CWNP.CWSP-208.v2025-12-29.q49

Exam Code:	CWSP-208
Exam Name:	Certified Wireless Security Professional (CWSP)
Certification Provider:	CWNP
Free Question Number:	49
Version:	v2025-12-29
# of views:	108
# of Questions views:	571
https://www.freecram.net/torrent/CWNP.CWSP-208.v2025-12-29.q49.html	

NEW QUESTION: 1
What drawbacks initially prevented the widespread acceptance and use of Opportunistic Key Caching (OKC)?
A. Sharing cached keys between controllers during inter-controller roaming created vulnerabilities that exposed the keys to attackers.
B. Because OKC is not defined by any standards or certification body, client support was delayed and sporadic early on.
C. Key exchanges during fast roams required processor-intensive cryptography, which was prohibitive for legacy devices supporting only TKIP.
D. The Wi-Fi Alliance continually delayed the creation of a client certification for OKC, even though it was defined by IEEE 802.11r.
Answer: (SHOW ANSWER)
Opportunistic Key Caching (OKC) is a non-standardized fast roaming method that allows clients to roam between APs without repeating the full 802.1X/EAP authentication process.
OKC was proposed by vendors (not the IEEE or Wi-Fi Alliance), so there was no formal certification early on.
This led to inconsistent and delayed client support, preventing widespread adoption.
Incorrect:
A). OKC does not involve inter-controller roaming in most scenarios; it's a local caching method.
C). The cryptographic overhead was not a significant barrier compared to lack of standardization.
D). OKC was not defined in IEEE 802.11r-Fast BSS Transition (FT) was.
References:
CWSP-208 Study Guide, Chapter 6 (Fast Secure Roaming)
CWNP Wireless Mobility Standards Overview

NEW QUESTION: 2

While performing a manual scan of your environment using a spectrum analyzer on a laptop computer, you notice a signal in the real time FFT view. The signal is characterized by having peak power centered on channel 11 with an approximate width of 20 MHz at its peak. The signal widens to approximately 40 MHz after it has weakened by about 30 dB.
What kind of signal is displayed in the spectrum analyzer?
A. A frequency hopping device is being used as a signal jammer in 5 GHz
B. A low-power wideband RF attack is in progress in 2.4 GHz, causing significant 802.11 interference
C. An 802.11g AP operating normally in 2.4 GHz
D. An 802.11a AP operating normally in 5 GHz
Answer: (SHOW ANSWER)
An 802.11g AP uses a 20 MHz-wide channel centered around a specific frequency (e.g., channel 11 at 2.462 GHz). On a spectrum analyzer:
The signal will peak at the center frequency with high power.
The width of approximately 20 MHz at peak and extending to 40 MHz as it drops 30 dB is typical for OFDM- based transmissions (802.11g uses OFDM).
Incorrect:
A). Frequency hopping is characteristic of Bluetooth and looks different on the spectrum (bursty, narrow signals that shift rapidly).
B). A wideband attack would appear more constant and not centered like a normal AP.
D). 802.11a operates in the 5 GHz band, not channel 11 (which is 2.4 GHz).
References:
CWSP-208 Study Guide, Chapter 6 (RF Analysis and Interference)
CWNP RF Spectrum Interpretation Guide

NEW QUESTION: 3
Given: XYZ Company has recently installed a controller-based WLAN and is using a RADIUS server to query authentication requests to an LDAP server. XYZ maintains user-based access policies and would like to use the RADIUS server to facilitate network authorization.
What RADIUS features could be used by XYZ to assign the proper network permissions to users during authentication? (Choose 2)
A. The RADIUS server can communicate with the DHCP server to issue the appropriate IP address and VLAN assignment to users.
B. The RADIUS server can support vendor-specific attributes in the ACCESS-ACCEPT response, which can be used for user policy assignment.
C. RADIUS can reassign a client's 802.11 association to a new SSID by referencing a username-to-SSID mapping table in the LDAP user database.
D. RADIUS can send a DO-NOT-AUTHORIZE demand to the authenticator to prevent the STA from gaining access to specific files, but may only employ this in relation to Linux servers.
E. RADIUS attributes can be used to assign permission levels, such as read-only permission, to users of a particular network resource.

Answer: (SHOW ANSWER)

Comprehensive Detailed Explanation:

B). Vendor-Specific Attributes (VSAs) allow integration with WLAN vendors' controllers to assign roles, VLANs, QoS levels, etc., during user authentication.

E). Standard or vendor-specific RADIUS attributes can dynamically assign permission levels based on group membership, department, or role.

Incorrect:

A). RADIUS does not directly manage DHCP functions.

C). SSID is selected by the user's device, not by the RADIUS server.

D). RADIUS uses ACCESS-REJECT, not "DO-NOT-AUTHORIZE," and it is not OS-specific.

References:

CWSP-208 Study Guide, Chapter 4 (RADIUS and Policy Assignment)

CWNP RADIUS Deployment Best Practices

NEW QUESTION: 4

Given: ABC Company secures their network with WPA2-Personal authentication and AES-CCMP encryption.

What part of the 802.11 frame is always protected from eavesdroppers by this type of security?

A. All MSDU contents

B. All MPDU contents

C. All PPDU contents

D. All PSDU contents

Answer: (SHOW ANSWER)

In WPA2-Personal with AES-CCMP:

The MSDU (MAC Service Data Unit), which includes the payload from Layer 3 and above, is encrypted.

This protects the actual application data (e.g., web content, email).

Frame headers (MAC headers) are not encrypted.

Incorrect:

B). MPDU includes MAC headers, which are not encrypted.

