Exam Code: 250-503

Exam Name: security management solutions

Vendor: Symantec

Version: DEMO

Part: A

1: Which Symantec Enterprise Security Manager (Symantec ESM) report lists the security checks in each module?
A.Policy
B.Domain
C.Security
D.Executive
Correct Answers: A

2: Which two network requirements must be met for communications across a WAN connection to successfully occur between Symantec Enterprise Security Manager (Symantec ESM) Manager running on host GS101 and Symantec ESM Agent running on host GS102? (Choose two.)
A.Hostnames must be resolvable.
B.Appropriate ports must be open.
C.Authentication server must be available.
D.Components must belong to the same Symantec ESM domain.
Correct Answers: A B

3: Which two does Symantec Enterprise Security Manager (Symantec ESM) have Best Practice Policies for? (Choose two.)
A.WU FTP Server
B.Oracle Database
C.MySQL Database
D.Checkpoint Firewall
Correct Answers: B D

4: A mission critical application must use the Windows 2000 guest account for management functions. Your organization's security policy states that the guest account should not be used for any reason. Which option should you use to temporarily prevent Symantec Enterprise Security Manager (Symantec ESM) from reporting the guest account as an exception while the application is reengineered to use another Windows 2000 user account?
A.rules
B.filters
C.exclusions
D.suppressions
Correct Answers: D

5: Which three operating systems are supported by the Symantec Enterprise Security Manager (Symantec ESM) Agent? (Choose three.)
A.HP-UX
B.OS/390
C.MacOS X
D.BSD UNIX

E.Windows 98
F.Red Hat Linux 7.x
G.Windows 2003 Server
Correct Answers: A F G

6: Which organization defines the Symantec Enterprise Security Manager (Symantec ESM) Best Practice Policies?
A.SANS Institute
B.The MITRE Corporation
C.CERT Coordination Center
D.Symantec Security Response
Correct Answers: D

7: What is one benefit of using Symantec Enterprise Security Manager (Symantec ESM)?
A.holistic risk mitigation
B.holistic security event correlation
C.automated and scheduled network assessments
D.automated security policy compliance management
Correct Answers: D

8: When new security updates are available when are the new modules transferred from the Symantec Enterprise Security Manager (Symantec ESM) Manager to the updatable participating Symantec Enterprise Security Manager (Symantec ESM) Agents?
A.during the next policy run
B.during an Agent synchronization
C.the next time the Manager restarts
D.when the Agents poll the Manager for configuration changes
Correct Answers: A

9: Which two are groupings of security checks in Symantec Enterprise Security Manager (Symantec ESM)? (Choose two.)
A.file systems and directories
B.process blocking and integrity
C.user accounts and authorization
D.system and domain administration
Correct Answers: A C

10: Which file does Symantec Enterprise Security Manager (Symantec ESM) initialize during the first run of a security module to identify computer changes?
A.Template
B.Snapshot
C.MasterPolicy
D.Suppressions
Correct Answers: B

11: Which module is included in the Symantec Enterprise Security Manager (Symantec ESM) base level Best Practice Policies?
A.File Watch
B.File Access
C.Backup Integrity
D.Password Strength
Correct Answers: D

12: Which statement describes the recommendations made in the ISO 17799?
A.It is technology neutral.
B.It secures Solaris computers.
C.It is designed for the health industry.
D.It reduces risk to bulk electric systems.
Correct Answers: A

13: What is a benefit of Symantec Enterprise Security Manager (Symantec ESM)?
A.Summary policy run results are stored in a relational database.
B.Symantec ESM Agents run at low priority to minimize resource consumption.
C.Symantec Host IDS port scan data can be incorporated into Symantec ESM policy runs.
D.Symantec Vulnerability Assessment audit data can be incorporated into Symantec ESM reports.
Correct Answers: B

14: Where are Symantec Enterprise Security Manager (Symantec ESM) reports stored?
A.Symantec ESM CIF computer
B.Symantec ESM Agent computer
C.Symantec ESM Console computer
D.Symantec ESM Manager computer
Correct Answers: C

15: Which Symantec Enterprise Security Manager (Symantec ESM) component is the CIF server a part of?
A.Agent
B.Bridge
C.Console
D.Manager
Correct Answers: D

16: Which two operating systems support a Symantec Enterprise Security Manager (Symantec ESM) Manager? (Choose two.)
A.AIX
B.OS/400
C.Windows 98
D.Red Hat Linux

E.Windows 2003
Correct Answers: A E

17: Which component is used to gather Symantec Enterprise Security Manager (Symantec ESM) data to Symantec Enterprise Security Architecture (SESA)?
A.relay
B.bridge
C.converter
D.forwarder
Correct Answers: B

18: Which three are true about Symantec Enterprise Security Manager (Symantec ESM) template files? (Choose three.)
A.They are suppressible.
B.They can be created from scratch.
C.They contain definitions of objects and their expected states.
D.They provide computer-specific information about properties of files.
Correct Answers: B C D

19: Which two components make up the Symantec Enterprise Security Manager (Symantec ESM) SANS/FBI Top 20 Best Practice Policy? (Choose two.)
A.checks
B.templates
C.snapshots
D.suppressions
Correct Answers: A B

20: Which security-related task can Symantec Enterprise Security Manager (Symantec ESM) be used for?
A.risk profile determination
B.notifies you of a system attack
C.assessing policy compliance on servers
D.consolidating management of all Symantec security products
Correct Answers: C