DUMPSBOSS.

Huawei Certified ICT Professional - Constructing Service Security Network (HCIP-Security-CSSN V3.0)

Huawei H12-722

Version Demo

Total Demo Questions: 10

Total Premium Questions: 173

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Tianyu Nei answered the role of safety filtering technology, which of the following is still correct? (multiple choice)

A. File filtering can reduce the risk of malicious code execution and virus infection in the internal network by blocking the transmission of fixed types of files, and it can also prevent

Prevent employees from leaking company confidential documents to the Internet.

B. Content filtering can prevent the disclosure of confidential information and the transmission of illegal information

C. The application behavior control function can finely control common HTTP behaviors and FTP behaviors.

D. Mail filtering refers to the management and control of mail sending and receiving, including preventing the flooding of spam and anonymous emails, and controlling the sending and receiving of illegal emails.

ANSWER: A B C D

QUESTION NO: 2

In the Huawei USG6000 product, after creating or modifying the security configuration file, the configuration content will not take effect immediately: you need to click the "Prompt" in the upper right corner of the interface.

"Hand in" to activate.

A. True

B. False

ANSWER: A

QUESTION NO: 3

In the anti-virus policy configuration of Huawei USG6000 product, what are the response methods of HTTP protocol? (multiple choice)

A. Warning

B. Block and push the page

C. A warning dialog box pops up

D. All access to the client is prohibited

ANSWER: A B

QUESTION NO: 4

Which of the following behaviors is a false positive of the intrusion detection system?

A. Unable to detect new types of worms

B. The process of trying to log in to the system is recorded

C. Use Ping to perform network detection and be alerted as an attack

D. Web-based attacks are not detected by the system

ANSWER: C

QUESTION NO: 5

For the description of the principles of HTTP Flood and HTTPS Flood blow defense, which of the following options are correct? (multiple choice)

A. HTTPS Flood defense modes include basic mode, enhanced mode and 302 redirection.

B. HTTPS Flood defense can perform source authentication by limiting the request rate of packets.

C. The principle of HTTPS Flood attack is to request URIs involving database operations or other URIs that consume system resources, causing server resource consumption.

Failed to respond to normal requests.

D. The principle of HTTPS Flood attack is to initiate a large number of HTTPS connections to the target server, causing the server resources to be exhausted and unable to respond to regular requests.

begging.

ANSWER: B C D

QUESTION NO: 6

Regarding the 3 abnormal situations of the file type recognition result, which of the following option descriptions is wrong?

A. File extension mismatch means that the file type is inconsistent with the file extension.

B. Unrecognized file type means that the file type cannot be recognized and there is no file extension.

C. File damage means that the file type cannot be identified because the file is damaged.

D. Unrecognized file type means that the file type cannot be recognized, and the file extension cannot be recognized.

ANSWER: D

QUESTION NO: 7

Which of the following options describes the IntelliSense engine IAE incorrectly?

A. IAE's content security detection functions include application identification and perception, intrusion prevention, and Web application security.

B. Full English name: intelligent Awareness Engine.

C. The core of C.IAE is to organically centralize all content security-related detection functions.

D. The security detection of the IAE engine is parallel, using a message-based file processing mechanism, which can receive file fragments and perform security checks.

ANSWER: D

QUESTION NO: 8

If you combine security defense with big data technology, which of the following statements are correct? (multiple choice)

A. In the learning process, you should start from collecting samples, analyze their characteristics and then perform machine learning.

B. Machine learning only counts a large number of samples, which is convenient for security administrators to view.

C. In the detection process, the characteristics of unknown samples need to be extracted and calculated to provide samples for subsequent static comparisons.

D. Security source data can come from many places, including data streams, messages, threat events, logs, etc.

ANSWER: A C D

QUESTION NO: 9

After enabling the IP policy, some services are found to be unavailable. Which of the following may be caused by? (multiple choice)

A. Only packets in one direction pass through the firewall

B. The same message passes through the firewall multiple times

C. IPS underreporting

D. Excessive traffic causes the Bypass function to be enabled

ANSWER: A B

QUESTION NO: 10

When using the two-way SSL function to decrypt HTTPS packets, the value of the reverse proxy level represents the number of times the packet can be decrypted.

A. True

B. False

ANSWER: B