Exam Code: 642-513

Exam Name: Securing Hosts Using Cisco Security Agent Exam (HIPS)

Vendor: CISCO

Version: DEMO

Part: A

1: 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
Correct Answers: D

2: Which three items make up rules? (Choose three.)
A.variables
B.applications
C.application classes
D.rule modules
E.policies
F.actions
Correct Answers: A C F

3: 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
Correct Answers: D

4: 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
Correct Answers: C

5: 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
Correct Answers: D

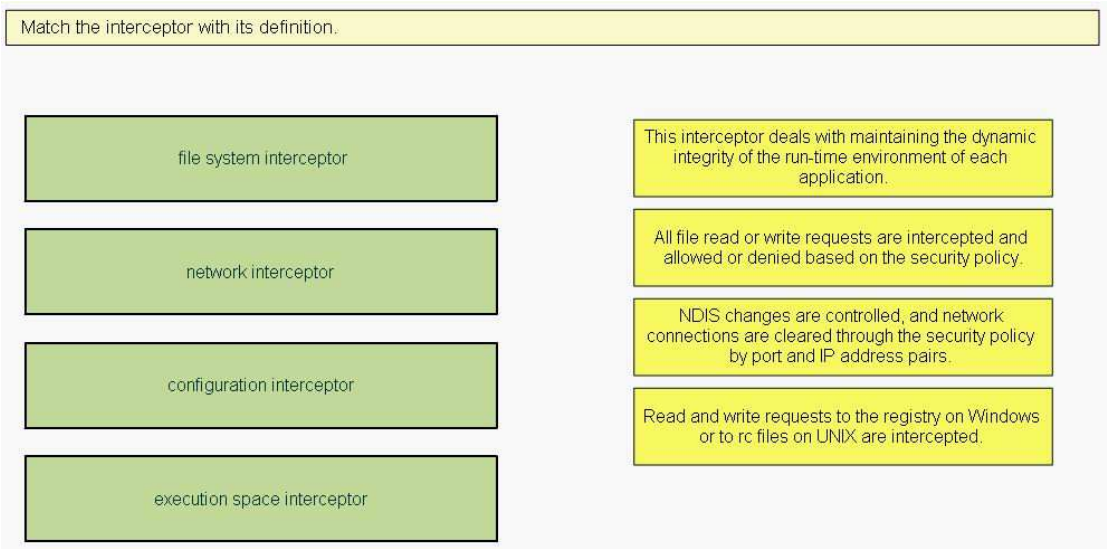
6: In which type of rules are network address sets used?
A.COM component access control rules
B.connection rate limit rules
C.network access control rules

D.file control rules
E.file access control rules
Correct Answers: C

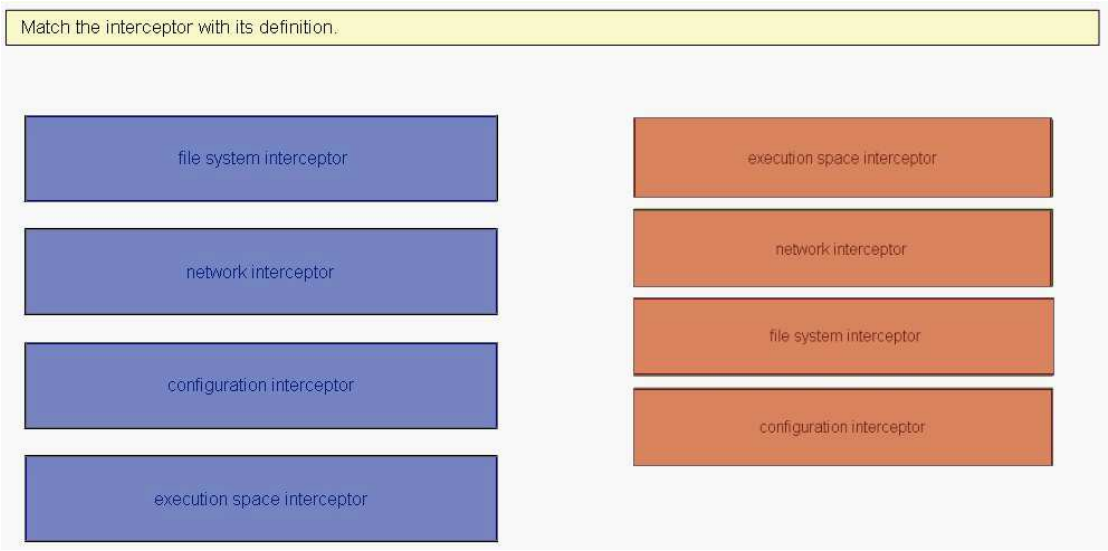
7: Which three of these does the buffer overflow rule detect on a UNIX operating system, based on the type of memory space involved? (Choose three.)
A.location space
B.stack space
C.slot space
D.data space
E.heap space
F.file space
Correct Answers: B D E

8: When should you use preconfigured application classes for application deployment investigation?
A.never
B.always
C.only for specific applications
D.only when applications require detailed analysis
Correct Answers: A

9: Drag Drop question



Correct Answers:



10: Which systems with specific operating systems are automatically placed into mandatory groups containing rules for that operating system? (Choose three.)
A.OS2
B.HPUX
C.Solaris
D.Mac OS
E.Linux
F.Windows
Correct Answers: C E F

11: What is the purpose of network access control rules?
A.to control access to network services
B.to control access to network addresses
C.to control access to both network services and network addresses
D.to control access to networks
Correct Answers: C

12: 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
Correct Answers: D

13: If a Solaris or Windows system is not rebooted after CSA installation, which three rules are only enforced when new files are opened, new processes are invoked, or new socket connections are made? (Choose three.)
A.COM component access rules
B.network shield rules

C.buffer overflow rules
D.network access control rules
E.file access control rules
F.demand memory access rules
Correct Answers: C D E

14: For which operating system is the network shield rule available?
A.OS2
B.Windows
C.Linux
D.Solaris
Correct Answers: D

15: What is the maximum number of characters that a policy name can contain?
A.24
B.32
C.48
D.64
Correct Answers: D