Exam Code: 250-501

Exam Name: intrusion protection solutions

Vendor: Symantec

Version: DEMO

Part: A

1: 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
Correct Answers: D

2: Which three types of network traffic should be considered suspicious by a deception-based intrusion system running on your corporate Intranet? (Choose three.)
A.FTP connection
B.broadcast traffic
C.HTTP get request
D.SSL logon attempt
Correct Answers: A C D

3: 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
Correct Answers: A C D

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

5: Which type of attacks are anomaly-based intrusion detection systems primarily designed to detect?
A.novel
B.known
C.host-based
D.network-based
Correct Answers: A

6: 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
Correct Answers: D

7: 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
Correct Answers: A D

8: What is a possible risk of operating a decoy-based intrusion detection system on your network?
A.Attackers could use the decoy to compromise another system making you liable.
B.Attackers learn how to circumvent your perimeter defense through the decoy.
C.The decoy reduces network performance by generating broadcast traffic on the network.
D.The decoy may give away information about your network and other legitimate systems
Correct Answers: A

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

10: Which activity compromises the integrity of forensic data collected during an incident response investigation of HostA?
A.modification of firewall settings to collect additional forensic data
B.modification of the system files on HostA to block further intrusions
C.modification of the network intrusion detection system's signature files
D.modification of the intrusion policy at HostA's IPS sensor to block further intrusions
Correct Answers: B

11: 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
Correct Answers: A B

12: Which Symantec Security Management System view displays Symantec Host IDS events?

A.Symantec Host IDS Events folder, Intrusion Detection Events view
B.Symantec Host IDS Events folder, Intrusion Detection Attack view
C.Intrusion Detection Family folder, Symantec Host IDS Events view
D.Intrusion Detection Reports folder, Symantec Host IDS Attack view
Correct Answers: C

13: Which two methods might you use to create custom policies? (Choose two.)
A.build from scratch
B.use the policy template
C.import system registry settings
D.export and modify a stock policy
Correct Answers: A D

14: Which service facilitates the automatic update of Symantec Host IDS stock policies?
A.Symantec LiveUpdate
B.Symantec PolicyEditor
C.Symantec PolicyUpdate
D.Symantec Host IDSUpdate
Correct Answers: A

15: Which statement is true regarding Symantec Host IDS policy behavior?
A.Policies are collected from Symantec Host IDS Agent computers.
B.Policies are distributed to all Symantec Host IDS Agent computers.
C.Policies are based on application settings on all computers running Symantec Host IDS.
D.Policies are monitored on all computers running Symantec Host IDS Manager services.
Correct Answers: B

16: Where are Symantec Host IDS events recorded?
A.the DataStore
B.the Directory
C.the Local Agent log
D.the Symantec Host IDS Manager
Correct Answers: A

17: Click the Exhibit button. What is the minimum number of Symantec Security Management System Console computers required to monitor the Boston office locally, while managing the entire Symantec Host IDS deployment from New York?
A.1
B.2
C.4
D.15
Correct Answers: B

18: Which solution provides a robust management and reporting framework for Symantec Host

IDS?
A.Symantec Security Management System
B.Symantec Host IDS Manager and Agent Tools
C.Symantec Intrusion Protection Enterprise Manager
D.Symantec Enterprise Security Management Console
Correct Answers: A

19: Which service is required to deploy a Symantec Enterprise Security Architecture Manager?
A.IBM HTTP Server
B.iPlanet Web Server
C.Netscape Web Server
D.Internet Information Server
Correct Answers: A

20: Which two types of policies are supported by Symantec Host IDS? (Choose two.)
A.stock
B.update
C.custom
D.best practice
Correct Answers: A C