2B0-023

(ES Advanced Dragon IDS)

Total Questions: 50

Last Updated: Jan 01, 2009

Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' 2B0-023 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

Question: 1

What are three primary common goals of a corporate/network security policy?

A. Authentication, Authorization and Accounting (AAA)
B. Security, Productivity and Adaptability (SPA)
C. Confidentiality, Integrity and Availability (CIA)
D. Authentication, Encryption and Compression (AEC)

Answer: C

Question: 2

Which of the following must an IDS administrator consider when deploying Dragon in accordance with a corporate security policy?

A. Must understand the purpose and scope of each aspect of the overall security policy
B. Must understand the security goals of each product in the organization (i.e., operating systems, routers, firewalls, NIDS, HIDS, VPN gateways)
C. Must understand the detailed configurations on each router within the security domain
D. Must understand how the security policy impacts the I.T. budget

Answer: A, B

Question: 3

What functions can Dragon accomplish as related to a corporate/network security policy?

A. Dragon agents can gather information about network security compromises and automatically produce corporate/network security policy documents
B. Dragon agents can detect and log security policy deviations
C. Dragon agents can assist with security policy enforcement via Active Responses
D. Dragon can evaluate a corporate/network policy to determine if it is complete and effective

Answer: B, C

Question: 4

Which vulnerability scanner and report format is required for use with the Dragon VCT?

A. MySQL; .msq formatted output
B. Nessis; .nfr formatted output
C. Nessus; .nes formatted output
D. Nessus; .nsr formatted output
E. NMAP; .nmp formatted output

Answer: D

Question: 5

Which of the follow esponse using Dragon?

A. Use the Dragon
B. Deploy Dragon
C. Deploy Dragon
D. Enable SSL and nel
E. Correlate Drago create new signatures as nece

Answer: D

Question: 6

Which of the follow

A. A database of k tem
B. A database of n IDS to correlate detected attacks
C. A dictionary of s ion security exposures
D. All of the above

Answer: C

Question: 7

Which of the follow nner?

A. Monitors health
B. Output is critica twork

Answer: D