[2022 Verified HPE6-A78 Dumps Q&As - 1 Year Free & Quickly Updates [Q20-Q44

[2022] Verified HPE6-A78 Dumps Q&As - 1 Year Free & Quickly Updates
Latest 2022 Realistic Verified HPE6-A78 Dumps - 100% Free HPE6-A78 Exam Dumps

NEW QUESTION 20

What is a benefit of deploying Aruba ClearPass Device insight?
* Highly accurate endpoint classification for environments with many devices types, including Internet of Things (loT)
* visibility into devices’ 802.1X supplicant settings and automated certificate deployment
* Agent-based analysts of devices’ security settings and health status, with the ability to implement quarantining
* Simpler troubleshooting of ClearPass solutions across an environment with multiple ClearPass Policy Managers

NEW QUESTION 21

You need to deploy an Aruba instant AP where users can physically reach It. What are two recommended options for enhancing security for management access to the AP? (Select two)
* Disable Its console ports
* Place a Tamper Evident Label (TELS) over its console port

* Disable the Web Ul.
* Configure WPA3-Enterpnse security on the AP
* install a CA-signed certificate

NEW QUESTION 22

An ArubaOS-CX switch enforces 802.1X on a port. No fan-through options or port-access roles are configured on the port The 802 1X supplicant on a connected client has not yet completed authentication Which type of traffic does the authenticator accept from the client?
* EAP only
* DHCP, DNS and RADIUS only
* RADIUS only
* DHCP, DNS, and EAP only

NEW QUESTION 23

From which solution can ClearPass Policy Manager (CPPM) receive detailed information about client device type OS and status?
* ClearPass Onboard
* ClearPass Access Tracker
* ClearPass OnGuard
* ClearPass Guest

NEW QUESTION 24

What is a benefit or Protected Management Frames (PMF). sometimes called Management Frame Protection (MFP)?
* PMF helps to protect APs and MCs from unauthorized management access by hackers.
* PMF ensures trial traffic between APs and Mobility Controllers (MCs) is encrypted.
* PMF prevents hackers from capturing the traffic between APs and Mobility Controllers.
* PMF protects clients from DoS attacks based on forged de-authentication frames

NEW QUESTION 25

What is a use case for tunneling traffic between an Aruba switch and an AruDa Mobility Controller (MC)?
* applying firewall policies and deep packet inspection to wired clients
* enhancing the security of communications from the access layer to the core with data encryption
* securing the network infrastructure control plane by creating a virtual out-of-band-management network
* simplifying network infrastructure management by using the MC to push configurations to the switches

NEW QUESTION 26

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?
* 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
* 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
* 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
* 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.

NEW QUESTION 27

You have detected a Rogue AP using the Security Dashboard Which two actions should you take in responding to this event? (Select two)
* There is no need to locale the AP If you manually contain It.
* This is a serious security event, so you should always contain the AP immediately regardless of your company’s specific policies.
* You should receive permission before containing an AP. as this action could have legal Implications.
* For forensic purposes, you should copy out logs with relevant information, such as the time mat the AP was detected and the AP’s MAC address.
* There is no need to locate the AP If the Aruba solution is properly configured to automatically contain it.

NEW QUESTION 28

What is one of the roles of the network access server (NAS) in the AAA framewonx?
* It authenticates legitimate users and uses policies to determine which resources each user is allowed to access.
* It negotiates with each user’s device to determine which EAP method is used for authentication
* It enforces access to network services and sends accounting information to the AAA server
* It determines which resources authenticated users are allowed to access and monitors each users session

NEW QUESTION 29

You have an Aruba Mobility Controller (MC). for which you are already using Aruba ClearPass Policy Manager (CPPM) to authenticate access to the Web Ul with usernames and passwords You now want to enable managers to use certificates to log in to the Web Ul CPPM will continue to act as the external server to check the names in managers’ certificates and tell the MC the managers’ correct rote in addition to enabling certificate authentication. what is a step that you should complete on the MC?
* Verify that the MC has the correct certificates, and add RadSec to the RADIUS server configuration for CPPM
* install all of the managers’ certificates on the MC as OCSP Responder certificates
* 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
* Create a local admin account mat uses certificates in the account, specify the correct trusted CA certificate and external authentication

NEW QUESTION 30

What is symmetric encryption?
* It simultaneously creates ciphertext and a same-size MAC.
* It any form of encryption mat ensures that thee ciphertext Is the same length as the plaintext.
* It uses the same key to encrypt plaintext as to decrypt ciphertext.
* It uses a Key that is double the size of the message which it encrypts.

