Vendor: Check Point

Exam Code: 156-315.80

Exam Name: Check Point Certified Security Expert - R80

Version: DEMO

QUESTION 1
Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidates management console. CPM allows the GUI client and management server to communicate via web services using _____.

A. TCP port 19009
B. TCP Port 18190
C. TCP Port 18191
D. TCP Port 18209

Answer: A

QUESTION 2
Which command is used to set the CCP protocol to Multicast?

A. cphaprob set_ccp multicast
B. cphaconf set_ccp multicast
C. cphaconf set_ccp no_broadcast
D. cphaprob set_ccp no_broadcast

Answer: B
Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk20576

QUESTION 3
Which packet info is ignored with Session Rate Acceleration?

A. source port ranges
B. source ip
C. source port
D. same info from Packet Acceleration is used

Answer: C
Explanation:
http://trlj.blogspot.com/2015/10/check-point-acceleration.html

QUESTION 4
Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?

A. Synchronized
B. Never been synchronized
C. Lagging
D. Collision

Answer: D
Explanation:
https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/120712

QUESTION 5
During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

A. Host having a Critical event found by Threat Emulation
B. Host having a Critical event found by IPS
C. Host having a Critical event found by Antivirus
D. Host having a Critical event found by Anti-Bot

Answer: D

QUESTION 6
In R80 spoofing is defined as a method of:

A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
B. Hiding your firewall from unauthorized users.
C. Detecting people using false or wrong authentication logins
D. Making packets appear as if they come from an authorized IP address.

Answer: D
Explanation:
IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.
Reference:
http://dl3.checkpoint.com/paid/74/74d596decb6071a4ee642fbdaae7238f/CP_R80_SecurityMana gement_AdminGuide.pdf?
HashKey=1479584563_6f823c8ea1514609148aa4fec5425db2&xtn=.pdf

QUESTION 7
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

A. UDP port 265
B. TCP port 265
C. UDP port 256
D. TCP port 256

Answer: D
Explanation:
Synchronization works in two modes:
Full Sync transfers all Security Gateway kernel table information from one cluster member to another. It is handled by the fwd daemon using an encrypted TCP connection on port 256.
Delta Sync transfers changes in the kernel tables between cluster members. Delta sync is handled by the Security Gateway kernel using UDP connections on port 8116.
Reference:
https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_ClusterXL_Ad minGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/ CP_R80.10_ClusterXL_AdminGuide/7288

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**