

Answer(s): D

---

16. After completing the installation of a new overlay WIPS for the purpose of rogue detection and security monitoring at your corporate headquarters, what baseline function MUST be performed in order to identify security threats?

A. WLAN devices that are discovered must be classified (rogue, authorized, neighbor, etc.) and a WLAN policy must define how to classify new devices.

B. Upstream and downstream throughput thresholds must be specified to ensure that service-level agreements are being met.

C. Separate security profiles must be defined for network operation in different regulatory domains

D. Authorized PEAP usernames must be added to the WIPS server's user database.

Answer(s): A

---

17. 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.

A. A WLAN router with wireless VLAN support

B. WPA2-Personal with support for LDAP queries

C. An autonomous AP system with MAC filters

D. A WLAN controller with RBAC features

E. A VPN server with multiple DHCP scopes

Answer(s): D

---

18. You must support a TSN as you have older wireless equipment that will not support the required processing of AES encryption. Which one of the following technologies will you use on the network so that a TSN can be implemented that would not be required in a network compliant with 802.11-2012 non-deprecated technologies?

A. RC4

B. CCMP

C. WEP

D. WPA2

Answer(s): A

---

19. Given: You view a protocol analyzer capture decode with the following protocol frames listed in the following order (excluding the ACK frames):

A. 802.1X with Dynamic WEP

B. WPA2-Personal authentication

C. 802.11 Open System authentication

D. Wi-Fi Protected Setup with PIN

E. Active Scanning

F. WPA2-Enterprise authentication

G. 4-Way Handshake

Answer(s): C,E,F,G

---

20. Given: You must implement 7 APs for a branch office location in your organization.

A. Administrative password

B. Output power

C. Fragmentation threshold

D. Cell radius

Answer(s): A
