Exam : 642-513

Title : Securing Hosts Using Cisco Security Agent

Ver : 09-25-07

QUESTION 1:

Certkiller chose the Cisco CSA product to protect the network against the newest attacks. 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
E. None of the above

Answer: D

Explanation:
Because Cisco Security Agent analyzes behavior rather than relying on signature matching, it never needs updating to stop a new attack. This zero-update architecture provides protection with reduced operational costs and can identify so-called "Day Zero" threats."
At a high level, Cisco(r) Security Agent is straightforward. It intercepts system calls between applications and the operating system, correlates them, compares the correlated system calls against a set of behavioral rules, and then makes an "allow" or"deny" decision based on the results of its comparison. This process is called INCORE, which stands for intercept, correlate, rules engine.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_white_paper0900aecd8020f448.shtml

QUESTION 2:

Certkiller has implemented the CSA product to provide security for all of their devices. 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

Explanation:
Cisco Security Agent provides threat protection for server and desktop computing systems, also known as endpoints. It helps to reduce operational costs by identifying, preventing, and eliminating known and unknown security threats. The Cisco Security Agent consolidates endpoint security functions in a single agent, providing:

1. Host intrusion prevention
2. Spyware/adware protection
3. Protection against buffer overflow attacks
4. Distributed firewall capabilities
5. Malicious mobile code protection
6. Operating-system integrity assurance
7. Application inventory
8. Audit log-consolidation

This provides security for endpoints at the network layer (layer 3) through the application layer (layer 7).

QUESTION 3:

The CSA architecture model is made up of three major components. Which three are they? (Choose three)

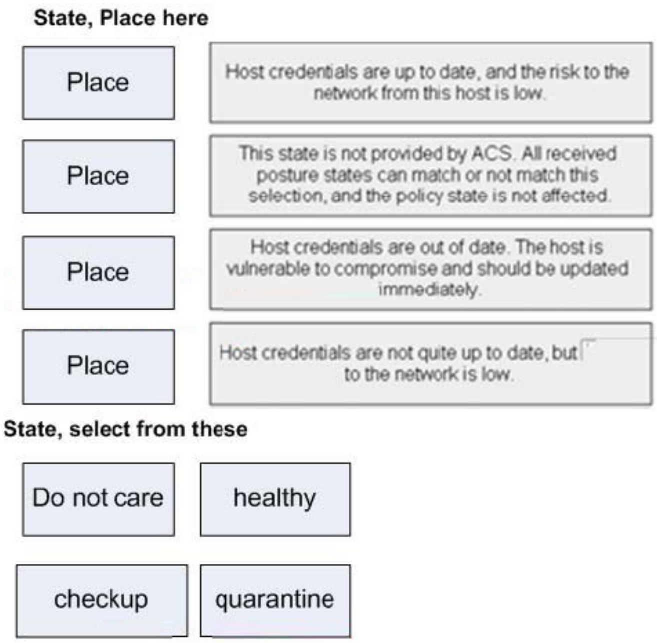
A. Cisco Trust Agent
B. Cisco Security Agent
C. Cisco Security Agent Management Center
D. Cisco Intrusion Prevention System
E. An administrative workstation
F. A syslog server

Answer: B, C, E

Explanation:
The CSA MC architecture model consists of a central management center which maintains a database of policies and system nodes, all of which have Cisco Security Agent software installed on their desktops and servers. The agents themselves, and an administrative workstations, combined with the Management Center, comprise the three aspects of the CSA architecture.
Agents register with CSA MC. CSA MC checks its configuration database for a record of the system. When the system is found and authenticated, CSA MC deploys a configured policy for that particular system or grouping of systems.

QUESTION 4:

DRAG DROP
As a Certkiller trainee you are required to matchthe Cisco Trust Agent posture state with its definition.



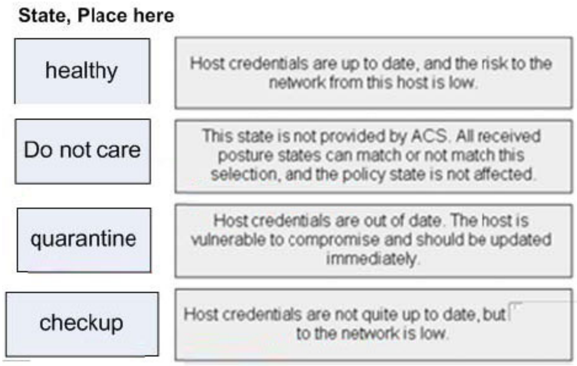
State, Place here

Place	Host credentials are up to date, and the risk to the network from this host is low.
Place	This state is not provided by ACS. All received posture states can match or not match this selection, and the policy state is not affected.
Place	Host credentials are out of date. The host is vulnerable to compromise and should be updated immediately.
Place	Host credentials are not quite up to date, but to the network is low.

State, select from these

Do not care
healthy
checkup
quarantine

Answer:

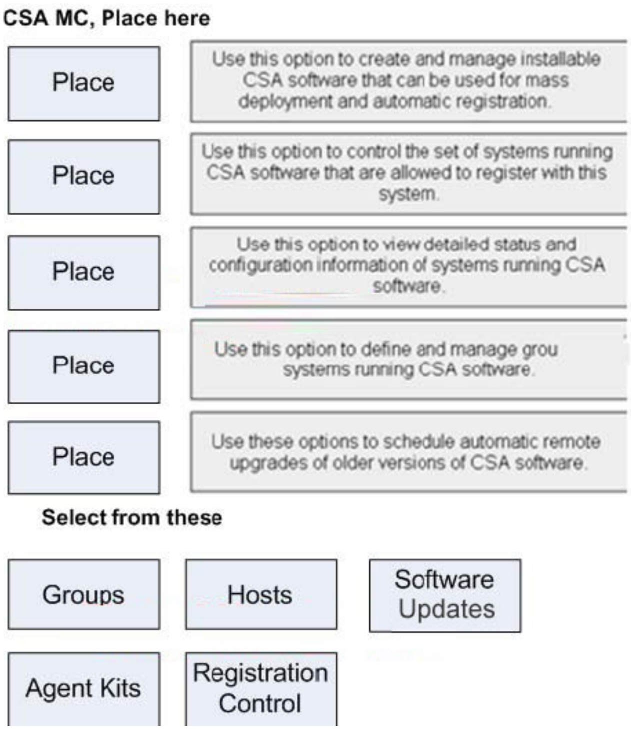


State, Place here

healthy	Host credentials are up to date, and the risk to the network from this host is low.
Do not care	This state is not provided by ACS. All received posture states can match or not match this selection, and the policy state is not affected.
quarantine	Host credentials are out of date. The host is vulnerable to compromise and should be updated immediately.
checkup	Host credentials are not quite up to date, but to the network is low.

QUESTION 5:

DRAG DROP
As a Certkiller student you are required to match the CSA MC view with the corresponding definition.



CSA MC, Place here

Place	Use this option to create and manage installable CSA software that can be used for mass deployment and automatic registration.
Place	Use this option to control the set of systems running CSA software that are allowed to register with this system.
Place	Use this option to view detailed status and configuration information of systems running CSA software.
Place	Use this option to define and manage grou systems running CSA software.
Place	Use these options to schedule automatic remote upgrades of older versions of CSA software.

Select from these

Groups

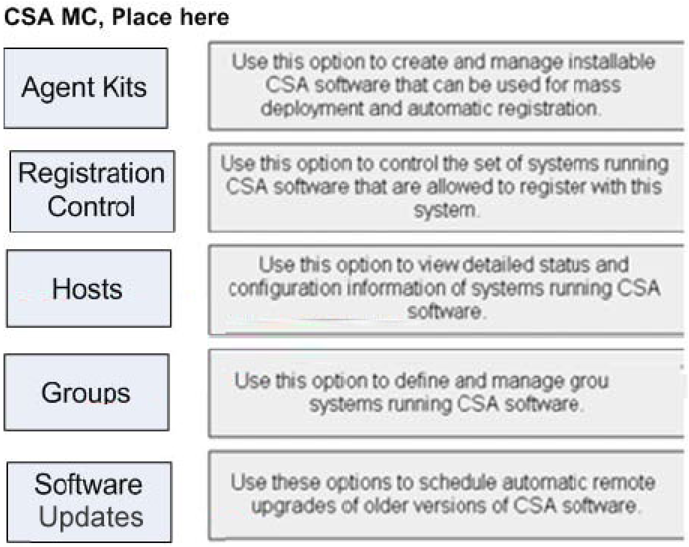
Hosts

Software Updates

Agent Kits

Registration Control

Answer:



CSA MC, Place here

Agent Kits	Use this option to create and manage installable CSA software that can be used for mass deployment and automatic registration.
Registration Control	Use this option to control the set of systems running CSA software that are allowed to register with this system.
Hosts	Use this option to view detailed status and configuration information of systems running CSA software.
Groups	Use this option to define and manage grou systems running CSA software.
Software Updates	Use these options to schedule automatic remote upgrades of older versions of CSA software.

