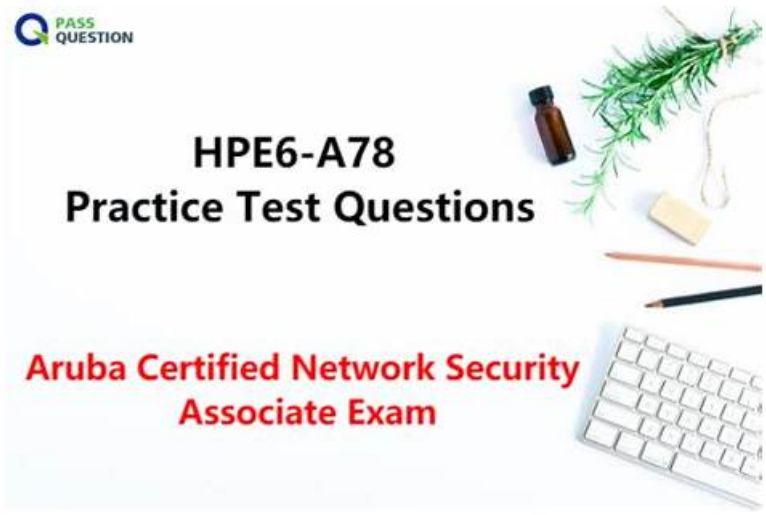
Valid HPE6-A78 Exam Bootcamp - 100% HPE6-A78 Accuracy



2026 Latest TestPassKing HPE6-A78 PDF Dumps and HPE6-A78 Exam Engine Free Share: https://drive.google.com/open?id=18RfUTyvbF5FQXBvNz6RqSl2M5BRVBVRU

We have applied the latest technologies to the design of our HP HPE6-A78 exam prep not only on the content but also on the displays. As a consequence you are able to keep pace with the changeable world and remain your advantages with our HP HPE6-A78 training braindumps. Besides, you can consolidate important knowledge for you personally and design customized study schedule or to-do list on a daily basis.

HP HPE6-A78 Certification Exam covers a wide range of topics related to network security, including security protocols, access control, firewalls, intrusion detection, and prevention systems. HPE6-A78 exam also covers security policies and procedures, risk assessment, and compliance regulations. Aruba Certified Network Security Associate Exam certification is an essential credential for network security professionals who want to advance their careers and demonstrate their expertise in network security. Aruba Certified Network Security Associate Exam certification program offers a comprehensive training program that helps individuals prepare for the exam and gain the necessary skills and knowledge to become certified Aruba Certified Network Security Associates.

>> Valid HPE6-A78 Exam Bootcamp <<

Updated Valid HPE6-A78 Exam Bootcamp - Easy and Guaranteed HPE6-A78 Exam Success

Experts at TestPassKing have also prepared HP HPE6-A78 practice exam software for your self-assessment. This is especially handy for preparation and revision. You will be provided with an examination environment and you will be presented with actual exam HP HPE6-A78 Exam Questions. This sort of preparation method enhances your knowledge which is crucial to excelling in the actual certification exam.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q150-Q155):

NEW QUESTION # 150
Which is a correct description of a stage in the Lockheed Martin kill chain?

- A. In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfiltrated.
- B. In the exploitation and installation phases, malware creates a backdoor into the infected system for the hacker.
- C. In the weaponization stage, which occurs after malware has been delivered to a system, the malware executes its function.
- D. In the delivery stage, malware collects valuable data and delivers or exfiltrates it to the hacker.

