Vendor: Cisco

Exam Code: 500-280

Exam Name: Securing Cisco Networks with Open Source Snort

Version: DEMO

QUESTION 1
What does packet sniffing do?

A. isolates datagrams into like groups
B. reads datagrams directly off the wire
C. transmits datagrams over a wireless network
D. rebuilds datagram streams

Answer: B

QUESTION 2
When building a platform for a Snort installation, which set of components is a major security concern?

A. IP address, mask, and gateway settings
B. host naming conventions
C. URL feed vendors
D. default accounts and settings

Answer: D

QUESTION 3
In the IP addressing scheme of your organization, each subnet consists of 4096 hosts, and the beginning of the addressing scheme is 172.16.0.0. Your remote office is allocated the range of addresses from the first subnet. What are the CIDR notation, network address, broadcast address, and valid IP address in your assigned range?

A. 172.16.0.0/24, 172.16.0.0, 172.16.8.255, 172.16.0.51
B. 172.16.0.0/20, 172.16.0.0, 172.16.15.255, 172.16.8.252
C. 172.16.0.0/16, 172.16.0.0, 172.16.32.255, 172.16.22.4
D. 172.16.0.0/12, 172.16.0.0, 172.16.64.255, 172.16.52.112

Answer: B

QUESTION 4
Which statement about implementing DAQ is true?

A. It is a shell script that works on any Linux platform.
B. It must be compiled separately.
C. You must obtain it from Sourceforge.
D. It is not open source.

Answer: B

QUESTION 5
Which version of libpcap does DAQ require?

A. 0.9.8 or later
B. 1.0.0 or later

C. any version
D. none

Answer: B

QUESTION 6
If Snort is installed and the sensor, database, and web server all reside on the same machine, to which ports should remote access of the sensor be restricted?

A. 22 and 443
B. 80 and 443
C. 443 and 3306
D. 23 and 80

Answer: A

QUESTION 7
To execute a command in Linux while in the directory where it is located, and be sure you are only running that particular copy, what would you use in front of the executable name?

A. ./
B. ../
C. ..\
D. .\

Answer: A

QUESTION 8
Which application can read Barnyard log_pcap output plug-in files?

A. SnortReport
B. BASE or ACID
C. tcpdump
D. Snorby

Answer: C

QUESTION 9
To accept input from Snort and produce various forms of output, the Barnyard architecture consists of which components?

A. preprocessors and reassemblers
B. preprocessors and detection engine
C. data processors and output plug-ins
D. data processors and reassemblers

Answer: C

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**