QUESTION 6:

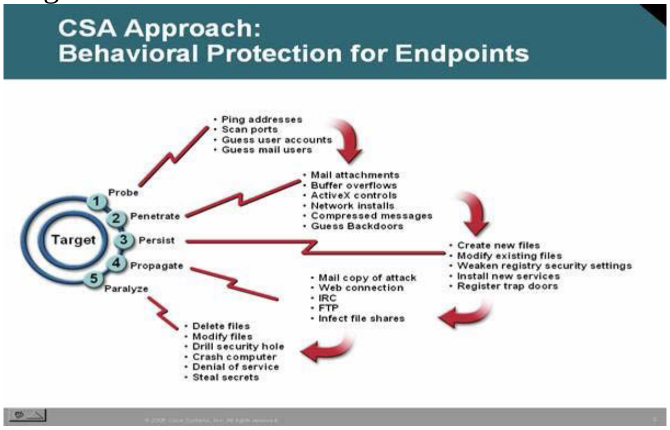
A hacker is attacking the Certkiller network and is currently in the penetration phase. Which two attacks could an attacker use during the penetrate phase of an attack? (Choose two)

A. Install new code

B. Modify configuration
C. Ping scans
D. Buffer overflow
E. Erase files
F. E-mail attachment
G. ICMP Flood

Answer: D, F

Explanation:
Exploit code is transferred to the vulnerable target in the penetrate phase. The goal of this phase is to get the target executing the exploit code through some attack vector like a buffer overflow or email attachment. The life cycle of an attack is shown in the following diagram:



CSA Approach:
Behavioral Protection for Endpoints

- Ping addresses
- Scan ports
- Guess user accounts
- Guess mail users

- Mail attachments
- Buffer overflows
- ActiveX controls
- Network installs
- Compressed messages
- Guess Backdoors

- Create new files
- Modify existing files
- Weaken registry security settings
- Install new services
- Register trap doors

- Mail copy of attack
- Web connection
- IRC
- FTP
- Infect file shares

- Delete files
- Modify files
- Drill security hole
- Crash computer
- Denial of service
- Steal secrets

Reference:
www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae55e.pdf

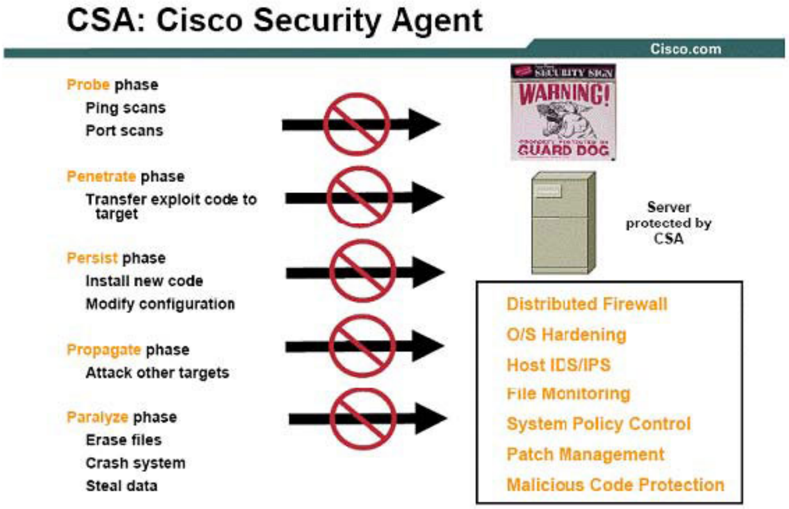
QUESTION 7:

Of the following choices, which 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
F. Penetrate systems
G. All of the above

Answer: C

Explanation:
The different phases of an attack are shown in the diagram below:



CSA: Cisco Security Agent

Cisco.com

Probe phase
Ping scans
Port scans

Penetrate phase
Transfer exploit code to target

Persist phase
Install new code
Modify configuration

Propagate phase
Attack other targets

Paralyze phase
Erase files
Crash system
Steal data

Server protected by CSA

Distributed Firewall
O/S Hardening
Host IDS/IPS
File Monitoring
System Policy Control
Patch Management
Malicious Code Protection

Reference:
http://www.cisco.com/hk/learning/security_day/files/outbreak_prevention_soln_nac_csa.pdf

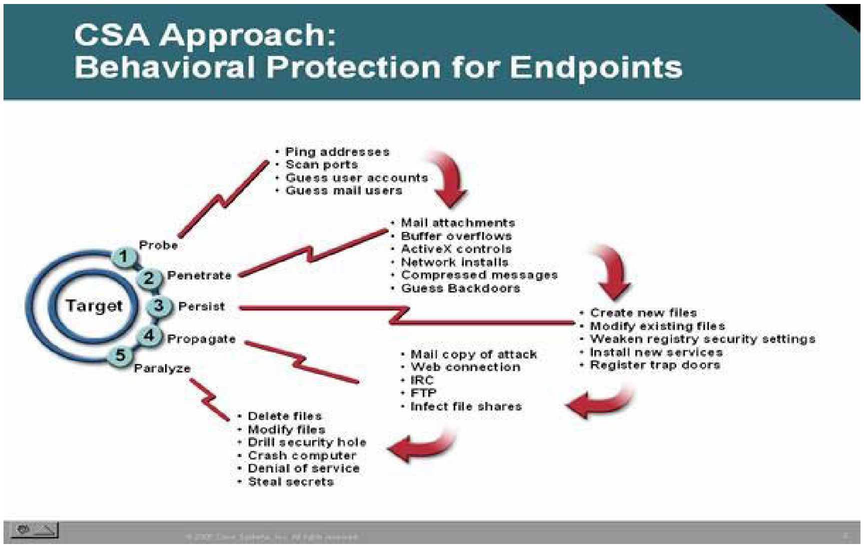
QUESTION 8:

A hacker has penetrated a network and now wants to reside on host. 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

Explanation:
The system attack cycle consists of 5 phases described below:
1. Vulnerable targets are identified in the probe phase. The goal of this phase is to find computers that can be subverted.
2. Exploit code is transferred to the vulnerable target in the penetrate phase. The goal of this phase is to get the target executing the exploit code through some attack vector like a buffer overflow.
3. When an exploit has been successful, the exploit code tries to make itself persistent on the target. The goal of the persist phase is to ensure that the attacker's code will be running and available to the attacker even if the target system reboots.
4. When an attacker has access to the organization's network, it extends the attack to other targets. The propagate phase looks for vulnerable neighboring devices to which it can spread the exploit code.
5. Only in the paralyze phase is damage done. Files are erased, systems fail, and distributed denial-of-service (DDoS) attacks are launched.



CSA Approach:
Behavioral Protection for Endpoints

Target

1 Probe
- Ping addresses
- Scan ports
- Guess user accounts
- Guess mail users

2 Penetrate
- Mail attachments
- Buffer overflows
- ActiveX controls
- Network installs
- Compressed messages
- Guess Backdoors

3 Persist
- Create new files
- Modify existing files
- Weaken registry security settings
- Install new services
- Register trap doors

4 Propagate
- Mail copy of attack
- Web connection
- IRC
- FTP
- Infect file shares

5 Paralyze
- Delete files
- Modify files
- Drill security hole
- Crash computer
- Denial of service
- Steal secrets

Reference:
www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae55e.pdf

---

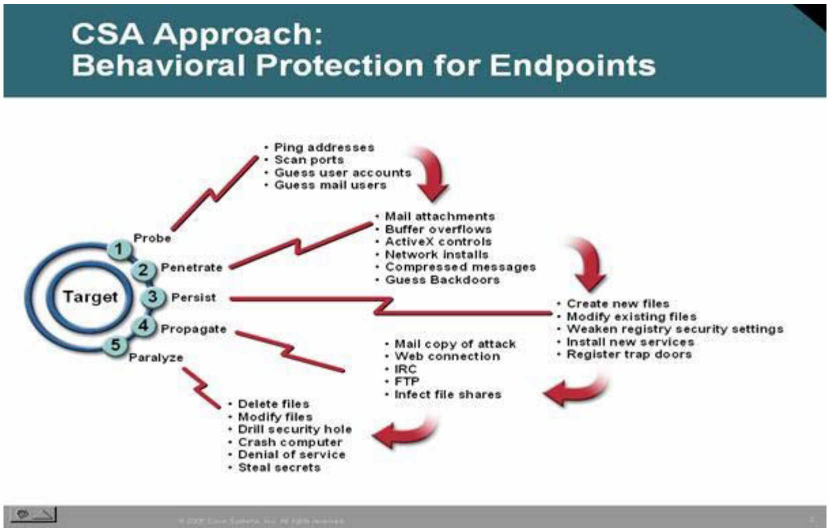
QUESTION 9:

Which two attacks could an attacker use on network 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: C, E

Explanation:
The system attack cycle consists of 5 phases described below:
1. Vulnerable targets are identified in the probe phase. The goal of this phase is to find computers that can be subverted.
2. Exploit code is transferred to the vulnerable target in the penetrate phase. The goal of this phase is to get the target executing the exploit code through some attack vector like a buffer overflow.
3. When an exploit has been successful, the exploit code tries to make itself persistent on the target. The goal of the persist phase is to ensure that the attacker's code will be running and available to the attacker even if the target system reboots.
4. When an attacker has access to the organization's network, it extends the attack to other targets. The propagate phase looks for vulnerable neighboring devices to which it can spread the exploit code.
5. Only in the paralyze phase is damage done. Files are erased, systems fail, and distributed denial-of-service (DDoS) attacks are launched.



CSA Approach:
Behavioral Protection for Endpoints

- Ping addresses
- Scan ports
- Guess user accounts
- Guess mail users

- Mail attachments
- Buffer overflows
- ActiveX controls
- Network installs
- Compressed messages
- Guess Backdoors

- Create new files
- Modify existing files
- Weaken registry security settings
- Install new services
- Register trap doors

- Mail copy of attack
- Web connection
- IRC
- FTP
- Infect file shares

- Delete files
- Modify files
- Drill security hole
- Crash computer
- Denial of service
- Steal secrets

Reference:
www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae55e.pdf

QUESTION 10:

A CSA Query User window has popped up on a Certkiller user's PC. What are the three options that can be given to a user when a Query User window appears? (Choose three)

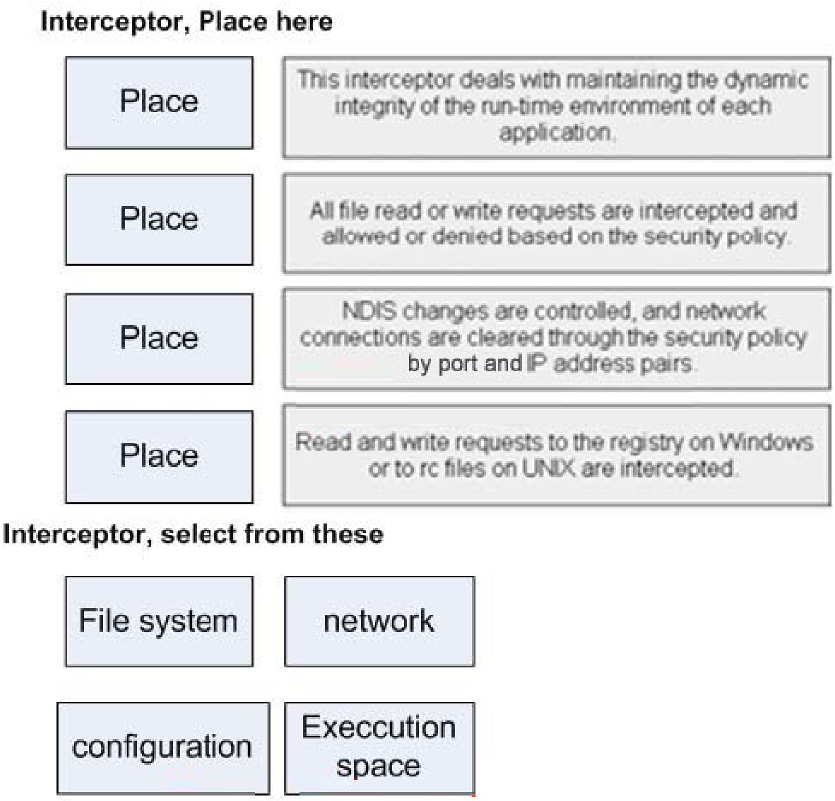
A. Allow
B. Accept
C. Deny
D. Kill
E. Terminate
F. Block

