Exam Code: 250-501
Intrusion Protection Solutions

Demo Version

To Access Full Version, Please go to
www.itexamworld.com

1. Which three organizations actively monitor the release of patches and upgrades from vendors? (Choose three.)
A. CERT
B. Microsoft
C. Symantec
D. Security Focus
E. Sun Microsystems
Answer: ACD

2. Which two types of policies are supported by Symantec Host IDS? (Choose two.)
A. basic
B. stock
C. default
D. custom
Answer: BD

3. Which communications method does the Symantec Enterprise Security Architecture Manager use to communicate with the Symantec Enterprise Security Architecture DataStore?
A. JDBC
B. ODBC
C. LDAPS
D. HTTPS
Answer: A

4. What does a Symantec ManHunt watchdog group provide?
A. sniffer detection
B. node redundancy
C. sensor aggregation
D. third-party event aggregation
Answer: B

5. What are three characteristics of Symantec ManHunt's response module? (Choose three.)
A. is priority-based
B. initiates traffic record
C. acts on classes of attacks
D. analyzes aggregated events
Answer: ABC

6. Which two benefits does Symantec Decoy Server provide? (Choose two.)
A. zero day attack detection
B. real-time network sniffing
C. early warning intrusion sensors
D. improved host-based intrusion performance
Answer: AC

7. Which two statements are true about intrusion protection? (Choose two.)
A. Intrusion protection devices only act as a perimeter defense against known attack patterns.
B. Intrusion protection technology must be combined with vulnerability assessment tools.
C. Intrusion protection solutions must include services that actively block malicious processes.
D. Intrusion protection can consist of any combination of host-based and network-based intrusion sensors.
Answer: CD

8. Which two technologies act as intrusion protection sensors? (Choose two.)
A. routers
B. host agents
C. deception hosts
D. managed switches
Answer: BC

9. Which two conditions affect the performance of network-based intrusion detection systems? (Choose two.)

A. local area network traffic congestion
B. resource utilization on sensor nodes
C. presence of a host-based intrusion detection system
D. concurrent support for intrusion detection across multiple platforms
Answer: AB

10. Which method is used by host-based intrusion protection systems to monitor file tampering and integrity?
A. file locking
B. disk encryption
C. checksum lists
D. operating system permissions
Answer: C

11. Which condition affects the performance of host-based intrusion detection system?
A. fragmented network traffic
B. resource utilization on monitored nodes
C. presence of a network-based intrusion detection system
D. concurrent support for intrusion detection across multiple platforms
Answer: B

12. What is a characteristic unique to a host-based intrusion protection solution?
A. service specific
B. protocol specific
C. topology specific
D. operating system specific
Answer: D

13. To which mode must you set the network interface on a network intrusion detection sensor to collect all packets?
A. report
B. receive
C. transfer
D. promiscuous
Answer: D

14. Which type of file provides vital information to a host-based intrusion detection system?
A. log
B. system
C. initialization
D. configuration
Answer: A

15. Which three types of traffic patterns do anomaly-based sensors report? (Choose three.)
A. allowed
B. overflow C.
suspicious D.
not allowed
Answer: BCD

16. Which three types of analyzers do anomaly-based sensors use? (Choose three.) A.
file
B. trend
C. packet
D. statistical
Answer: BCD

17. Which type of attacks are anomaly-based intrusion detection systems primarily designed to detect? A.
novel
B. known
C. host-based

D. network-based
Answer: A

18. Which type of intrusion detection solution is most likely to require regular updates to remain effective?
A. host-based
B. network-based
C. anomaly-based
D. signature-based
Answer: D

19. Which type of device is associated with passive intrusion detection strategies?
A. firewall
B. packet filter
C. network sniffer
D. management console
Answer: C

20. Which two states are monitored by statistical anomaly filters to detect changes in network activity? (Choose two.)
A. protocol traffic rates
B. changes in file sizes
C. user account misuse
D. users' activity over the network
Answer: AD