C). PPDU includes preamble and physical-layer components, which are never encrypted.

D). PSDU includes the MAC header and frame body; again, headers are not encrypted.

References:

CWSP-208 Study Guide, Chapter 3 (Frame Protection)

IEEE 802.11 Frame Structure Guide

NEW QUESTION: 5

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.
Answer: (SHOW ANSWER)
RBAC enables dynamic assignment of different access privileges (e.g., VLAN, ACLs, bandwidth) to users even when they connect through the same SSID. This simplifies SSID management while maintaining fine- grained access control.
Incorrect:
A). Admission control is a QoS/WMM function, not RBAC.
B). Access category (AC) affects frame prioritization, not file/app access.
D). Multiple EAP types are supported in authentication servers-not directly tied to RBAC.
References:
CWSP-208 Study Guide, Chapter 6 (Role-Based Access Control and SSID Simplification)

NEW QUESTION: 6
What are the three roles of the 802.1X framework, as defined by the 802.1X standard, that are performed by the client STA, the AP (or WLAN controller), and the RADIUS server? (Choose 3)
A. Enrollee
B. Registrar
C. AAA Server
D. Authentication Server
E. Supplicant
F. Authenticator
G. Control Point
Answer: (SHOW ANSWER)
The IEEE 802.1X framework consists of three defined roles:
Supplicant (E): The client device (STA) that requests access to the network.
Authenticator (F): The network device (usually an AP or switch) that enforces access control and acts as an intermediary between the supplicant and the authentication server.
Authentication Server (D): Typically a RADIUS server that validates credentials and responds with access decisions.
Incorrect:
A & B. Enrollee and Registrar are roles in Wi-Fi Protected Setup (WPS), not 802.1X.
C). AAA Server is a broader term; the specific role in 802.1X is "Authentication Server." G). "Control Point" is not a formal 802.1X role.
References:
CWSP-208 Study Guide, Chapter 4 (802.1X Authentication Roles)

NEW QUESTION: 7

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
Answer: (SHOW ANSWER)
For troubleshooting fast roaming (e.g. 802.11r) across channels, a portable protocol analyzer with dual- or multi-band 802.11n adapters enables:
Simultaneous packet capture on different channels
Capturing handoff-related frames and timing analysis in roaming scenarios This setup allows detailed capture of reassociation, authentication, and 4-Way Handshake processes, essential for diagnosing roaming delays.
Other options (WIPS, spectrum analyzer, autonomous AP) do not support detailed 802.11 frame capture across multiple channels during roaming events.
References:
CWSP#207 Study Guide, Chapter 6 (Roaming Troubleshooting)

NEW QUESTION: 8
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
Answer: (SHOW ANSWER)
Comprehensive Detailed Explanation:
On public Wi-Fi hotspots (typically unsecured), attackers often perform:
Eavesdropping: By passively listening to unencrypted traffic, an attacker can capture credentials or sensitive data.
Social engineering: Users may be tricked into entering their credentials on a spoofed login page or disclosing them directly through phishing or manipulation.
These are the most effective and common methods for credential theft in open network environments.
Incorrect:

B & C. Physical theft is not network-based and not relevant to hotspot-based credential acquisition.
D). Authentication cracking is not applicable to open networks with captive portals.
E). Code injection/XSS may happen in web apps but are not directly methods for acquiring hotspot credentials.
References:
CWSP-208 Study Guide, Chapter 5 (Threats and Attacks)
CWNP Security Essentials: Eavesdropping and Social Engineering in WLANs

NEW QUESTION: 9
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
Answer: (SHOW ANSWER)
To prevent data decryption:
B). The 4-Way Handshake derives and installs unique unicast keys (PTKs) on both client and AP.
F). The GTK is used to encrypt broadcast and multicast frames, ensuring group traffic is protected.
Incorrect:
A). Multi-factor authentication enhances identity assurance but not encryption.
C). PLCP CRC checks for transmission errors but does not secure data.
D). EPP is not a valid or recognized encryption protocol.
E). ICV was used in WEP and is cryptographically weak.
References:
CWSP-208 Study Guide, Chapter 3 (Key Hierarchy and 4-Way Handshake)
IEEE 802.11i Standard

NEW QUESTION: 10
A. All WLAN clients will reassociate to the consultant's software AP if the consultant's software AP provides the same SSID on any channel with a 10 dB SNR improvement over the authorized AP.
B. A higher SSID priority value configured in the Beacon frames of the consultant's software AP will take priority over the SSID in the authorized AP, causing the clients to reassociate.

C. When the RF signal between the clients and the authorized AP is temporarily disrupted and the consultant's software AP is using the same SSID on a different channel than the authorized AP, the clients will reassociate to the software AP.
D. If the consultant's software AP broadcasts Beacon frames that advertise 802.11g data rates that are faster rates than XYZ's current 802.11b data rates, all WLAN clients will reassociate to the faster AP.
Answer: (SHOW ANSWER)
Clients seek connectivity when their connection is lost. If the attacker broadcasts a matching SSID on a different channel and the client is disconnected (via RF jamming or deauthentication), the client will often reassociate with the stronger signal or first-responding AP broadcasting the same SSID, even if it's rogue.
Incorrect:
A). SNR alone doesn't force reassociation-clients consider multiple factors.
B). SSID priority is not a standardized field influencing client behavior.
D). Clients won't reassociate based purely on advertised data rates unless connectivity is disrupted and other AP parameters are more attractive.
References:
CWSP-208 Study Guide, Chapter 5 (Hijacking and Evil Twin Attacks)
CWNP Roaming Behavior and Signal Loss Analysis
IEEE 802.11-2016 Standard (Association and Reassociation Behavior)