Answer: A, C, E

Explanation:
Query User: Some application behaviors will be legitimate under some circumstances and suspicious at other times. For example, when an application is writing a DLL file to the System32 directory, it could be part of a user-initiated software installation, or it could be a virus being installed without the user being aware of it. To manage events where the user's intent is a critical determining factor, Cisco Security Agent can be configured to query the user with a pop-up window. The text of the user query is configurable by the Cisco security Agent administrator;careful consideration should be given to make the query text as clear as possible to the common user. The user query pop-up window can be designed to offer the user any or all of these radio button options: Allow, Deny, or Terminate.
Reference:
http://www.cisco.com/web/about/security/intelligence/05_10_Tuning-Cisco-Security-Agent.html

QUESTION 11:

DRAG DROP
As a Certkiller student, you are tasked with matchingthe interceptor type with its definition below:



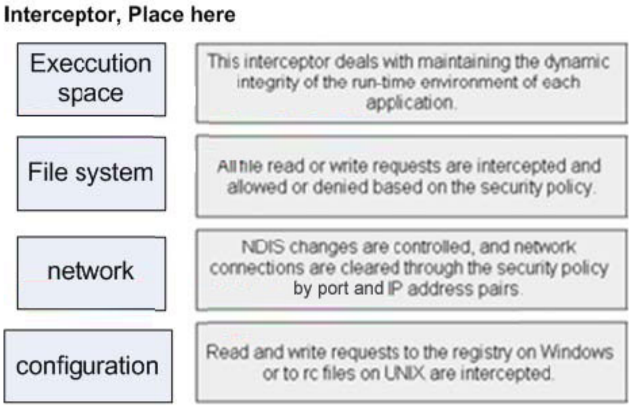
Interceptor, Place here

Place	This interceptor deals with maintaining the dynamic integrity of the run-time environment of each application.
Place	All file read or write requests are intercepted and allowed or denied based on the security policy.
Place	NDIS changes are controlled, and network connections are cleared through the security policy by port and IP address pairs.
Place	Read and write requests to the registry on Windows or to rc files on UNIX are intercepted.

Interceptor, select from these

File system	network
configuration	Execcution space

Answer:



Interceptor, Place here

Execcution space	This interceptor deals with maintaining the dynamic integrity of the run-time environment of each application.
File system	All file read or write requests are intercepted and allowed or denied based on the security policy.
network	NDIS changes are controlled, and network connections are cleared through the security policy by port and IP address pairs.
configuration	Read and write requests to the registry on Windows or to rc files on UNIX are intercepted.

QUESTION 12:

The CSA Management Center is being installed on a Certkiller server. 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
E. None of the above

Answer: B

Explanation:
CSAMC can only be installed after CommonServices is installed, but it can be installed before or after RME. As part of CSAMC installation you will first install Microsoft SQL Server Desktop Engine followed by CSAMC.
On a system where CSAMC has not been installed, the setup program first installs MSDE with Service Pack 3. If the CSA MC installation program detects any other database type attached to an existing installation of MSDE or a version of MSDE or SQL Server 2000 that does not have at least Service Pack 3, the installation will abort.
Note: For installation exceeding 500 agents, we recommend that you install Microsoft SQL Server 2000 instead of using the Microsoft SQL Server Desktop Engine that is provided with VMS.
Reference:
http://www.cisco.com/en/US/products/sw/cscowork/ps2330/products_installation_guide_chapter09186a00804d1

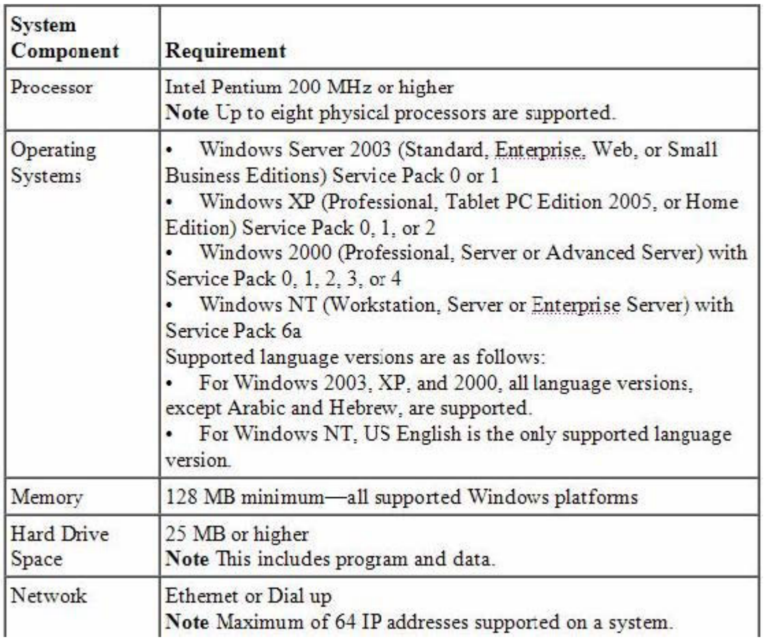
QUESTION 13:

The Cisco Security Agent has been installed on Certkiller hosts running a variety of operating systems. Which three operating systems are supported for deployment of CSA? (Choose three)

A. OS2
B. HPUX
C. Linux
D. Solaris
E. AIX
F. Windows
G. Atari

Answer: C, D, F

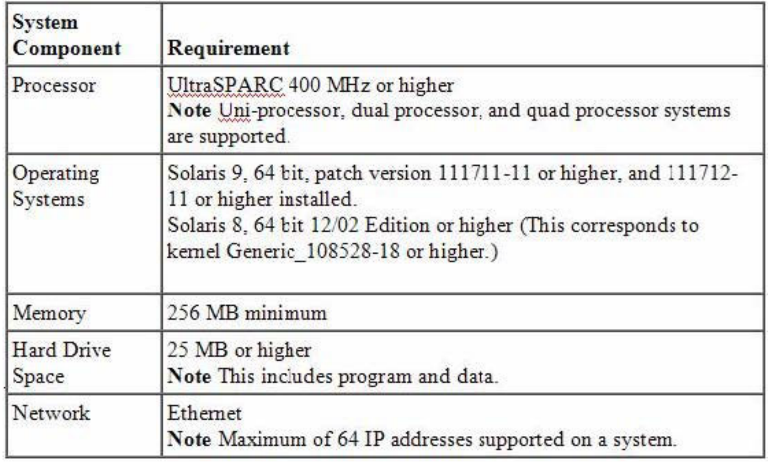
Explanation:
The Cisco Security Agent is supported on Windows, Linux, and Solaris operating systems. The tables below list the system requirements for each.
Agent Requirements (Windows)



System Component	Requirement
Processor	Intel Pentium 200 MHz or higher **Note** Up to eight physical processors are supported.
Operating Systems	• Windows Server 2003 (Standard, Enterprise, Web, or Small Business Editions) Service Pack 0 or 1 • Windows XP (Professional, Tablet PC Edition 2005, or Home Edition) Service Pack 0, 1, or 2 • Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4 • Windows NT (Workstation, Server or Enterprise Server) with Service Pack 6a Supported language versions are as follows: • For Windows 2003, XP, and 2000, all language versions, except Arabic and Hebrew, are supported. • For Windows NT, US English is the only supported language version.
Memory	128 MB minimum—all supported Windows platforms
Hard Drive Space	25 MB or higher **Note** This includes program and data.
Network	Ethernet or Dial up **Note** Maximum of 64 IP addresses supported on a system.

To run the Cisco Security Agent on your Solaris server systems, the requirements are as follows:

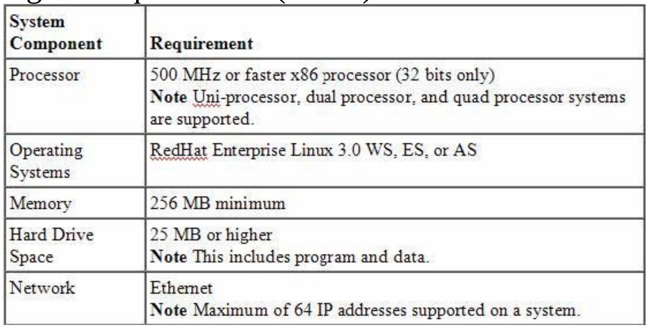
Agent Requirements (Solaris)



System Component	Requirement
Processor	UltraSPARC 400 MHz or higher **Note** Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	Solaris 9, 64 bit, patch version 111711-11 or higher, and 111712-11 or higher installed. Solaris 8, 64 bit 12/02 Edition or higher (This corresponds to kernel Generic_108528-18 or higher.)
Memory	256 MB minimum
Hard Drive Space	25 MB or higher **Note** This includes program and data.
Network	Ethernet **Note** Maximum of 64 IP addresses supported on a system.

To run the Cisco Security Agent on your Linux systems, the requirements are as follows:

Agent Requirements (Linux)



System Component	Requirement
Processor	500 MHz or faster x86 processor (32 bits only) **Note** Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	RedHat Enterprise Linux 3.0 WS, ES, or AS
Memory	256 MB minimum
Hard Drive Space	25 MB or higher **Note** This includes program and data.
Network	Ethernet **Note** Maximum of 64 IP addresses supported on a system.

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

QUESTION 14:

A Certkiller end user is attempting to install the CSA on their PC. Which type of privileges must this user have on a host system to install CSA?

