

New HPE6-A78 Exam Review, Latest HPE6-A78 Exam Pdf



VCE & PDF
Pass4itSure.com

<https://www.pass4itsure.com/hpe6-a78.html>
2022 Latest pass4itsure HPE6-A78 PDF and VCE dumps Download

HPE6-A78^{Q&As}

Aruba Certified Network Security Associate

Pass HP HPE6-A78 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/hpe6-a78.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



Latest HPE6-A78 Dumps | HPE6-A78 Practice Test | HPE6-A78 Braindumps

1 / 7

P.S. Free 2026 HP HPE6-A78 dumps are available on Google Drive shared by ActualTestsQuiz <https://drive.google.com/open?id=1IOLgbJmOZStlY1XGI5SrMbazi5j9Cp4>

Have tough-minded boy only, ability appeases billows, hoist the sails Yuan Hang. Our HP HPE6-A78 exam dumps are the first step to bring you achievement. It provides you with pdf real questions and answers. By choosing it, you must put through HP HPE6-A78 Certification that other people think it is very difficult. After you get the certification, you can lighten your heart and start a new journey.

HP HPE6-A78 exam is a valuable certification for individuals interested in network security. HPE6-A78 exam covers a wide range of topics and is designed to test candidates on their ability to identify and mitigate network security threats. With the right preparation and dedication, candidates can successfully pass the exam and become certified Aruba Network Security Associates, opening up many career opportunities in the IT industry.

HP HPE6-A78 exam covers a wide range of topics, including basic security concepts, network security technologies, wireless security, and firewall technologies. HPE6-A78 Exam also focuses on Aruba products and technologies, such as the Aruba Mobility Controller, ClearPass Policy Manager, and ArubaOS. Candidates who pass HPE6-A78 exam will have a solid understanding of network security concepts and will be able to implement and manage Aruba-based network security solutions.

>> New HPE6-A78 Exam Review <<

Latest HPE6-A78 Exam Pdf - Practice HPE6-A78 Test

With the rapid development of IT technology, the questions in the IT certification exam are also changing. Therefore, ActualTestsQuiz also keeps updating test questions and answers. And if you purchase ActualTestsQuiz HP HPE6-A78 Practice Test materials, we will provide you with free updates for a year. As long as the questions updates, ActualTestsQuiz will immediately send the latest questions and answers to you which guarantees that you can get the latest materials at any time. ActualTestsQuiz can not only help you pass the test, but also help you learn the latest knowledge. Never pass up a good chance to have the substantial materials.

HP HPE6-A78 (Aruba Certified Network Security Associate) Certification Exam is designed to test the knowledge and skills of professionals who want to pursue a career in network security. Aruba Certified Network Security Associate Exam certification exam validates the candidate's ability to implement and manage the security of wireless networks using Aruba products and technologies. HPE6-A78 Exam covers a wide range of topics including network security fundamentals, security technologies, wireless security, and Aruba security solutions.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q39-Q44):

NEW QUESTION # 39

How can hackers implement a man-in-the-middle (MITM) attack against a wireless client?

- A. The hacker runs an NMap scan on the wireless client to find its MAC and IP address. The hacker then connects to another network and spoofs those addresses.
- **B. The hacker connects a device to the same wireless network as the client and responds to the client's ARP requests with the hacker device's MAC address.**
- C. The hacker uses spear-phishing to probe for the IP addresses that the client is attempting to reach. The hacker device then spoofs those IP addresses.
- D. The hacker uses a combination of software and hardware to jam the RF band and prevent the client from connecting to any wireless networks.

Answer: B

Explanation:

A common method for hackers to perform a man-in-the-middle (MITM) attack on a wireless network is by ARP poisoning. The attacker connects to the same network as the victim and sends false ARP messages over the network. This causes the victim's device to send traffic to the attacker's machine instead of the legitimate destination, allowing the attacker to intercept the traffic.

NEW QUESTION # 40

You need to set up Aruba network infrastructure devices for management with SNMP. The SNMP server has this SNMPv3 user configured on it: username: airwave auth algorithm: sha auth key: fyluqp18@S!9a priv algorithm: aes priv key: 761oxaiaoeu19& What correctly describes the setup on the infrastructure device?

- A. You must configure the "airwave" server as an authorized user. Then, configure a separate user for this device with its own keys.
- B. You must configure a user with the same name and algorithms, but the keys should be unique to this device.
- C. You must configure a user with the same name and keys, but can choose algorithms that meet the device's needs.
- **D. You must configure a user with exactly the same name, algorithms, and keys.**

Answer: D

Explanation:

In SNMPv3, security is paramount and each SNMP entity (client or agent) needs to have a user with a security name (username) and optionally, a security level which determines whether authentication and encryption are used. When configuring SNMPv3 users on network infrastructure devices, it is essential to match the username, authentication (auth) algorithm, authentication key (auth key), privacy (priv) algorithm, and privacy key (priv key) exactly as they are configured on the SNMP server to ensure successful communication.