NEW QUESTION 31

You are managing an Aruba Mobility Controller (MC). What is a reason for adding a “Log Settings” definition in the ArubaOS Diagnostics > System > Log Settings page?
* Configuring the Syslog server settings for the server to which the MC forwards logs for a particular category and level
* Configuring the MC to generate logs for a particular event category and level, but only for a specific user or AP.

* Configuring a filter that you can apply to a defined Syslog server in order to filter events by subcategory
* Configuring the log facility and log format that the MC will use for forwarding logs to all Syslog servers

NEW QUESTION 32

What is an Authorized client as defined by ArubaOS Wireless Intrusion Prevention System (WIP)?
* a client that has a certificate issued by a trusted Certification Authority (CA)
* a client that is not on the WIP blacklist
* a client that has successfully authenticated to an authorized AP and passed encrypted traffic
* a client that is on the WIP whitelist.

NEW QUESTION 33

What is a guideline for managing local certificates on an ArubaOS-Switch?
* Before installing the local certificate, create a trust anchor (TA) profile with the root CA certificate for the certificate that you will install
* Install an Online Certificate Status Protocol (OCSP) certificate to simplify the process of enrolling and re-enrolling for certificate
* Generate the certificate signing request (CSR) with a program offline, then, install both the certificate and the private key on the switch in a single file.
* Create a self-signed certificate online on the switch because ArubaOS-Switches do not support CA-signed certificates.

NEW QUESTION 34

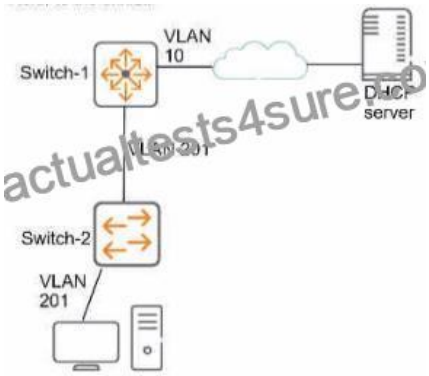
What is an example or phishing?
* An attacker sends TCP messages to many different ports to discover which ports are open.
* An attacker checks a user’s password by using trying millions of potential passwords.
* An attacker lures clients to connect to a software-based AP that is using a legitimate SSID.
* An attacker sends emails posing as a service team member to get users to disclose their passwords.

NEW QUESTION 35

What is one way that Control Plane Security (CPsec) enhances security for me network?
* It protects wireless clients’ traffic tunneled between APs and Mobility Controllers, from eavesdropping
* It prevents Denial of Service (DoS) attacks against Mobility Controllers’ (MCs”) control plane.
* It prevents access from unauthorized IP addresses to critical services, such as SSH on Mobility Controllers (MCs).
* It protects management traffic between APs and Mobility Controllers (MCs) from eavesdropping.

NEW QUESTION 36

Refer to the exhibit.



This company has ArubaOS-Switches. The exhibit shows one access layer switch, Swllcn-2. as an example, but the campus actually has more switches. The company wants to slop any internal users from exploiting ARP What Is the proper way to configure the switches to meet these requirements?
* On Switch-1, enable ARP protection globally, and enable ARP protection on ail VLANs.
* On Switch-2, make ports connected to employee devices trusted ports for ARP protection
* On Swltch-2, enable DHCP snooping globally and on VLAN 201 before enabling ARP protection
* On Swltch-2, configure static PP-to-MAC bindings for all end-user devices on the network

NEW QUESTION 37

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

NEW QUESTION 38

How should admins deal with vulnerabilities that they find in their systems?
* They should apply fixes, such as patches, to close the vulnerability before a hacker exploits it.
* They should add the vulnerability to their Common Vulnerabilities and Exposures (CVE).
* They should classify the vulnerability as malware. a DoS attack or a phishing attack.
* They should notify the security team as soon as possible that the network has already been breached.

