Exam Code: 2B0-023

Exam Name: ES Advanced Dragon IDS

Vendor: Enterasys Networks

Version: DEMO

Part: A

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)
Correct Answers: C

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
Correct Answers: A B

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
Correct Answers: B C

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
Correct Answers: D

5: Which of the following is NOT a recommended means of vulnerability response using Dragon?
A.Use the Dragon NMAP PERL scripts to tune the dragon.net file
B.Deploy Dragon Deceptive Services (Honeypot)
C.Deploy Dragon Vulnerability Correlation Tool
D.Enable SSL and AES on the Network Sensor to DPM communication channel
E.Correlate Dragon forensics reports with vulnerability scanner output, and create new signatures as necessary
Correct Answers: D

6: Which of the following best describes the function of CVE?

A.A database of known attacks that can be loaded into an IDS or similar system
B.A database of numerically cross-referenced IDS events that can help any IDS to correlate detected attacks
C.A dictionary of standardized names for vulnerabilities and other information security exposures
D.All of the above
Correct Answers: C

7: Which of the following is NOT a function of a network vulnerability scanner?
A.Monitors health of software applications
B.Output is critical in helping an IDS administrator know the state of the network
C.Catalogs vulnerabilities
D.Shuts down vulnerable TCP/UPD ports to prevent intrusion
Correct Answers: D

8: Which of the following CONSUME event data from the Dragon Ring Buffer?
A.Alarmtool agent
B.Replication agent
C.Connection Manager
D.Consumer Agent
Correct Answers: A B

9: Which of the following best describes the Host Sensor Event Detection Engine (EDE)?
A.Scrutinizes events, either altering the contents of the event or discarding it
B.Generates alerts or guarantees delivery of events to destinations
C.Analyzes events and produces categorized event forensics reports
D.Detects an event and forwards it to the Host Sensor framework for processing
Correct Answers: D

10: Which of the following best describe some scalability features of the Dragon Event Flow Processor (EFP)?
A.Consolidates events from multiple Dragon Policy Managers into one stream
B.Aggregated events from an EFP can be forwarded to other EFPs in a hierarchy
C.An EFP cannot simultaneously support Dragon Realtime Console, Forensics Console and Alarmtool
D.EFPs can be secured by a firewall and configured to initiate Sensor connections from inside the firewall
Correct Answers: B D

11: In which Host Sensor module can a "wrapped module" be used?
A.Event Detection Engine (EDE)
B.Event Filter Engine (EFE)
C.Event Alerting Engine (EAE)
D.All of the above
E.A and C only

Correct Answers: D

12: In which Host Sensor configuration file are custom (wrapped or native) modules defined?
A.dragon.net
B.dragon.cfg
C.dsquire.net
D.dsquire.cfg
Correct Answers: D

13: Which of the following best describes the Host Sensor Event Filter Engine (EFE)?
A.Scrutinizes events, either altering the contents of the event or discarding it
B.Generates alerts or guarantees delivery of events to destinations
C.Analyzes events and produces categorized event forensics reports
D.Detects an event and forwards it to the Host Sensor framework for processing
Correct Answers: A

14: What is a Host Sensor "Virtual Sensor", and in what module is it activated?
A.Saves system memory by deploying a "thin client" Host Sensor that reports to a fully-functioning remote Host Sensor; activated in EDE module
B.Consolidates events from multiple event sources by assigning a virtual name to an event based on its source IP; activated in the EFE module
C.Detects virtual events that are technically not harmful but should be logged anyway; activated in the EAE module
D.Deters attacks in background mode (virtually) that the Host Sensor EDE detects; activated in Alarmtool
Correct Answers: B

15: What term best describes the process of deploying a local EFP that only processes IDS events from the Network and Host Sensors directly attached to it?
A.Local Flow Processing (LFP)
B.IDS Data Partitioning
C.Strict Event Flow
D.Flexible Event Flow
Correct Answers: B

16: In the Host Sensor Event Alerting Engine (EAE), what is the function of Hexadecimal Screen Dump?
A.Redirects screen display (stdout) to a dragon.db file
B.For troubleshooting on UNIX platforms, allows Host Sensor to display events to the screen as they occur
C.In the event of a system compromise, copies (dumps) the attackers screen output to a log file for later analysis
D.In the event of a system compromise, initializes TCPDUMP on the Host Sensor terminal screen
Correct Answers: B

17: Given a scenario where you have created and deployed a Host Sensor policy for monitoring a specific Windows file for attribute changes (increased, truncated, etc.), what is the result if you try to delete this file while it is being monitored by Host Sensor?
A.The file will be deleted, and Host Sensor will log an event
B.The file will be deleted, and the operating system will experience a buffer overflow when Host Sensor next attempts to monitor this file
C.The file will not be deleted because Windows will report the file as being used by another person or program
D.Host Sensor will interrupt the file deletion request, log an attack, and send an Active Response to prevent further deletion attempts
Correct Answers: C

18: Which of the following best describes the generally recommended method for writing Dragon Network Sensor signatures?
A.Narrow the focus of the signature as much as possible, compare normal usage to abnormal usage, and create alerts for the abnormal usage
B.Detect an attack, scan the network for vulnerabilities, create appropriate signatures
C.Monitor network traffic with a sniffer, import sniffer filters into Dragon, and convert them into the appropriate Dragon signatures
D.Export your corporate security policy in ASCII format and import this file into the Dragon Host Sensor policy library signature conversion utility
Correct Answers: A

19: In what Dragon configuration file could you create additional Network Sensor event groups?
A.dragon.net
B.dragon.sigs
C.dragon.cfg
D.dragon.conf
E.driders.cfg
Correct Answers: D

20: Which Host Sensor definition file specifies file resources that are to be monitored?
A.dsquire.net
B.dsquire.sigs
C.dsquire.pollib
D.dsquire.cfg
Correct Answers: A