NEW QUESTION: 11
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: (SHOW ANSWER)
A). WPA2-Enterprise authentication: The multiple EAP Request/Response exchanges followed by an EAP Success and a 4-Way Handshake (EAPOL-Key frames) indicate 802.1X authentication, characteristic of WPA2-Enterprise.
C). 802.11 Open System authentication: Two Auth frames (request and response) without encryption negotiation signify Open System Authentication - a default in RSN setups.
F). Active Scanning: Begins with Probe Request and Probe Response - part of an active scan process.
G). 4-Way Handshake: Identified by four sequential EAPOL-Key frames, completing the authentication process in WPA2.
References:
CWSP-208 Study Guide, Chapter 6 - Frame Analysis of Enterprise Authentication CWNP
CWSP-208 Objectives: "EAP Authentication Flow" and "4-Way Handshake Analysis"

NEW QUESTION: 12
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: (SHOW ANSWER)
In a security context, outdated firmware is one of the most critical vulnerabilities. Firmware updates typically patch known security issues, fix bugs, and provide new features or improved encryption support. If the APs have not been updated or checked in over 18 months, they could be running firmware with known exploits or lacking critical security patches, making firmware review a top priority.
References:
CWSP-208 Study Guide, Chapter 8 - WLAN Security Lifecycle and Maintenance CWNP
CWSP-208 Objectives: "Firmware and Security Patch Management"

NEW QUESTION: 13
Joe's new laptop is experiencing difficulty connecting to ABC Company's 802.11 WLAN using 802.1X/EAP PEAPv0. The company's wireless network administrator assured Joe that his laptop was authorized in the WIPS management console for connectivity to ABC's network before it was given to him. The WIPS termination policy includes alarms for rogue stations, roque APs, DoS attacks and unauthorized roaming.

What is a likely reason that Joe cannot connect to the network?
A. Joe disabled his laptop's integrated 802.11 radio and is using a personal PC card radio with a different chipset, drivers, and client utilities.
B. Joe's integrated 802.11 radio is sending multiple Probe Request frames on each channel.
C. An ASLEAP attack has been detected on APs to which Joe's laptop was trying to associate. The WIPS responded by disabling the APs.
D. Joe configured his 802.11 radio card to transmit at 100 mW to increase his SNR. The WIPS is detecting this much output power as a DoS attack.
Answer: (SHOW ANSWER)
WIPS systems often enforce policies based on MAC addresses and associated hardware fingerprints. If Joe uses a different wireless adapter than the one authorized, it may trigger a rogue device or unauthorized client alarm-even if it's the same laptop. This behavior is common in environments with strict WIPS enforcement policies.

NEW QUESTION: 14
Wireless Intrusion Prevention Systems (WIPS) provide what network security services? (Choose 2)
A. Application-layer traffic inspection
B. Wireless vulnerability assessment
C. Analysis and reporting of AP CPU utilization
D. Policy enforcement and compliance management
E. Configuration distribution for autonomous APs
Answer: (SHOW ANSWER)
WIPS systems provide proactive security by continuously scanning for threats and ensuring WLAN policy compliance. Their capabilities include:
B). Wireless vulnerability assessment: Scanning for misconfigured APs, weak encryption, and unauthorized devices.
E). Policy enforcement and compliance: Ensuring security settings adhere to enterprise or regulatory requirements and alerting on deviations.
Other options like application-layer inspection and AP CPU monitoring are outside the WIPS function scope.
References:
CWSP-208 Study Guide, Chapter 7 - WIPS Services and Capabilities
CWNP CWSP-208 Objectives: "WIPS Threat Mitigation and Enforcement"

NEW QUESTION: 15
For a WIPS system to identify the location of a rogue WLAN device using location patterning (RF fingerprinting), what must be done as part of the WIPS installation?
A. All WIPS sensors must be installed as dual-purpose (AP/sensor) devices.
B. A location chipset (GPS) must be installed with it.
C. At least six antennas must be installed in each sensor.

D. The RF environment must be sampled during an RF calibration process.

Answer: (SHOW ANSWER)

For a WIPS system to perform location patterning (also called RF fingerprinting), it must first perform an RF calibration or RF site survey. This process involves sampling signal strengths from known locations to develop a model of how signals propagate in the environment. This "fingerprint" is then used to triangulate or estimate the positions of rogue devices.

NEW QUESTION: 16

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: (SHOW ANSWER)

When compliance reporting and forensic analysis are required and the WLAN vendor's centralized management system does not provide it, deploying a dedicated overlay WIPS is the most effective solution.

Overlay WIPS uses dedicated sensors independent of the WLAN's operational radios, offering detailed threat detection, compliance logging, and reporting capabilities that often surpass native WLAN features.

