HP

HPE6-A78

Aruba Certified Network Security Associate Exam

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 9.0

Question: 1

What is a vulnerability of an unauthenticated Dime-Heliman exchange?

A. A hacker can replace the public values exchanged by the legitimate peers and launch an MITM attack.
B. A brute force attack can relatively quickly derive Diffie-Hellman private values if they are able to obtain public values
C. Diffie-Hellman with elliptic curve values is no longer considered secure in modem networks, based on NIST recommendations.
D. Participants must agree on a passphrase in advance, which can limit the usefulness of Diffie- Hell man in practical contexts.

Answer: A

Explanation:
The vulnerability of an unauthenticated Diffie-Hellman exchange, particularly when it comes to the risk of a man-in-the-middle (MITM) attack, is a significant concern. In this scenario, a hacker can intercept the public values exchanged between two legitimate parties and substitute them with their own. This allows the attacker to decrypt or manipulate the messages passing between the two original parties without them knowing. This answer is based on the fundamental principles of how Diffie-Hellman key exchange works and its vulnerabilities without authentication mechanisms. Reference materials from cryptographic textbooks and security protocols detail these vulnerabilities, such as those found in standards and publications by organizations like NIST.

Question: 2

What is a difference between radius and TACACS+?

A. RADIUS combines the authentication and authorization process while TACACS+ separates them.
B. RADIUS uses TCP for Its connection protocol, while TACACS+ uses UDP tor its connection protocol.
C. RADIUS encrypts the complete packet, white TACACS+ only offers partial encryption.
D. RADIUS uses Attribute Value Pairs (AVPs) in its messages, while TACACS+ does not use them.

Answer: A

Explanation:
RADIUS and TACACS+ are both protocols used for networking authentication, but they handle the processes of authentication and authorization differently. RADIUS (Remote Authentication Dial-In User Service) combines authentication and authorization into a single process, whereas TACACS+ (Terminal Access Controller Access-Control System Plus) separates these processes. This separation in TACACS+ allows more flexible policy enforcement and better control over commands a user can execute. This

difference is well-documented in various network security resources, including Cisco's technical documentation and security protocol manuals.

Question: 3

A company has an Aruba solution with a Mobility Master (MM) Mobility Controllers (MCs) and campus Aps. What is one benefit of adding Aruba Airwave from the perspective of forensics?

A. Airwave can provide more advanced authentication and access control services for the AmbaOS solution
B. Airwave retains information about the network for much longer periods than ArubaOS solution
C. Airwave is required to activate Wireless Intrusion Prevention (WIP) services on the ArubaOS solution
D. AirWave enables low level debugging on the devices across the ArubaOS solution

Answer: B

Explanation:
Adding Aruba Airwave to an Aruba solution that includes a Mobility Master (MM), Mobility Controllers (MCs), and campus APs offers several benefits, notably in the realm of network forensics. One of the significant advantages is that Airwave can retain detailed information about the network for much longer periods than what is typically possible with just ArubaOS solutions. This extensive data retention is crucial for forensic analysis, allowing network administrators and security professionals to conduct thorough investigations of past incidents. With access to historical data, professionals can identify trends, pinpoint security breaches, and understand the impact of specific changes or events within the network over time.
:
Aruba's official product documentation and user guides for Airwave and ArubaOS, which outline features, benefits, and use cases related to network management and forensic capabilities.
Industry case studies and whitepapers that discuss the implementation and advantages of integrating Airwave into existing network infrastructure for enhanced monitoring and security.

Question: 4

What role does the Aruba ClearPass Device Insight Analyzer play in the Device Insight architecture?

A. It resides in the cloud and manages licensing and configuration for Collectors
B. It resides on-prem and provides the span port to which traffic is mirrored for deep analytics.
C. It resides on-prem and is responsible for running active SNMP and Nmap scans
D. It resides In the cloud and applies machine learning and supervised crowdsourcing to metadata sent by Collectors

Answer: D

Explanation:

The Aruba ClearPass Device Insight Analyzer plays a crucial role within the Device Insight architecture by residing in the cloud and applying machine learning and supervised crowdsourcing to the metadata sent by Collectors. This component of the architecture is responsible for analyzing vast amounts of data collected from the network to identify and classify devices accurately. By utilizing machine learning algorithms and crowdsourced input, the Device Insight Analyzer enhances the accuracy of device detection and classification, thereby improving the overall security and management of the network.
:
Aruba ClearPass official documentation and whitepapers that detail the functionality and deployment of the Device Insight Analyzer.
Technical articles and presentations on network security solutions that discuss the use of machine learning and data analytics in device management.

Question: 5

What is a correct guideline for the management protocols that you should use on ArubaOS-Switches?

A. Disable Telnet and use TFTP instead.
B. Disable SSH and use https instead.
C. Disable Telnet and use SSH instead
D. Disable HTTPS and use SSH instead

Answer: C

Explanation:
In managing ArubaOS-Switches, the best practice is to disable less secure protocols such as Telnet and use more secure alternatives like SSH (Secure Shell). SSH provides encrypted connections between network devices, which is critical for maintaining the security and integrity of network communications. This guideline is aligned with general security best practices that prioritize the use of protocols with strong, built-in encryption mechanisms to prevent unauthorized access and ensure data privacy.
Reference: This is a general network management and security practice recommended across various platforms, including but not limited to ArubaOS-Switch documentation and other network security resources.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/