

# **Examcollection**

<http://www.ipass4sure.com/examcollection.htm>

# 2B0-018

**Enterasys**  
*ES Dragon IDS*

<http://www.ipass4sure.com/exams.asp?examcode=2B0-018>

The 2B0-018 practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The 2B0-018 Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently. The 2B0-018 exam is very challenging, but with our 2B0-018 questions and answers practice exam, you can feel confident in obtaining your success on the 2B0-018 exam on your FIRST TRY!

## Enterasys 2B0-018 Exam Features

- Detailed questions and answers for 2B0-018 exam
- Try a demo before buying any Enterasys exam
- 2B0-018 questions and answers, updated regularly
- Verified 2B0-018 answers by Experts and bear almost 100% accuracy
- 2B0-018 tested and verified before publishing
- 2B0-018 examcollection vce questions with exhibits
- 2B0-018 same questions as real exam with multiple choice options

Acquiring Enterasys certifications are becoming a huge task in the field of I.T. More over these exams like 2B0-018 exam are now continuously updating and accepting this challenge is itself a task. This 2B0-018 test is an important part of Enterasys certifications. We have the resources to prepare you for this. The 2B0-018 exam is essential and core part of Enterasys certifications and once you clear the exam you will be able to solve the real life problems yourself. Want to take advantage of the Real 2B0-018 Test and save time and money while developing your skills to pass your Enterasys 2B0-018 Exam? Let us help you climb that ladder of success and pass your 2B0-018 now!

# **DEMO EXAM**

For Full Version visit

<http://www.ipass4sure.com/allexams.asp>

**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?



## Pass4sure Certification Exam Features;

- Pass4sure offers over **2500** Certification exams for professionals.
- More than **98,800** Satisfied Customers Worldwide.
- Average **99.8%** Success Rate.
- Over **120** Global Certification Vendors Covered.
- Services of **Professional & Certified Experts** available via support.
- Free **90 days** updates to match real exam scenarios.
- **Instant Download Access!** No Setup required.
- Price as low as **\$19**, which is 80% more **cost effective** than others.
- **Verified answers** researched by industry experts.
- Study Material **updated** on regular basis.
- Questions / Answers are downloadable in **PDF** format.
- Mobile Device Supported (**Android, iPhone, iPod, iPad**)
- **No authorization** code required to open exam.
- **Portable** anywhere.
- **Guaranteed Success.**
- **Fast**, helpful support **24x7**.



View list of All certification exams offered;  
<http://www.ipass4sure.com/all exams.asp>

View list of All Study Guides (SG);  
<http://www.ipass4sure.com/study-guides.asp>

View list of All Audio Exams (AE);  
<http://www.ipass4sure.com/audio-exams.asp>

Download Any Certification Exam DEMO.  
<http://www.ipass4sure.com/samples.asp>

To purchase Full version of exam click below;  
<http://www.ipass4sure.com/all exams.asp>

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	

and many others.. See complete list [Here](#)

