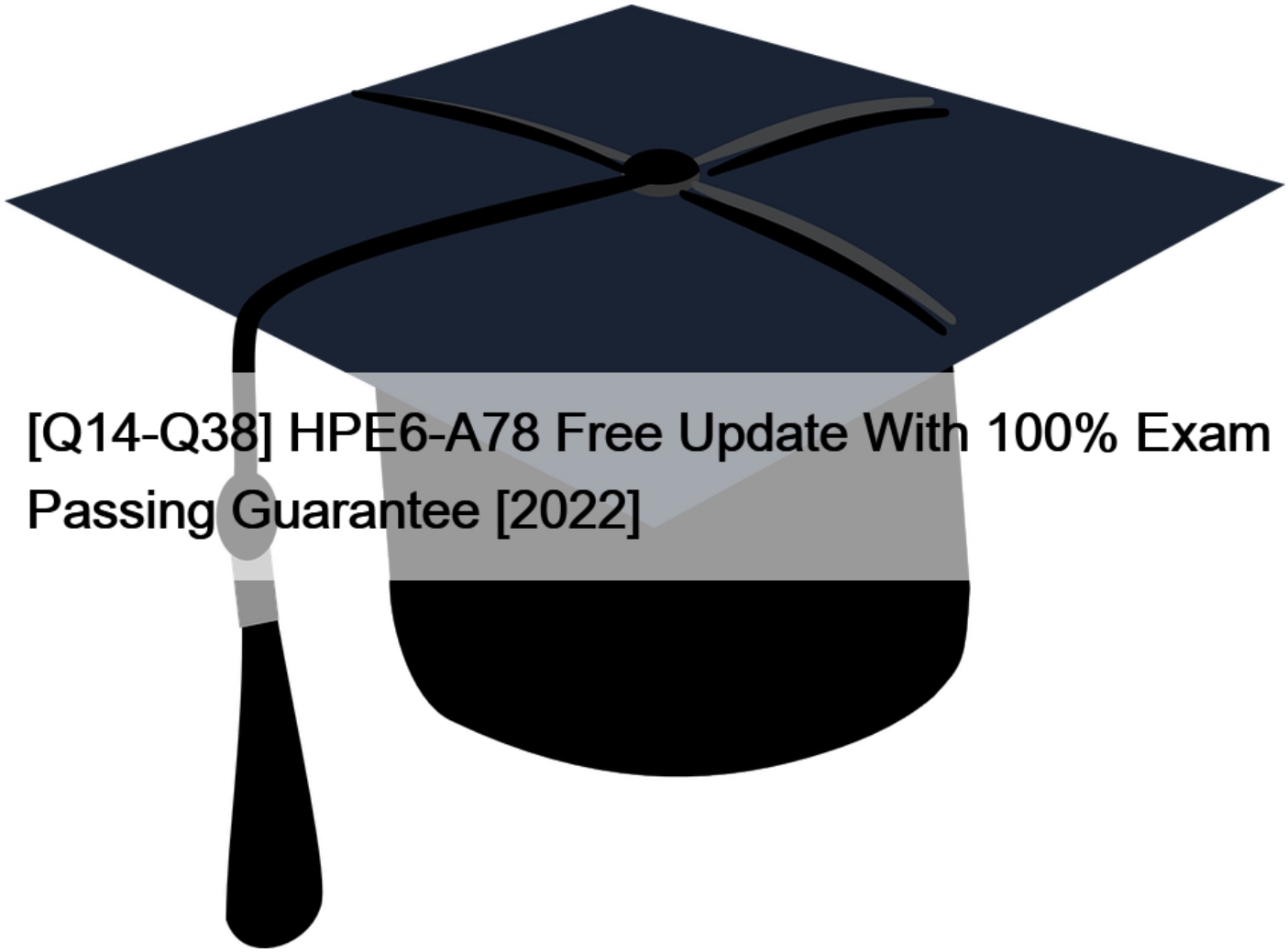
[Q14-Q38 HPE6-A78 Free Update With 100% Exam Passing Guarantee [2022



HPE6-A78 Free Update With 100% Exam Passing Guarantee [2022]
[Nov-2022] Verified HP Exam Dumps with HPE6-A78 Exam Study Guide

Q14. 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

Q15. 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

Q16. How does the ArubaOS firewall determine which rules to apply to a specific client’s traffic?
* The firewall applies every rule that includes the dent’s IP address as the source.
* The firewall applies the rules in policies associated with the client’s wlan
* The firewall applies thee rules in policies associated with the client’s user role.
* The firewall applies every rule that includes the client’s IP address as the source or destination.

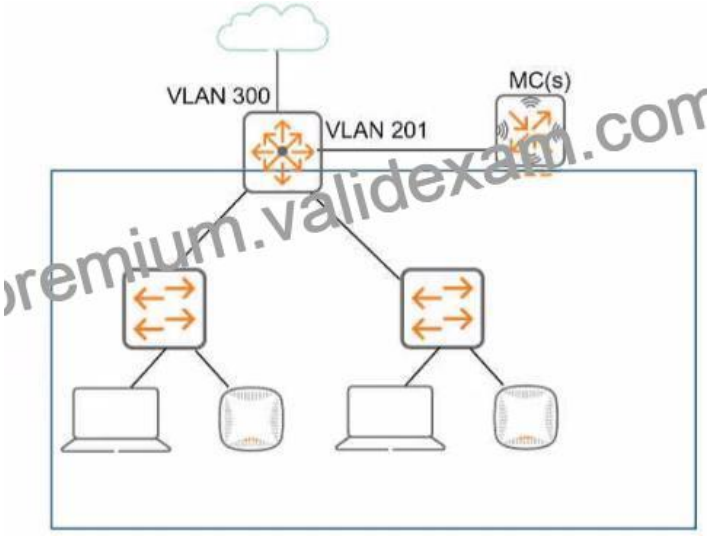
Q17. Which attack is an example or social engineering?
* An email Is used to impersonate a Dank and trick users into entering their bank login information on a fake website page.
* A hacker eavesdrops on insecure communications, such as Remote Desktop Program (RDP). and discovers login credentials.
* A user visits a website and downloads a file that contains a worm, which sell-replicates throughout the network.
* An attack exploits an operating system vulnerability and locks out users until they pay the ransom.