Answer: B

Explanation:
The Lockheed Martin Cyber Kill Chain is a framework that outlines the stages of a cyber attack, from initial reconnaissance to achieving the attacker's objective. It is often referenced in HPE Aruba Networking security documentation to help organizations understand and mitigate threats. The stages are: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives.
Option A, "In the weaponization stage, which occurs after malware has been delivered to a system, the malware executes its function," is incorrect. The weaponization stage occurs before delivery, not after. In this stage, the attacker creates a deliverable payload (e.g., combining malware with an exploit). The execution of the malware happens in the exploitation stage, not weaponization.
Option B, "In the exploitation and installation phases, malware creates a backdoor into the infected system for the hacker," is correct. The exploitation phase involves the attacker exploiting a vulnerability (e.g., a software flaw) to execute the malware on the target system. The installation phase follows, where the malware installs itself to establish persistence, often by creating a backdoor (e.g., a remote access tool) to allow the hacker to maintain access to the system. These two phases are often linked in the kill chain as the malware gains a foothold and ensures continued access.
Option C, "In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfiltrated," is incorrect. The reconnaissance stage occurs at the beginning of the kill chain, where the attacker gathers information about the target (e.g., network topology, vulnerabilities). Assessing the impact and exfiltration occurs in the Actions on Objectives stage, the final stage of the kill chain.
Option D, "In the delivery stage, malware collects valuable data and delivers or exfiltrates it to the hacker," is incorrect. The delivery stage involves the attacker transmitting the weaponized payload to the target (e.g., via a phishing email). Data collection and exfiltration occur later, in the Actions on Objectives stage, not during delivery.
The HPE Aruba Networking Security Guide states:
"The Lockheed Martin Cyber Kill Chain outlines the stages of a cyber attack. In the exploitation phase, the attacker exploits a vulnerability to execute the malware on the target system. In the installation phase, the malware creates a backdoor or other persistence mechanism, such as a remote access tool, to allow the hacker to maintain access to the infected system for future actions." (Page 18, Cyber Kill Chain Overview Section) Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"The exploitation and installation phases of the Lockheed Martin kill chain involve the malware gaining a foothold on the target system. During exploitation, the malware is executed by exploiting a vulnerability, and during installation, it creates a backdoor to ensure persistent access for the hacker, enabling further stages like command and control." (Page 420, Threat Mitigation Section)
:
HPE Aruba Networking Security Guide, Cyber Kill Chain Overview Section, Page 18.
HPE Aruba Networking AOS-8 8.11 User Guide, Threat Mitigation Section, Page 420.

NEW QUESTION # 151
You are troubleshooting an authentication issue for Aruba switches that enforce 802 IX10 a cluster of Aruba ClearPass Policy Manager (CPPMs) You know that CPPM Is receiving and processing the authentication requests because the Aruba switches are showing Access-Rejects in their statistics However, you cannot find the record tor the Access-Rejects in CPPM Access Tracker What is something you can do to look for the records?

- A. Go to the CPPM Event Viewer, because this is where RADIUS Access Rejects are stored.
- B. Click Edit in Access viewer and make sure that the correct servers are selected.
- C. Make sure that CPPM cluster settings are configured to show Access-Rejects
- D. Verify that you are logged in to the CPPM Ul with read-write, not read-only, access

Answer: C

Explanation:
If Access-Reject records are not showing up in the CPPM Access Tracker, one action you can take is to ensure that the CPPM cluster settings are configured to display Access-Rejects. Cluster-wide settings in CPPM can affect which records are visible in Access Tracker. Ensuring that these settings are correctly configured will allow you to view all relevant authentication records, including Access-Rejects.
:
ClearPass Policy Manager documentation that includes information on cluster settings and Access Tracker configurations.
Troubleshooting guides for ClearPass that provide steps to resolve issues with viewing authentication records.

NEW QUESTION # 152

Refer to the exhibit.
How can you use the thumbprint?

