



Exam : 643-531

Title : Cisco Secure Intrusion Detection Systems

Ver : 11-08-07

QUESTION 1

Which statement is true regarding the IDS Sensor communications?

- A. RDEP uses SSL for secured internal communications.
- B. RDEP uses SSH for secure external communications.
- C. PostOffice protocol uses IPSec for secured external communications.
- D. IDAPI uses HTTPS for secured internal communications.
- E. cidCU uses SSH for secured external communications.

Answer: A

Explanation:

Data Acquisition

The Cisco IDS RDEP Info Mediator acquires data from the RDEP server across a secure TCP link using SSL. This data is held in IDIOM XML format (Cisco's XML format). The Cisco IDS RDEP Info Mediator parses the data into events and sends them to the Cisco Info Server.

B RDEP does not use SSH for external communications

C PostOffice protocol does not encrypt

PostOffice Features

The PostOffice protocol provides a critical communication link between your Director platform and your IDS sensors. Being the primary method of communication, the PostOffice protocol must support certain necessary functionality:

- Reliability
- Redundancy
- Fault tolerance

D IDAPI I COULDN'T FIND ANYTHING ABOUT IDAPI AND HTTPS

E and nothing for E

Reference:

http://www.cisco.com/en/US/products/sw/netmgmtsw/ps996/products_technical_reference_chapter09186a00801c847a.html

QUESTION 2

What is the purpose of the PuTTYgen utility in IDS MC?

- A. Generates SSL certificates for IDS Sensors.
- B. Generates SSH public and private keys for IDS Sensors.
- C. Generates SSH public and private keys for IDS MC server.
- D. Generates shared secret keys for IDS Sensors and IDS MC server.
- E. Generates SSL keys for administrative client access to IDS MC server.

Answer: C

Explanation:

To use SSH keys in IDS MC or Security Monitor, follow these steps:

Step 1 To use SSH keys in IDS MC or Security Monitor for Windows 2000, follow these steps:

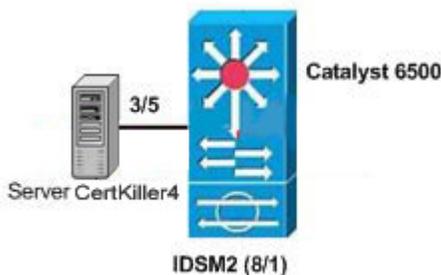
- Use PuttyGen to generate your keys. Instructions are available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html> .
- Copy the public key to the sensor's `~.ssh/authorized_keys` file.
- Save the private key. We recommend the name `sensorname.key` for the private key and we use it in this example.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d972.html

QUESTION 3

Exhibit:



Refer to the exhibit. Server Certkiller 4 is in VLAN 8. The Catalyst 6500 is running Catalyst OS. Which command represents a valid configuration step to permit the IDS M2 to monitor traffic sent to and from VLAN3, VLAN4, and VLAN5?

- `6500(config)# monitor session 1 source vlan 3, 4, 5`
- `6500(config)# monitor session 1 source 3-5 both`
- `6500(config)# monitor session 1 destination idsm`
- `6500>(enable) set span 3 -5 8/1 both`
- `6500>(enable) set span source vlan-list 3 - 5 destination interface 8/1 both create`

Answer: A

Explanation:

`Switch(config)# monitor session {session_number} {source {interface type/num} | {vlan vlan_ID}} [, | - | rx | tx | both]`

Specifies the SPAN session number (1 through 6), the source interfaces (FastEthernet or GigabitEthernet), or VLANs (1 through 1005), and the traffic direction to be monitored.

Reference:

Configuring SPAN

QUESTION 4

Match the most appropriate filtering method to the capture configuration that restricts the VLANs monitored on a trunk port. Use each option only once.

Clear trunk and set trunk commands	place here
filter keyword in set rspan command	place here
allow vlan keyword in switchport capture command	place here
filter keyword in monitor session command	place here

Use these

Catalyst OS using remote SPAN	Catalyst IOS using remote SPAN
Catalyst OS using VACLs	Catalyst IOS using mls ip ids

Answer:

Clear trunk and set trunk commands	Catalyst OS using VACLs
filter keyword in set rspan command	Catalyst OS using remote SPAN
allow vlan keyword in switchport capture command	Catalyst IOS using remote SPAN
filter keyword in monitor session command	Catalyst IOS using mls ip ids

Comment:

Clear trunk and set trunk commands -----> [Catalyst OS using VACLs]

filter keyword in set rspan command ---> [Catalyst OS using remote SPAN]

allow vlan keyword in switchport capture command ----> [Catalyst IOS using remote SPAN]

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/span.pdf

Section : Local SPAN and RSPAN Guidelines and Restrictions

filter keyword in monitor session command -----> [Catalyst IOS using mls ip ids]

Refer to :http://psyber.letifer.org/downloads/priv/cisco_switch_commands.pdf

QUESTION 5

Which type of signature engine is characterized by single packet conditions?

