2B0-018

Enterasys

ES Dragon IDS

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 2B0-018 exam in first attempt and also get high scores to acquire Enterasys certification.

If you use OfficialCerts 2B0-018 Certification questions and answers, you will experience actual 2B0-018 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Enterasys exam prep covers over 95% of the questions and answers that may be appeared in your 2B0-018 exam. Every point from pass4sure 2B0-018 PDF, 2B0-018 review will help you take Enterasys 2B0-018 exam much easier and become Enterasys certified.

Here's what you can expect from the OfficialCerts Enterasys 2B0-018 course:

** Up-to-Date Enterasys 2B0-018 questions as experienced in the real exam.*
** 100% correct Enterasys 2B0-018 answers you simply can't find in other 2B0-018 courses.*
** All of our tests are easy to download. Your file will be saved as a 2B0-018 PDF.*
** Enterasys 2B0-018 brain dump free content featuring the real 2B0-018 test questions.*

Enterasys 2B0-018 certification exam is of core importance both in your Professional life and Enterasys certification path. With Enterasys certification you can get a good job easily in the market and get on your path for success. Professionals who passed Enterasys 2B0-018 exam training are an absolute favorite in the industry.
You will pass Enterasys 2B0-018 certification test and career opportunities will be open for you.

http://www.studentidisinistra.org/?testid=exams.asp?examcode=2B0-018

Question: 1
Which of the following is NOT a typical function of an Intrusion Detection System?

A - Monitors segment traffic to detect suspicious activity
B - Monitors network traffic and corrects attacks
C - Monitors traffic patterns to report on malicious events
D - Monitors individual hosts (HIDS) or network segments (NIDS)

Answer: B

Question: 2
Which best describes a SYN Flood attack?

A - Attacker redirects unusually large number of SYN/ACK packets
B - Attacker sends relatively large number of altered SYN packets
C - Attacker floods a host with a relatively large number of unaltered SYN packets
D - Attacker floods a host with an unusually large number of legitimate ACK packets

Answer: B

Question: 3
Which best describes a type of attack that aims to prevent the use of a service or host?

A - Reconnaissance
B - Denial of Service
C - IP Spoofing
D - Exploit

Answer: B

Question: 4
Which of the following is NOT a valid detection method used by Dragon Network Sensor?

A - Signature detection
B - Protocol detection
C - Policy detection
D - Anomaly detection

Answer: C

Question: 5
Which of the following is NOT a function of Dragon Forensics Console?

A - Allows for central configuration of Active Response mechanisms to deter network attacks
B - Centrally analyzes activity as it is occurring or has occurred over time
C - Correlates events together across Network Sensor, Host Sensor, and any other infrastructure system (e.g., firewall, router) for which messages have been received (via Host Sensor log forwarding)
D - Provides the tools for performing a forensics level analysis and reconstructing an attackers session

Answer: A

Question: 6
Which of the following does NOT describe Dragon Host Sensors Multi-Detection methods?

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google