- A. install this thumbprint on management stations the stations can then authenticate with the thumbprint instead of admins having to enter usernames and passwords.
- B. When you first connect to the switch with SSH from a management station, make sure that the thumbprint matches to ensure that a man-in-t he-mid die (MITM) attack is not occurring
- C. Copy the thumbprint to other Aruba switches to establish a consistent SSH Key for all switches this will enable managers to connect to the switches securely with less effort
- D. Install this thumbprint on management stations to use as two-factor authentication along with manager usernames and passwords, this will ensure managers connect from valid stations

Answer: B

Explanation:
The thumbprint (also known as a fingerprint) of a certificate or SSH key is a hash that uniquely represents the public key contained within. When you first connect to the switch with SSH from a management station, you should ensure that the thumbprint matches what you expect. This is a security measure to confirm the identity of the device you are connecting to and to ensure that a man-in-the-middle (MITM) attack is not occurring. If the thumbprint matches the known good thumbprint of the switch, it is safe to proceed with the connection.
:
SSH and network security protocols that discuss the importance of verifying the identity of devices before initiating a secure connection.
IT security guides that provide best practices for avoiding MITM attacks during SSH sessions.

NEW QUESTION # 153
What is one of the roles of the network access server (NAS) in the AAA framewonx?

- A. It determines which resources authenticated users are allowed to access and monitors each users session
- B. It negotiates with each user's device to determine which EAP method is used for authentication
- C. It enforces access to network services and sends accounting information to the AAA server
- D. It authenticates legitimate users and uses policies to determine which resources each user is allowed to access.

Answer: C

Explanation:
In the AAA (Authentication, Authorization, and Accounting) framework, the role of the Network Access Server (NAS) is to act as a gateway that enforces access to network services and sends accounting information to the AAA server. The NAS initially requests authentication information from the user and then passes that information to the AAA server. It also enforces the access policies as provided by the AAA server after authentication and provides accounting data to the AAA server based on user activity.
:
Technical literature on AAA protocols which often includes a description of the roles and responsibilities of a Network Access Server.
Network security resources that discuss the NAS function within the AAA framework.

NEW QUESTION # 154
Your Aruba Mobility Master-based solution has detected a rogue AP Among other information the ArubaOS Detected Radios page lists this Information for the AP SSID = PubllcWiFI BSSID = a8M27 12 34:56 Match method = Exact match Match type = Eth-GW-wired-Mac-Table The security team asks you to explain why this AP is classified as a rogue. What should you explain?

- A. The AP Is connected to your LAN because It is transmitting wireless traffic with your network's default gateway's MAC address as a source MAC Because it does not belong to the company, it is a rogue
- B. The AP has been detected as launching a DoS attack against your company's default gateway. This qualities it as a rogue which needs to be contained with wireless association frames immediately
- C. The AP is spoofing a routers MAC address as its BSSID. This indicates mat, even though WIP cannot determine whether the AP is connected to your LAN. it is a rogue.
- D. The ap has a BSSID mat matches authorized client MAC addresses. This indicates that the AP is spoofing the MAC address to gam unauthorized access to your company's wireless services, so It is a rogue

Answer: A

Explanation:
The AP is classified as a rogue because it is connected to your LAN and is transmitting wireless traffic with your network's default gateway's MAC address as a source MAC. In this scenario, the 'Match method = Exact match' and 'Match type = Eth-GW-wired-Mac-Table' indicates that the rogue AP has been detected by matching the Ethernet gateway's MAC address, which is on the wired network, implying that the rogue AP is connected to the corporate LAN. Since the AP does not belong to the company, its presence on the network is unauthorized and is thus classified as a rogue AP.
:
ArubaOS documentation on rogue AP detection and classification.
Wireless security best practices that explain how the presence of unauthorized APs on the LAN constitutes a security threat.

NEW QUESTION # 155
.....

We even guarantee our customers that they will pass HP HPE6-A78 Exam easily with our provided study material and if they failed to do it despite all their efforts they can claim a full refund of their money (terms and conditions apply). The third format is the desktop software format which can be accessed after installing the software on your Windows computer or laptop. The Aruba Certified Network Security Associate Exam has three formats so that the students don't face any serious problems and prepare themselves with fully focused minds.