Question 1

Question Type: MultipleChoice

Refer to the exhibit.

Management User

Enable local authentication:

Enable console block:

Management Users	
NAME	ROLE
admin	root

\+

General   **Admin**   AirWave   CPSec   Certificates   SNMP

> Management User

⌄ **Admin Authentication Options**

Default role:	root
Enable:	☑
MSCHAPv2:	☐
Server group:	ClearPass_Mgmt
Management telnet access:	☐
Login activities persistence period:	0 days

This Aruba Mobility Controller (MC) should authenticate managers who access the Web UI 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?

Options:

A- Change the local user role to read-only

B- Clear the MSCHAP check box

C- Disable local authentication

D- Change the default role to 'guest-provisioning'

Answer:

D

Question 2

Question Type: MultipleChoice

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?

Options:

A- EAP only

B- DHCP, DNS and RADIUS only

C- RADIUS only

D- DHCP, DNS, and EAP only

Answer:

A

Question 3

Question Type: MultipleChoice

You configure an ArubaOS-Switch to enforce 802.1X authentication with ClearPass Policy Manager (CPPM) denned 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)

Options:

A- users are logging in with the wrong usernames and passwords or invalid certificates.

B- Clients are configured to use a mismatched EAP method from the one In the CPPM service.

C- The RADIUS shared secret does not match between the switch and CPPM.

D- CPPM does not have a network device defined for the switch's IP address.

E- Clients are not configured to trust the root CA certificate for CPPM's RADIUS/EAP certificate.

Answer:

A, E

Question 4

Question Type: **MultipleChoice**

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?

Options:

A- MAC address d8:50:e6:f3;6d;a4; Client Classification Authorized; AP Classification, interfering

B- MAC address d8:50:e6 f3;6e;c5; Client Classification Interfering. AP Classification Neighbor

C- MAC address d8:50:e6:f3;6e;60; Client Classification Interfering. AP Classification Interfering

D- MAC address d8:50:e6:f3;TO;ab; Client Classification Interfering. AP Classification Rogue

Answer:

C

Question 5

Question Type: MultipleChoice

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

Options:

A- ClearPass Onboard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain

B- ClearPass Device Insight can automatically discover end-user devices and deploy the proper certificates to them

C- ClearPass OnGuard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain

D- in a Windows domain, domain group policy objects (GPOs) can automatically install computer, but not user certificates

Answer:

A

Question 6

Question Type: MultipleChoice

What is one way a noneypot can be used to launch a man-in-the-middle (MITM) attack to wireless clients?

Options:

A- it uses a combination or software and hardware to jam the RF band and prevent the client from connecting to any wireless networks

B- 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.

C- it examines wireless clients' probes and broadcasts the SSIDs in the probes, so that wireless clients will connect to it automatically.

D- 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.

Answer:

D

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

Mobility Controller > **Aruba_MC**

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

Aruba7030-US, 8.6.0.3

Auth Servers   AAA Profiles   L2 Authentication   L3 Authentication   User Rules   Advanced

Server Groups 3

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SER\
default	1	--	--	1
internal	1	--	--	Load Balance
MyEmployees_dot1_svg	1	--	--	0

+

Server Group > MyEmployees_dot1_svg	**Servers**	Options	Server Rules

NAME	TYPE	IP ADDRESS	TRIM FQDN	MAT
clearpass	RADIUS	10.5.5.5	--	0

You have set up a RADIUS server on an ArubaOS Mobility Controller (MC) when you created a WLAN named "MyEmployees .You now want to enable the MC to accept change of authorization (CoA) messages from this server for wireless sessions on this WLAN.

What Is a part of the setup on the MC?

A- Create a dynamic authorization, or RFC 3576, server with the 10.5.5.5 address and correct shared secret.

B- Install the root CA associated with the 10 5.5.5 server's certificate as a Trusted CA certificate.

C- Configure a ClearPass username and password in the MyEmployees AAA profile.

D- Enable the dynamic authorization setting in the 'clearpass' authentication server settings.

Answer:

B

Question 8

Question Type: MultipleChoice

Which attack is an example or social engineering?

Options:

A- An email Is used to impersonate a Dank and trick users into entering their bank login information on a fake website page.

B- A hacker eavesdrops on insecure communications, such as Remote Desktop Program (RDP). and discovers login credentials.

C- A user visits a website and downloads a file that contains a worm, which sell-replicates throughout the network.

D- An attack exploits an operating system vulnerability and locks out users until they pay the ransom.
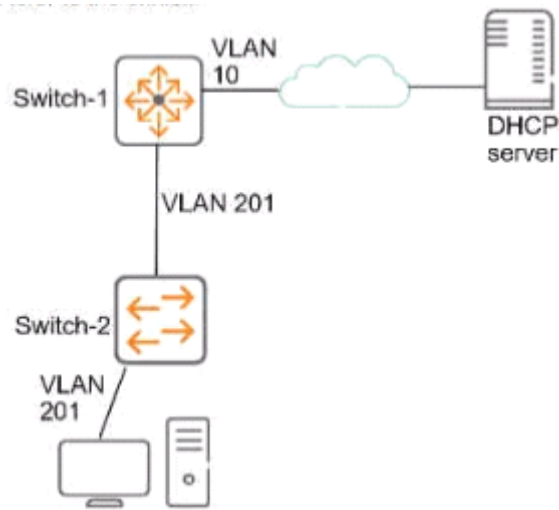
Answer:

A

Question 9

Question Type: MultipleChoice

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?

Options:

A- On Switch-1, enable ARP protection globally, and enable ARP protection on ail VLANs.

B- On Switch-2, make ports connected to employee devices trusted ports for ARP protection

C- On Swltch-2, enable DHCP snooping globally and on VLAN 201 before enabling ARP protection

D- On Swltch-2, configure static PP-to-MAC bindings for all end-user devices on the network

Answer:

D

Question 10

Question Type: MultipleChoice

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?

Options:

A- Renew CPPM's RADIUS/EAP certificate

B- Reset the user credentials

C- Check CPPM Event viewer.

D- Check connectivity between CPPM and a backend directory server

Answer:

C

Question 11

Question Type: MultipleChoice

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?

Options:

A- Create a TA profile on the ArubaOS-Switches with the root CA certificate for ClearPass's HTTPS certificate

B- Create device fingerprinting profiles on the ArubaOS-Switches that include SNMP. and apply the profiles to edge ports

C- Create remote mirrors on the ArubaOS-Swrtches that collect traffic on edge ports, and mirror it to CPPM's IP address.

D- Create SNMPv3 users on ArubaOS-CX switches, and make sure that the credentials match those configured on CPPM

Answer:

B