- A. other
- B. string
- C. atomic
- D. traffic

Answer: C

Signature Structure

As previously discussed, signature implementations deal with packet headers and packet payloads. The structure of the signatures deals with the number of packets that must be examined to trigger an alarm. Two types of signature structures exist and these are as follows:

- Atomic
- Composite

Atomic Structure

Some attacks can be detected by matching IP header information (context based) or string information contained in a single IP packet (content based). Any signatures that

can be matched with a single packet fall into the atomic category. Because atomic signatures examine individual packets, there's no need to collect or store state information.

An example of an atomic signature is the SYN-FIN signature (signature ID 3041).

This signature looks for packets that have both the SYN and FIN flags set. The SYN flag indicates this is a packet attempting to begin a new connection. The FIN flag indicates this packet is attempting to close an existing connection. These two flags shouldn't be used together and, when they are, this is an indication some intrusive activity might exist.

QUESTION 6

Which protocol does the Monitoring Center for Security use to monitor alarms on a PIX Firewall?

- A. SSL
- B. SSH
- C. Syslog
- D. PostOffice
- E. Not supported (Security Monitor does not support this platform)

Answer: C

Explanation:

Adding a PIX Firewall or Cisco IDS Host Sensor

PIX Firewalls and Cisco IDS Host Sensors use syslog messages to communicate with Security Monitor.

You do not have to add syslog devices because Security Monitor monitors all syslog traffic on the UDP port. However, if you want the syslog device name to appear in reports (instead of the device IP address), add the device configuration to Security Monitor.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3991/products_user_guide_chapter09186a008018d92b.html#881443

QUESTION 7

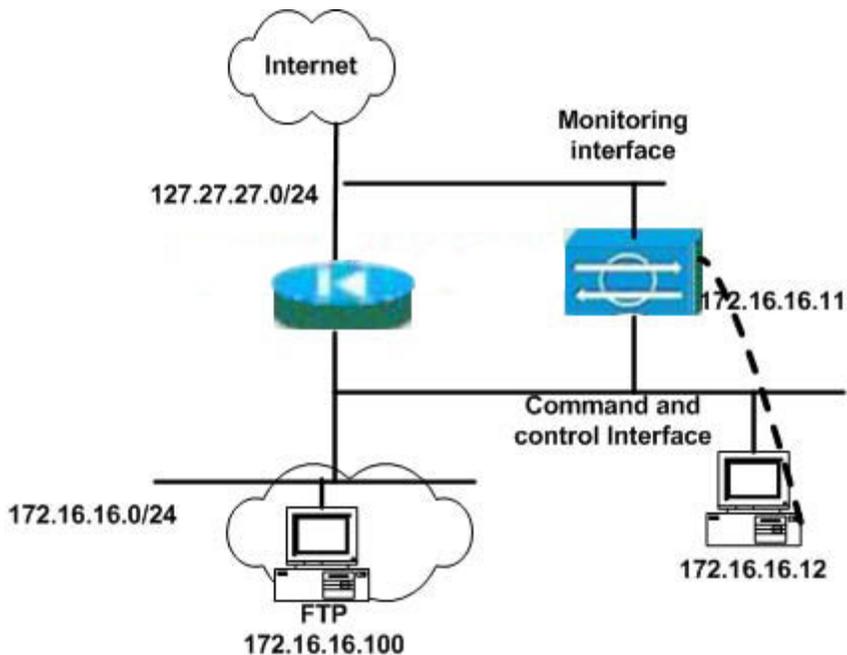
You have recently been employed by Certkiller . You have inspected the configuration of Certkiller 's IDS-4215 Sensor. You decide to modify access on user accounts and return some of the system's parameters to a known baseline by performing the following actions:

- 1) Create a backup of the running configuration to a remote FTP server.
- 2) Verify existing accounts and access privileges.
- 3) Delete the service account.
- 4) Reduce the access rights of your assistant, Certkiller, from administrative access to one that can only monitor IDS events and tune IDS signatures.
- 5) Return all SERVICE HTTP signatures to their default settings.

Use the information in the following table to complete these tasks.

CISCO IDS Parameters	Settings
Sensor administrator	CertKiller/CertKiller1636

username/password		
FTP server address		172.16.16.100
FTP username/password		admin/password2
FTP upload directory		/CertKiller5287
Bac	file name	
sistant's account user ID		CertKiller



Click on the picture of the host connected to an IDS Sensor by a serial console cable.