References:

CWSP-208 Study Guide, Chapter 7 - Overlay vs Integrated WIPS

CWNP CWSP-208 Objectives: "Compliance Monitoring and Forensics"

NEW QUESTION: 17
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. Authorized PEAP usernames must be added to the WIPS server's user database.
B. WLAN devices that are discovered must be classified (rogue, authorized, neighbor, etc.) and a WLAN policy must define how to classify new devices.
C. Separate security profiles must be defined for network operation in different regulatory domains
D. Upstream and downstream throughput thresholds must be specified to ensure that service-level agreements are being met.
Answer: B (LEAVE A REPLY)
After deploying a WIPS, an essential baseline activity is to classify all detected devices in the RF environment. These classifications allow the system to enforce security policies and detect policy violations.
Classifications include:
Authorized (managed devices)
Rogue (unauthorized, possibly dangerous)
Neighbor (not part of your network but legitimate)
External or Ad hoc devices
Without this initial classification, WIPS cannot properly assess threats or trigger alarms.
References:
CWSP-208 Study Guide, Chapter 7 - WIPS Classification and Threat Management CWNP
CWSP-208 Objectives: "Device Classification and Policy Enforcement"

NEW QUESTION: 18
What security vulnerabilities may result from a lack of staging, change management, and installation procedures for WLAN infrastructure equipment? (Choose 2)
A. The WLAN system may be open to RF Denial-of-Service attacks
B. WIPS may not classify authorized, rogue, and neighbor APs accurately
C. Authentication cracking of 64-bit Hex WPA-Personal PSK
D. Management interface exploits due to the use of default usernames and passwords for AP management
E. AES-CCMP encryption keys may be decrypted
Answer: (SHOW ANSWER)
Without proper staging, change management, and installation procedures, significant vulnerabilities may arise:

(B) WIPS relies on a known database of authorized APs and clients. If devices are deployed without proper registration and staging, WIPS cannot accurately classify devices as authorized, rogue, or neighbor.
(D) If APs are installed without changing default credentials, attackers can exploit them through common web or SNMP-based management interfaces.
This undermines both operational visibility and network security posture.
References:
CWSP-208 Study Guide, Chapter 8 - WLAN Security Design and Architecture CWNP CWSP-208 Official Objectives: "Security Design and Policy Implementation"

NEW QUESTION: 19
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
Answer: (SHOW ANSWER)
A WIPS (Wireless Intrusion Prevention System) is designed to monitor WLAN activity and provide visualization and reporting related to:
Security threats (e.g., DoS attacks, rogue devices)
Policy compliance (e.g., allowed SSIDs, encryption types)
Rogue threat classification (e.g., rogue, neighbor, ad hoc)
The dashboard displaying this type of security-centric overview is characteristic of a WIPS platform.
References:
CWSP-208 Study Guide, Chapter 7 - WIPS Visualization and Monitoring
CWNP CWSP-208 Objectives: "Threat Visualization and Reporting"

NEW QUESTION: 20
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: (SHOW ANSWER)
An 802.11a/g-based WIPS cannot detect rogue activity that occurs in 802.11n/ac-specific modes, including Greenfield (HT-only) operation and use of 40 MHz channels, which are not part of the 802.11a/g specification. Greenfield mode disables legacy support, so a WIPS limited to 802.11a/g radios won't even

"see" these frames. This leaves a significant blind spot for detecting certain types of rogue devices or attacks using newer PHYs.
References:
CWSP-208 Study Guide, Chapter 7 - WIPS Capabilities and Limitations
CWNP CWSP-208 Objectives: "Protocol Compatibility and Threat Detection"

NEW QUESTION: 21
The IEEE 802.11 standard defined Open System authentication as consisting of two auth frames and two assoc frames. In a WPA2-Enterprise network, what process immediately follows the 802.11 association procedure?
A. Group Key Handshake
B. 802.1X/EAP authentication
C. DHCP Discovery
D. 4-Way Handshake
E. Passphrase-to-PSK mapping
F. RADIUS shared secret lookup
Answer: (SHOW ANSWER)
In WPA2-Enterprise:
After successful Open System authentication and 802.11 association, the next step is 802.1X/EAP authentication via EAPOL frames.
This phase establishes user identity and derives the PMK.
Incorrect:
A). Group Key Handshake comes after the 4-Way Handshake.
C). DHCP occurs after authentication and key negotiation.
D). 4-Way Handshake follows successful 802.1X authentication.
E). PSK mapping applies to WPA2-Personal, not Enterprise.
F). The RADIUS shared secret is pre-configured between authenticator and RADIUS server-not part of real- time negotiation.
References:
CWSP-208 Study Guide, Chapter 3 (Authentication and Association Flowchart) IEEE 802.11-2012 Standard

NEW QUESTION: 22
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.
Answer: (SHOW ANSWER)
Client VLAN assignment at the controller can be achieved through:
B). RADIUS attributes (e.g., Tunnel-Private-Group-ID) for dynamic VLAN assignment.
C). Static mappings in the WLAN controller's local user DB.
D). SSID-to-VLAN bindings assign traffic from specific SSIDs to specific VLANs.
Incorrect:
A). The AP connects to the controller over a tunneled link. VLAN configuration at the AP's Ethernet port does not impact client VLAN assignment in centralized forwarding mode.
References:
CWSP-208 Study Guide, Chapter 6 (Dynamic VLAN Assignment)
CWNP WLAN Controller Configuration Guides

NEW QUESTION: 23
What TKIP feature was introduced to counter the weak integrity check algorithm used in WEP?
A. 32-bit ICV (CRC-32)
B. Sequence counters
C. RC5 stream cipher
D. Michael
E. Block cipher support
Answer: (SHOW ANSWER)
TKIP (used with WPA) introduced "Michael" as a message integrity check (MIC) algorithm to replace the insecure CRC-32 used in WEP. Michael:
Adds tamper protection to each packet.
Helps detect packet forgery.
Incorrect:
A). CRC-32 was used in WEP and proven weak.
B). Sequence counters help prevent replay attacks, not integrity checking.
C). RC5 is not used in WLAN security.
E). TKIP does not support block ciphers-it uses RC4, a stream cipher.
References:
CWSP-208 Study Guide, Chapter 3 (TKIP Security Features)

