QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

Cisco

CWSP-205

Certified Wireless Security Professional

QUESTION: 107
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. What statement indicates why Mary cannot access the network from her laptop computer?

A. The nearby WIPS sensor categorized Mary's protocol analyzer adapter as a threat and is performing a deauthentication flood against her computer.
B. The PEAP client's certificate was voided when the protocol analysis software assumed control of the wireless adapter.
C. The protocol analyzer's network interface card (NIC) drivers are still loaded and do not support the version of PEAP being used.
D. Mary's supplicant software is using PEAPv0/EAP-MSCHAPv2, and the access point is using PEAPv1/EAP- GTC.

Answer: C

QUESTION: 108
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. ISA99
B. HIPAA
C. PCI-DSS
D. Directive 8500.01

Answer: C

QUESTION: 109
Given: You view a protocol analyzer capture decode with the following protocol frames listed in the following order (excluding the ACK frames):
1) 802.11 Probe Request and 802.11 Probe Response
2) 802.11 Auth and another 802.11 Auth
2) 802.11 Assoc Req and 802.11 Assoc Rsp

4) EAPOL-Start
5) EAP Request and EAP Response
6) EAP Request and EAP Response
7) EAP Request and EAP Response
8) EAP Request and EAP Response
9) EAP Request and EAP Response
10) EAP Success
19) EAPOL-Key (4 frames in a row)
What are you seeing in the capture file? (Choose 4)

A. WPA2-Enterprise authentication
B. WPA2-Personal authentication
C. 802.11 Open System authentication
D. 802.1X with Dynamic WEP
E. Wi-Fi Protected Setup with PIN
F. Active Scanning
G. 4-Way Handshake

Answer: A, C, F, G

QUESTION: 110
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

Answer: B, E

QUESTION: 111
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

Answer: A, C, E

QUESTION: 112
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

Answer: B

QUESTION: 113
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

Answer: B

QUESTION: 114
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.

Answer: C

QUESTION: 115
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: D

QUESTION: 116
ABC Company has deployed a Single Channel Architecture (SCA) solution to help overcome some of the common problems with client roaming. In such a network, all APs are configured with the same channel and BSSID. PEAPv0/EAP-MSCHAPv2 is the only supported authentication mechanism. As the Voice over Wi-Fi (STA-1) client moves throughout this network, what events are occurring?

A. STA-1 initiates open authentication and 802.11 association with each AP prior to roaming.
B. The WLAN controller is querying the RADIUS server for authentication before the association of STA-1 is moved from one AP to the next.

C. STA-1 controls when and where to roam by using signal and performance metrics in accordance with the chipset drivers and 802.11k.
D. The WLAN controller controls the AP to which STA-1 is associated and transparently moves this association in accordance with the physical location of STA-1.

Answer: D

QUESTION: 117
Select the answer option that arranges the numbered events in the correct time sequence (first to last) for a client associating to a BSS using EAP-PEAPv0/MSCHAPv2.
1. Installation of PTK
2. Initiation of 4-way handshake
3. Open system authentication
4. 802.11 association
5. 802.1X controlled port is opened for data traffic
6. Client validates server certificate
7. AS validates client credentials

A.3--4--6--7--2--1--5
B.4--3--5--2--7--6--1
C.5--3--4--2--6--7--1
D.6--1--3--4--2--7—5
E.4--3--2--7--6--1--5
F.3--4--7--6--5--2--1

Answer: A

QUESTION: 118
Given: You have implemented strong authentication and encryption mechanisms for your enterprise 802.11 WLAN using 802.1X/EAP with AES-CCMP. For users connecting within the headquarters office, what other security solution will provide continuous monitoring of both clients and APs with 802.11-specific tracking?

A. IPSec VPN client and server software
B. Internet firewall software
C. Wireless intrusion prevention system
D. WLAN endpoint agent software
E. RADIUS proxy server

Answer: C

QUESTION: 119
You must locate non-compliant 802.11 devices. Which one of the following tools will you use and why?

A. A spectrum analyzer, because it can show the energy footprint of a device using WPA differently from a device using WPA2.
B. A spectrum analyzer, because it can decode the PHY preamble of a non-compliant device.
C. A protocol analyzer, because it can be used to view the spectrum energy of non-compliant 802.11 devices, which is always different from compliant devices.
D. A protocol analyzer, because it can be used to report on security settings and regulatory or rule compliance

Answer: D