Exam Number/Code: C2150-561

Exam Name: IBM Security Network Intrusion Prevention System V4.3 Implementation

Version: Demo

QUESTION: 1

Where is the provinfo file stored?

A. /var/cache
B. /var/support/
C. root directory
D. admin directory

Answer: B

QUESTION: 2

How is a firewall rule configured to block remote desktop (RDP) access for all interfaces and all Virtual Local Area Networks?

A. protocol=TCP, source port exclude RDP
B. action=ignore,select Interfaces, protocol=TCP, port=3389
C. keep all default settings but change the target port to 3389
D. action=drop, protocol=UDP, target port uncheck any and enter 3389

Answer: C

QUESTION: 3

Which interface mode is required in order for quarantine response rules to work?

A. Bypass Mode
B. Inline Protection Mode
C. Inline Simulation Mode
D. Passive Monitoring Mode

Answer: B

QUESTION: 4

Where would a user be added to allow a remote user to access the IBM Security Network Intrusion Prevention System V4.3 Local Management Interface?

A. the Remote Access policy in IBM Security SiteProtector System (SiteProtector)
B. the User Management utility in SiteProtector
C. the Accounts and Passwords page in the Web interface
D. the Password Management menu in the SSH Configuration menu

Answer: C

QUESTION: 5

What are two restrictions placed on remote users using IBM Security Network Intrusion Prevention System V4.3? (Choose two.)

A. They cannot reboot the appliance.
B. They cannotlog in to the local console.
C. They cannot change the local user account passwords.
D. They cannot save changes to policies in the Web interface.
E. They cannot log in to the appliance when the authentication server is down.

Answer: C,E

QUESTION: 6

Which file is accessed on the IBM Security Network Intrusion Prevention System V4.3 appliance to determine why it is Active with Errors in IBM Security SiteProtector System?

A. Boot log file
B. Kernel log file
C. Engine0 log file
D. Messages log file

Answer: D

QUESTION: 7

Which area of the IBM Protocol Analysis Module technology prevents Skype from using enterprise network bandwidth?

A. Data Security

B. Application Control
C. Threat Detection and Prevention
D. Client-side ApplicationProtection

Answer: B

QUESTION: 8

Where in the IBM Security SiteProtector System Console can a customer find the link status of the Security Interfaces on an IBM Security Network Intrusion Prevention System appliance?

A. the networkinfo sectionunder Module Status in the appliance Properties screen
B. the Intrusion Prevention section under Module Status in the appliance Properties screen
C. the Security Interfaces section on the Health Summary Network tab in the appliance Properties screen
D. the Internal Communication section on the Health Summary System tab in the appliance Properties screen

Answer: A

QUESTION: 9

A customer wants to change the severity of an IBM Protocol Analysis Module signature from high to low in a given protection domain. Which policy meets this requirement?

A. Security Events
B. Open Signatures
C. System Updates
D. X-Force Virtual Patch

Answer: A

QUESTION: 10

Where in the Local Management Interface is the location of the date and time of the last backupof an IBM Security Network Intrusion Prevention System V4.3 viewable?

A. Evidence log
B. Message log
C. System Dashboard
D. Security Dashboard

Answer: C