

The best learning assistants

Exam : **Cisco 642-513**

Title : Securing Hosts Using Cisco
Security

Update : Demo



1. For which layers of the OSI reference model does CSA enforce security?

- A. Layer 1 through Layer 4
- B. Layer 1 through Layer 7
- C. Layer 2 through Layer 4
- D. Layer 3 through Layer 7

Answer:D

2. Cisco Security Agent provides Day Zero attack prevention by using which of these methods?

- A. using signatures to enforce security policies
- B. using API control to enforce security policies
- C. using stateful packet filtering to enforce security policies
- D. using algorithms that compare application calls for system resources to the security policies

Answer:D

3. Which one of the five phases of an attack attempts to become resident on a target?

- A. probe phase
- B. penetrate phase
- C. persist phase
- D. propagate phase
- E. paralyze phase

Answer:C

4. Which two attacks could an attacker use during the probe phase of an attack? (Choose two.)

- A. buffer overflow
- B. install new code
- C. ping scans
- D. erase files
- E. port scans

Answer:CE

5. Which two attacks could an attacker use during the penetrate phase of an attack? (Choose two.)

- A. install new code
- B. modify configuration
- C. ping scans
- D. buffer overflow
- E. erase files
- F. e-mail attachment

Answer:DF

6. Which attack could an attacker use during the propagate phase of an attack?

- A. ping scans
- B. crash systems
- C. attack other targets

- D. erase files
- E. steal data

Answer:C

7. Which three operating systems are supported for deployment of CSA? (Choose three.)
- A. OS2
 - B. HPUX
 - C. Linux
 - D. Solaris
 - E. AIX
 - F. Windows

Answer:CDF

8. Which protocol is required for the administrative workstation to communicate with the CSA MC?
- A. SSH
 - B. Telnet
 - C. SSL
 - D. IPSec

Answer:C

9. Which application loads when installing the CSA MC to run the local database?
- A. Microsoft Access
 - B. Microsoft SQL Server Desktop Engine
 - C. Microsoft SQL Server
 - D. Oracle

Answer:B

10. What application is installed on the server after the CSA MC is installed?
- A. Cisco Trust Agent
 - B. ACS
 - C. SQL
 - D. CSA

Answer:D

11. What are the three CSA MC administrator roles? (Choose three.)
- A. access
 - B. Configure
 - C. deploy
 - D. view
 - E. monitor
 - F. administer

Answer:BCE

12. Which protocol should never be disabled on the CSA MC?

- A. SSH
- B. Telnet
- C. IPSec
- D. SSL

Answer:D

13. Which port is used to access the CSA MC from the administrative workstation?

- A. 21
- B. 23
- C. 1741
- D. 1802

Answer:C

14. Which of these is a reason for using groups to administer Agents?

- A. to link similar devices together
- B. to complete configuration changes on groups instead of hosts
- C. to complete the same configuration on like items
- D. to apply the same policy to hosts with similar security requirements

Answer:D

15. How can the Agent kit be sent out to host machines?

- A. via a URL that is e-mailed to clients
- B. via a TFTP server
- C. via an FTP server
- D. via a Telnet server

Answer:A

16. Which type of privileges must you have on a host system to install CSA?

- A. superuser
- B. administrator
- C. user
- D. viewer

Answer:B

17. Which view within the CSA MC allows users to see a continuously refreshed view of the most recently logged event records?

- A. Event Log
- B. Event Monitor
- C. Event Sets
- D. Event Alerts

Answer:B

18. Which view within the CSA MC allows users to see a view of event records based on filtering criteria

such as time and severity?

- A. Event Summary
- B. Event Log
- C. Event Monitor
- D. Event Sets
- E. Event Alerts

Answer: B

19. Which view within the CSA MC allows users to see overall system status information, including a summary of recorded events, agent configuration, and activity?

- A. Status Summary
- B. Event Log
- C. Event Monitor
- D. Event Sets
- E. Alerts

Answer: A

20. Which definitions can be used to allow consistent configuration of policies across multiple systems and can also be used for event reporting purposes?

- A. hosts
- B. software updates
- C. Agent kits
- D. registration control
- E. groups

Answer: E

21. Which three make up the CSA architecture model? (Choose three.)

- A. Cisco Trust Agent
- B. Cisco Security Agent
- C. Cisco Security Agent Management Center
- D. Cisco Intrusion Prevention System
- E. an administrative workstation
- F. a syslog server

Answer: BCE

22. Which Agent kit should be installed on the CSA MC?

- A. the default Windows Agent kit
- B. the default UNIX Agent kit
- C. the default CSA Agent kit
- D. the Agent kit that is automatically installed

Answer: D

23. What is the purpose of the Audit Trail function?

- A. to generate a report listing events matching certain criteria, sorted by event severity

- B. to generate a report listing events matching certain criteria, sorted by group
- C. to generate a report showing detailed information for selected groups
- D. to display a detailed history of configuration changes

Answer:D

24. Which action do you take when you are ready to deploy your CSA configuration to systems?

- A. select
- B. clone
- C. deploy
- D. generate rules

Answer:D

25. When a rule is cloned, which part of the rule is not cloned?

- A. sets
- B. rule modules
- C. hosts
- D. variables

Answer:D

26. What is the purpose of the Compare tool?

- A. to save data that has been configured
- B. to compare individual rules
- C. to compare individual rule modules
- D. to compare and merge configurations

Answer:D

27. Which three items make up rules? (Choose three.)

- A. variables
- B. applications
- C. application classes
- D. rule modules
- E. policies
- F. actions

Answer:ACF

28. Which two items make up Agent kits? (Choose two.)

- A. groups
- B. hosts
- C. policies
- D. rules
- E. network shim

Answer:AE

29. What action must happen before a system that has CSA can download policies configured for it?

- A. The system must be rebooted.
- B. The system must install Agent kits.
- C. The system must be polled by the CSA MC.
- D. The system must register with the CSA MC.

Answer:D

30. What is a benefit of putting hosts into groups?

- A. There is no need to configure rules.
- B. There is no need to configure rule modules.
- C. The administrator can deploy rules in test mode.
- D. The administrator does not have to deploy rules in test mode.

Answer:C

ExamSavior.com was founded in 2006. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially [Adobe](#), [Apple](#), [Citrix](#), [Comptia](#), [EMC](#), [HP](#), [HuaWei](#), [LPI](#), [Nortel](#), [Oracle](#), [SUN](#), [Vmware](#) and so on. And help you pass any IT Certification exams at the first try.

You can reach us at any of the email addresses listed below.

English Customer:

Sales : sales@examsavior.com

Support: support@examsavior.com

Website: www.examavior.com

