



Exam Code: 2B0-101

Exam Name: ESSE Recertification

Vendor: Enterasys Networks

Version: DEMO

Part: A

1: The attack category is for events that

- A. Attempt to discover weaknesses
- B. Map the structure of the network
- C. Have the potential to compromise the integrity of an end system.
- D. Deny access to resources

Correct Answers: C

2: Virtual Sensors can segregate traffic by?

- A. IP Address, VLAN, Port
- B. IP Address, VLAN, Port, Protocol
- C. IP Address, VLAN, Port, Protocol, Application
- D. IP Address, VLAN, Port, Application

Correct Answers: B

3: In an Event Flow Processor (EFP) a consumer can be?

- A. A Sensor or an Event Channel
- B. An Event channel only
- C. An Event channel or an Agent
- D. An Agent only

Correct Answers: C

4: Before the host Sensor can be deployed

- A. It must be associated with a virtual sensor
- B. It must be associated with a host policy
- C. Its key must be added to the /usr/dragon/bin directory
- D. Its address must be added to /etc/hosts

Correct Answers: B

5: Which of the following Dragon Agents is used for detecting changes to host files?

- A. Real Time Console
- B. MD5 Sum
- C. Alarm Tool
- D. Database

Correct Answers: B

6: In a standalone deployment the system will have?

- A. A net-config-client.xml file
- B. A net-config-server.xml file
- C. A net-config-server.xml and a net-config-client.xml file
- D. A net-config-server.xml, a net-config-client.xml and a net-config-reports.xml file

Correct Answers: C

7: MD5 checksums are

- A. Stored in a protected directory on the host
- B. Appended to the protected file
- C. Passed up the event channel to the MD5 Agent
- D. Stored in the /usr/dragon/bin directory on the Enterprise Management Server (EMS)

Correct Answers: C

8: Which of the following best describes the commit operation?

- A. It uses the configuration channel to push a configuration to a device
- B. It uses the event channel to push a configuration to a device
- C. It writes a configuration change to the Enterprise Management Server (EMS) database
- D. It writes a configuration change to the management clients database

Correct Answers: C

9: Which of the following Dragon Agents sends notifications when the sensors detect an event that match a rule?

- A. Real Time Console
- B. MD5 Sum
- C. Alarm Tool
- D. Database

Correct Answers: C

10: Signature OS

- A. Applies signature to network traffic originating from the specified OS
- B. Is used for writing Host signatures
- C. Is optional on Network signatures
- D. Is required on all signatures

Correct Answers: B

11: Dragonctl is used to?

- A. Start, stop and monitor the dragon processes on the remote node
- B. Write log files
- C. Monitor the Ring Buffer
- D. Maintain configuration channel connections

Correct Answers: A

12: Virtual sensor names?

- A. Are included in events they generate
- B. Must match the sensor key
- C. Must include the device name
- D. Require separate keys

Correct Answers: A

13: Agents can be deployed?

- A. Only on non-forwarding Event Flow Processor (EFPs)
- B. Only on forwarding Event Flow Processor (EFPs)
- C. Only on the Enterprise Management Server (EMS) station
- D. On any Event Flow Processor (EFP)

Correct Answers: D

14: The host policy MD5 detection module

- A. Detects any changes in the contents of protected file
- B. Detects file size increases
- C. Detects file truncations
- D. Detects ownership changes

Correct Answers: A

15: Traffic direction refers to traffic flows in relation to the

- A. Server
- B. Protected network
- C. Client
- D. DMZ

Correct Answers: B

16: The master Alarm Tool Default policy

- A. Is write locked
- B. Is writable
- C. Cannot be copied
- D. Cannot be associated with an Agent

Correct Answers: A

17: Which alarm type is best described as: collects information for x period of time, then send event notifications

- A. Real Time
- B. Summary
- C. Dynamic
- D. Interval

Correct Answers: B

18: Agent status will show as Not Available until?

- A. The agent is committed
- B. The agent is deployed
- C. The agent is selected
- D. The remote node is deployed

Correct Answers: B

19: Agents can be deployed on?

- A. Only the Enterprise Management Server (EMS)

- B.Any managed node with a networked sensor deployed
- C.Any managed node with host sensor deployed
- D.Any managed node

Correct Answers: D

20: If a packet matched the rules for two virtual sensors it will be evaluated by?

- A.Both sensors
- B.The first sensor it matches
- C.The default sensor
- D.Overlapping rules are not permitted

Correct Answers: B