Q18. A company has an ArubaOS controller-based solution with a WPA3-Enterprise WLAN. which authenticates wireless clients to Aruba ClearPass Policy Manager (CPPM). The company has decided to use digital certificates for authentication A user’s Windows domain computer has had certificates installed on it However, the Networks and Connections window shows that authentication has tailed for the user. The Mobility Controllers (MC’s) RADIUS events show that it is receiving Access-Rejects for the authentication attempt.

What is one place that you can you look for deeper insight into why this authentication attempt is failing?
* the reports generated by Aruba ClearPass Insight
* the RADIUS events within the CPPM Event Viewer
* the Alerts tab in the authentication record in CPPM Access Tracker
* the packets captured on the MC control plane destined to UDP 1812

Q19. What is one difference between EAP-Tunneled Layer security (EAP-TLS) and Protected EAP (PEAP)?
* EAP-TLS creates a TLS tunnel for transmitting user credentials, while PEAP authenticates the server and supplicant during a TLS handshake.
* EAP-TLS requires the supplicant to authenticate with a certificate, hut PEAP allows the supplicant to use a username and password.
* EAP-TLS begins with the establishment of a TLS tunnel, but PEAP does not use a TLS tunnel as part of Its process
* EAP-TLS creates a TLS tunnel for transmitting user credentials securely while PEAP protects user credentials with TKIP encryption.

Q20. 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.

Q21. 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

Q22. 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.

Q23. 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.

Q24. 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

Q25. 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

Q26. What are the roles of 802.1X authenticators and authentication servers?
* The authenticator stores the user account database, while the server stores access policies.

* The authenticator supports only EAP, while the authentication server supports only RADIUS.
* The authenticator is a RADIUS client and the authentication server is a RADIUS server.
* The authenticator makes access decisions and the server communicates them to the supplicant.

Q27. 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

Q28. Refer to the exhibit.

```
Switch# show crypto host-public-key fingerprint
3072 9c:04:01:0e:e6:93:b1:4e:1f:f6:95:a9:74:9e:c0:f9: host_ssh2.pu
```

How can you use the thumbprint?
* 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
* 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
* 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
* install this thumbprint on management stations the stations can then authenticate with the thumbprint instead of admins having to enter usernames and passwords.

Q29. 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

Q30. A company has an Aruba solution with a Mobility Master (MM) Mobility Controllers (MCs) and campus Aps.

What is one benefit of adding Aruba Airwave from the perspective of forensics?
* Airwave can provide more advanced authentication and access control services for the AmbaOS solution
* Airwave retains information about the network for much longer periods than ArubaOS solution
* Airwave is required to activate Wireless Intrusion Prevention (WIP) services on the ArubaOS solution
* AirWave enables low level debugging on the devices across the ArubaOS solution

Q31. What is a vulnerability of an unauthenticated Dime-Heliman exchange?
* A hacker can replace the public values exchanged by the legitimate peers and launch an MITM attack.
* A brute force attack can relatively quickly derive Diffie-Hellman private values if they are able to obtain public values
* Diffie-Hellman with elliptic curve values is no longer considered secure in modem networks, based on NIST recommendations.
* Participants must agree on a passphrase in advance, which can limit the usefulness of Diffie- Hell man in practical contexts.

Q32. You have been asked to rind logs related to port authentication on an ArubaOS-CX switch for events logged in the past several

hours But. you are having trouble searching through the logs What is one approach that you can take to find the relevant logs?
* Add the “-C and *-c port-access” options to the “show logging” command.
* Configure a logging Tiller for the “port-access” category, and apply that filter globally.
* Enable debugging for “portaccess” to move the relevant logs to a buffer.
* Specify a logging facility that selects for “port-access” messages.

Q33. You are configuring ArubaOS-CX switches to tunnel client traffic to an Aruba Mobility Controller (MC).

What should you do to enhance security for control channel communications between the switches and the MC?
* Create one UBT zone for control traffic and a second UBT zone for clients.
* Configure a long, random PAPI security key that matches on the switches and the MC.
* install certificates on the switches, and make sure that CPsec is enabled on the MC
* Make sure that the UBT client vlan is assigned to the interface on which the switches reach the MC and only that interface.

Q34. 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.

Q35. 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?
* Renew CPPM’s RADIUS/EAP certificate
* Reset the user credentials
* Check CPPM Event viewer.
* Check connectivity between CPPM and a backend directory server

Q36. 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

Q37. Which is a correct description of a stage in the Lockheed Martin kill chain?
* In the delivery stage, malware collects valuable data and delivers or exfilltrated it to the hacker.
* In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfilltrated.
* In the weaponization stage, which occurs after malware has been delivered to a system, the malware executes Its function.
* In the exploitation and installation phases, malware creates a backdoor into the infected system for the hacker.

Authentic Best resources for HPE6-A78 Online Practice Exam: https://www.validexam.com/HPE6-A78-latest-dumps.html]