

Exam : **2B0-018**

Title : **ES Dragon IDS**

Version : **DEMO**

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

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

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

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

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

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

A. Monitors output to a hosts system and audit logs

B. Monitors a hosts files via MD5 integrity-checking

C. Monitors a hosts specified network interface promiscuously for anomalous activity

D. Monitors a hosts specific file attributes for changes to owner, group, permissions and file size

E. Monitors a Windows hosts Registry for attributes that should not be accessed and/or modified

Answer: C

7. What is the method that Dragon uses to secure the communication between the remote management host and Dragon Policy Manager?

A. SSH

B. SSL

C. IPSec

D. MD5

Answer: B

8. What is the primary and default source of event data for Dragon RealTime Console?

A. dragon.log.xxx

B. dragon.db

C. Ring Buffer

D. Dragon Workbench

Answer: C

9. For what purpose can Dragon Workbench be used?

- A. Read data from TCPDUMP trace/capture file and write to dragon.db for later analysis
- B. Read data from dragon.db file and write to a TCPDUMP trace/capture file for later analysis
- C. Read data from RealTime Console and write to a TCPDUMP trace/capture file for later analysis
- D. This functionality is ONLY available on Dragon Appliances

Answer: A

10. What is one benefit of Dragon Network Sensors dual network interface capability as deployed on a non-Dragon Appliance system?

- A. Secure management and reporting on one interface; Network Sensor invisible on other interface
- B. Allows for collection of event data from both interfaces simultaneously
- C. Allows for protocol detection from one interface, and anomaly detection from the other interface
- D. This functionality is ONLY available on Dragon Appliances

Answer: A

www.Pass4itSure.com

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.

www.Pass4itSure.com

Trying our product !

- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.	 Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.	 Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.
---	---	--

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © 2004-2014, All Rights Reserved.

Get Latest & Actual IT Exam Dumps with VCE and PDF from Pass4itSure.
<https://www.Pass4itSure.com>