Answer:

login: Certkiller

password: Certkiller 1636

sensor#

1.sensor# copy current-config ftp://admin@172.16.16.100/ Certkiller 5287/backup-cfg

password: password2

2. sensor# show user all

3. sensor# config terminal

sensor(config)#no username service(service is the username for service account)

4.sensor(config)# privilege user Certkiller operator

5.sensor(config)#service virtual-sensor-configuration VirtualSensor

sensor(config-vsc)#reset service.http all

Comments:

1/Login to the sensor

```
Username: Certkiller
password: Certkiller 1636
Sensor#
2/Backup the current configuration
Sensor#copy current-config backup-cfg <ENTER>
3/Backup the file to a ftp server
Sensor#ftp://admin@172.16.16.100/ Certkiller 5287/backup-cfg <ENTER>
4/List all accounts
Sensor#show users all <ENTER>
...
5/Remove service account
Sensor# configure terminal <ENTER>
Sensor(config)# no username <service account> service <ENTER>
6/Modify Certkiller user right
Sensor(config)# username Certkiller privilege viewer <ENTER>
7/Modify signature
Sensor# cd /usr/nr/bin
Sensor#.SigWizMenu
-----
Current Sig Data File '/usr/nr/etc/SigData.conf'
Current Sig User File '/usr/nr/etc/SigUser.conf'
Current Settings File '/usr/nr/etc/SigSettings.conf'
-----
1 - Tune Signature Parameters
2 - Add NEW Custom Signature
3 - Set Custom Signature Severity/Action
4 - Edit Signature Address Mapping
5 - Delete Signature Tunings and Custom Signatures
6 - Other 3.x Tokens
7 - Display Signatures
8 - Global Settings
x - EXIT
```

QUESTION 8

Which signature engine would be the best choice when creating a signature to examine EIGRP packets, which uses protocol number 88?

- A. SERVICE.GENERIC
- B. ATOMIC.L3.IP
- C. OTHER
- D. ATOMIC.IPOPTIONS
- E. ATOMIC.IP.ROUTING

Answer: B

Explanation:

ATOMIC.L3.IP is a general-purpose Layer 3 inspector. It can handle DataLength and Protocol Number comparisons. It also has some hooks for fragment and partial ICMP comparisons. None of the parameters are required, so a simple signature meaning "any IP packet" can be written.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_installation_and_configuration_guide_chapter09186a008014a214.html

QUESTION 9

Which command does a Catalyst switch running Catalyst OS use to block attacks, as directed by an IDS blocking Sensor?

- A. acl
- B. shun
- C. conduit
- D. access-list
- E. set security acl

Answer: D

Explanation:

If you configure the sensor for blocking, every VLAN you configure is controlled solely by the sensor, even if no blocks are applied. The default VACL used by the sensor sets permit ip any any as the last entry in the VACL. You cannot restrict or configure the sensor-controlled switch directly with VACLs, and all traffic not being currently blocked will be allowed through the switch on the controlled interface.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/13870_01.htm#xtocid22

QUESTION 10

Which two methods are available to retrieve Sensor IP logs for analysis? (Choose two)

- A. Copy using FTP
- B. Import to IDS MC
- C. Download via IDM
- D. Archive using SCP
- E. Upload using Security Monitor

Answer: B

Explanation:

Downloading IP Logs

The Ip Logs page displays all IP logs that are available for downloading on the system. There is a hyperlink to each log file that is available for download. First, you have to turn on IP logging from Administration > IP Logging. The results of what you configure on that page

show up in the list on the Ip Logs page. for the procedure. You can also generate IP logs by setting a signature's EventAction to log. When the sensor detects an attack based on this signature, it automatically creates an IP log.

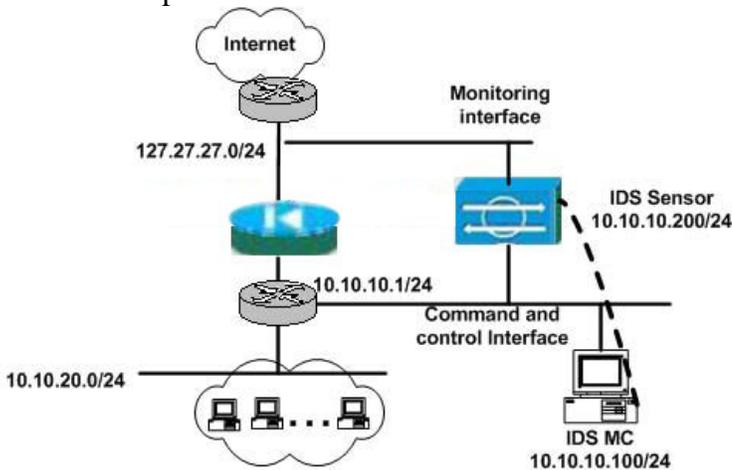
Exporting Event Logs. Exporting Event logs configuration panel can be used to configure the automatic exporting of event logs to an FTP server.

QUESTION 11

You are a network security at Certkiller Inc. Certkiller is installing new Cisco IDS Sensors. Your responsibility is to configure the new Sensors to permit remote access only from trusted hosts. Perform this task on one of the Sensors using the command line interface (CLI). Refer to the following information and network topology graphic to permit access from the IDS MC management station only to the Sensor. Since this is a new installation, you must remove the default allowed network address. Important: Verify your configuration setting prior to saving, and then save your configuration when finished.

