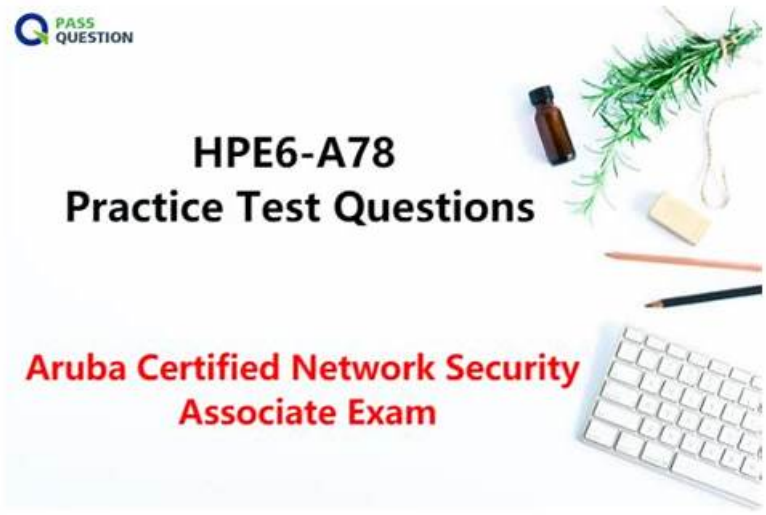
Free PDF Quiz 2025 HP HPE6-A78: Latest New Aruba Certified Network Security Associate Exam Exam Pattern



BONUS!!! Download part of BraindumpStudy HPE6-A78 dumps for free: https://drive.google.com/open?id=1leAj6R-Rg30CssAoKADWz0humuF8LDCW

Our BraindumpStudy aims at helping you reward your efforts on preparing for HPE6-A78 exam. If you don't believe it, you can try our product demo first; after you download and check our HPE6-A78 free demo, you will find how careful and professional our Research and Development teams are. If you are still preparing for other IT certification exams except HPE6-A78 Exam, you can also find the related exam dumps you want in our huge dumps and study materials.

HP HPE6-A78 (Aruba Certified Network Security Associate) Certification Exam is designed to test the skills and knowledge of network security professionals who work with Aruba products and solutions. Aruba is a leading provider of networking and security solutions for enterprises, governments, and other organizations. The HPE6-A78 exam covers a range of topics related to network security, including authentication, encryption, access control, and threat detection and mitigation.

HP HPE6-A78 exam, also known as the Aruba Certified Network Security Associate (ACNSA) exam, is designed to test and validate a candidate's knowledge and skills in implementing and managing network security solutions using Aruba products and technologies. Aruba Certified Network Security Associate Exam certification is ideal for network engineers, security professionals, and IT administrators who want to enhance their knowledge and expertise in network security and gain recognition in the industry.

>> New HPE6-A78 Exam Pattern <<

HP New HPE6-A78 Exam Pattern Exam | HPE6-A78: Aruba Certified Network Security Associate Exam – 100% free

Our Aruba Certified Network Security Associate Exam test torrent boost 99% passing rate and high hit rate so you can have a high probability to pass the exam. Our HPE6-A78 study torrent is compiled by experts and approved by the experienced professionals. The questions and answers of our HPE6-A78 study tool have simplified the important information and seized the focus and are updated frequently by experts to follow the popular trend in the industry. Because of these wonderful merits the client can pass the HPE6-A78 Exam successfully with high probability.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q112-Q117):

NEW QUESTION # 112
How should admins deal with vulnerabilities that they find in their systems?

- A. They should classify the vulnerability as malware. a DoS attack or a phishing attack.
- B. They should notify the security team as soon as possible that the network has already been breached.

- C. They should add the vulnerability to their Common Vulnerabilities and Exposures (CVE).
- D. They should apply fixes, such as patches, to close the vulnerability before a hacker exploits it.

Answer: D

Explanation:
When vulnerabilities are identified in systems, it is crucial for administrators to act immediately to mitigate the risk of exploitation by attackers. The appropriate response involves applying fixes, such as software patches or configuration changes, to close the vulnerability. This proactive approach is necessary to protect the integrity, confidentiality, and availability of the system resources and data. It's important to prioritize these actions based on the severity and exploitability of the vulnerability to ensure that the most critical issues are addressed first.References:
Best practices in system security management.

NEW QUESTION # 113
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.

NEW QUESTION # 114
How should admins deal with vulnerabilities that they find in their systems?

- A. They should classify the vulnerability as malware. a DoS attack or a phishing attack.
- B. They should notify the security team as soon as possible that the network has already been breached.
- C. They should add the vulnerability to their Common Vulnerabilities and Exposures (CVE).
- D. They should apply fixes, such as patches, to close the vulnerability before a hacker exploits it.

Answer: D

NEW QUESTION # 115
A company has HPE Aruba Networking Mobility Controllers (MCs), campus APs, and AOS-CX switches. The company plans to use HPE Aruba Networking ClearPass Policy Manager (CPPM) to classify endpoints by type. This company is using only CPPM and no other HPE Aruba Networking ClearPass solutions.
The HPE Aruba Networking ClearPass admins tell you that they want to use HTTP User-Agent strings to help profile the endpoints. What should you do as a part of setting up Mobility Controllers (MCs) to support this requirement?

