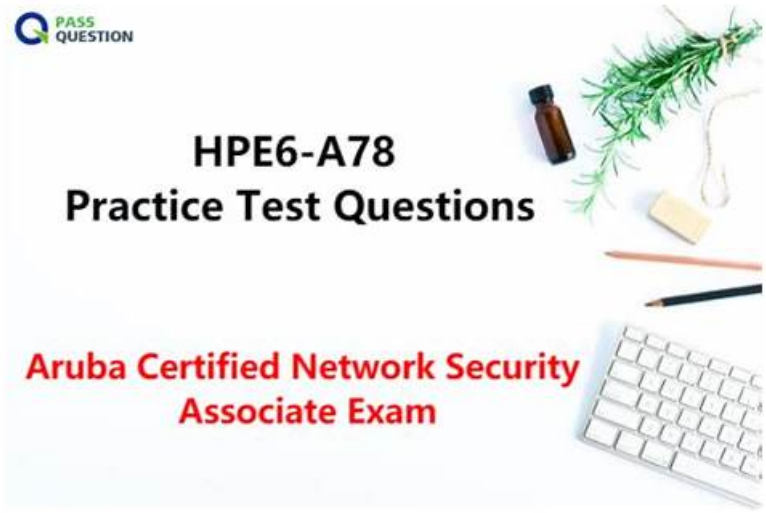
Pass Guaranteed Quiz 2026 High-quality HP HPE6-A78: Aruba Certified Network Security Associate Exam Study Material



P.S. Free & New HPE6-A78 dumps are available on Google Drive shared by Lead2Passed: https://drive.google.com/open?id=1uNErr-PcPUtkOqLByqxUAXABMzZy77Vi

We are a group of IT experts to provide professional study materials to people preparing HP certification exam. There are free demo you can download to check the accuracy of our HPE6-A78 Braindumps. It just needs to take one or two days to practice Lead2Passed HPE6-A78 dumps torrent and review the key points of our pass guide. Clearing exam is 100% guaranteed.

HPE6-A78 exam is a must-have certification for those who want to pursue a career in network security. Aruba Certified Network Security Associate Exam certification validates the candidate's knowledge and skills required to configure and troubleshoot Aruba security solutions. Aruba Certified Network Security Associate Exam certification also helps individuals to gain recognition in the industry and opens up new career opportunities. Moreover, this certification demonstrates the candidate's commitment to continuous learning and professional development.

To prepare for the HP HPE6-A78 exam, candidates can take advantage of various study materials, such as online courses, study guides, and practice exams. These resources can help candidates gain a deeper understanding of the exam topics and develop the necessary skills to pass the exam.

HPE6-A78 certification is designed to validate the skills of IT professionals in network security, particularly in the context of Aruba solutions. HPE6-A78 Exam covers a wide range of topics, including network security fundamentals, firewall policies, VPN technologies, and wireless security. It also tests the candidates' abilities to configure and manage Aruba products such as ClearPass, Mobility Controllers, and Instant Access Points.

>> HPE6-A78 Study Material <<

2026 High Hit-Rate HPE6-A78 Study Material | HPE6-A78 100% Free Latest Exam Online

We have chosen a large number of professionals to make HPE6-A78 learning question more professional, while allowing our study materials to keep up with the times. Of course, we do it all for you to get the information you want, and you can make faster progress. You can also get help from HPE6-A78 exam training professionals at any time when you encounter any problems. We can be sure that with the professional help of our HPE6-A78 Test Guide you will surely get a very good experience. Good materials and methods can help you to do more with less. Choose HPE6-A78 test guide to get you closer to success.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q48-Q53):

NEW QUESTION # 48
What is one way that Control Plane Security (CPsec) enhances security for me network?

- A. It protects management traffic between APs and Mobility Controllers (MCs) from eavesdropping.
- B. It prevents Denial of Service (DoS) attacks against Mobility Controllers' (MCs") control plane.
- C. It prevents access from unauthorized IP addresses to critical services, such as SSH on Mobility Controllers (MCs).
- D. It protects wireless clients' traffic tunneled between APs and Mobility Controllers, from eavesdropping

Answer: A

Explanation:
Control Plane Security (CPsec) enhances security in the network by protecting management traffic between APs and Mobility Controllers (MCs) from eavesdropping. CPsec ensures that all control and management traffic that transits the network is encrypted, thus preventing potential attackers from gaining access to sensitive management data. It helps in securing the network's control plane, which is crucial for maintaining the integrity and privacy of the network operations.
:
Aruba Networks' CPsec documentation.

NEW QUESTION # 49
Which is an accurate description of a type of malware?