Cisco IDS Parameters	Settings
Sensor operator username/password	operator/CertKiller1636
Sensor administrator username/password	admin/CertKiller1636
Sensor IP address:	10.10.10.200/24
Default allowed network address:	10.0.0.0/8

Click on the picture of the host connected to an IDS Sensor by a serial console cable.



Answer:

It exists two ways to configure sensor's access control list:

- With the Configuration Utility (sysconfig-sensor) with root access
- In Command Line like a router (config terminal, ...) with operator access

Answer 1:

1/ Login to the sensor

Username:admin

password: Certkiller 1636

2/ Run sysconfig-sensor

#sysconfig-sensor

IDS Sensor Initial Configuration Utility

Choose a value to configure on of the following paramters:

1 - IP Address

2 - IP Netmask

3 - IP Host Name

4 - Default Route

5 - Access Control List

6 - Communications Infrastructure

7 - Date/Time and Time Zone

8 - Passwords

9 - Secure Communications

10- Display

x - Exit

Selection: 5 <ENTER>

3/ Enter the default netmask (10.)

Access Control List

You can modify the list of IP address and networks that are allowed to log into the sensor. A TCP Wrapper application enforces this list.

If a host with an IP address that is not in this list attempts to log into the Sensor, the

TCP connection will automatically be closed.WARNING: If you have changed the IP address of Sensor,

list the host addresses from which you log in remotely.

This list must contain only host IP address and not host names. The Sensor by default does not use ANY type of name service (for example, DNS, NIS, NIS+).

List the network addresses with just the network portion of the address. For example: 192.9.200.

Current list:

10.

Enter an address to add to the list. If the address entered is already in the list, it will be deleted from it.

IP address:: 10. <ENTER>

4/Save the configuration

Write network acces control configuration to disk (y/n)? Y <ENTER>

5/Exit

IDS Sensor Initial Configuration Utility

Choose a value to configure on of the following paramters:

1 - IP Address

2 - IP Netmask

- 3 - IP Host Name
- 4 - Default Route
- 5 - Access Control List
- 6 - Communications Infrastructure
- 7 - Date/Time and Time Zone
- 8 - Passwords
- 9 - Secure Communications
- 10- Display
- x - Exit

Selection: x <ENTER>

Answer 2:

- a. Enter configure terminal mode:
sensor# configure terminal
- b. Enter host configuration mode:
sensor(config)# service host
- c. Enter network parameters configuration mode:
sensor(config-Host)# networkParams
- d. View the current settings:
sensor(config-Host-net)# show settings
networkParams

ipAddress: 10.10.10.200
netmask: 255.255.255.0 default: 255.255.255.0
defaultGateway: 10.10.10.1
hostname: sensor
telnetOption: disabled default: disabled
accessList (min: 0, max: 512, current: 1)

- ipAddress: 10.0.0.0
netmask: 255.0.0.0 default: 255.255.255.255
- e. Remove the 10.0.0.0 network from the access list:
sensor(config-Host-net)# no accessList ipAddress 10.0.0.0 netmask 255.0.0.0
- f. Verify the change
ensor(config-Host-net)# show settings
networkParams

ipAddress: 10.10.10.200
netmask: 255.255.255.0 default: 255.255.255.0
defaultGateway: 10.10.10.1
hostname: sensor
telnetOption: disabled default: disabled
accessList (min: 0, max: 512, current: 0)

- g. Exit network parameters configuration mode:
sensor(config-Host-net)# exit

sensor(config-Host)#exit
Enter yes to apply the changes.

QUESTION 12

Given these signature engines, which would be the best choice when creating a signature to detect intruders that are scanning for open port number 80 using stealth scanning techniques?

- A. ATOMIC.TCP
- B. SERVICE.TCP.HTTP
- C. ATOMIC.IPORTIONS
- D. SERVICE.HTTP

Answer: A

Explanation:

ATOMIC.TCP Engine Parameters

Table A-9 lists the ATOMIC.TCP engine parameters.

Table A-9 ATOMIC.TCP Engine Parameters

Parameter Name	Data Type	Protected	Required	Description
DstPort	NUMBER (0-65535)	No	No	A single Destination Port to match.
Mask	BITSET (FIN SYN RST PSH ACK URG ZERO)	No	Yes	The mask used in TcpFlags comparison.
PortRange	NUMBER (0-2)	No	No	The destination port: Only Low Ports (1), Only High Ports (2), or All. (0)
PortRangeSource	NUMBER (0-2)	No	No	The source port: Only Low Ports (1), Only High Ports (2), or All (0).
SinglePacketRegex	STRING	No	No	A regular expression to search for in a single TCP packet.
SrcPort	NUMBER (0-65535)	No	No	A single Source Port to match.
TcpFlags	BITSET (FIN SYN RST PSH ACK URG ZERO)	No	Yes	The TCP Flags to match when masked by Mask.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_installation_and_configuration_guide_chapter09186a008014a214.html#787365

QUESTION 13

Which type of attack is characterized by an intruder targeting networks or systems to retrieve data or escalate their privileges?