A. Superuser
B. Administrator
C. User
D. Viewer
E. Guest

Answer: B

Explanation:
Once you build an agent kit on CSA MC, you deliver the generated URL, via email for example, to end users so that they can download and install the Cisco Security Agent. They access the URL to download and then install the kit. This is the recommended method of agent kit distribution. End users must have administrator privileges on their systems to install the agent.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

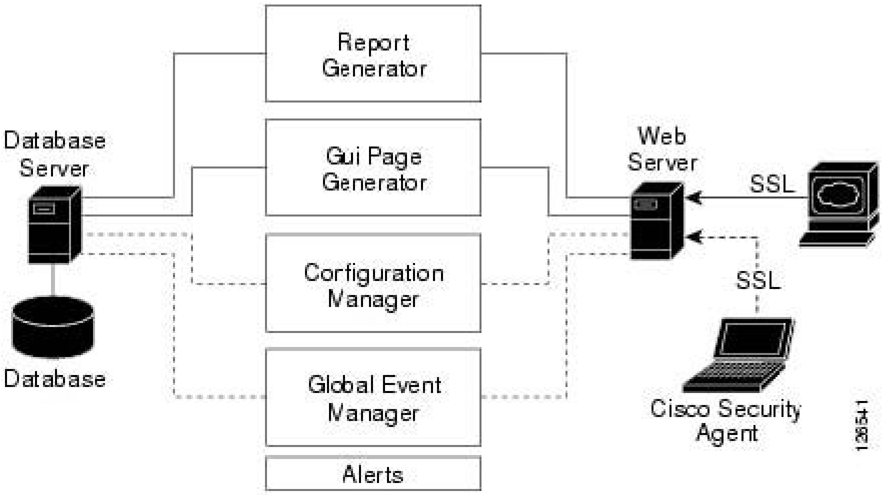
QUESTION 15:

The Certkiller security administrator uses a dedicated workstation to communicate with the CSA MC. Which protocol is required for the administrative workstation to communicate with the CSA MC?

A. SSH
B. Telnet
C. SSL
D. IPSec
E. FTP
F. HTTP

Answer: C

Explanation:
The components that make up the CSA MC are shown in the following diagram:



The web browser, shown on the right in the diagram, represents any web browser on any system across an enterprise from which administrators can securely access the CSA MC web-based interface. Communications between the web browser and the web server occur over SSL, allowing administrators to securely access the database of rule configurations from any location.

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

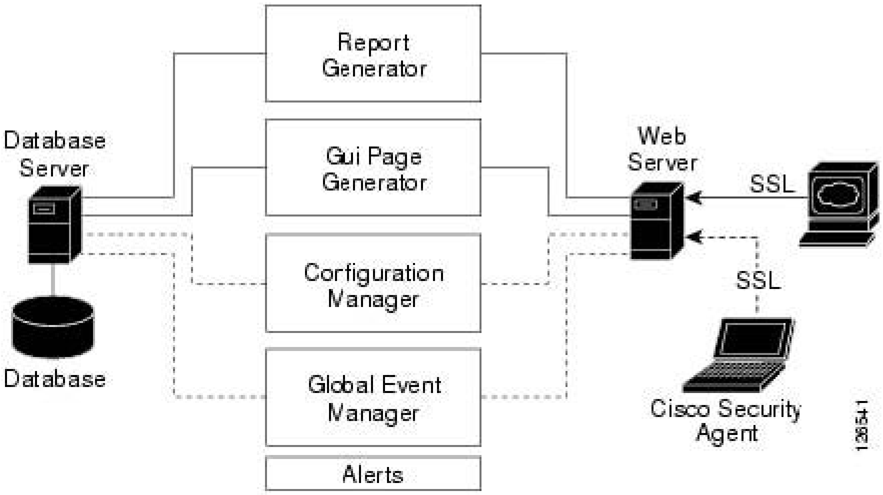
QUESTION 16:

The CSA Management Center is being configured and installed in the Testing network. Which protocol should never be disabled on the CSA MC?

A. SSH
B. Telnet
C. IPSec
D. SSL
E. All of the above

Answer: D

Explanation:
The CSA MC Components are shown below:



The web browser, shown on the right in the diagram, represents any web browser on any system across an enterprise from which administrators can securely access the CSA MC web-based interface. Communications between the web browser and the web server occur over SSL, allowing administrators to securely access the database of rule configurations from any location. The SSL service should not be disabled, or communications to the MC will be lost.
The web server provides the means of communication between the web browser and all other CSA MC system components. The web server displays reporting information, configuration version data, and event logging data.

QUESTION 17:

The Certkiller security administrator is installing the CSA MC program on a server.
What application is installed on the server after the CSA MC is installed?

A. Cisco Trust Agent
B. ACS
C. SOL
D. CSA
E. Cisco Works

Answer: D

Explanation:
When the CSA MC installation completes, an agent installation automatically begins. It is recommended that an agent protect the CSA MC system. (You may uninstall the agent separately if you choose, but this is not the recommended configuration.)
If an agent is already installed on a system to which you are installing CSA MC, that agent will automatically be upgraded by the CSA MC agent installation.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

QUESTION 18:

What are the three CSA MC Administrator roles that could be found in the Certkiller CSA Management Center? (Choose three)

A. Access
B. Configure
C. Deploy
D. View
E. Monitor
F. Administer
G. Root

Answer: B, C, E

Explanation:
Administrators can have different levels of CSA MC database access privileges. The initial administrator created by the CiscoWorks installation automatically has configuration privileges.
CiscoWorks/CSA MC Administrator Roles:
Configure-If the CiscoWorks administrator has the Network Administrator or System Administrator option enabled, this provides full read and write access to the CSA MC database.
Deploy-If the CiscoWorks administrator has only the Network Operations option enabled, this provides full read and partial write access to the CSA MC database. Administrators can manage hosts and groups, attach policies, create kits, schedule software updates, and perform all monitoring actions.
Monitor-If the CiscoWorks administrator has none of the roles listed in the first two bullets enabled, this provides administrators with read access to the entire CSA MC database. Administrators can also create reports, alerts, and event sets.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

QUESTION 19:

Communications to the CSA MC passes through a firewall in the Certkiller network and the associated ports need to be allowed through this firewall. Which port is used to access the CSA MC from the administrative workstation?

A. 21
B. 23
C. 1741
D. 1802
E. 666

Answer: C

Explanation:
Port 1741 is the port for Common Management Foundation (CMF) web serveraccess, and is used by Cisco Works and the Cisco CSA MC. To access CSA MC from a remote location, launch a browser application on the remote host and enter the following as the URL:
http://<ciscoworks system hostname>:1741
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 20:

What happens if the Agent UI control rule is not present in any active rule modules within the Certkiller CSA MC?

A. The Agent UI becomes present on the Certkiller system
B. The Agent UI is not present on the Certkiller system
C. The Agent UI is visible on the Certkiller system
D. The Agent UI is not visible on the Certkiller system

Answer: D

Explanation:
Use the Agent UI rule to control how the agent user interface is displayed to end users. In the absence of this rule, end users have no visible agent UI. If this rule is present in a module, you can select to display the agent UI and one or more controls to the end user. These controls give the user the ability to change certain aspects of their agent security.
Note: This rule only applies to Windows and Linux platforms. The agent UI is not supported on Solaris systems.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 21:

The Certkiller security administrator needs to configure a new policy. Which view would you use to create a new policy within the CSA MC?

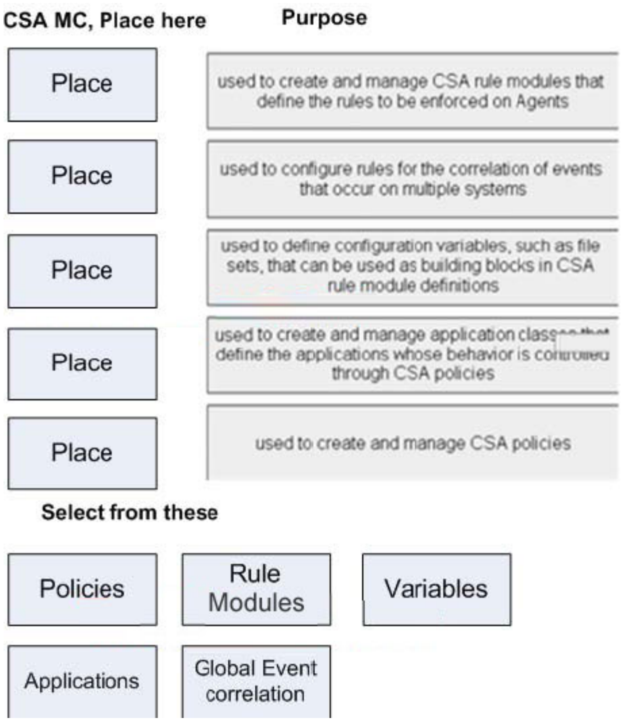
A. Configuration> Rules> Policies
B. Configuration> Policies
C. Systems> Policies
D. Systems> Rules> Policies
E. None of the above

Answer: B

Explanation:
Generally, when you configure a policy, you are combining multiple rule modules under a common name. That policy name is then attached to a group of hosts and it uses the rules that comprise the policy to control the actions that are allowed and denied on those hosts. You can have several different types of rules in a rule module and consequently within one policy.
The policy level is the common ground by which host groups acquire the rules that make up their security policy. You can attach rule modules of differing architectures to the same policy. This way, you can configure task-specific, self-contained, inclusive policies across all supported architectures (Windows, Solaris, Linux) for software that is supported on all platforms.
To configure a policy, do the following:
Step1
Move the mouse over Configuration in the menu bar of CSA MC and select Policies from the drop-down menu that appears. The policy list view appears.
Step2
Click the New button to create a new policy entry. This takes you to the policy configuration page.
Step3
In the available policy configuration fields, enter the following information:
Name-This is a unique name for this policy grouping of rule modules. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, and underscores.
Description-This is an optional line of text that is displayed in the list view and helps you to identify this particular policy.
Step4
Select one or more Target architecture types for the policy. You can have one policy, for example - an Apache Web Server policy, and have all three architecture checkboxes selected. This way, each architecture specific rule module for Apache can be attached and deployed through one single Apache policy.
Step5
Click the Save button.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 22:

DRAG DROP
You are a student at the Certkiller University. Your instructor asks you to match the CSA MC view on the left with its purpose on the right below:



CSA MC, Place here	Purpose
Place	used to create and manage CSA rule modules that define the rules to be enforced on Agents
Place	used to configure rules for the correlation of events that occur on multiple systems
Place	used to define configuration variables, such as file sets, that can be used as building blocks in CSA rule module definitions
Place	used to create and manage application classes that define the applications whose behavior is controlled through CSA policies
Place	used to create and manage CSA policies