- A. Rootkits can help hackers gain elevated access to a system and often actively conceal themselves from detection.
- B. A Trojan is any type of malware that replicates itself and spreads to other systems automatically.
- C. Worms are usually delivered in spear-phishing attacks and require users to open and run a file.
- D. Malvertising can only infect a system if the user encounters the malware on an untrustworthy site.

Answer: A

Explanation:
Malware (malicious software) is a broad category of software designed to harm or exploit systems. HPE Aruba Networking documentation often discusses malware in the context of network security threats and mitigation strategies, such as those detected by the Wireless Intrusion Prevention (WIP) system.
Option A, "Worms are usually delivered in spear-phishing attacks and require users to open and run a file," is incorrect. Worms are a type of malware that replicate and spread automatically across networks without user interaction (e.g., by exploiting vulnerabilities). They are not typically delivered via spear-phishing, which is more associated with Trojans or ransomware. Worms do not require users to open and run a file; that behavior is characteristic of Trojans.
Option B, "Rootkits can help hackers gain elevated access to a system and often actively conceal themselves from detection," is correct. A rootkit is a type of malware that provides hackers with privileged (elevated) access to a system, often by modifying the operating system or kernel. Rootkits are designed to hide their presence (e.g., by concealing processes, files, or network connections) to evade detection by antivirus software or system administrators, making them a stealthy and dangerous type of malware.
Option C, "A Trojan is any type of malware that replicates itself and spreads to other systems automatically," is incorrect. A Trojan is a type of malware that disguises itself as legitimate software to trick users into installing it. Unlike worms, Trojans do not replicate or spread automatically; they require user interaction (e.g., downloading and running a file) to infect a system.
Option D, "Malvertising can only infect a system if the user encounters the malware on an untrustworthy site," is incorrect. Malvertising (malicious advertising) involves embedding malware in online ads, which can appear on both trustworthy and untrustworthy sites. For example, a legitimate website might unknowingly serve a malicious ad that exploits a browser vulnerability to infect the user's system, even without the user clicking the ad.
The HPE Aruba Networking Security Guide states:
"Rootkits are a type of malware that can help hackers gain elevated access to a system by modifying the operating system or kernel. They often actively conceal themselves from detection by hiding processes, files, or network connections, making them difficult to detect and remove. Rootkits are commonly used to maintain persistent access to a compromised system." (Page 22, Malware Types Section) Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"The Wireless Intrusion Prevention (WIP) system can detect various types of malware. Rootkits, for example, are designed to provide hackers with elevated access and often conceal themselves to evade detection, allowing the hacker to maintain control over the infected system for extended periods." (Page 421, Malware Threats Section)
:
HPE Aruba Networking Security Guide, Malware Types Section, Page 22.
HPE Aruba Networking AOS-8 8.11 User Guide, Malware Threats Section, Page 421.

NEW QUESTION # 50
You have deployed a new Aruba Mobility Controller (MC) and campus APs (CAPs). One of the WLANs enforces 802.IX authentication lo Aruba ClearPass Policy Manager {CPPM) When you test connecting the client to the WLAN. the test falls 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 # 51
You are checking the Security Dashboard in the Web UI for your AOS solution and see that Wireless Intrusion Prevention (WIP) has discovered a rogue radio operating in ad hoc mode with open security. What correctly describes a threat that the radio could pose?

- A. It could open a backdoor into the corporate LAN for unauthorized users.
- B. It could be attempting to conceal itself from detection by changing its BSSID and SSID frequently.
- C. It is flooding the air with many wireless frames in a likely attempt at a DoS attack.
- D. It is running in a non-standard 802.11 mode and could effectively jam the wireless signal.

