Q&A

Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt.
----- Guaranteed.

KILL EXAMS

PASS ✓

killexams.com

Cisco

500-275

Securing Cisco Networks with Sourcefire FireAMP Endpoints

100%

BEST

100%

ORDER FULL VERSION

Question #153

Which option is one of the three methods of updating the IP addresses in Sourcefire Security Intelligence?

- A. subscribe to a URL intelligence feed
- B. subscribe to a VRT
- C. upload a list that you create
- D. automatically upload lists from a network share

Answer: C

Question #154

Which statement is true in regard to the Sourcefire Security Intelligence lists?

- A. The global blacklist universally allows all traffic through the managed device.
- B. The global whitelist cannot be edited.
- C. IP addresses can be added to the global blacklist by clicking on interactive graphs in Context Explorer.
- D. The Security Intelligence lists cannot be updated.

Answer: C

Question #155

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 #156

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 #157

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 #158

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 #159

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 #160

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 #161

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

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

Answer: C

Question #162

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

Question #163

Barnyard has a mode of operation that reads the most current unified log file and processes new unified files as they become available. What is this mode called?

- A. one-shot
- B. continual
- C. continual with checkpoint
- D. unified

Answer: B

Question #164

What does the log_dump output plug-in do?

- A. converts data into a format similar to Snort ASCII packet dump mode
- B. converts data into a format similar to Snort fast alert mode
- C. converts log data to PCAP-formatted output
- D. converts data to CVS format

Answer: A

Question #165

Which output method is the fastest for Snort?

- A. unified2
- B. database
- C. binary (tcpdump)
- D. CSV

Answer: A

Question #166

Which command-line argument can you use with Snort to produce a binary output file?

- A. -B
- B. -b
- C. -u
- D. -U

Answer: B

Question #167

Which command-line argument can you use with Snort to read a previously created file?

- A. -O
- B. -o
- C. -p
- D. -r

Answer: D

Question #168

What must you do to produce ASCII-formatted output from Snort?

- A. Do nothing because Snort produces ASCII output by default.
- B. Use the -K ascii switch when you start Snort from the command line.
- C. Compile Snort with the -K ascii flag in the configure command.
- D. Use a third-party application to convert native Snort output to ASCII.

Answer: B

Question #169

For which application is Snort output suitable?

- A. tcpdump
- B. Wireshark
- C. any application that can read PCAP format
- D. NMap

Answer: C

SAMPLE QUESTIONS

These questions are for demo purpose only. **Full version** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

ORDER FULL VERSION
Special Discount Coupon

Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.

For More exams visit https://killexams.com/vendors-exam-list
Kill your exam at First Attempt....Guaranteed!