



2B0-101

(ESSE Recertification)

Total Questions: 100

Last Updated: Jan 01, 2009

Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' 2B0-101 study guide is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this guide. An average of approximately 10 to 20 hours should be spent to study this guide and you will surely pass your exam. It's our guarantee.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Guarantee

If you study this guide properly and still unable to pass the exam, please send us a scanned copy of your official score at: refund@techeXams.ws. We will happily reimburse the cost of this study guide or send you an exchange of study guide of your choice free of cost.

Feedback

If you find any possible improvement, then please do let us know. We are always interested in improving the quality of this product. Feedback can be send at: feedback@techeXams.ws

Copyright

techXams holds the copyright of this material. techXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Question: 1

The attack category is for events that

- A. Attempt to discover weaknesses
- B. Map the structure of the network
- C. Have the potential to compromise the integrity of an end system.
- D. Deny access to resources

Answer: C

Question: 2

Virtual Sensors can segregate traffic by?

- A. IP Address, VLAN, Port
- B. IP Address, VLAN, Port, Protocol
- C. IP Address, VLAN, Port, Protocol, Application
- D. IP Address, VLAN, Port, Application

Answer: B

Question: 3

In an Event Flow Processor (EFP) a consumer can be?

- A. A Sensor or an Event Channel
- B. An Event channel only
- C. An Event channel or an Agent
- D. An Agent only

Answer: C

Question: 4

Before the host Sensor can be deployed

- A. It must be associated with a virtual sensor
- B. It must be associated with a host policy
- C. Its key must be added to the /usr/dragon/bin directory
- D. Its address must be added to /etc/hosts

Answer: B

Question: 5

Which of the following Dragon Agents is used for detecting changes to host files?

- A. Real Time Cons
- B. MD5 Sum
- C. Alarm Tool
- D. Database

Answer: B

Question: 6

In a standalone dep

- A. A net-config-clie
- B. A net-config-ser
- D. A net-config-ser

ient.xml file
 xml file

Answer: C

Question: 7

MD5 checksums are

- A. Stored in a prot
- B. Appended to th
- C. Passed up the e
- D. Stored in the /u

erver (EMS)

Answer: C

Question: 8

Which of the follow

- B. It u
- C. It writes
- D. It writes a con

abase

Answer: C

2B0-101 Demo Exam