Select from these

Policies

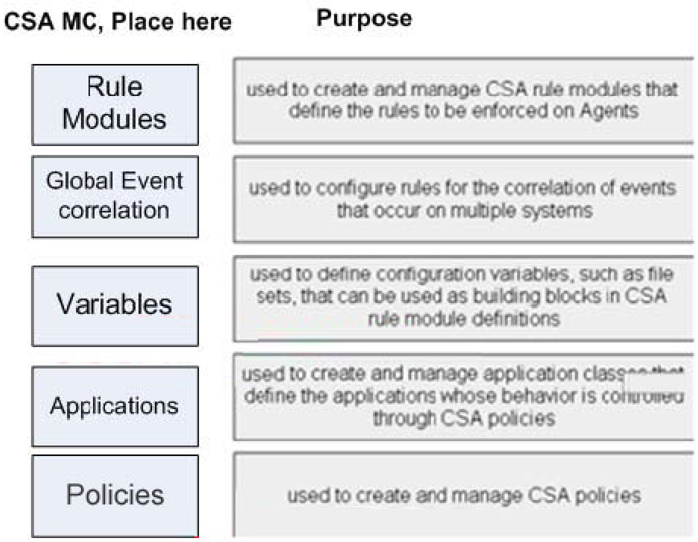
Rule Modules

Variables

Applications

Global Event correlation

Answer:



CSA MC, Place here	Purpose
Rule Modules	used to create and manage CSA rule modules that define the rules to be enforced on Agents
Global Event correlation	used to configure rules for the correlation of events that occur on multiple systems
Variables	used to define configuration variables, such as file sets, that can be used as building blocks in CSA rule module definitions
Applications	used to create and manage application classes that define the applications whose behavior is controlled through CSA policies
Policies	used to create and manage CSA policies

QUESTION 23:

One of the tools available on the Certkiller Management Center for Cisco Security Agents is the Compare Tool. What is the purpose of this 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
E. None of the above

Answer: D

Explanation:
When you select the checkbox next to 2 items (you cannot compare more than 2 configurations at a time) and click the Compare button, CSA MC displays the configurations side by side and highlights the differences in red. Once you've examined how the configurations compare, you can select to merge specific rules, to copy rules to another module, or to copy rules to a new module. Additionally, you can attach and detach groups and policies. (You can compare application classes and variables, but you can only copy and merge rules from the compare page.)
The purpose of this compare tool is to assist you after you've imported configurations or upgraded CSA MC. These processes can cause you to have duplicate or very similar configuration items. Comparing and merging configurations can help you to more easily consolidate duplicate items. This Compare utility is also available for Groups, Policies, Application Classes, and Variables.
Feature notes:
When you compare rule modules, the similar rules within those modules are displayed side by side with the differences highlighted in red. If there are no differences, rule description text appears in black.
If there is a rule in one modules and no corresponding similar rule in the second modules, there is nothing displayed beside that rule in the comparison.
If you have rules in your modules comparison that have the same description, application class and other configuration items, they will not appear side by side if they have different logging options selected or different Allow/Deny actions. Logging and allow/deny actions change the priority of the rule within the policy. If the priority is not the same for each rule, they are not displayed side by side.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 24:

The Certkiller security administrator is cloning configurations in the CSA MC.
When a rule is cloned, which part of the rule is not cloned?

A. Sets
B. Rule modules
C. Hosts
D. Variables
E. None of the above

Answer: D

Explanation:
In the CSA MC, Use the Clone button in conjunction with the checkboxes beside each list view item. To clone a particular configuration, select its checkbox and click the Clone button. You can clone one item at a time. New links to the cloned configurations appear in the list view.
Note:
When you clone an item that contains variable items like file sets or network services, the cloned rule uses the same variables used in the original rule. The variables themselves are not cloned.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 25:

A new CSA is being installed on the Certkiller network. Which Agent kit should be installed on the Certkiller 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
E. None of the above

Answer: D

Explanation:
The Management Center for Cisco Security Agents ships with preconfigured agent kits you can use to download and install agents if they meet your initial needs (accessible from System>Agent kits in the menu bar). There are prebuilt kits for desktops, servers, CiscoWorks VMS Systems, and others. These kits place hosts in the corresponding groups and enforce the associated policies of each group. (If you use a preconfigured agent kit, you do not have to build your own kit
When an agent is installed on a host, the agent automatically and transparently registers itself with CSA MC. It now appears in the CSA MC database as part of the groups designated in the kit, and will enforce policies that are applied to those groups.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

---

QUESTION 26:

Groups have been configured in the Certkiller CSA MC. 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
E. None of the above

Answer: D

Explanation:
The system hosts across your network, including mobile systems in the field, must download Cisco Security Agent software and register with Management Center for Cisco Security Agents to receive the security policies configured for them. When you are ready to apply policies to the hosts running agents, having those hosts placed into common groups streamlines the process of assigning policies to several hosts at once. To place hosts into groups, you must first analyze the security needs of each host system and map out a security plan. Hosts with similar requirements can then be grouped together.
Host groups reduce the administrative burden of managing a large number of agents. All hosts across your network, including mobile systems in the field, must exist as registered host entries in the Management Center for Cisco Security Agents for policy configurations to be assigned to them.
Grouping individual host systems together provides the following advantages:
It lets you consistently apply the same set of policies across multiple host systems.
It lets you apply Alert mechanisms and Event Set parameters based on group configurations.
It lets you use Test Mode to try out policies on groups of hosts before you actively enforce those policies.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 27:

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. Agents kits
D. Registration control
E. Groups

Answer: E

Explanation:
Host groups reduce the administrative burden of managing a large number of agents. Grouping hosts together also lets you apply the same policy to a number of hosts. A group is the only element required to build agent kits. Grouping individual host systems

together provides the following advantages:
It lets you consistently apply the same set of policies across multiple host systems.
It lets you apply Alert mechanisms and Event Set parameters based on group configurations.
It lets you use Test Mode to try out policies on groups of hosts before you actively enforce those policies.
You can group hosts together based on any criteria that best fits your enterprise. For example:
Group hosts according to system function, such as web servers. Then you would create a policy that corresponds specifically to the needs of your web servers and distribute it to that group.
Group hosts according to business groups, such as finance, operations, and marketing. Distribute policies based on each business group's individual needs.
Group hosts according to geographical or topological location. For example, group hosts based on their subnet designation for reporting purposes.
Group hosts according to their importance to your organization. Place mission-critical systems into a common group to apply critical alert level configurations to them.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 28:

The Certkiller network utilizes hosts with a variety of operating systems. Which three 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

Answer: C, E, F

Explanation:
CSA MC provides three auto-enrollment architectural groups (Windows, Solaris, Linux) that are mandatory for all hosts of a given OS architecture. By providing group auto-enrollment for hosts, any policies you attach to these groups also become mandatory by association. You might want to use these mandatory groups to apply policies which prevent some critical service from being inadvertently banned. For example, you could attach policies to prevent DNS or DHCP from being disabled by an overly restrictive rule.
Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 29:

The Certkiller CSA administrator has just added some of the Certkiller hosts into a group. 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
E. None of the above

Answer: C

Explanation:
Using Test Mode
Test Mode is useful when you are installing a new host or are modifying a host configuration and want to understand the ramifications without actually impacting host operation. When operating in test mode, the agent will not deny any action or operation even if an associated policy says it should be denied. Instead, the agent will allow the action but log an event if a deny or query rule is triggered (if logging is enabled for the rule) and log an event when an allow rule with logging enabled is triggered. This helps you to understand the impact of deploying a policy on a host before enforcing it. If examining the logs shows you that the policy is working as intended on a group, you can then remove the Test Mode designation.
When using Group test mode (available from the Rule Overrides category), you may also want to enable Verbose logging mode. This way, the agent will not suppress any log messages as it normally does when several of the same log messages are received.
Group Test Mode
You can turn on test mode in two places within the MC. If it is enabled on the group level, all rules on hosts within test mode groups are in test mode.
If a host belongs to a group with test mode selected, all policies associated with that host are in test mode (even if the host is part of another group that does not have test mode selected), not just the policies applied to the test group. Therefore, test mode applies to the host as a whole, not to specific policies.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 30:

An agent kid was built on a Certkiller CSA, MC. How can this 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
E. None of the above

Answer: A
Reference:
Once you build an agent kit on CSA MC, you deliver the generated URL, via email for example, to end users so that they can download and install the Cisco Security Agent. They access the URL to download and then install the kit. This is the recommended method of agent kit distribution. But you may also point users to a URL for the CiscoWorks system. This URL will allow them to see all kits that are available. That URL is:
https://<ciscoworks system name>/csamc50/kits
If you are pointing users to the "kits" URL and you have multiple agent kits listed here, be sure to tell users which kits to download.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

---

QUESTION 31:

A new group has been created in which some Certkiller hosts need to be moved to. Which action must be taken before a host can enforce rules when it has been moved to a new group?

A. Save
B. Generate rules
C. Deploy
D. Clone
E. Write to memory

Answer: B

Explanation:
Once you have configured a policy and attached it to a new group, you need to distribute the policy to the agents that are part of this new group. We do this by first generating our rule programs.
Click Generate rules in the bottom frame of CSA MC. All pending database changes ready for distribution appear.
If everything looks okay, you can click the Generate button that now appears in the bottom frame. This distributes your policy to the agents.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

QUESTION 32:

The Certkiller CSA administrator is building agent kits for distribution. Which two items make up Agent kits? (Choose two)

A. Groups
B. Hosts
C. Policies
D. Rules
E. Network shim

Answer: A, C

Explanation:
Host groups reduce the administrative burden of managing a large number of agents. Grouping hosts together also lets you apply the same policy to a number of hosts.
A group is the only element required to build Cisco Security Agent kits. When hosts register with CSA MC, they are automatically put into their assigned group or groups. Once hosts are registered you can edit their grouping at any time. Once this is accomplished you can configure some policies and distribute them to installed and registered Cisco Security Agents.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

QUESTION 33:

How can you configure a Certkiller host to poll in to the Certkiller CSA MC before its scheduled polling interval; using the CSA MC?

A. Click the Poll button on the Agent UI
B. Choose the Poll Now button on the CSA MC
C. Choose the Send Polling Hint option in the CSA MC
D. Enter a polling interval in the appropriate box on the CSA MC

Answer: C

Explanation:
Hosts poll into CSA MC to retrieve policies. You can shorten or lengthen this polling time in the Group configuration page. You can also send a hint message to tell hosts to poll in before their set polling interval.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

QUESTION 34:

A new agent kit was created in the Certkiller CSA network, and needs to be downloaded to end users. What status is shown when an Agent kit is prepared for downloading to hosts?