NEW QUESTION 39

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

NEW QUESTION 40

What correctly describes the Pairwise Master Key (PMK) in thee specified wireless security protocol?
* In WPA3-Enterprise, the PMK is unique per session and derived using Simultaneous Authentication of Equals.
* In WPA3-Personal, the PMK is unique per session and derived using Simultaneous Authentication of Equals.
* In WPA3-Personal, the PMK is derived directly from the passphrase and is the same tor every session.
* In WPA3-Personal, the PMK is the same for each session and is communicated to clients that authenticate

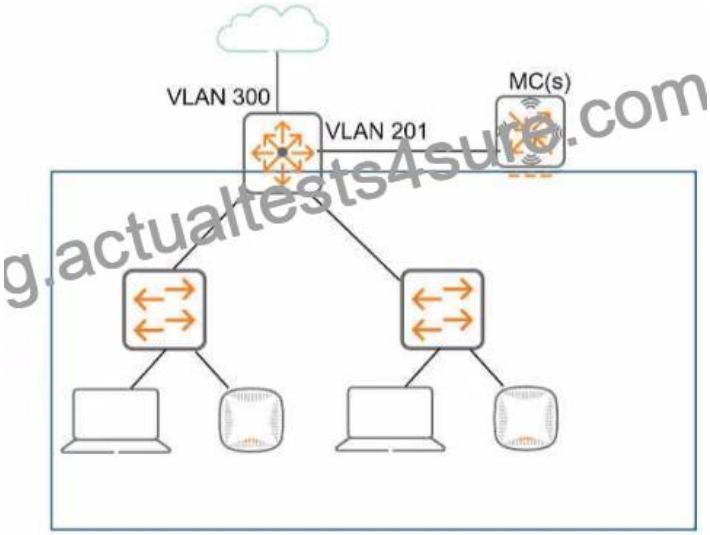
NEW QUESTION 41

What is a guideline for creating certificate signing requests (CSRs) and deploying server Certificates on ArubaOS Mobility

Controllers (MCs)?
* Create the CSR online using the MC Web Ul if your company requires you to archive the private key.
* if you create the CSR and public/private Keypair offline, create a matching private key online on the MC.
* Create the CSR and public/private keypair offline If you want to install the same certificate on multiple MCs.
* Generate the private key online, but the public key and CSR offline, to install the same certificate on multiple MCs.

NEW QUESTION 42

Refer to the exhibit, which shows the current network topology.



You are deploying a new wireless solution with an Aruba Mobility Master (MM). Aruba Mobility Controllers (MCs). and campus APs (CAPs). The solution will Include a WLAN that uses Tunnel for the forwarding mode and Implements WPA3-Enterprise security What is a guideline for setting up the vlan for wireless devices connected to the WLAN?
* Assign the WLAN to a single new VLAN which is dedicated to wireless users
* Use wireless user roles to assign the devices to different VLANs in the 100-150 range
* Assign the WLAN to a named VLAN which specified 100-150 as the range of IDs.
* Use wireless user roles to assign the devices to a range of new vlan IDs.

NEW QUESTION 43

What is one practice that can help you to maintain a digital chain or custody In your network?
* Enable packet capturing on Instant AP or Moodily Controller (MC) datepath on an ongoing basis
* Enable packet capturing on Instant AP or Mobility Controller (MC) control path on an ongoing basis.
* Ensure that all network infrastructure devices receive a valid clock using authenticated NTP
* Ensure that all network Infrastructure devices use RADIUS rather than TACACS+ to authenticate managers

HP HPE6-A78 Exam Syllabus Topics:

TopicDetailsTopic 1- Explain common security protocols and their use cases- Compare endpoint classifications methodsTopic 2- Explain attack stages and kill chain- Identify the difference between a threat and a vulnerabilityTopic 3- View and acknowledge WIPS and WIDS, alarms- Troubleshoot with access trackerTopic 4- Collect and monitor historical network pattern data- Describe firewall (PEF), dynamic segmentation, RBAC, AppRFTopic 5- Compare and contrast wireless LAN methodologies- Describe user roles and policy enforcementTopic 6- Identify and evaluate discovered endpoints- Describe common security threatsTopic 7- Disable insecure protocols and follow best practices for implement secure management protocols such as SSH, HTTPSTopic 8- Compare and contrast wired LAN methodologies- Explain the purpose and methods of a packet capture

HPE6-A78 Dumps PDF and Test Engine Exam Questions: https://www.actualtests4sure.com/HPE6-A78-test-questions.html]