Easily To Pass New HPE6-A78 Verified & Correct Answers [Jul 18, 2023 [Q21-Q45

Easily To Pass New HPE6-A78 Verified & Correct Answers [Jul 18, 2023
Free HPE6-A78 Exam Files Downloaded Instantly

NEW QUESTION 21

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 22

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.

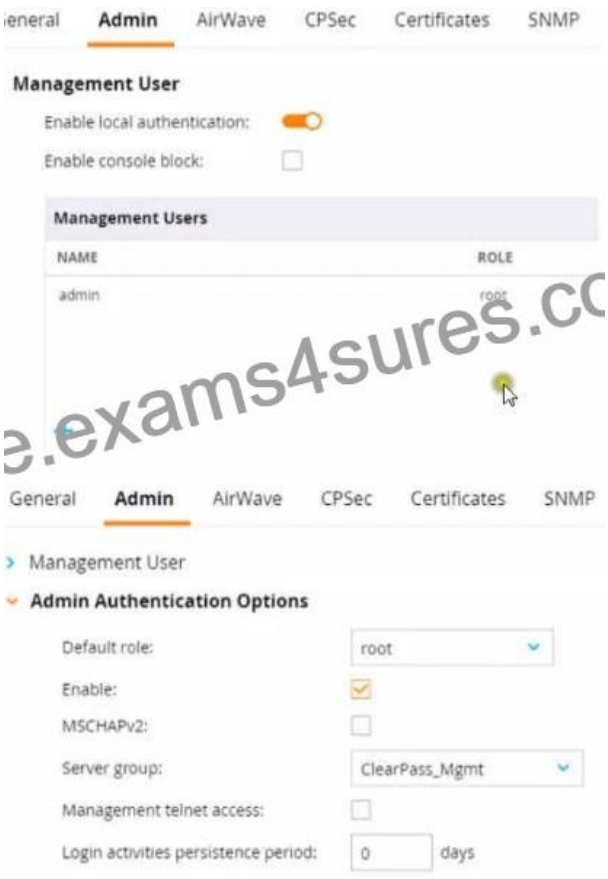
* PMF protects clients from DoS attacks based on forged de-authentication frames

NEW QUESTION 23

What is a difference between radius and TACACS+?
* RADIUS combines the authentication and authorization process while TACACS+ separates them.
* RADIUS uses TCP for Its connection protocol, while TACACS+ uses UDP tor its connection protocol.
* RADIUS encrypts the complete packet, white TACACS+ only offers partial encryption.
* RADIUS uses Attribute Value Pairs (AVPs) in its messages, while TACACS+ does not use them.

NEW QUESTION 24

Refer to the exhibit.



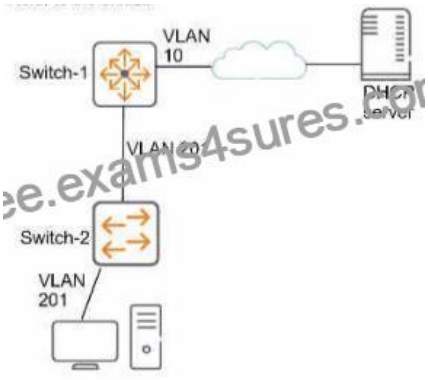
This Aruba Mobility Controller (MC) should authenticate managers who access the Web Ul to ClearPass Policy Manager (CPPM) ClearPass admins have asked you to use RADIUS and explained that the MC should accept managers’ roles in Aruba-Admin-Role VSAs Which setting should you change to follow Aruba best security practices?
* Change the local user role to read-only
* Clear the MSCHAP check box
* Disable local authentication
* Change the default role to “guest-provisioning”

NEW QUESTION 25

You have been instructed to look in the ArubaOS Security Dashboard’s client list Your goal is to find clients mat belong to the company and have connected to devices that might belong to hackers Which client fits this description?
* MAC address d8:50:e6:f3;6d;a4; Client Classification Authorized; AP Classification, interfering
* MAC address d8:50:e6 f3;6e;c5; Client Classification Interfering. AP Classification Neighbor
* MAC address d8:50:e6:f3;6e;60; Client Classification Interfering. AP Classification Interfering
* MAC address d8:50:e6:f3;TO;ab; Client Classification Interfering. AP Classification Rogue

NEW QUESTION 26

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 27

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 28

What is a benefit or using network aliases in ArubaOS firewall policies?
* You can associate a reputation score with the network alias to create rules that filler traffic based on reputation rather than IP.
* You can use the aliases to translate client IP addresses to other IP addresses on the other side of the firewall
* You can adjust the IP addresses in the aliases, and the rules using those aliases automatically update
* You can use the aliases to conceal the true IP addresses of servers from potentially untrusted clients.