A. Prepared
B. Ready
C. Needs rule generation
D. Complete
E. None of the above

Answer: B

Explanation:
Agent Kit Status
When you create an agent kit, it is given one of three status levels based on how far into the configuration you've progressed. Those status levels are as follows:
Ready: This means the agent kit is ready for download to host systems.
Needs rule generation: This means that all agent kit configuration parameters are complete, but you must generate rules before the kit can be downloaded.
Incomplete: This means that you have not configured all the necessary parameters for this agent kit. You must complete the configuration and then generate rules before the kit can be downloaded.
Undeployable: This status will only occur if you have ungenerated kits on the MC and then you upgrade the MC to a newer version. Agent kits that were created but never generated and have an old version number can never be deployed and should be deleted.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 35:

Software updates are available for numerous Certkiller users. Which operating system does not receive a notification window when a software update is available from the CSA MC?

A. Linux
B. Windows
C. HPUX
D. Solaris
E. All of the above

Answer: D

Explanation:

The status window of the agent user interface can provide end users with all of the following:
The host name of the machine on which this agent is installed.
The name of the CSA MC with which this agent is registered.
The date and time the agent registered with CSA MC.
The date and time when the agent last polled in to CSA MC (data is not downloaded each time the agent polls).
The date and time the agent last downloaded data from CSA MC.
Lets users know if there is a software version update available for their agent.
Note: The Cisco Security Agent user interface appearance and functionality is the same on all Windows and Linux platforms. However, The Cisco Security Agent user interface does not run on Solaris systems. The Solaris agent has a utility (csactl) to provide some of the capabilities that the Windows and Linux agents provide in their user interface.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 36:

A Certkiller host is trying to download policies from the CSA MC. 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
E. All of the above

Answer: D

Explanation:
The CSA MC architecture model consists of a central management center which maintains a database of policies and system nodes, all of which have Cisco Security Agent software installed on their desktops and servers.
Agents register with CSA MC. CSA MC checks its configuration database for a record of the system. When the system is found and authenticated, CSA MC deploys a configured policy for that particular system or grouping of systems.
There are several elements you must configure to create policies that are distributed to the agents. First, you must configure host groups and create Cisco Security Agent kits. After the agents are installed on systems throughout your network, they register with CSA MC. Then, they are automatically placed into their assigned groups. When you generate rules, agents receive the policies intended for them.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 37:

The Certkiller security administrator is in the process of naming a policy in the MC. What is the maximum number of characters that a policy name can contain?

A. 24
B. 32
C. 48
D. 64
E. 128

Answer: D

Explanation:
The policy name is a unique name for this group of hosts. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, and underscores.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

QUESTION 38:

A sniffer and protocol detection rule has been configured in the Certkiller CSA network. What is the purpose of this sniffer and protocol detection rule?

A. to stop sniffers from running on a network
B. to allow sniffers to run on a network
C. to cause an event to be logged when non-IP protocols and sniffer programs are detected running on systems
D. to deny non-IP protocols and sniffer programs from running on systems
E. None of the above

Answer: C

Explanation:
Use the Sniffer and protocol detection rule to cause an event to be logged when non-IP protocols and packet sniffer programs are detected running on systems.
Non-IP protocols, such as IPX, AppleTalk, and NetBEUI, are used to provide distributed computing workgroup functions between server and clients and/or sharing between peer clients.
A packet sniffer (also controlled by this rule type) is a program that monitors and analyzes network traffic. Using this information, a network manager can troubleshoot network problems. A sniffer can also be used illegitimately to capture data being transmitted on a network. Sensitive information such as login names and passwords can be extracted from this data and used to break into systems.

The Sniffer and protocol detection rule is a monitoring tool. By adding this rule to a policy, you are causing an event to be logged when any non-IP protocols and packet sniffer programs are detected running on systems which receive this rule.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 39:

Connection rate rules are in place within the Certkiller CSA network. What is the purpose of these connection rate limit rules?

A. To limit the number of connections to an application
B. To limit the number of calls to the kernel in a specified time frame
C. To limit the number of network connections within a specified time frame
D. To limit the number of malformed connection requests to a web server
E. None of the above

Answer: C

Explanation:
Use the connection rate limit rule to control the number of network connections that can be sent or received by systems within a specified time frame. This is useful in preventing attacks aimed at bringing down system services, for example, denial of service attacks (server connection rate limiting). This is also useful in preventing the propagation of denial of service attacks (client connection rate limiting).
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_release_note09186a008019b760.html#65518

QUESTION 40:

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

Answer: C, D, E

Explanation:
If a system is not rebooted following the agent installation, the following functionality is

not immediately available. (This functionality becomes available the next time the system is rebooted.)
Windows agents:
Network Shield rules are not applied until the system is rebooted.
Network access control rules only apply to new socket connections. Network server services should be stopped and restarted for full network access control security without a system reboot.
Data access control rules are not applied until the web server service is restarted.
Solaris and Linux agents, when no reboot occurs after install, the following caveats exist
Buffer overflow protection is only enforced for new processes.
File access control rules only apply to newly opened files.
Data access control rules are not applied until the web server service is restarted.
At this time, the agent automatically and transparently registers with CSA MC.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 41:

The Certkiller security administrator is ready to deploy CSA configurations to the Certkiller hosts. 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
E. Push

Answer: D

Explanation:
Generate Rule Programs:
After a policy has been configured and attached to a group that was created, the next task is to distribute the policy to the agents that are part of the group. We do this by first generating our rule programs. Once you click the Make Kit button and generate rules, CSA MC produces a kit for distribution
Click Generate rules in the bottom frame of CSA MC. All pending database changes ready for distribution appear.
If everything looks okay, you can click the Generate button that now appears in the bottom frame. This distributes your policy to the agents.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

QUESTION 42:

Rules are being created for the Certkiller CSA network environment. Which three items make up rules? (Choose three)

A. Variables
B. Applications
C. Application classes
D. Rule modules
E. Policies
F. Actions

Answer: A, C, F

Explanation:
A policy is a collection of rule modules. A rule module is a collection of rules. The rule module acts as the container for these rules while the policy serves as the unit of attachment to groups. Machines with similar security needs are grouped together and assigned one or more policies that specifically target the needs of the group. Rules are made up of variables, application classes, and actions.
You use configuration variables to help build the rules that form your policies. Using variables makes it easy for you to maintain policies by letting you make any necessary modifications in one place and having those changes instantiated across all rules and policies.
Access control rules are application-centric. The application classes, those shipped with CSA MC and the ones you configure yourself, are the key to the rules you build as part of your security policies.
Incorrect Answers:
B: Application classes are used in the creation of rules, not the applications themselves.
D: Rule modules consist of one or more rules. Rules make up rule modules, not the other way around.
E: Rules are used to create policies, not the other way around.

QUESTION 43:

The Certkiller CSA network uses both Windows and UNIX stations. Choose three types of rules that apply to both Windows and UNIX systems (Choose three)

A. Agent service control rules
B. Agent UI control rules
C. Application control rules
D. COM component access control rules
E. File version control rules

Answer: A, B, C

Explanation:
The following rule types are available for both Windows and UNIX policies.
Agent Service Control
Use the Agent service control rule to control whether administrators are allowed to stop agent security and whether end users can disable security via the agent UI security slide bar.
Agent UI Control
Use the Agent UI rule to control how the agent user interface is displayed to end users. In the absence of this rule, end users have no visible agent UI. If this rule is present in a module, you can select to display the agent UI and one or more controls to the end user. These controls give the user the ability to change certain aspects of their agent security.
Application Control
Use Application control rules to control what applications can run on designated agent systems. This rule type does not control what application can access what resources as do other access control rules. This rule type can stop selected applications from running on systems. If you deny an application class (in total) in this rule, users cannotuse any application in that class.
With this rule, you can also prevent an application from running only if that application was invoked by another application you specify. This way, you could prevent a command prompt from running on a system if it is invoked by an application that has downloaded content from the network.
Connection Rate Limit
Use the connection rate limit rule to control the number of network connections that can be sent or received by applications within a specified time frame. This is useful in preventing attacks aimed at bringing down system services, e.g. denial of service attacks (server connection rating limiting). This is also useful in preventing the propagation of denial of service attacks (client connection rate limiting).
Data Access Control
Use data access control rules on Web servers to detect clients making malformed web server requests where such requests could crash or hang the server. A malformed request could also be an attempt by an outside client to retrieve configuration information from the web server or to run exploited code on the server. This rule detects and stops such web server attacks by examining the URI portion of the HTTP request.
File Access Control
Use file access control rules to allow or deny what operations (read, write) selected applications can perform on files. You should understand that file protection encompasses read/write access. Directory protection encompasses directory deletes, renames, and new directory creation.
Network Access Control
Use network access control rules to control access to specified network services and network addresses. You can also use this rule type to listen for applications attempting to offer unknown or not sanctioned services.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 44:

Data Access Control Rules are being configured in the Certkiller CSA MC. Which portion of an HTTP request is examined by data access control rules?

A. The TCP header
B. The UDP header
C. The URI portion of the request
D. The URL portion of the request
E. The HTTP payload

Answer: C

Explanation:
Use data access control rules on Web servers to detect clients making malformed web server requests where such requests could crash or hang the server. A malformed request could also be an attempt by an outside client to retrieve configuration information from the web server or to run exploited code on the server. This rule detects and stops such web server attacks by examining the URI portion of the HTTP request.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 45:

Network access control rules have been implemented in the Certkiller CSA network. 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
E. None of the above

Answer: C

Explanation:
Use network access control rules to control access to specified network services and network addresses. You can also use this rule type to listen for applications attempting to offer unknown or not sanctioned services.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 46:

Which two of the following file access rule criteria can you use to allow or deny the operations that the selected applications can perform on files within the Certkiller network? (Choose two)

A. The application attempting to access the file
B. The application attempting to access the service or address
C. The operation attempting to act on the file
D. The direction of the communications
E. The address with which a system is attempting to communicate

Answer: A, C

Explanation:
Use file access control rules to allow or deny what operations (read, write) selected applications can perform on files. You should understand that file protection encompasses read/write access. Directory protection encompasses directory deletes, renames, and new directory creation.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 47:

Network access rules have been implemented into the Certkiller CSA network.
Which two of the following network access rules can you use to control access to specified network services? (Choose two)

A. The application attempting to access the file
B. The application attempting to access the service or address
C. The operation attempting to act on the file
D. The direction of the communications

Answer: B, D

Explanation:
Use network access control rules to control access to specified network services and network addresses. You can also use this rule type to listen for applications attempting to offer unknown or not sanctioned services.
From the pulldown menu in the CSA MC, select server, client, client or server, or listener (for more information on the listener option) depending on the direction or type of connection you are controlling or listening for. Select one or more preconfigured application classes here to indicate the application(s) whose access to the listed services and addresses you want to exercise control over.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 48:

CSA rules need to be applied to the Certkiller windows stations. Which two types of rules apply to Windows systems only? (Choose two)

A. Agent service control rules
B. Clipboard access control rules
C. Agent UI control rules
D. COM component access control rules
E. Data access control rules

Answer: B, D

Explanation:
Windows Only Rules
The following rules are only available for Windows Rule Modules.
Clipboard Access Control
Use the clipboard access control rule to dictate which applications can access information that is written to the clipboard. When writing security policies, you may want to protect information from being accessed by other applications or network processes. To fully protect this information, you must consider preventing other applications from accessing protected information that may have been written to the clipboard.
COM Component Access Control
Use COM component access control rules to allow or deny applications from accessing specified COM components. COM is the Microsoft Component Object Model, the technology that allows objects to interact across process and machine boundaries as easily as within a single process. Each of the Microsoft Office applications (Word, Excel, Powerpoint, etc.)
exposes an "Application" COM component which can be used to create macros or utility scripts. While this is useful functionality, it can be used
maliciously by an inadvertently downloaded Visual Basic script.
File Version Control
Use the File version control rule to control the software versions of applications users can run on their systems. For example, if there is a known security hole in one or more versions of a particular application, this rule would prevent those specific versions from running, but would allow any versions not included in this rule to run unimpeded.
Kernel Protection
Use the Kernel protection rule to prevent unauthorized access to the operating system. In effect, this rule prevents drivers from dynamically loading after system startup. You can specify exceptions to this rule for authorized drivers that you are allowing to load any time after the system is finished booting.
NT Event Log
Use the NT Event log rule to have specified NT Event Log items appear in the CSA MC Event Log for selected groups.
Registry Access Control

Use registry access control rules to allow or deny applications from writing to specified registry keys.
Service Restart
Use the Service restart rule to have the agent restart Windows NT services that have gone down on a system or are simply not responding to service requests.
Sniffer and Protocol Detection
Use the Sniffer and protocol detection rule to cause an event to be logged when non-IP protocols and packet sniffer programs are detected running on systems.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 49:

Many of the Certkiller workstations are UNIX based and CSA rules need to be created for them. Which two types of rules are UNIX-only rules?

A. Network interface control rules
B. COM component access control rules
C. Connection rate limit rules
D. File access control rules
E. Rootkit/kernel protection rules

Answer: A, E

Explanation:
UNIX Only Rules:
The following rules are only available for UNIX Rule Modules.
Network Interface Control
Use the Network interface control rule to specify whether applications can open a device and act as a sniffer (promiscuous mode). A packet sniffer is a program that monitors and analyzes network traffic. Using this information, a network manager can troubleshoot network problems. A sniffer can also be used illegitimately to capture data being transmitted on a network. Sensitive information such as login names and passwords can be extracted from this data and used to break into systems.
Resource Access Control
Use the Resource access control rule to protect systems from symbolic link attacks. In this type of attack, an attacker attempts to determine the name of a temporary file prior to its creation by a known application. If the name is determined correctly, the attacker could then create a symbolic link to the target file for which the user of the application has write permissions. The application process would then overwrite the contents of the target file with its own output when it tries to write the named temporary file.
Rootkit/ kernel Protection
Use the Rootkit / kernel protection rule to control unauthorized access to the operating system. In effect, this rule controls drivers attempting to dynamically load after boot

time. You can use to this rule to specify authorized drivers that you are allowing to load any time after the system is finished booting.
Syslog Control
Use the Syslog control rule to have specified Solaris and Linux Syslog items appear in the CSA MC Event Log for selected groups.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 50:

The rootKit/kernel protection rule is being utilized in the Certkiller CSA network.
What is the purpose of this rootkit/ kernel protection rule?

A. To restrict access to the operating system
B. To log access to the operating system
C. To restrict user access to the operating system
D. To restrict administrator access to the operating system
E. All of the above

Answer: A

Explanation:
Use the Rootkit / kernel protection rule to control unauthorized access to the operating system. In effect, this rule controls drivers attempting to dynamically load after boot time. You can use to this rule to specify authorized drivers that you are allowing to load any time after the system is finished booting.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 51:

The Certkiller CSA network utilizes the network interface control rule. What is the purpose of this rule?

A. To prevent applications from opening devices and acting as a sniffer
B. To provide protocol stack hardening rules
C. To prevent users from opening devices that can act as a sniffer
D. To provide filtering of undesired traffic at the network interface level
E. None of the above

Answer: A

Explanation:
Use the Network interface control rule to specify whether applications can open a device

and act as a sniffer (promiscuous mode). A packet sniffer is a program that monitors and analyzes network traffic. Using this information, a network manager can troubleshoot network problems. A sniffer can also be used illegitimately to capture data being transmitted on a network. Sensitive information such as login names and passwords can be extracted from this data and used to break into systems.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00804
2

QUESTION 52:

The Agent UI rule is used to control how the agent user interface is displayed to end users. What action is taken on user query windows when the Agent UI is not present on a system?

A. The default action is always taken
B. All actions are denied
C. All actions are allowed
D. All actions are allowed and logged
E. None of the above

Answer: A

Explanation:
When there is no agent UI present, there are no query user pop-up boxes displayed. The default is immediately taken on all query user rules and heuristics that are present in the assigned polices. (Note that this does not apply to cases where the end user manually exits the agent UI. Only the administrator controlled agent UI rule can affect query pop-up displays on the end user system.)
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805
a

QUESTION 53:

The system API rule is being used in the Certkiller CSA network. For which operating system is the system API control rule available?

A. OS2
B. Windows
C. Linux
D. Solaris
E. None of the above.

Answer: B

Explanation:
The System API control rule detects several forms of malicious programming code that is installed on a system by an unsuspecting user either thinking that he or she is running some other type of program, or as a result of some other activity such as reading an attachment to an email message. Once installed, these malicious programs (for example, Trojans) may allow others to access and virtually take over a system across the network. Other errant programs may be set up to automatically send mail messages or other types of network traffic (including system passwords) while the system owner is unaware of what is occurring.
Note: Although the system API rule is common to Windows and Unix systems, this rule type is not available for UNIX policies. The system API rule is for Windows only.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 54:

New rules were applied to a Certkiller workstation, but the station has not yet been rebooted. Which rules will not be enforced if you fail to reboot a Windows system following installation of the CSA?

A. Network access control rules
B. Buffer overflow rules
C. COM component access control rules
D. Network shield rules
E. None of the above

Answer: D

Explanation:
If a system is not rebooted following the agent installation, the following functionality is not immediately available. (This functionality becomes available the next time the system is rebooted.)
Windows agents:
Network Shield rules are not applied until the system is rebooted.
Network access control rules only apply to new socket connections. Network server services should be stopped and restarted for full network access control security without a system reboot.
Data access control rules are not applied until the web server service is restarted.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_chapter09186a00805aeb

QUESTION 55:

The network shield rule is being applied to devices within the Certkiller CSA network. For which operating system is the network shield rule available?

A. OS2
B. Windows
C. Linux
D. Solaris
E. None of the above

Answer: B

Explanation:
The Network shield rule provides network protocol stack hardening capabilities. The features available here require that the network shim be enabled on an agent system. If the network shim is not enabled, these rules have no effect when applied. This rule only applies to Windows based operating systems.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 56:

Numerous UNIX stations exist on the Certkiller LAN that have been prone to buffer overflow attacks. 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

Answer: B, D, E

Explanation:
A buffer overflow is what happens when two conditions are met: Firstly, an application is coded in a manner such that it trusts that all users of that application will provide the application with reasonable and expected data. Secondly, the application is provided larger quantities of data than it is capable of correctly handling. When these events come together, an application can behave in unexpected and unintentional ways.
For applications with special privileges, this can result in external users gaining access to machine resources and privileges which they normally would not be able to acquire. In other words, a hostile, network-based attack on a privileged, trusted application via buffer overflows can result in undesirable parties gaining access to your system.

In the case of UNIX operating systems, there are three distinct types of buffer overruns which can occur, based upon the type of memory space involved: stack, data, and heap.
Stack space is used to store data and information which is local to the piece of code currently being executed in an application, and contains stored away control flow information for the application.
Data space is used to store data with fixed sizes which needs to be shared among different parts of an application. Often, content in data space has been given initial values.
Heap space is dynamically given out to applications, with the intent that it is relatively short-lived, of varying size based upon the input datasets, and is frequently visible to numerous sub-components of an application.
Note:
This rule is UNIX specific. Some corresponding Windows functionality is available from the System API control rule page.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 57:

The Certkiller security administrator is viewing investigation reports generated by the CSA MC. 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

Answer: A

Explanation:
Application Deployment Investigation is mainly comprised of the reporting capabilities it provides once all the data is collected. You can organize the gathered data in various manners to provide information on how your enterprise operates, the resources that are accessed, resource and application usage time frames, and a great deal more. In turn, this data can inform the crafting of your policies while you create a more secure environment for all your users to operate within.
While you cannot configure what types of information you collect using deployment investigation (including the use of preconfigured application classes) you can organize the information that is gathered in various ways.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 58:

In the Certkiller Management Center, network address sets need to be configured.
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

Answer: C

Explanation:
Network Address Sets
Configure network address sets for use in network access control rules to impose restrictions on specified IP addresses or a range of addresses. Once configured, you can simply enter the name of the address set in any network access control rules you create.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008047

QUESTION 59:

The Certkiller security manager has configured file sets for use in the Certkiller CSA network. In which type of rules are file sets used?

A. COM component access control rules
B. Resource access control rules
C. File version control rules
D. File access control rules
E. All of the above

Answer: D

Explanation:
Configure file sets for use in file access control rules and application classes. File sets are groupings of individual files and directories under one common name. This name is then used in rules that control directory and file permissions and restrictions. All the parameters that exist under that name are then applied to the rule where the name is used.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 60:

Agent kits are being built on the Certkiller MC to be installed on user stations. What can you optionally install when you choose the Quiet Install option when creating a new Windows Agent kit?

