

[2024 Use Real HP Dumps - 100% Free HPE6-A78 Exam Dumps [Q37-Q61]



[2024] Use Real HP Dumps - 100% Free HPE6-A78 Exam Dumps
Realistic HPE6-A78 Dumps Latest HP Practice Tests Dumps

QUESTION 37

What is a benefit of Opportunistic Wireless Encryption (OWE)?

- * It allows both WPA2-capable 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 to 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

QUESTION 38

What is symmetric encryption?

- * It simultaneously creates ciphertext and a same-size MAC.
- * It any form of encryption that ensures that the 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.

QUESTION 39

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 UI 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.

QUESTION 40

You are troubleshooting an authentication issue for Aruba switches that enforce 802.1X 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 for 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 UI 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.

QUESTION 41

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

QUESTION 42

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.

QUESTION 43

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.

QUESTION 44

You are deploying an Aruba Mobility Controller (MC). What is a best practice for setting up secure management access to the ArubaOS Web UI?

- * Avoid using external manager authentication for the Web UI.
- * Change the default 4343 port for the web UI to TCP 443.
- * Install a CA-signed certificate to use for the Web UI server certificate.
- * Make sure to enable HTTPS for the Web UI and select the self-signed certificate installed in the factory.

QUESTION 45

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.

QUESTION 46

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, but 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.

QUESTION 47

An ArubaOS-CX switch enforces 802.1X on a port. No fallback 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

QUESTION 48

What is one way that Control Plane Security (CPsec) enhances security for the 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.

QUESTION 49

You have been instructed to look in the ArubaOS Security Dashboard's client list. Your goal is to find clients that 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

QUESTION 50

Which attack is an example of social engineering?

- * An email is used to impersonate a bank 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 self-replicates throughout the network.
- * An attack exploits an operating system vulnerability and locks out users until they pay the ransom.

QUESTION 51

What are some functions of an ArubaOS user role?

- * The role determines which authentication methods the user must pass to gain network access
- * The role determines which firewall policies and bandwidth contracts apply to the client's 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

QUESTION 52

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 exfiltrates it to the hacker.
- * In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfiltrated.
- * 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.

QUESTION 53

You configure an ArubaOS-Switch to enforce 802.1X authentication with ClearPass Policy Manager (CPPM) defined as the RADIUS server. Clients cannot authenticate. You check Aruba ClearPass Access Tracker and cannot find a record of the authentication attempt.

What are two possible problems that have this symptom? (Select two)

- * users are logging in with the wrong usernames and passwords or invalid certificates.
- * Clients are configured to use a mismatched EAP method from the one in the CPPM service.
- * The RADIUS shared secret does not match between the switch and CPPM.
- * CPPM does not have a network device defined for the switch's IP address.
- * Clients are not configured to trust the root CA certificate for CPPM's RADIUS/EAP certificate.

QUESTION 54

What is a key feature of the ArubaOS firewall?

- * The firewall is stateful which means that it 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 filter traffic primarily based on wireless 802.11 headers, making it ideal for mobility environments

QUESTION 55

What is a correct guideline for the management protocols that you should use on ArubaOS-Switches?

- * Disable Telnet and use TFTP instead.
- * Disable SSH and use https instead.
- * Disable Telnet and use SSH instead
- * Disable HTTPS and use SSH instead

QUESTION 56

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-Switches 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

QUESTION 57

How does the ArubaOS firewall determine which rules to apply to a specific client's traffic?

- * The firewall applies every rule that includes the client's IP address as the source.
- * The firewall applies the rules in policies associated with the client's wlan
- * The firewall applies the 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.

QUESTION 58

Which correctly describes a way to deploy certificates to end-user devices?

- * ClearPass Onboard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain
- * ClearPass Device Insight can automatically discover end-user devices and deploy the proper certificates to them
- * ClearPass OnGuard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain
- * in a Windows domain, domain group policy objects (GPOs) can automatically install computer, but not user certificates

QUESTION 59

Refer to the exhibit.

```
Switch# show crypto host-public-key fingerprint
3072 9c:04:01:0e:e6:93:b1:4e:1f:f6:9b: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-the-middle (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.

QUESTION 60

What is one way that WPA3-Enterprise enhances security when compared to WPA2-Enterprise?

- * WPA3-Enterprise is more secure against password leaking because all users have their own username and password
- * WPA3-Enterprise prevents eavesdropping on other users' wireless traffic by a user who knows the passphrase for the WLAN.
- * WPA3-Enterprise is more resistant to passphrase cracking because it requires passphrases to be at least 12 characters
- * WPA3-Enterprise is more complicated to deploy because it requires a backend authentication server

HPE6-A78 Dumps PDF - HPE6-A78 Real Exam Questions Answers:

https://www.test4engine.com/HPE6-A78_exam-latest-braindumps.html