NEW QUESTION 29

What role does the Aruba ClearPass Device Insight Analyzer play in the Device Insight architecture?
* It resides in the cloud and manages licensing and configuration for Collectors
* It resides on-prem and provides the span port to which traffic is mirrored for deep analytics.
* It resides on-prem and is responsible for running active SNMP and Nmap scans
* It resides In the cloud and applies machine learning and supervised crowdsourcing to metadata sent by Collectors

NEW QUESTION 30

What is a benefit of Opportunistic Wireless Encryption (OWE)?
* It allows both WPA2-capabie and WPA3-capable clients to authenticate to the same WPA-Personal WLAN
* It offers more control over who can connect to the wireless network when compared with WPA2-Personal
* It allows anyone lo connect, but provides better protection against eavesdropping than a traditional open network
* It provides protection for wireless clients against both honeypot APs and man-in-the-middle (MUM) attacks

NEW QUESTION 31

What is a Key feature of me ArubaOS firewall?
* The firewall is stateful which means that n can track client sessions and automatically allow return traffic for permitted sessions
* The firewall Includes application layer gateways (ALGs). which it uses to filter Web traffic based on the reputation of the destination web site.
* The firewall examines all traffic at Layer 2 through Layer 4 and uses source IP addresses as the primary way to determine how to control traffic.
* The firewall is designed to fitter traffic primarily based on wireless 802.11 headers, making it ideal for mobility environments

NEW QUESTION 32

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 33

Your ArubaoS solution has detected a rogue AP with Wireless intrusion Prevention (WIP). Which information about the detected radio can best help you to locate the rogue device?
* the match method
* the detecting devices
* the match type
* the confidence level

NEW QUESTION 34

What is one way a noneypot can be used to launch a man-in-the-middle (MITM) attack to wireless clients?
* it uses a combination or software and hardware to jam the RF band and prevent the client from connecting to any wireless networks
* it runs an NMap scan on the wireless client to And the clients MAC and IP address. The hacker then connects to another network and spoofs those addresses.
* it examines wireless clients’ probes and broadcasts the SSlDs in the probes, so that wireless clients will connect to it automatically.
* it uses ARP poisoning to disconnect wireless clients from the legitimate wireless network and force clients to connect to the hacker’s wireless network instead.

NEW QUESTION 35

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 36

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 37

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 38

What are some functions of an AruDaOS user role?
* The role determines which authentication methods the user must pass to gain network access
* The role determines which firewall policies and bandwidth contract apply to the clients traffic
* The role determines which wireless networks (SSiDs) a user is permitted to access
* The role determines which control plane ACL rules apply to the client’s traffic

NEW QUESTION 39

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 40

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 41

A company with 382 employees wants to deploy an open WLAN for guests. The company wants the experience to be as follows:

```
* Guests select the WLAN and connect without having to enter a password.
* Guests are redirected to a welcome web page and log in.
```

The company also wants to provide encryption for the network for devices mat are capable, you implement Tor the WLAN?

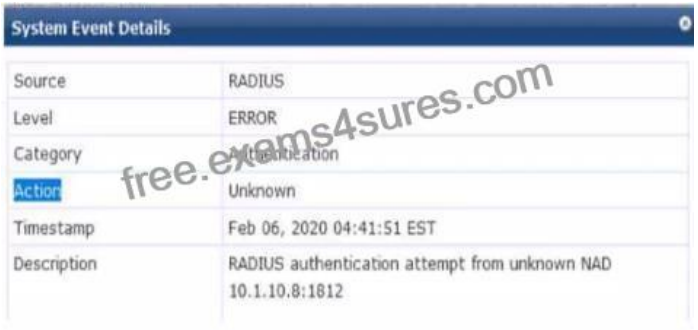
Which security options should
* WPA3-Personal and MAC-Auth
* Captive portal and WPA3-Personai
* Captive portal and Opportunistic Wireless Encryption (OWE) in transition mode
* Opportunistic Wireless Encryption (OWE) and WPA3-Personal

NEW QUESTION 42

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

NEW QUESTION 43

Refer to the exhibit.



You are deploying a new ArubaOS Mobility Controller (MC), which is enforcing authentication to Aruba ClearPass Policy Manager (CPPM). The authentication is not working correctly, and you find the error shown In the exhibit in the CPPM Event Viewer.

What should you check?
* that the MC has been added as a domain machine on the Active Directory domain with which CPPM is synchronized
* that the snared secret configured for the CPPM authentication server matches the one defined for the device on CPPM
* that the IP address that the MC is using to reach CPPM matches the one defined for the device on CPPM
* that the MC has valid admin credentials configured on it for logging into the CPPM

NEW QUESTION 44

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.