A. The Agent kit shim
B. The protocol shim
C. The network shim
D. The policy shim
E. All of the above

Answer: C

Explanation:
In some circumstances, you may not want users to enable the network shim on their systems as part of the agent installation. (Note that the network shim is not optional on UNIX systems.) For example, if users have VPN software or a personal firewall installed on their systems, the network shim's Portscan detection, SYN flood protection, and malformed packet detection capabilities may be in conflict with VPNs and personal firewalls. (There are no conflicts with the Cisco VPN client.)
If you check the Quiet install checkbox when you make kits, you can also select whether the network shim is installed as part of the Quiet install process.
To allow users to select whether or not to install the network shim themselves, you would create kits as non-quiet installations. (Do not select the Quiet install checkbox.) This way, users are prompted to enable the network shim during the agent installation.

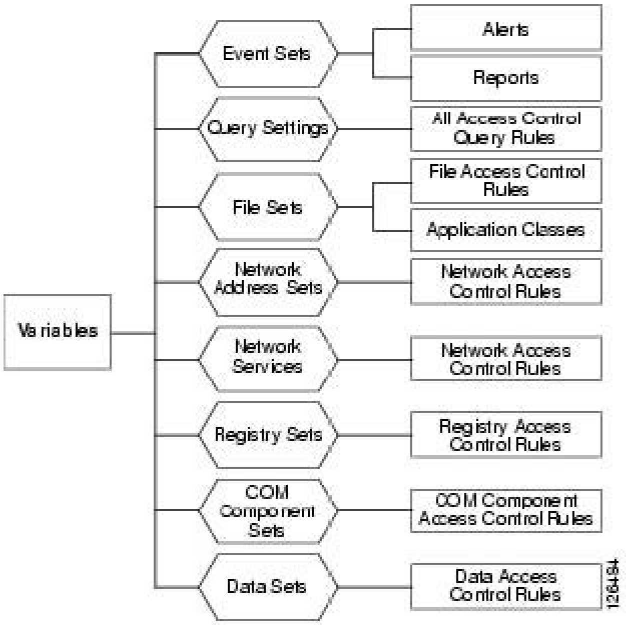
QUESTION 61:

In the Certkiller CSA network, variables are used in the rule sets. Which of the following are types of variables used for CSA? (Choose three)

A. Global sets
B. File sets
C. API sets
D. Data sets
E. Network address sets

Answer: B, D, E

Explanation:
The diagram below displays how variables relate to access control rules. In the diagram, variables (Event Sets, Query Settings, File Sets, Network Address Sets, Network Services, Registry Sets, COM Component Sets, and Data Sets) are shown on the left and the rule types they can be applied to are shown on the right.
Variable Use in Rules:


Variables
Event Sets
Query Settings
File Sets
Network Address Sets
Network Services
Registry Sets
COM Component Sets
Data Sets
Alerts
Reports
All Access Control Query Rules
File Access Control Rules
Application Classes
Network Access Control Rules
Network Access Control Rules
Registry Access Control Rules
COM Component Access Control Rules
Data Access Control Rules
126484

Note:
Using variables is optional (note that Application Classes are included in this diagram, but they are not optional). Nearly all the information used in variable configurations can also be entered directly into corresponding rule configuration fields. Variables are simply a tool meant to simplify the creation of rules, especially if the same configurations are used in multiple rules.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 62:

Access Control rules are being configured for use in the Certkiller CSA network so that query user options can be used. Which operating system does not allow Query User options?

A. OS2
B. Windows
C. Linux
D. Solaris
E. HPUX

Answer: D

Explanation:
When you create access control rules, beyond simply allowing or denying a specific action, you can select to query the user when an action triggers the rule in question. The user can then decide to allow the action, deny it, or terminate the process at that time. When you select to query the user, you are also crafting explanation text to display to the

user and whether to allow, deny, or terminate the action by default if the query is not answered within 5 minutes. If the user is not logged in to the system, the default action is taken immediately.
Query configurations are a Variable setting which allows you to decide which radio button options are displayed in the pop-up query box, which action is the default, whether the answer given by the user is to be remembered, and what the query text to be displayed will be.
For a Query setting, the response to the query is relevant to the question, not the resource. For example, if a File access control rule queries the user for a response and that identical query is also configured for a Network access control rule, the user is not queried again when the Network access control rule triggers. The query response from the previous File access control rule is automatically taken.
Note: For Solaris rules, Query user options are not available. Instead, the default action is immediately taken.
For Windows and Linux agents, agent settings (including user queries) are configurable by the administrator. If the agent UI is hidden for the group, there are no query user pop-up boxes displayed. The default is immediately taken on all query user rules and heuristics that are present in the assigned polices.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 63:

The Certkiller security administrator is viewing the audit trail in the CSA MC.
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
E. None of the above

Answer: D

Explanation:
Accessible from the Reports drop-down list in the menu bar, the Audit Trail page displays a list of changes administrators have made to the CSA MC database. These changes are displayed according to the following information:
The change itself.
The type of change (configuration category: policies, file sets, groups, and so on).
The date and time the change was made.
The administrator who made the change.
Click the Change Filter link to edit the audit trail viewing parameters according to the following:
Start date (enter date parameters using the same formats as in the Event Log).

End date.
The administrator who made the changes.
The change type (configuration category: policies, file sets, groups, and so on).
The number of changes to display per viewing page.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 64:

The Certkiller security Administrator wants to view the most recent events on the CSA MC. 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
E. None of the above

Answer: B

Explanation:
Similar to the Event Log, the Event Monitor, available from the Events category in the menu bar, lets you view system events provided by registered agents according to designated severity levels, and the host that generated the event. You can also enter the number of events to be displayed (default value is the last 50 events). Click the Change link to access a pop-up window from which you can edit these values and change the event filter.
Unlike the Event Log page, the Event Monitor page automatically refreshes itself at set intervals. The event list is updated with the latest events each time the page refreshes. The footer of this page provides a Refresh button and a Pause button. Use the Refresh button to refresh the page immediately without waiting for the set refresh interval to occur. Use the Pause button to immediately stop the page from refreshing. The set refresh interval will then stop at wherever it is in the countdown. This pause feature is useful when you are testing policies and you want to mark a certain place as a starting point for receiving new events. When you click it, the Pause button becomes a Resume button.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 65:

The Certkiller security administrator is viewing the log files in the CSA MC. Which information is logged for file access control rules?

A. Port and direction
B. Registry key
C. Process path
D. PROGID/CLSID
E. All of the above

Answer: C

Explanation:
The CSA MC Event Log does not contain every occurrence of an event from a system.
Duplicate events are not logged for an hour after the first occurrence.
The following information is logged for each rule type.
File access control logging-Process path and file names and file operation are logged.
Network access control logging-Process path, network address, port and direction are logged.
Registry access control logging-Process path and registry key are logged.
COM component access control logging-Process path and COM component PROGID/CLSID are logged.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

QUESTION 66:

The Certkiller security administrator is viewing the logs in the CSA MC. What information is logged for registry access control?

A. Port and direction
B. Registry key
C. Registry access events
D. PROGID/CLSID
E. All of the above

Answer: B

Explanation:
How Logging Works:
The CSA MC Event Log does not contain every occurrence of an event from a system.
Duplicate events are not logged for an hour after the first occurrence.
The following information is logged for each rule type.
File access control logging-Process path and file names and file operation are logged.
Network access control logging-Process path, network address, port and direction are logged.
Registry access control logging-Process path and registry key are logged.
COM component access control logging-Process path and COM component PROGID/CLSID are logged.

A duplicate event is defined as follows:
For file access controls , the name of the application and the file being accessed are the same.
For network access controls, the name of the application, the remote address, and the network service port are the same.
For registry access controls, the name of the application and the registry key name and value name are the same.
For COM component access controls, the name of the application and the COM component PROGID or CLSID are the same.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 67:

The Certkiller CSA MC administrator wants to log all of the deny actions. When you choose the Log All Deny Actions option within a group, how are deny actions logged?

A. Deny actions are logged every 5 minutes
B. Deny actions are logged every 10 minutes
C. Every deny action is logged regardless of the specific rule settings
D. Only those deny actions that are configured within specific rules are logged
E. None of the above

Answer: C

Explanation:
Enable Log all deny actions to turn on logging for all deny rules running on hosts within the group regardless of the individual rule settings for the policy attached to the group. You may wish to use this feature to turn on all deny logging for diagnostic purposes.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008042

QUESTION 68:

The Certkiller security administrator needs to view specific events in the CSA MC. 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

Explanation:
The Event Log view, available from the Events category in the menu bar, lets you view system events provided by registered agents according to designated time frames, event severity levels, and the system that generated the event.
The information displayed at the top of the Event Log page (controlled by the settings in the Change Filter window, see next section) tells you the following:
Filter by eventset: This displays the name of the Event Set, if any, used to filter the event log view.
or Define a filter with the following parameters:
Time range: This is the current time range set for the event log filter.
Severity: This is the current minimum and maximum severity range set for the event log filter.
Host: This displays which hosts have generated the events viewable in the event log (set as part of the filter).
Rule Module: From the pulldown list, select a rule module to search for events generated by that module.
Rule ID: Enter the ID number for a rule to search for events generated by that rule.
Events per page: This is the current value set for the number of events displayed on each page of the event log (set as part of the filter).
Filter text: Enter a text string here to either include or exclude in your event message search.
Filter out similar events: When event filtering is enabled (it's enabled by default), the event log displays an aggregation of events.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a

---

QUESTION 69:

The Certkiller security administrator wants to view CSA events in the MC. 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
F. None of the above

Answer: A

Explanation:

Status Summary

Status Summary-When you first login, the Status Summary view appears. This page supplies overall system summary information including recorded events and agent rule versions. You can access this page at any time by selecting it from the Events category in the menu bar. The various summary categories available from this page are as follows.

Network Status

By default, items in the Network Status category do not appear in the list if their number is 0. Simply expand the Network Status view to see all available status items. The status items listed here generally have to do with overall host statistics such as hosts that are not running with up-to-date software versions or the latest rule programs. You can view the number of hosts running in test mode or learn mode, etc. Additionally, the numbers that appear in this status section are clickable and take you to a list of the hosts that comprise that number.

Most Active

Use the links available in the Most Active section to view the Hosts, Rules, Applications, or Rule/Application pairs that have been the most active or triggered the most (logged the most events to the MC). This information is useful to help you tune your policies for rules that are being tripped too often. This can also alert you to common unwanted occurrences that may be triggering across your enterprise. Additionally, you can purge the events that appear in these lists.

Event Counts Per Day

A colored graph displays the event log according to severity level. Click on a color in the graph to view logged events of that severity level.

Database Maintenance

If there is an alert present in the Database Maintenance category, we recommend that you access the Database Maintenance page from Maintenance in the menu bar and shrink the database.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a00805a