HPE6-A85^Q&As

Aruba Certified Campus Access Associate

Pass HP HPE6-A85 Exam with 100% Guarantee

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

What is a weakness introduced into the WLAN environment when WPA2-Personal is used for security?

A. It uses X 509 certificates generated by a Certification Authority

B. The Pairwise Temporal Key (PTK) is specific to each session

C. The Pairwise Master Key (PMK) is shared by ail users

D. It does not use the WPA 4-Way Handshake

Correct Answer: C

Explanation: The weakness introduced into WLAN environment when WPA2-Personal is used for security is that PMK Pairwise Master Key (PMK) is a key that is derived from PSK Pre-shared Key (PSK) is a key that is shared between two parties before communication begins , which are both fixed. This means that all users who know PSK can generate PMK without any authentication process. This also means that if PSK or PMK are compromised by an attacker, they can be used to decrypt all traffic encrypted with PTK Pairwise Temporal Key (PTK) is a key that is derived from PMK, ANonce AuthenticatorNonce (ANonce) is a random number generated by an authenticator (a device that controls access to network resources, such as an AP), SNonce Supplicant Nonce (SNonce) is a random number generated by supplicant (a device that wants to access network resources, such as an STA), AA Authenticator Address (AA) is MAC address of authenticator, SA Supplicant Address (SA) is MAC address of supplicant using Pseudo-Random Function (PRF). PTK consists of four subkeys: KCK Key Confirmation Key (KCK) is used for message integrity check, KEK Key Encryption Key (KEK) is used for encryption key distribution, TK Temporal Key (TK) is used for data encryption, MIC Message Integrity Code (MIC) key. . The other options are not weaknesses because: It uses X 509 certificates generated by a Certification Authority: This option is false because WPA2-Personal does not use X 509 certificates or Certification Authority for authentication. X 509 certificates and Certification Authority are used in WPA2- Enterprise mode, which uses 802.1X and EAP Extensible Authentication Protocol (EAP) is an authentication framework that provides support for multiple authentication methods, such as passwords, certificates, tokens, or biometrics. EAP is used in wireless networks and point-to-point connections to provide secure authentication between a supplicant (a device that wants to access the network) and an authentication server (a device that verifies the credentials of the supplicant). for user authentication with a RADIUS server Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service . The Pairwise Temporal Key (PTK) is specific to each session: This option is false because PTK being specific to each session is not a weakness but a strength of WPA2-Personal. PTK being specific to each session means that it changes periodically during communication based on time or number of packets transmitted. This prevents replay attacks and increases security of data encryption. It does not use the WPA 4-Way Handshake: This option is false because WPA2- Personal does use the WPA 4-Way Handshake for key negotiation. The WPA 4- Way Handshake is a process that allows the station and the access point to exchange ANonce and SNonce and derive PTK from PMK. The WPA 4-Way Handshake also allows the station and the access point to verify each other\\'s PMK and confirm the installation of PTK.

References: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management
https://www.cwnp.com/wp- content/uploads/pdf/WPA2.pdf

QUESTION 2

What are two advantages of a UXl? (Select two.)

A. A UXl can be used without any internet connection

B. A UXl helps to calculate the best WiFi channels in a remote location

C. A UXl behaves like a client/user

D. A UXl measures the Wi-Fi coverage of all APs in the given location.

E. A UXl can check different applications, such as HTTP VOIP or Office 365.

Correct Answer: CE

Explanation: A UXI (User Experience Insight) is a device that simulates user behavior and tests network performance from the user perspective. It can check different applications, such as HTTP, VOIP, or Office 365, and measure metrics

such as latency, jitter, packet loss, and throughput.

References:https://www.arubanetworks.com/products/networking/user-experience-insight/

QUESTION 3

What is an advantage of using Layer 2 MAC authentication?

A. it matches user names to MAC address

B. No setup is required on the client

C. MAC allow lists are easily maintained over time

D. MAC identifiers are hard to spoof

Correct Answer: B

Explanation: Layer 2 MAC authentication is a method of authenticating devices based on their MAC addresses without requiring any client-side configuration or credentials. The switch sends the MAC address of the device to an authentication server such as ClearPass or RADIUS, which checks if the MAC address is authorized to access the network. If yes, the switch grants access to the device based on the assigned role and policies. If no, the switch denies access or redirects the device to a captive portal for further authentication.

References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/1-overview/mac-authentication.htm

QUESTION 4

The noise floor measures 000000001 milliwatts, and the receiver\\'s signal strength is - 65dBm. What is the Signal to Noise Ratio?

A. 35 dBm

B. 15 dBm

C. 45 dBm

D. 25 dBm

Correct Answer: D

Explanation: The signal to noise ratio (SNR) is a measure that compares the level of a desired signal to the level of background noise. SNR is defined as the ratio of signal power to the noise power, often expressed in decibels (dB). A high

SNR means that the signal is clear and easy to detect or interpret, while a low SNR means that the signal is corrupted or obscured by noise and may be difficult to distinguish or recover3. To calculate the SNR in dB, we can use the following

formula:

SNR (dB) = Signal power (dBm) - Noise power (dBm) In this question, we are given that the noise floor measures -90 dBm (0.000000001 milliwatts) and the receiver\\'s signal strength is -65 dBm (0.000316 milliwatts). Therefore, we can plug

these values into the formula and get:

SNR (dB) = -65 dBm - (-90 dBm) SNR (dB) = -65 dBm + 90 dBm SNR (dB) = 25 dBm Therefore, the correct answer is that the SNR is 25 dBm.

References: https://en.wikipedia.org/wiki/Signal-to-noise_ratio

QUESTION 5

When using Aruba Central what can identify recommended steps to resolve network health issues and allows you to share detailed information with support personnel?

A. Overview Dashboard

B. OAlOps

C. Alerts and Events

D. Audit Trail

Correct Answer: B

Explanation: OAlOps is a feature of Aruba Central that uses artificial intelligence and machine learning to identify recommended steps to resolve network health issues and allows you to share detailed information with support personnel. OAlOps provides insights into network performance, root cause analysis, anomaly detection, proactive alerts, and automated remediation actions.OAlOps also integrates with Aruba User Experience Insight (UXI) sensors to measure and improve user experience across wired and wireless networks.

References:https://www.arubanetworks.com/assets/ds/DS_ArubaCentral.pdf