NEW QUESTION: 24
Given: Your company has just completed installation of an IEEE 802.11 WLAN controller with 20 controller- based APs. The CSO has specified PEAPv0/EAP-MSCHAPv2 as the only authorized

WLAN authentication mechanism. Since an LDAP-compliant user database was already in use, a RADIUS server was installed and is querying authentication requests to the LDAP server.
Where must the X.509 server certificate and private key be installed in this network?
A. Supplicant devices
B. LDAP server
C. Controller-based APs
D. WLAN controller
E. RADIUS server
Answer: (SHOW ANSWER)
With PEAPv0/EAP-MSCHAPv2:
The TLS tunnel is created between the supplicant and the RADIUS server.
Therefore, the RADIUS server must have the X.509 server certificate and private key to authenticate itself and establish the tunnel.
Incorrect:
A). Supplicants verify the server's certificate, not hold it.
B). LDAP server is used for querying, not for EAP termination.
C). APs and
D). Controllers pass the authentication info but don't require certificates for PEAP termination.
References:
CWSP-208 Study Guide, Chapter 4 (EAP Types and TLS Tunnel Establishment) CWNP EAP Deployment Guidelines

NEW QUESTION: 25
What security benefits are provided by endpoint security solution software? (Choose 3)
A. Can prevent connections to networks with security settings that do not conform to company policy
B. Can collect statistics about a user's network use and monitor network threats while they are connected
C. Can restrict client connections to networks with specific SSIDs and encryption types
D. Can be used to monitor for and prevent network attacks by nearby rogue clients or APs
Answer: (SHOW ANSWER)
Endpoint security software can:
A). Enforce network access policies by validating that security settings meet organizational standards.
B). Monitor usage for auditing and threat detection.
C). Limit network connectivity based on SSID names, encryption, and authentication parameters.
Incorrect:
D). Detecting rogue APs and clients is typically done by WIPS, not endpoint security agents.
References:
CWSP-208 Study Guide, Chapter 7 (Client Security and Endpoint Enforcement) CWNP Endpoint Security and Compliance Policies

NEW QUESTION: 26
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
Answer: (SHOW ANSWER)
Given that only consumer-grade routers are used and no RADIUS server or enterprise infrastructure is mentioned, WPA2-Personal is the most secure option available. It uses a pre-shared key (PSK) for authentication and AES-CCMP for encryption, offering strong protection for small businesses lacking enterprise equipment.
Enterprise methods such as WPA2-Enterprise, 802.1X, and EAP-PEAP require a RADIUS server or authentication backend, which isn't supported in typical consumer-grade routers.
References:
CWSP-208 Study Guide, Chapter 3 (WLAN Security Technologies)
CWNP Wi-Fi Security Deployment Guide for Small Businesses
CWNP E-Learning Modules: WPA2-PSK vs WPA2-Enterprise

NEW QUESTION: 27
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
Answer: (SHOW ANSWER)
802.11w, also known as Protected Management Frames (PMF), is designed to protect specific types of 802.11 management frames such as disassociation and deauthentication frames. These frames were previously sent unencrypted and could be spoofed by attackers to disconnect clients (DoS attacks). With 802.11w, these frames are cryptographically protected, mitigating such attacks.

PMF also includes replay protection for these management frames, preventing attackers from capturing and replaying them to disrupt network connectivity.
References:
CWSP-208 Study Guide, Chapter 6 (Wireless LAN Security Solutions)
IEEE 802.11w-2009 amendment
CWNP Whitepapers on PMF and Management Frame Protection

NEW QUESTION: 28
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: (SHOW ANSWER)
WIPS systems provide proactive security by continuously scanning for threats and ensuring WLAN policy compliance. Their capabilities include:
B). Wireless vulnerability assessment: Scanning for misconfigured APs, weak encryption, and unauthorized devices.
E). Policy enforcement and compliance: Ensuring security settings adhere to enterprise or regulatory requirements and alerting on deviations.
Other options like application-layer inspection and AP CPU monitoring are outside the WIPS function scope.
References:
CWSP-208 Study Guide, Chapter 7 - WIPS Services and Capabilities
CWNP CWSP-208 Objectives: "WIPS Threat Mitigation and Enforcement"

NEW QUESTION: 29
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.
Answer: (SHOW ANSWER)

When connecting over untrusted public networks:
An IPSec VPN provides encryption and authentication from the client to the corporate network. This protects against eavesdropping, man-in-the-middle attacks, and spoofed hotspots.
Incorrect:
B). HTTPS only protects web sessions-not all traffic.
C). Enterprise WIPS at the office won't protect remote users.
D). Laptop-based WIPS software is rare and less effective than using a VPN.
E). 802.1X/PEAP is not designed for remote use over public hotspots.
F). FTP is not secure; secure alternatives include SFTP or FTPS.
References:
CWSP-208 Study Guide, Chapter 6 (VPNs and Remote Security)
CWNP Remote Access Security Best Practices

NEW QUESTION: 30

A. RSNA connections require TKIP or CCMP.
B. RSNA connections require BIP and do not support TKIP, CCMP or WEP.
C. RSNA connections require CCMP and do not support TKIP or WEP.
D. RSNA connections do not work in conjunction with VLANs.
Answer: (SHOW ANSWER)
RSNA (Robust Security Network Association), as defined by 802.11i, requires:
TKIP (WPA) or CCMP (WPA2) for encryption.
WEP is deprecated and not supported for RSNA since it does not meet RSN standards.
Incorrect:
B & C. BIP is not required for RSNA formation-it is used for management frame protection (802.11w).
D). VLANs are orthogonal to RSNA-network segmentation does not interfere with RSNA formation.
References:
CWSP-208 Study Guide, Chapter 3 (RSNA Formation and Key Hierarchy)
IEEE 802.11i and 802.11-2012 Standards