- A. Access attack
- B. Reconnaissance attack
- C. Denial of Service attack

D. Authorization attack

Answer: A

Access Attacks

Access is a broad term used to describe any attack that requires the intruder to gain unauthorized

access to a secure system with the intent to manipulate data, elevate privileges, or simply access the system. The term "access attack" is used to describe any attempt to gain system access, perform data manipulation, or elevate privileges.

System Access Attacks System access is the act of gaining unauthorized access to a system for which the attacker doesn't have a user account. Hackers usually gain access to a device by running a script or a hacking tool, or exploiting a known vulnerability of an application or service running on the host.

Data Manipulation Access Attacks Data manipulation occurs when an intruder simply reads, copies, writes, deletes, or changes data that isn't intended to be accessible by the intruder. This could be as simple as finding a share on a Windows 9x or NT computer, or as difficult as attempting to gain access to a credit bureau's information, or breaking into the department of motor vehicles to change a driving record.

Elevating Privileges Access Attacks Elevating privileges is a common type of attack. By elevating privileges an intruder can gain access to files, folders or application data that the user account was not initially granted access to. Once the hacker has gained a high-enough level of access, they can install applications, such as backdoors and Trojan horses, to allow further access and reconnaissance. A common goal of hackers is to

QUESTION 14

Which user account role on a Cisco IDS Sensor allows a user to perform all Sensor operations?

- A. Operator
- B. Viewer
- C. Service
- D. Administrator

Answer: D

Explanation:

User Roles

The CLI for IDS version 4.0 supports three user roles: Administrator, Operator, and Viewer. The privilege levels for each role are different; therefore, the menus and available commands vary for each role.

- Administrators-This user role has the highest level of privileges. Administrators have unrestricted view access and can perform the following functions:
 - o Add users and assign passwords.
 - o Enable and disable control of physical interfaces and interface groups.
 - o Assign physical sensing interfaces to interface groups.

- o Modify the list of hosts allowed to connect to the sensor as configuring or viewing agents.
- o Modify sensor address configuration.
- o Tune signatures.
- o Assign virtual sensor configuration to interface groups.
- o Manage routers.
- Operators-This user role has the second highest level of privileges. Operators have unrestricted view access and can perform the following functions:
 - o Modify their passwords.
 - o Tune signatures.
 - o Manage routers.
- Viewers-This user role has the lowest level of privileges. Viewers can view configuration and event data and can perform the following function:
 - o Modify their passwords.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_command_reference_chapter09186a0080147174.html#699963

QUESTION 15

Which is one method of communication between IDS Event Viewer and the IDS device?

- A. HTTPS
- B. SSH
- C. IPSec
- D. PostOffice

Answer: A

Explanation:

To specify the communication protocol IDS Event Viewer should use when connecting to the sensor, select the Use encrypted connection (https) or Use non-encrypted connection (http) radio button.

Reference:

Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1

QUESTION 16

Which signature description best describes a string signature engine?

- A. Network reconnaissance detection.
- B. Regular expression-based pattern inspection for multiple transport protocols.
- C. Layer 5, 6, and 7 services that require protocol analysis.
- D. State-based, regular expression-based, pattern inspection and alarm functionality for TCP streams.

Answer:

Explanation:

About STRING Engines

The STRING engine provides regular expression-based pattern inspection and alarm functionality for multiple transport protocols including TCP, UDP and ICMP.

Regular expressions are a powerful and flexible notational language that allow you to describe text. In the context of pattern matching, regular expressions allow a succinct description of any arbitrary pattern. Regular expressions are compiled into a data structure called a pattern matcher, which is then used to match patterns in data.

The STRING engine is a generic string-based pattern matching inspection engine for TCP, UDP, and ICMP protocols. This STRING engine uses a new Regex engine that can combine multiple patterns into a single pattern-matching table allowing for a single search through the data. The new regex has the alternation "|" operator also known as the OR operator. There are three STRING engines: STRING.TCP, STRING.UDP, and STRING.ICMP.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_installation_and_configuration_guide_chapter09186a008014a214.html#788540

QUESTION 17

Exhibit:

	Parameter Name	Value	Default	Required
13	<input type="radio"/> Protocol	TCP	TCP	Yes
14	<input type="radio"/> RegexString			Yes
15	<input type="radio"/> ResetAfterIdle	15	15	No
16	<input type="radio"/> ServicePorts	80,3128,8000,9010,8080,8888	80,3128,8000,9010,8080,8888	Yes
17	<input type="radio"/> SigComment			No
18	<input type="radio"/> SigStringInfo			No
19	<input type="radio"/> SigVersion			No
20	<input type="radio"/> StorageKey	STREAM	STREAM	Yes

Refer to the exhibit. To create a custom signature that detects the word "Classified Information" circulating in email and FTP communications, choose the STRING.TCP signature engine to create the custom signature.