Answer: A

Explanation:
The AOS Security Dashboard in an AOS-8 solution (Mobility Controllers or Mobility Master) provides visibility into wireless threats detected by the Wireless Intrusion Prevention (WIP) system. The scenario describes a rogue radio operating in ad hoc mode with open security. Ad hoc mode in 802.11 allows devices to communicate directly with each other without an access point (AP), forming a peer-to-peer network. Open security means no encryption or authentication is required to connect.
Ad Hoc Mode Threat: An ad hoc network created by a rogue device can pose significant risks, especially if a corporate client connects to it. Since ad hoc mode allows direct device-to-device communication, a client that joins the ad hoc network might inadvertently bridge the corporate LAN to the rogue network, especially if the client is also connected to the corporate network (e.g., via a wired connection or another wireless interface).
Option B, "It could open a backdoor into the corporate LAN for unauthorized users," is correct. If a corporate client connects to the rogue ad hoc network (e.g., due to a misconfiguration or auto-connect setting), the client might bridge the ad hoc network to the corporate LAN, allowing unauthorized users on the ad hoc network to access corporate resources. This is a common threat with ad hoc networks, as they bypass the security controls of the corporate AP infrastructure.
Option A, "It could be attempting to conceal itself from detection by changing its BSSID and SSID frequently," is incorrect. While changing BSSID and SSID can be a tactic to evade detection, this is not a typical characteristic of ad hoc networks and is not implied by the scenario. Ad hoc networks are generally visible to WIP unless explicitly hidden.
Option C, "It is running in a non-standard 802.11 mode and could effectively jam the wireless signal," is incorrect. Ad hoc mode is a standard 802.11 mode, not a non-standard one. While a rogue device could potentially jam the wireless signal, this is not a direct threat posed by ad hoc mode with open security.
Option D, "It is flooding the air with many wireless frames in a likely attempt at a DoS attack," is incorrect. There is no indication in the scenario that the rogue radio is flooding the air with frames. While ad hoc networks can be used in DoS attacks, the primary threat in this context is the potential for unauthorized access to the corporate LAN.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"A rogue radio operating in ad hoc mode with open security poses a significant threat, as it can open a backdoor into the corporate

LAN. If a corporate client connects to the ad hoc network, it may bridge the ad hoc network to the corporate LAN, allowing unauthorized users to access corporate resources. This is particularly dangerous if the client is also connected to the corporate network via another interface." (Page 422, Wireless Threats Section) Additionally, the HPE Aruba Networking Security Guide notes:
"Ad hoc networks detected by WIP are a concern because they can act as a backdoor into the corporate LAN. A client that joins an ad hoc network with open security may inadvertently allow unauthorized users to access the corporate network, bypassing the security controls of authorized APs." (Page 73, Ad Hoc Network Threats Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, Wireless Threats Section, Page 422.
HPE Aruba Networking Security Guide, Ad Hoc Network Threats Section, Page 73.

NEW QUESTION # 52
Your company policies require you to encrypt logs between network infrastructure devices and Syslog servers. What should you do to meet these requirements on an ArubaOS-CX switch?

- A. Set up RadSec and then enable Syslog as a protocol carried by the RadSec tunnel.
- B. Specify the Syslog server with the TLS option and make sure the switch has a valid certificate.
- C. Specify the Syslog server with the UDP option and then add an CPsec tunnel that selects Syslog.
- D. Specify a priv key with the Syslog settings that matches a priv key on the Syslog server.

Answer: B

Explanation:
To ensure secure transmission of log data over the network, particularly when dealing with sensitive or critical information, using TLS (Transport Layer Security) for encrypted communication between network devices and syslog servers is necessary:
Secure Logging Setup: When configuring an ArubaOS-CX switch to send logs securely to a Syslog server, specifying the server with the TLS option ensures that all transmitted log data is encrypted.
Additionally, the switch must have a valid certificate to establish a trusted connection, preventing potential eavesdropping or tampering with the logs in transit.
Other Options:
Option B, Option C, and Option D are less accurate or applicable for directly encrypting log data between the device and Syslog server as specified in the company policies.

NEW QUESTION # 53
.....

When you prepare for HP HPE6-A78 certification exam, it is unfavorable to blindly study exam-related knowledge. There is a knack to pass the exam. If you make use of good tools to help you, it not only can save your much more time and also can make you sail through HPE6-A78 test with ease. If you want to ask what tool it is, that is, of course Lead2Passed HP HPE6-A78 exam dumps.

- HPE6-A78 Valid Test Prep □ HPE6-A78 Real Exam □ HPE6-A78 Study Material □ Open 「 www.pdfvce.com 」 and search for ▹ HPE6-A78 ◃ to download exam materials for free □HPE6-A78 Real Exam
- Is HP HPE6-A78 Questions – Best Way To Clear The Exam? □ The page for free download of ➠ HPE6-A78 □ on ➡ www.dumpsmaterials.com □□□ will open immediately □Valid Test HPE6-A78 Format
- Is HP HPE6-A78 Questions – Best Way To Clear The Exam? □ Search on ➠ www.pdfvce.com □ for □ HPE6-A78 □ to obtain exam materials for free download □HPE6-A78 Interactive Course
- HPE6-A78 Reliable Exam Question □ HPE6-A78 Reliable Exam Question □ Composite Test HPE6-A78 Price □ Search for ✔ HPE6-A78 □✔□ and easily obtain a free download on （ www.practicevce.com ） □Simulation HPE6-A78 Questions
- bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, mecabricks.com, Disposable vapes

BTW, DOWNLOAD part of Lead2Passed HPE6-A78 dumps from Cloud Storage: https://drive.google.com/open?id=1uNErr-PcPUtkOqLByqxUAXABMzZy77Vi