NEW QUESTION: 31

Given: The Marketing department's WLAN users need to reach their file and email server as well as the Internet, but should not have access to any other network resources.
What single WLAN security feature should be implemented to comply with these requirements?
A. Mutual authentication
B. Captive portal
C. Role-based access control
D. Group authentication
E. RADIUS policy accounting
Answer: (SHOW ANSWER)

Role-Based Access Control (RBAC) allows administrators to define user roles and enforce network access permissions based on the user's identity. By implementing RBAC in the WLAN, you can:
Grant the Marketing group access only to the file/email server and the Internet Prevent access to other internal resources This single feature enables fine-grained restriction without needing multiple SSIDs or ACLs.
Other options don't provide the necessary flexibility:
A). Mutual authentication ensures secure identity verification but doesn't control network access scope B & D & E do not provide targeted resource-level access control References:
CWSP#207 Study Guide, Chapter 6 (Access Control Policy and RBAC)

NEW QUESTION: 32
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: (SHOW ANSWER)
PCI-DSS (Payment Card Industry Data Security Standard) applies to all entities that process, store, or transmit credit card data. Since Point-of-Sale (PoS) systems handle such transactions in retail environments, the wireless network supporting them must comply with PCI-DSS. This includes encrypting wireless transmissions, segmenting network traffic, and implementing WIPS for rogue detection and logging.
References:
CWSP-208 Study Guide, Chapter 3 - WLAN Policy & Regulatory Compliance
CWNP CWSP-208 Objectives: "Industry Standards & Compliance (e.g., PCI-DSS, HIPAA)"

NEW QUESTION: 33
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: (SHOW ANSWER)
Many protocol analyzers require special drivers or place the NIC into monitor/promiscuous mode. When used this way, the original driver stack may be altered or replaced. Afterward, if not correctly reloaded, the adapter may lack full 802.1X support or required encryption features. This is likely the case here - Mary's WLAN adapter is still under the control of or affected by the analyzer's NIC driver, which doesn't support PEAP properly.
References:
CWSP-208 Study Guide, Chapter 6 - Protocol Analysis Limitations and NIC Driver Issues CWNP
CWSP-208 Objectives: "Troubleshooting WLAN Authentication and Driver Conflicts"

NEW QUESTION: 34
You are using a protocol analyzer for random checks of activity on the WLAN. In the process, you notice two different EAP authentication processes. One process (STA1) used seven EAP frames (excluding ACK frames) before the 4-way handshake and the other (STA2) used 11 EAP frames (excluding ACK frames) before the 4- way handshake.
Which statement explains why the frame exchange from one STA required more frames than the frame exchange from another STA when both authentications were successful? (Choose the single most probable answer given a stable WLAN.)
A. STA1 and STA2 are using different cipher suites.
B. STA2 has retransmissions of EAP frames.
C. STA1 is a reassociation and STA2 is an initial association.
D. STA1 is a TSN, and STA2 is an RSN.
E. STA1 and STA2 are using different EAP types.
Answer: E (LEAVE A REPLY)
Different EAP types involve varying numbers of exchanges:
EAP-TLS, for example, involves more exchanges due to certificate negotiation.
EAP-MD5 or PEAP might involve fewer steps.

Thus, the most likely reason for different frame counts during successful authentication is the use of different EAP types.
Incorrect:
A). Cipher suites are negotiated after EAP, not during it.
B). Retransmissions would typically cause noticeable delay and not result in exactly 11 frames.
C). Reassociation does not significantly reduce EAP frame count.
D). RSN/TSN differences are not directly related to EAP exchange length.
References:
CWSP-208 Study Guide, Chapter 4 (EAP Protocol Operation)
IEEE 802.1X and EAP Behavior Documentation

NEW QUESTION: 35
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.
What security implementation will allow the network administrator to achieve this goal?
A. Implement an SSID with WPA2-Personal that sends all broadcast traffic using AES-CCMP and unicast traffic using either TKIP or 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 allows both AES-CCMP and TKIP clients to connect.
D. Implement two separate SSIDs on the AP-one for WPA-Personal using TKIP and one for WPA2- Personal using AES-CCMP.
Answer: (SHOW ANSWER)

NEW QUESTION: 36
When using a tunneled EAP type, such as PEAP, what component is protected inside the TLS tunnel so that it is not sent in clear text across the wireless medium?
A. X.509 certificates
B. User credentials
C. Server credentials
D. RADIUS shared secret
Answer: (SHOW ANSWER)
In tunneled EAP types (e.g., PEAP, EAP-TTLS):
A secure TLS tunnel is first established using the server's certificate.
Then, user credentials (e.g., username/password) are sent through the encrypted tunnel to ensure confidentiality.

