Vendor: Check Point

Exam Code: 156-581

Exam Name: Check Point Certified Troubleshooting Administrator - R81 (CCTA)

Version: DEMO

QUESTION 1
What is the most efficient way to view large fw monitor captures and run filters on the file?

A. wireshark
B. CLISH
C. snoop
D. CLI

Answer: A

QUESTION 2
Check Point's self-service knowledge base of technical documents and tools covers everything from articles describing how to fix specific issues, understand error messages and to how to plan and perform product installation and upgrades. This knowledge base is called:

A. SupportDocs
B. SupportCenterBase
C. SecureDocs
D. SecureKnowledge

Answer: D

QUESTION 3
Which of the following System Monitoring Commands (Linux) shows process resource utilization, as well as core and memory utilization?

A. top
B. free
C. ps
D. df

Answer: A

QUESTION 4
Is it possible to analyze ICMP packets with tcpdump?

A. No, since ICMP does not have any source or destination ports, but specification of port numbers is mandatory
B. Yes, tcpdump is not limited to tcp specific issues
C. No, tcpdump works from layer 4. ICMP is located in the network layer (layer 3), therefore is not applicable to this scenario
D. No, use fw monitor instead

Answer: A

QUESTION 5
Which of the following is NOT a way to insert fw monitor into the chain when troubleshooting packets throughout the chain?

A. Relative position using alias
B. Relative position using id
C. Absolution position
D. Relative position using location

Answer: D

QUESTION 6
The Check Point FW Monitor tool captures and analyzes incoming packets at multiple points in the traffic inspections. Which of the following is the correct inspection flow for traffic?

A. (o) — pre-outbound, (0)- post-inbound, (i) — pre-inbound, (I) — post-inbound
B. (I) — pre-inbound, (i)- post-inbound, (0) — pre-outbound, (o) — post-outbound
C. (i) — pre-inbound, (I)- post-inbound, (o) — pre-outbound. (O) — post-outbound
D. (0) — post-outbound, (o)- pre-outbound, (I) — post-inbound. (i) — pre-inbound

Answer: C

QUESTION 7
Which of the following CLI commands is best to use for getting a quick look at appliance performance information in Gaia?

A. fw stat
B. cphaprob stat
C. top
D. fw monitor

Answer: C

QUESTION 8
Which of the following is a valid way to capture general packets on Check Point gateways?

A. Wireshark
B. tcpdump
C. Firewall logs
D. Network taps

Answer: B

QUESTION 9
What are the four ways to insert an FW Monitor into the firewall kernel chain?

A. Absolute position using location, relative position using alias, general position, all positions
B. Relative position using location, relative position using alias, absolute position. all positions
C. Absolute position using location, absolute position using alias, relative position, all positions
D. Relative position using geolocation, relative position using inertial navigation, absolute position, all positions

Answer: D

QUESTION 10
Some users from your organization have been reporting some connection problems with CIFS since this morning. You suspect an IPS issue after an automatic IPS update last night. So you want to perform a packet capture on uppercase I only directly after the IPS chain module (position 4 in the chain) to check if the packets pass the IPS. What command do you need to run?

A. fw monitor -pi 5 -e <filterexpression>
B. fw monitor -pI asm <filterexpression>
C. tcpdump -eni any <fitterexpression>
D. fw monitor -mI -pI 5 -e <filterexperession>

Answer: D

QUESTION 11
When running a debug with fw monitor, which parameter will create a more verbose output?

A. -D
B. -d
C. -I
D. -i

Answer: A

QUESTION 12
Which is the correct 'fw monitor syntax for creating a capture file for loading it into Wireshark?

A. fw monitor -e 'accept <FILTER EXPRESSION>; » Output.cap
B. This cannot be accomplished as it is not supported with R80.10
C. fw monitor -e 'accept <FILTER EXPRESSION>: -file Output.cap
D. fw monitor -e 'accept <FILTER EXPRESSION>; -o Output.cap

Answer: D

QUESTION 13
Johnny works as a firewall administrator in ALPHA Corporation. He is also an Account Administrator in the Check Point UserCenter for his company. When searching through SecureKnowledge he found an article which can help him but he couldn't access the article, because has no permission to access it. What could cause this problem?

A. ALPHA Corporation's Support contract expired, or he is not Check Point certified professional
B. Johnny must be Check Point Certified Security Master to get access articles with higher Technical Level
C. Only Check Point Support Engineers have access to articles with higher Technical Level
D. ALPHA Corporation's Support contract expired

Answer: A

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**