HPE6-A85 Q&As

Aruba Certified Campus Access Associate

Pass HP HPE6-A85 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/hpe6-a85.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which device configuration group types can a user define in Aruba Central during group creation? (Select two.)

A. Security group

B. Template group

C. Default group

D. Ul group

E. ESP group

Correct Answer: BC

Explanation: Aruba Central allows you to create device configuration groups that define common settings for devices within each group. You can create different types of groupsdepending on your network requirements and management

preferences. Two types of groups that you can define in Aruba Central during group creation are:

Template group: A template group allows you to create configuration templates using variables and expressions that can be applied to multiple devices or device groups. Template groups provide flexibility and scalability for managing large-

scale deployments with similar configurations.

Default group: A default group is automatically created when you add devices to Aruba Central for the first time. The default group contains basic configuration settings that are applied to all devices that are not assigned to any other group.

You can modify or delete the default group as needed.

References: https://www.arubanetworks.com/techdocs/Central/latest/content/nms/device- groups.htm

https://www.arubanetworks.com/techdocs/Central/latest/content/nms/template- groups.htm

https://www.arubanetworks.com/techdocs/Central/latest/content/nms/default- group.htm

QUESTION 2

What does WPA3-Personal use as the source to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network?

A. Session-specific information (MACs and nonces)

B. Opportunistic Wireless Encryption (OWE)

C. Simultaneous Authentication of Equals (SAE)

D. Key Encryption Key (KEK)

Correct Answer: A

Explanation: The source that WPA3-Personal uses to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network is session-specific information (MACs and nonces). WPA3-Personal uses

Simultaneous Authentication of Equals (SAE) to replace PSK authentication in WPA2-Personal. SAE is a secure key establishment protocol that uses a Diffie-Hellman key exchange to derive a shared secret between two parties without

revealing it to an eavesdropper. SAE involves the following steps:

The station and the access point exchange Commit messages that contain their MAC addresses and random numbers called nonces.

The station and the access point use their own passwords and the received MAC addresses and nonces to calculate a shared secret called SAE Password Element (PE).

The station and the access point use their own PE and the received MAC addresses and nonces to calculate a shared secret called SAE Key Seed (KS). The station and the access point use their own KS and the received MAC addresses

and nonces to calculate a shared secret called SAE Key Confirmation Key (KCK).

The station and the access point use their own KCK and the received MAC addresses and nonces to calculate a confirmation value called SAE Confirm. The station and the access point exchange Confirm messages that contain their SAE

Confirm values.

The station and the access point verify that the received SAE Confirm values match their own calculated values. If they match, the authentication is successful and the station and the access point have established a shared secret called SAE

PMK.

The SAE PMK is different for each session because it depends on the MAC addresses and nonces that are exchanged in each authentication process. The SAE PMK is used as an input for the 4-way handshake that generates the Pairwise

Temporal Key (PTK) for encrypting data frames.

The other options are not sources that WPA3-Personal uses to generate a different PMK each time a station connects to the wireless network because:

Opportunistic Wireless Encryption (OWE): OWE is a feature that provides encryption for open networks without requiring authentication or passwords. OWE uses a similar key establishment protocol as SAE, but it does not generate a PMK.

Instead, it generates a Pairwise Secret (PS) that is used as an input for the 4-way handshake that generates the PTK.

Simultaneous Authentication of Equals (SAE): SAE is not a source, but a protocol that uses session-specific information as a source to generate a different PMK each time a station connects to the wireless network. Key Encryption Key (KEK): KEK is not a source, but an output of the 4-way handshake that generates the PTK. KEK is used to encrypt group keys that are distributed by the access point.

References: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e https://www.wi-fi.org/file/wi- fi-alliance-unlicensed-spectrum-in-the-us https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access- points/wpa3-dep-guide-og.html https://info.support.huawei.com/info- finder/encyclopedia/en/WPA3.html https://rp.os3.nl/2019-2020/p99/presentation.pdf

QUESTION 3

When performing live firmware upgrades on Aruba APs. which technology partitions all the APs based on RF neighborhood data minimizing the impact on clients?

A. Aruba ClientMatch

B. Aruba Ai insights

C. Aruba AirMatch

D. Aruba ESP

Correct Answer: C

Explanation: Aruba AirMatch is a feature that optimizes RF Radio Frequency. RF is any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an

electromagnetic field is created that then is able to propagate through space. performance and user experience by using machine learning algorithms and historical data to dynamically adjust AP power levels, channel assignments, and

channel width. AirMatch performs live firmware upgrades on Aruba APs by partitioning all the APs based on RFneighborhood data and minimizing the impact on clients. AirMatch uses a rolling upgrade process that upgrades one partition at a

time while ensuring that adjacent partitions are not upgraded simultaneously.

References:

https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdfhttps://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/arm/AirMatch.htm

QUESTION 4

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 5

When using the OSPF dynamic routing protocol on an Aruba CX switch, what must match on the neighboring devices to exchange routes?

A. Hello timers

B. DR configuration

C. ECMP method

D. BDR configuration

Correct Answer: A

Explanation: OSPF Open Shortest Path First. OSPF is a link-state routing protocol that uses a hierarchical structure to create a routing topology for IP networks. OSPF routers exchange routing information with their neighbors using Hello packets, which are sent periodically on each interface. To establish an adjacency Adjacency is a relationship formed between selected neighboring routers for the purpose of exchanging routing information., OSPF routers must agree on several parameters, including Hello timers, which specify how often Hello packets are sent on an interface. If the Hello timers do not match between neighboring routers, they will not form an adjacency and will not exchange routes. References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/osfp/osfp.htm