Incorrect:
A). Certificates are exchanged during tunnel establishment, not protected within it.
C). Server credentials are used to establish the tunnel, not protected inside it.
D). The RADIUS shared secret secures communication between AP/controller and RADIUS server-not sent via the tunnel.
References:
CWSP-208 Study Guide, Chapter 4 (Tunneled EAP Methods)
IEEE 802.1X and EAP Specifications

NEW QUESTION: 37
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
Answer: (SHOW ANSWER)
Role-Based Access Control (RBAC) enables dynamic assignment of permissions and access rights based on a user's job function. A WLAN controller with RBAC:
Can apply policies post-authentication.
Controls access to internal services (e.g., file shares, apps).
Assigns users to different VLANs or applies firewall rules based on roles.
Incorrect:
A). MAC filtering is not scalable or secure.
B). WPA2-Personal does not support user-based policies or LDAP integration.
C). DHCP scope assignment is not linked to user roles.
E). VLAN assignment via SSID is static and does not consider job function.
References:
CWSP-208 Study Guide, Chapter 6 (Access Control and Role-Based Policies) CWNP Enterprise WLAN Design Practices

NEW QUESTION: 38
You are using a utility that takes input and generates random output. For example, you can provide the input of a known word as a secret word and then also provide another known word as salt input. When you process the input it generates a secret code which is a combination of letters and numbers with case sensitivity. For what is the described utility used? (Choose 3)
A. Generating passwords for WLAN infrastructure equipment logins
B. Generating PMKs that can be imported into 802.11 RSN-compatible devices

C. Generating secret keys for RADIUS servers and WLAN infrastructure devices
D. Generating passphrases for WLAN systems secured with WPA2-Personal
E. Generating dynamic session keys used for IPSec VPNs
Answer: (SHOW ANSWER)
A utility that combines a secret and salt to generate a random string is effectively a key derivation tool. It can be used to:
Generate PMKs (Pairwise Master Keys) to preload ready-made keys into RSN devices Generate shared secrets (e.g., RADIUS shared secrets, WLAN controller keys) Create strong passphrases for WPA2-Personal networks Using it for IPSec session keys is less common (those are usually dynamically negotiated), and creating management passwords is possible but not the main us

NEW QUESTION: 39
Given: In XYZ's small business, two autonomous 802.11ac APs and 12 client devices are in use with WPA2- Personal.
What statement about the WLAN security of this company is true?
A. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt the data traffic of other users.
B. A successful attack against all unicast traffic on the network would require a weak passphrase dictionary attack and the capture of the latest 4-Way Handshake for each client.
C. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.
D. An unauthorized WLAN user with a protocol analyzer can decode data frames of authorized users if he captures the BSSID, client MAC address, and a user's 4-Way Handshake.
E. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.
Answer: (SHOW ANSWER)
In WPA2-Personal, each client derives its Pairwise Transient Key (PTK) based on a shared Pairwise Master Key (PMK) and values exchanged during the 4-Way Handshake. Therefore, even if the passphrase is cracked, an attacker must still capture the 4-Way Handshake for each target client in order to decrypt their unicast traffic.
Incorrect:
A). Incorrect because cracking the passphrase allows decrypting data traffic after capturing the 4-Way Handshake.
C). WPA2 encrypts multicast and broadcast traffic using the GTK, which unauthorized clients cannot derive.
D). Capturing BSSID and MAC isn't enough without knowing the passphrase and the full 4-Way Handshake.
E). Hijacking is harder in WPA2-Personal due to the dynamic PTK derived per session.
References:
CWSP-208 Study Guide, Chapter 3 (WPA2-PSK Key Management)
CWNP Learning: WLAN Encryption and PTK Derivation

NEW QUESTION: 40

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.
Answer: (SHOW ANSWER)
Comprehensive Detailed Explanation:
In 802.1X/EAP-based authentication:
After Open System authentication, clients send EAP messages via the uncontrolled port.
The Controlled Port remains blocked until the 802.1X/EAP and 4-Way Handshake processes are complete.
Incorrect:
A). The AP or controller is the authenticator, not the client.
B). EAP types must match between supplicant and server.
D). Controlled port remains blocked until full authentication and key negotiation completes.
References:
CWSP-208 Study Guide, Chapter 4 (802.1X Controlled and Uncontrolled Port Behavior) IEEE 802.1X Framework Details

NEW QUESTION: 41
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
Answer: (SHOW ANSWER)
Mutual authentication involves both the client and the authentication server verifying each other's identity before network access is granted. This prevents attackers from spoofing an access point (AP) and luring clients to connect to rogue APs (often used in wireless hijacking or evil twin attacks). When mutual authentication (typically via 802.1X with EAP-TLS) is used, clients will not connect unless they can verify the server certificate, which thwarts hijacking attempts.
References:
CWSP-208 Study Guide, Chapter 4 (Authentication and Access Control)

CWNP E-Learning: 802.1X and EAP Authentication Framework
IEEE 802.1X and WPA2-Enterprise concepts

NEW QUESTION: 42
What elements should be addressed by a WLAN security policy? (Choose 2)
A. Enabling encryption to prevent MAC addresses from being sent in clear text
B. How to prevent non-IT employees from learning about and reading the user security policy
C. End-user training for password selection and acceptable network use
D. The exact passwords to be used for administration interfaces on infrastructure devices
E. Social engineering recognition and mitigation techniques
Answer: (SHOW ANSWER)
A strong WLAN security policy should encompass both technical controls and user education.
C). Educating users about secure password creation and acceptable use policies helps reduce risks due to weak authentication and misuse.
E). Social engineering is a common attack vector, and educating users to recognize and report such attempts is critical.
Incorrect:
A). MAC addresses are always transmitted in the clear, even with encryption.
B). Policies should be shared with users to promote compliance and awareness.
D). Passwords for administrative systems should not be disclosed in public documentation or policy documents.
References:
CWSP-208 Study Guide, Chapter 2 (Security Policies and End-User Training) CWNP WLAN Security Policy Templates

NEW QUESTION: 43
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
Answer: (SHOW ANSWER)
EAP-TTLS (Tunneled Transport Layer Security) supports flexible inner authentication methods including:
MS-CHAPv2
EAP-GTC (Generic Token Card)
EAP-TLS (in some configurations)
This versatility allows EAP-TTLS to be used with a wide range of back-end authentication systems, while only requiring a server-side certificate.