Which two parameters must be customized to detect the desired information? (Choose two)

- A. SigStringInfo
- B. SigComment
- C. RegexString
- D. StorageKey
- E. ServicePorts

Answer: C

Explanation:
STRING Engine Parameters

Table A-37 lists the STRING engine parameters.

Table A-37 STRING Engine Parameters

Parameter Name	Data Type	Protected	Required	Description
Direction ¹	BOOLEAN	Yes	Yes	Indicates whether to inspect traffic destined to or coming from the service ports.
EndMatchOffset	NUMBER	Yes	No	The exact stream offset in bytes that the RegexpString must use to report the match.
MinMatchLength ²	NUMBER	Yes	No	The minimum number of bytes the RegexpString must match.
RegexpString ³	STRING	Yes	Yes	The Regular Expression pattern.

Parameter Name	Data Type	Protected	Required	Description
ServicePorts	SET	No	Yes	A comma-separated list of ports or port ranges where the target service may reside.
StripTelnetOptions	BOOLEAN	Yes	No	Strips the Telnet option control characters from the data stream before the pattern is searched. Primarily used as an IDS anti-evasion tool.

1. ToService or FromService.

2. This parameter requires the regular expression to have a repetition operator such as * or +, otherwise it is rejected. RegexpStrings without repetition are fixed length and always have the same match length.

3. The RegexpString needs to be a string in the form of a regular expression.

Reference:

Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.0

QUESTION 18

Which best describes a required signature parameter attribute?

- A. The default signature parameter value cannot be changed.
- B. The signature parameter value cannot be modified for custom signatures.
- C. The signature parameter must be defined for all signatures.
- D. The signature parameter value can be defined for custom signatures only.

Answer: C

Explanation:

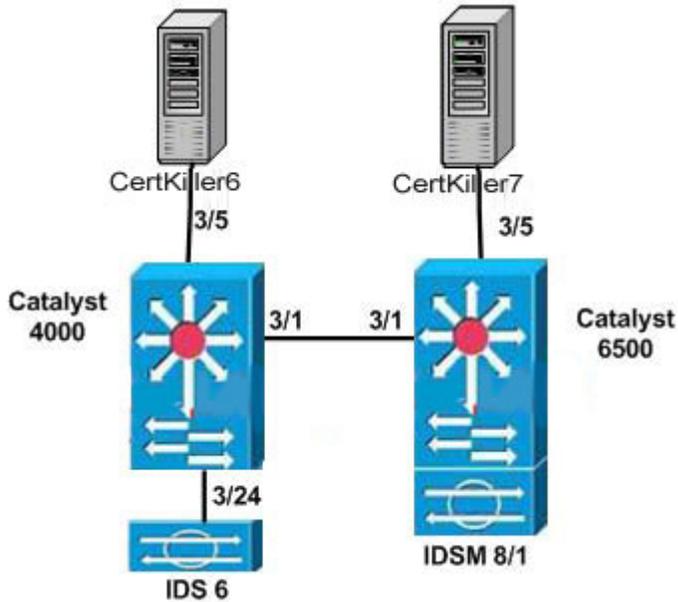
If a parameter is required, you must define it for all signatures-both default signatures and custom signatures.

Reference:

Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.0

QUESTION 19

Exhibit:



Refer to the exhibit. All switches are connected through Fast Ethernet connections. The RSPAN VLAN is 99. Both the Catalyst 4000 and Catalyst 6500 are running Catalyst OS. Which command represents a valid configuration step to permit Sensor IDS6 to monitor traffic sent to Server Certkiller 7?

- A. 6500(config)# remote-span 99
- B. 6500>(enable) set rspan source 3/5 99 tx create
- C. 4000>(enable) set rspan source vlan 99 destination interface fastEthernet 3/24
- D. 4000>(enable) set rspan destination 99 3/24
- E. 4000>(config)# monitor session 2 destination interface fastEthernet 3/24

Answer: B

Explanation:

Configuring RSPAN from the CLI

The first step in configuring an RSPAN session is to select an RSPAN VLAN for the RSPAN session that does not exist in any of the switches that will participate in RSPAN. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in the VTP domain.

Use VTP pruning to get efficient flow of RSPAN traffic or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

Once the RSPAN VLAN is created, you configure the source and destination switches using the set rspan command.

To configure RSPAN source ports, perform this task in privileged mode:

	Task	Command
--	------	---------

Step 1	Configure RSPAN source ports. Use this command on each of the source switches participating in RSPAN.	set rspan source { <i>mod/ports... vlans...sc0</i> } { <i>rspan_vlan</i> } [rx tx both] [multicast { enable disable }] [filter <i>vlans...</i>] [create]	
---------------	---	--	--

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007f323.html

QUESTION 20

What are two basic types of Cisco IDS signature parameters? (Choose two)

- A. Protected
- B. Master
- C. Sub-signature
- D. Local
- E. Required

Answer: B C

QUESTION 21

Which three are Sensor servlets that leverage the IDS Sensor's cidWebServer application? (Choose three)

- A. IEV
- B. IDM
- C. IDS MC
- D. IPlog Server
- E. IPfilter Server
- F. Transaction Server

Answer:

QUESTION 22

Which command does a PIX Firewall use to block attacks, as directed by an IDS blocking Sensor?

