Free Questions for 156-585 by go4braindumps

Shared by Pruitt on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

How many captures does the command "fw monitor -p all" take?

Options:

A- All 15 of the inbound and outbound modules

B- All 4 points of the fw VM modules

C- 1 from every inbound and outbound module of the chain

D- The -p option takes the same number of captures, but gathers all of the data packet

Answer:

C

Question 2

Question Type: **MultipleChoice**

After kernel debug with "fw ctl debug" you received a huge amount of information It was saved in a very large file that is difficult to open and analyze with standard text editors Suggest a solution to solve this issue.

Options:

A- Use 'fw ctl zdebug' because of 1024KB buffer size

B- Divide debug information into smaller files Use 'fw ctl kdebug -f -o 'filename' -m 25 - s '1024'

C- Reduce debug buffer to 1024KB and run debug for several times

D- Use Check Point InfoView utility to analyze debug output

Answer:

C

Question 3

Question Type: **MultipleChoice**

The management configuration stored in the Postgres database is partitioned into several relational database Domains, like - System, User, Global and Log Domains. The User Domain stores the network objects and security policies. Which of the following is stored in the Log Domain?

Options:

A- Configuration data of Log Servers and saved queries for applications

B- Active Logs received from Security Gateways and Management Servers

C- Active and past logs received from Gateways and Servers

D- Log Domain is not stored in Postgres database, it is part of Solr indexer only

Answer:

D

Question 4

Question Type: **MultipleChoice**

Which command is most useful for debugging the fwaccel module?

Options:

A- fw zdebug

B- securexl debug

C- fwaccel dbg

D- fw debug

Answer:

C

Question 5

Question Type: **MultipleChoice**

Which of the following is NOT a vpn debug command used for troubleshooting?

Options:

A- fw ctl debug -m fw + conn drop vm crypt

B- vpn debug trunc

C- pclient getdata sslvpn

D- vpn debug on TDERROR_ALL_ALL=5

Answer:

C

Question 6

Question Type: MultipleChoice

Where do Protocol parsers register themselves for IPS?

Options:

A- Passive Streaming Library

B- Other handlers register to Protocol parser

C- Protections database

D- Context Management Infrastructure

Answer:

A

Question 7

Question Type: MultipleChoice

Which one of the following is NOT considered a Solr core partition:

Options:

A- CPM_0_Revisions

B- CPM_Global_A

C- CPM_Gtobal_R

D- CPM_0_Disabled

Answer:

D

Question 8

Question Type: MultipleChoice

What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

Options:

A- .cap

B- .exe

C- .tgz

D- .pcap

Answer:

A

To Get Premium Files for 156-585 Visit

https://www.p2pexams.com/products/156-585

For More Free Questions Visit

https://www.p2pexams.com/checkpoint/pdf/156-585

20%
DISCOUNT