This is because the SNMPv3 security model relies on a combination of a username and a pair of keys (authentication and privacy keys) to uniquely identify and secure communication between the agent and the manager. The keys are used to verify the integrity (auth key) and confidentiality (priv key) of the messages. Using the same algorithms ensures that the messages can be properly encrypted and decrypted on both ends.

NEW QUESTION # 41

You have deployed a new Aruba Mobility Controller (MC) and campus APs (CAPs). One of the WLANs enforces 802.1X authentication to Aruba ClearPass Policy Manager (CPPM). When you test connecting the client to the WLAN, the test fails. You check Aruba ClearPass Access Tracker and cannot find a record of the authentication attempt. You ping from the MC to CPPM, and the ping is successful.

What is a good next step for troubleshooting?

- A. Renew CPPM's RADIUS/EAP certificate
- B. Reset the user credentials
- C. Check CPPM Event viewer.
- D. Check connectivity between CPPM and a backend directory server

Answer: C

Explanation:

When dealing with a failed 802.1X authentication attempt to a WLAN enforced by Aruba ClearPass Policy Manager (CPPM) where no record of the attempt is seen in ClearPass Access Tracker, a good next troubleshooting step is to check the CPPM Event Viewer. Since you are able to successfully ping from the Mobility Controller to CPPM, this indicates that there is network connectivity between these two devices.

The lack of a record in Access Tracker suggests that the issue may not be with the RADIUS/EAP certificate or user credentials, but possibly with the ClearPass service itself or its reception of authentication requests.

The Event Viewer can provide detailed logs that might reveal internal errors or misconfigurations within CPPM that could prevent it from processing authentication attempts properly.

NEW QUESTION # 42

A company has Aruba Mobility Controllers (MCs), Aruba campus APs, and ArubaOS-CX switches. The company plans to use ClearPass Policy Manager (CPPM) to classify endpoints by type. The ClearPass admins tell you that they want to run Network scans as part of the solution. What should you do to configure the infrastructure to support the scans?

- A. Create device fingerprinting profiles on the ArubaOS-Switches that include SNMP, and apply the profiles to edge ports
- B. Create SNMPv3 users on ArubaOS-CX switches, and make sure that the credentials match those configured on CPPM
- C. Create remote mirrors on the ArubaOS-Switches that collect traffic on edge ports, and mirror it to CPPM's IP address.
- D. Create a TA profile on the ArubaOS-Switches with the root CA certificate for ClearPass's HTTPS certificate

Answer: B

Explanation:

To configure the infrastructure to support network scans as part of the ClearPass Policy Manager (CPPM) solution, creating SNMPv3 users on ArubaOS-CX switches is necessary. Ensuring that the credentials for these SNMPv3 users match those configured on CPPM is crucial for enabling CPPM to perform network scans effectively. SNMPv3 provides a secure method for network management by offering authentication and encryption, which are essential for safely conducting scans that classify endpoints by type. This configuration allows CPPM to communicate securely with the switches and gather necessary data without compromising network security.

References:

ArubaOS-CX configuration manuals that discuss SNMP settings.

Network management and security guidelines that emphasize the importance of secure SNMP configurations for network scanning and monitoring.

NEW QUESTION # 43

You have an Aruba Mobility Controller (MC), for which you are already using Aruba ClearPass Policy Manager (CPPM) to authenticate access to the Web UI with usernames and passwords. You now want to enable managers to use certificates to log in to the Web UI. CPPM will continue to act as the external server to check the names in managers' certificates and tell the MC the managers' correct role in addition to enabling certificate authentication. What is a step that you should complete on the MC?

- A. Verify that the MC trusts CPPM's HTTPS certificate by uploading a trusted CA certificate. Also, configure a CPPM username and password on the MC
- B. Create a local admin account that uses certificates in the account, specify the correct trusted CA certificate and external

- C. install all of the managers' certificates on the MC as OCSP Responder certificates
- D. Verify that the MC has the correct certificates, and add RadSec to the RADIUS server configuration for CPPM

Explanation:

Additionally, configuring a username and password for CPPM on the MC might be necessary to secure and facilitate communication between the MC and CPPM. This setup ensures that certificate-based authentication is securely validated, maintaining secure access control for the Web UI.

Best practices for secure authentication and certificate management in enterprise network environments.

• • • • •

[illegible]

DOWNLOAD the newest ActualTestsQuiz HPE6-A78 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1IOLgbJmOZStfY1XGI5SrMbaztb5j9Cp4>