- A. acl
- B. shun
- C. conduit
- D. access
- E. set security acl ip

Answer: B

Explanation:

PIX Firewall

You can configure sensors can to use the PIX Firewall to block hosts. A new API command on the PIX Firewall has been created, shun [ip], which tells the PIX Firewall which hosts to block. Existing PIX Firewall ACLs are not altered by device management. You cannot use preshun or postshun ACLs for the PIX Firewall, instead you must create ACLs directly on the PIX Firewall.

The PIX Firewall does not support the ShunNet command. Therefore, do not send a ShunNet to sensors that control PIX Firewalls. Instead, you can manually configure the ACLs on the PIX Firewall to deny the network that is to be blocked. If the sensor controls other devices in addition to a PIX Firewall, you can send a ShunNet to the sensor, but you must also manually configure the PIX Firewall to ensure that the network is blocked by all devices controlled by the sensor. Be aware that any ShunHost that contains a host address that belongs to the network specified in the ShunNet command does not cause an update to any of the devices controlled by the sensor. Device Management does not update the device ACLs if the blocked host is already covered by a ShunNet.

The PIX Firewall in particular does not attempt to block that host even though it does not support the ShunNet command.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/13870_01.htm#xtocid23

QUESTION 23

What type of evasive technique is characterized by sending control characters to disguise an attack?

- A. Flooding
- B. Fragmentation
- C. Obfuscation
- D. Exceeding maximum transmission unit size

Answer: C

Explanation:

Intrusion Detection Systems inspect network traffic for suspect or malicious packet formats, data payloads and traffic patterns. Intrusion detection systems typically implement obfuscation defense - ensuring that suspect packets cannot easily be disguised with UTF and/or hex encoding and bypass the Intrusion Detection systems. Recently, the CodeRed worm has targeted an unpatched vulnerability with many MicroSoft IIS systems and also highlighted a different encoding technique supported by MicroSoft IIS systems.

Reference:

http://www.cisco.com/en/US/products/products_security_advisory09186a00800b139f.shtml

QUESTION 24

How is automatic IP logging enabled on Sensor?

- A. It is enabled by default for all signatures.
- B. It is enabled by default for all master signatures only.
- C. It is enabled by default for all high-severity signature alarms.
- D. It must be manually configured for individual signatures.

Answer: D

Explanation:

Attacks or other misuses of network resources can be defined as network intrusions. Network intrusions can be detected by sensors that use a signature-based technology. A signature is a set of rules that your sensor uses to detect typical intrusive activity, such as denial of service (DoS) attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define.

The sensor compares the list of signatures with network activity. When a match is found, the sensor takes an action, such as logging the event or sending an alarm to IDS Event Viewer. Sensors allow you to modify existing signatures and define new ones.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. For example, some network applications or operating systems may send out numerous ICMP messages, which a signaturebased detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by tuning your sensors.

To configure a sensor to monitor network traffic for a particular signature, you must enable the signature. By default, the most critical signatures are enabled when you install IDS Device Manager. When an attack is detected that matches an enabled signature, the sensor generates an alert event (formerly known as an alarm), which is stored in the sensor's event store. The alert events, as well as other events, may be retrieved from the event store by web-based clients. By default the sensor logs all Informational alarms or higher. If you have added IDS Event Viewer as a destination, the alarm is sent to the IDS Event Viewer database and you can view the alarm in IDS Event Viewer.

Configuring IP Logging

You can configure a sensor to generate an IP session log when the sensor detects an attack. When IP logging is configured as a response action for a signature and the signature is triggered, all packets to and from the source address of the alarm are logged for a specified period of time. You can set the number of minutes events are logged.

Reference:

Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1

QUESTION 25

Which statement is true regarding the service account on an IDS Sensor?

- A. Only users with the administrator role can be assigned to the service account.
- B. The service account is used for advanced signature tuning operations.
- C. Cisco TAC personnel must create the service account.
- D. Only one user can be assigned to the service account.

Answer: D

Explanation:

Creating the Service Account

You should create a service account for TAC to use during troubleshooting. Although more than one user can have access to the sensor, only one user can have service privileges on a sensor. The service account is for support purposes only.

Caution Do not make modifications to the sensor through the service account except under the direction of TAC. If you use the service account to configure the sensor, your configuration is not supported by TAC. We do not support the addition and/or running of an additional service to the operating system through the service account, because it affects the proper performance and proper functioning of the other IDS services. TAC does not support a sensor on which additional services have been added.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_installation_guide_chapter09186a00801b0e31.html#271

QUESTION 26

Which protocol does an administrator use to communicate with the IDS MC Sensors from their desktop?