- A. Create datapath mirrors that use the CPPM's IP address as the destination.
- B. Create an IF-MAP profile, which specifies credentials for an API admin account on CPPM.
- C. Create control path mirrors to mirror HTTP traffic from clients to CPPM.
- D. Create a firewall whitelist rule that permits HTTP and CPPM's IP address.

Answer: A

Explanation:
HPE Aruba Networking ClearPass Policy Manager (CPPM) uses device profiling to classify endpoints, and one of its profiling methods involves analyzing HTTP User-Agent strings to identify device types (e.g., iPhone, Windows laptop). HTTP User-Agent

strings are sent in HTTP headers when a client accesses a website. For CPPM to profile devices using HTTP User-Agent strings, it must receive the HTTP traffic from the clients. In this scenario, the company is using Mobility Controllers (MCs), campus APs, and AOS-CX switches, and CPPM is the only ClearPass solution in use.
HTTP User-Agent Profiling: CPPM can passively profile devices by analyzing HTTP traffic, but it needs to receive this traffic. In an AOS-8 architecture, the MC can mirror client traffic to CPPM for profiling. Since HTTP traffic is part of the data plane (user traffic), the MC must mirror the data plane traffic (not control plane traffic) to CPPM.
Option A, "Create datapath mirrors that use the CPPM's IP address as the destination," is correct. The MC can be configured to mirror client HTTP traffic to CPPM using a datapath mirror (also known as a GRE mirror). This involves setting up a mirror session on the MC that sends a copy of the client's HTTP traffic to CPPM's IP address. CPPM then analyzes the HTTP User-Agent strings in this traffic to profile the endpoints. For example, the command mirror session 1 destination ip <CPPM-IP> source ip any protocol http can be used to mirror HTTP traffic to CPPM.
Option B, "Create an IF-MAP profile, which specifies credentials for an API admin account on CPPM," is incorrect. IF-MAP (Interface for Metadata Access Points) is a protocol used for sharing profiling data between ClearPass and other systems (e.g., Aruba Introspect), but it is not used for sending HTTP traffic to CPPM for profiling. Additionally, IF-MAP is not relevant when only CPPM is in use.
Option C, "Create control path mirrors to mirror HTTP traffic from clients to CPPM," is incorrect. Control path (control plane) traffic includes management traffic between the MC and APs (e.g., AP registration, heartbeats), not client HTTP traffic. HTTP traffic is part of the data plane, so a datapath mirror is required, not a control path mirror.
Option D, "Create a firewall whitelist rule that permits HTTP and CPPM's IP address," is incorrect. A firewall whitelist rule on the MC might be needed to allow traffic to CPPM, but this is not the primary step for enabling HTTP User-Agent profiling. The key requirement is to mirror the HTTP traffic to CPPM, which is done via a datapath mirror, not a firewall rule.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"To enable ClearPass Policy Manager (CPPM) to profile devices using HTTP User-Agent strings, the Mobility Controller (MC) must mirror client HTTP traffic to CPPM. This is done by creating a datapath mirror session that sends a copy of the client's HTTP traffic to CPPM's IP address. For example, use the command mirror session 1 destination ip <CPPM-IP> source ip any protocol http to mirror HTTP traffic to CPPM. CPPM then analyzes the HTTP User-Agent strings to classify endpoints by type (e.g., iPhone, Windows laptop)." (Page 350, Device Profiling with CPPM Section) Additionally, the HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide notes:
"HTTP User-Agent profiling requires ClearPass to receive HTTP traffic from clients. In an Aruba Mobility Controller environment, configure a datapath mirror to send HTTP traffic to ClearPass's IP address. ClearPass will parse the HTTP User-Agent strings to identify device types and operating systems, enabling accurate profiling." (Page 249, HTTP User-Agent Profiling Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, Device Profiling with CPPM Section, Page 350.
HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, HTTP User-Agent Profiling Section, Page 249.

NEW QUESTION # 116
Two wireless clients, client 1 and client 2, are connected to an ArubaOS Mobility Controller. Subnet 10.1.10.10/24 is a network of servers on the other side of the ArubaOS firewall. The exhibit shows all three firewall rules that apply to these clients.

Refer to the exhibit.

Global Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION

+

Rules of this Role only

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION
Ipv4	any	any	svc-dhcp	permit
Ipv4	user	10.1.5.5	svc-dns	permit
Ipv4	user	10.1.10.0 255.255.255.0	svc-https	permit

+

Which traffic is permitted?

- A. an HTTPS request from 10.1.10.10 to client 1 and an HTTPS re-sponse from client 1 to 10.1.10.10
- B. an HTTPS request from client 1 to client 2 and an HTTPS request from client 2 to client 1
- C. an HTTPS request from client 1 to 10.1.10.10 and an HTTPS request from 10.1.10.11 to client 1
- D. an HTTPS request from client 1 to 10.1.10.10 and an HTTPS response from 10.1.10.10 to client 1

Answer: D

Explanation:
Based on the exhibit showing the firewall rules, the following traffic is permitted:
Client 1 is allowed to send HTTPS traffic to any destination within the subnet 10.1.10.0/24 because there is a permit rule for the user to access svc-https to that subnet.
Responses to initiated connections are typically allowed by stateful firewalls; hence, an HTTPS response from 10.1.10.10 to client 1 is expected to be permitted even though it is not explicitly mentioned in the firewall rules (assuming the stateful nature of the firewall).

NEW QUESTION # 117
.....