Free Questions for PAM-SEN by braindumpscollection

Shared by Saunders on 29-01-2024

Question 1

Question Type: **MultipleChoice**

Which file must you edit to ensure the PSM for SSH server is not hardened automatically after installation?

Options:

A- vault.ini

B- user.cred

C- psmpparms

D- psmgw.config

Answer:

C

Question 2

Question Type: **MultipleChoice**

What is a prerequisite step before CyberArk can be configured to support RADIUS authentication?

Options:

A- Log on to the PrivateArk Client, display the User properties of the user to configure, run the Authentication method drop-down list, and select RADIUS authentication.

B- In the RADIUS server, define the CyberArk Vault as a RADIUS client/agent. Most Voted

C- In the Vault installation folder, run CAVaultManager as administrator with the SecureSecretFiles command.

D- Navigate to /Server/Conf and open DBParm.ini and set the RadiusServersInfo parameter.

Answer:

B

Question 3

Question Type: MultipleChoice

In large-scale environments, it is important to enable the CPM to focus its search operations on specific Safes instead of scanning all Safes it sees in the Vault.

How is this accomplished?

Options:

A- Administration Options > CPM Settings

B- AllowedSafe Parameter on each platform policy

C- MaxConcurrentConnection parameter on each platform policy

D- Administration > Options > CPM Scanner

Answer:

B

Question 4

Question Type: **MultipleChoice**

In addition to disabling Windows services or features not needed for PVWA operations, which tasks does PVWA_Hardening.ps1 perform when run? (Choose two.)

Options:

A- performs IIS hardening

B- configures all group policy settings

C- renames the local Administrator Account

D- configures Windows Firewall

E- imports the CyberArk INF configuration

Answer:

A, D

Question 5

Question Type: MultipleChoice

After installing the Vault, you need to allow Firewall Access for Windows Time service to sync with NTP servers 10.1.1.1 and 10.2.2.2.

What should you do?

Options:

A- Edit DBParm.ini to add: AllowNonStandardFWAddresses=[10.1.1.1,10.2.2.2],Yes,123:outbound/udp. Most Voted

B- Edit DBParm.ini to add: NTPServer=[10.1.1.1:123/UDP,10.2.2.2:123/UDP].

C- Edit DBParm.ini to add: AllowNonStandardFWAddresses=[10.1.1.1,10.2.2.2],Yes,123:outbound/udp,123:inbound/udp.

D- Edit the Windows Firewall configuration to add a rule for Port 123/udp outbound to 10.1.1.1 and 10.2.2.2.

Answer:

D

Question 6

Question Type: **MultipleChoice**

Which command should be executed to harden a Vault after registering it to Azure?

Options:

A- HardenAzureFW.ps1 Most Voted

B- ExecuteStage ./Hardening/HardeningConf.xml

C- HardenVaultFW.ps1

D- ExecuteStage ./PostInstallation/PostInstallation.xml

Answer:

C

Question 7

Question Type: **MultipleChoice**

Which statement is correct about a post-install hardening?

Options:

A- The Vault must be hardened during the Vault installation process. Most Voted

B- After the Vault server is installed, you must join the server to the Enterprise Domain and reboot the host.

C- It is executed after Vault installation by running CAVaultHarden.exe and hardening options can be edited by changing the Hardening.ini file. Most Voted

D- If it is mandated by an organization's IT governance, you do not have to execute Vault hardening; however, server hardening cannot be reversed.

Answer:

C

Question 8

Question Type: **MultipleChoice**

As a member of a PAM Level-2 support team, you are troubleshooting an issue related to load balancing four PVWA servers at two data centers. You received a note from your Level-1 support team stating ''When testing PVWA website from a workstation, we noticed that the ''Source IP of last sign-in'' was shown as the VIP (Virtual IP address) assigned to the four PVWA servers instead of the workstation IP where the PVWA site was launched from.''

Which step should you take?

Options:

A- Verify the ''LoadBalancerClientAddressHeader'' parameter setting in PVWA configuration file Web.config is set to ''X-Forwarded-For''.

B- Add the VIP (Virtual IP address) assigned to the four PVWA servers to the certificates issued for all four PVWA servers, if missing.

C- Add a firewall rule to allow the testing workstation to connect to the VIP (Virtual IP address) assigned to the four PVWA servers on Port TCP 443.

D- Edit the dbparm.ini file on the Vault server and add the IP or subnet of the workstation to the whitelist.

Answer:

A

Question 9

Question Type: **MultipleChoice**

You are installing the HTML5 gateway on a Linux host using the RPM provided.

After installing the Tomcat webapp, what is the next step in the installation process?

Options:

A- Deploy the HTML5 service (guacd). Most Voted

B- Secure the connection between the guacd and the webapp.

C- Secure the webapp and JWT validation endpoint.

D- Configure ASLR.

Answer:

B

Question 10

Question Type: MultipleChoice

What is required before the first CPM can be installed?

Options:

A- The environment must have at least one Vault and one PVWA installed.

B- The Vault environment must have at least one account stored in a safe.

C- Custom platforms must be downloaded from the CyberArk Marketplace.

D- The PSM component must be installed and proper functionality validated.

Answer:

A