Exam Code: 2B0-018

Exam Name: ES Dragon IDS

Vendor: Enterasys Networks

Version: DEMO

Part: A

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)
Correct Answers: 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
Correct Answers: 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
Correct Answers: 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
Correct Answers: 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
Correct Answers: 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
Correct Answers: 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
Correct Answers: 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
Correct Answers: 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
Correct Answers: 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
Correct Answers: A

11: Which component of Dragon is most responsible for enabling hierarchical deployments?
A.Dragon Network Sensor
B.Dragon Security Information Manager
C.Dragon Event Flow Processor
D.Dragon Hierarchy Agent
Correct Answers: C

12: What might be one benefit of configuring a Dragon Host Sensor Server?
A.To provide IKE-level security for Host Sensors deployed in a corporate DMZ

B.To centrally collect NIDS-event data from Network Sensors
C.To collect HIDS-event data from systems on which it is not possible or practical to deploy a Dragon Host Sensor
Correct Answers: C

13: How many Dragon Policy Managers can simultaneously manage a single Dragon Network/Host Sensor?
A.1
B.2
C.10
D.Unlimited
Correct Answers: A

14: Why might an IDS administrator configure Dragon Enterprise Management Server to INITIATE outbound connections to remote Network/Host Sensors?
A.To increase performance when traversing a corporate DMZ
B.To provide the additional security that is inherent in the Server-initiated communication
C.Dragon only allows server-initiated (outbound) connections
D.To integrate Dragon into MSSP or other environments where firewalls prohibit inbound connections from Network/Host Sensors
Correct Answers: D

15: Which of the following best describes the relationship between policies and signatures on a Dragon Host Sensor?
A.Policies can contain O/S-specific signatures
B.Signatures can contain O/S-specific policies
C.Policies and signatures are combined in a single library
D.Policies and signatures are unrelated
Correct Answers: A

16: What two modes are available when installing a Dragon Host Sensor?
A.Standalone and Enterprise
B.Local and Remote
C.Active and Standby
Correct Answers: A

17: What is the recommended method to start all installed Dragon components in Enterprise mode?
A../dragon enterprise
B../driders enterprise
C../dragonctl start
D../dragonctl enterprise
Correct Answers: C

18: Which of the following is NOT a recommended means for a Dragon Network Sensor to collect event data over multiple switched links?
A.Port Redirection
B.Network Tap(s)
C.Port Trunking
D.Strategic deployment of multiple Dragon Network Sensors
Correct Answers: C

19: Which of the following is required in order for the Dragon installation script (install.pl) to be completed?
A.Dragon license key
B.Pre-configured user and group named dragon
C.Active link to the internet
Correct Answers: B

20: What is one method of de-activating a Dragon Policy Manager on a Linux host?
A../dragonctl kill PolicyManager
B../dragonctl kill policy-manager
C../dragonctl stop PolicyManager
D../dragonctl stop policy-manager
Correct Answers: C