Incorrect:
A). H-REAP (now FlexConnect) is a Cisco AP deployment mode, not an EAP type.
B). EAP-GTC is a simple authentication method and not a tunnel or container for others.
D). PEAP typically supports MS-CHAPv2 but not EAP-GTC or EAP-TLS as inner methods.
E). LEAP uses MS-CHAPv1 and is considered deprecated and insecure.
References:
CWSP-208 Study Guide, Chapter 4 (EAP Methods)

NEW QUESTION: 44
Given: ABC Hospital wishes to create a strong security policy as a first step in securing their 802.11 WLAN.
Before creating the WLAN security policy, what should you ensure you possess?
A. Awareness of the exact vendor devices being installed
B. Management support for the process
C. End-user training manuals for the policies to be created
D. Security policy generation software
Answer: (SHOW ANSWER)
Developing a robust WLAN security policy requires buy-in from executive or senior management. Without management support, it's difficult to enforce compliance, allocate resources, or prioritize security among other organizational objectives. This foundational step ensures that policy creation and enforcement are feasible and aligned with organizational goals.
Incorrect:
A). Device/vendor specifics are addressed later during implementation.
C). End-user training materials are created after the policy is finalized.
D). Security policy software can assist, but is not essential compared to management support.
References:
CWSP-208 Study Guide, Chapter 2 (Policy Development and Implementation) CWNP WLAN Lifecycle Framework

NEW QUESTION: 45
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.
Answer: (SHOW ANSWER)
This solution meets all the requirements:
Captive portals allow simple authentication for guest users.
VLAN separation enforces network segmentation.
HTTPS ensures authentication is encrypted.
Incorrect:
A). Separate controllers are unnecessary and costly.
B). WIPS enforcement is reactive, not proactive for normal access control.
C). ACLs alone don't enforce authentication.
E). VPN requirements would be overly complex for guests.
References:
CWSP-208 Study Guide, Chapter 6 (Guest Network Architecture & Captive Portal Authentication)

NEW QUESTION: 46
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. WEP
B. RC4
C. CCMP
D. WPA2
Answer: (SHOW ANSWER)
A Transitional Security Network (TSN) allows legacy stations to interoperate by using older encryption methods. If AES (CCMP) is unsupported by older equipment, the network can fall back to TKIP, which uses RC4 as its encryption algorithm. TKIP enables AES encryption on newer devices while accommodating legacy clients.
Options A, C, D are current or deprecated standards with AES; only RC4 matches the transitional need.
References:
CWSP#207 Study Guide, Chapter 3 (TSN, TKIP, AES-CCMP)

NEW QUESTION: 47
Given: During 802.1X/LEAP authentication, the username is passed across the wireless medium in clear text.
From a security perspective, why is this significant?
A. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.
B. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.
C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.
D. The username can be looked up in a dictionary file that lists common username/password combinations.
Answer: (SHOW ANSWER)
In Cisco LEAP (Lightweight EAP), the username is sent in clear text as part of the 802.1X authentication process. LEAP uses a challenge/response authentication mechanism that is susceptible to offline dictionary attacks because the attacker only needs to know the username and capture the challenge/response exchange to perform brute-force guessing of passwords. The username is used in generating the hash for the authentication exchange, making its disclosure critical for an attacker.
Incorrect:
A). PACs are used in EAP-FAST, not LEAP.
C). The 4-Way Handshake nonces are unrelated to the username.
D). While dictionary files may include username/password combos, the cryptographic significance in LEAP is due to the challenge/response mechanism.
References:
CWSP-208 Study Guide, Chapter 4 (EAP Types and Authentication Attacks)
CWNP Whitepaper: LEAP Vulnerabilities

NEW QUESTION: 48
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
Answer: (SHOW ANSWER)
AAA stands for:
Authentication: Validates user identity (Option 1).
Authorization: Grants access to specific resources based on policy (Option 3).
Accounting: Tracks user activity (Option 2).
This ordering matches standard network security architecture:
Who are you? # Authentication
What are you allowed to do? # Authorization
What did you do? # Accounting
Incorrect:
A-C. Misplace or mislabel AAA functions.
References:
CWSP-208 Study Guide, Chapter 4 (AAA Framework)
CWNP AAA and WLAN Policy Documents

NEW QUESTION: 49
You perform a protocol capture using Wireshark and a compatible 802.11 adapter in Linux. When viewing the capture, you see an auth req frame and an auth rsp frame. Then you see an assoc req frame and an assoc rsp frame. Shortly after, you see DHCP communications and then ISAKMP protocol packets. What security solution is represented?
A. 802.1X/EAP-TTLS
B. Open 802.11 authentication with IPSec
C. 802.1X/PEAPv0/MS-CHAPv2
D. WPA2-Personal with AES-CCMP
E. EAP-MD5
Answer: B (LEAVE A REPLY)
The frame sequence described shows:
802.11 Open System authentication and association

DHCP communication (for IP configuration)
ISAKMP packets, which are part of IPSec (used for key exchange and tunnel negotiation) This indicates that link-layer authentication is not used, but instead, higher-layer encryption (IPSec VPN) secures communications.
Incorrect:
A and C. Would show EAP negotiation and 802.1X authentication frames.
D). WPA2-Personal would include a 4-Way Handshake before DHCP.
E). EAP-MD5 does not involve ISAKMP and is used within 802.1X authentication.
References:
CWSP-208 Study Guide, Chapter 4 (IPSec and Upper-Layer Security)
Wireshark Frame Analysis of IPSec Tunnels