- A. Telnet
- B. RDEP
- C. IDAPI
- D. HTTP
- E. HTTPS

Answer: E

Explanation:

To specify the communication protocol IDS Event Viewer should use when connecting to the sensor, select the Use encrypted connection (https) or Use non-encrypted connection (http) radio button.

Reference:

Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1

QUESTION 27

How are IDS devices added into IDS Event Viewer?

- A. IDS devices are automatically discovered by IEV.
- B. IDS devices initiate a connection request to IEV.
- C. IDS devices must be manually entered into IEV.
- D. IDS device's alarms are automatically sensed by IEV.

Answer: C

Explanation:

Before IDS Event Viewer can receive events from a sensor, you must add the sensor to the list of devices that IDS Event Viewer monitors.

Reference:

Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1

QUESTION 28

From which partition can a Cisco IDS Sensor switch module be re-imaged?

- A. Application partition
- B. Recovery partition
- C. Maintenance partition for the blade
- D. Service partition

Answer: C

Explanation:

Re-imaging the IDS Module from the Maintenance Partition

You can re-image the IDS module from the maintenance partition. After you re-image the IDS module, you must initialize the IDS module using the setup command.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps5052/prod_release_note09186a008015e2d1.html#28249

QUESTION 29

Which feature of IDS Event Viewer provides detailed signature and vulnerability information?

- A. Cisco Secure Encyclopedia
- B. Cisco Network Security Encyclopedia
- C. Network Security Database
- D. Cisco Secure Network Database

Answer: C

Explanation:

• Network security database (NSDB)-The NSDB provides instant access to specific information about the attacks, hyperlinks, potential countermeasures, and related vulnerabilities. Because the NSDB is an HTML database, it can be personalized for each user to include operation-specific information such as response and escalation procedures for specific attacks.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_data_sheet09186a008014873f.html

QUESTION 30

What type of attack is most likely to result from the presence of a shared folder in a Windows operating system?

- A. Denial of Service Attack
- B. Access Attack
- C. Reconnaissance attack
- D. Man-in-the-middle

Answer: B

Explanation:

Access Attacks

Access is a broad term used to describe any attack that requires the intruder to gain unauthorized access to a secure system with the intent to manipulate data, elevate privileges, or simply access the system. The term "access attack" is used to describe any attempt to gain system access, perform data manipulation, or elevate privileges.

System Access Attacks System access is the act of gaining unauthorized access to a system for which the attacker doesn't have a user account. Hackers usually gain access to a device by running a script or a hacking tool, or exploiting a known vulnerability of an application or service running on the host.

Data Manipulation Access Attacks Data manipulation occurs when an intruder simply reads, copies, writes, deletes, or changes data that isn't intended to be accessible by the intruder. This could be as simple as finding a share on a Windows 9x or NT computer, or as difficult as attempting to gain access to a credit bureau's information, or breaking into the department of motor vehicles to change a driving record.

Reference:

CCSP Osborne page 810

QUESTION 31

Select the three true statements regarding the Master Blocking Sensor communications?
(Choose three)

- A. A Master Blocking Sensor can use Telnet to communicate with a PIX Firewall.
- B. A Blocking Forwarding Sensor uses SSH to communicate with a Master Blocking Sensor.
- C. An IDS v4.0 Sensor can server as a Master Blocking Sensor for IDS v3.x and IDS v4.0 Sensors.
- D. A Master Blocking Sensor can communicate block requests to another Master Blocking Sensor.
- E. A Master Blocking Sensor uses RDEP to communicate with a Blocking Forwarding Sensor.
- F. A Blocking Forwarding Sensor can communicate block requests to another Blocking Forwarding Sensor.

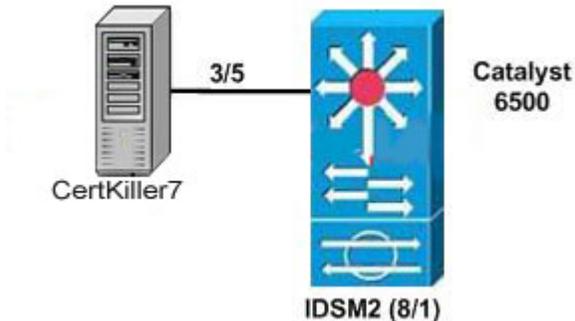
Answer: A B D

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_installation_and_configuration_guide_chapter09186a00801a0c57.html

QUESTION 32

Exhibit:



Refer to the exhibit.

Which command represents a valid configuration step to permit the IDSM-2 to monitor traffic sent to and from VLAN3, VLAN4, and VLAN5?

- A. 6500(config)# monitor session 1 source vlan 3, 4, 5 both
- B. 6500(config)# monitor session 1 destination idsm
- C. 6500>(enable) set span source vlan-list 3- 5 destination interface 8/1 both create
- D. 6500>(enable) set span 3 - 5 8/1 both
- E. This feature is not supported in this configuration.

Answer: A

Explanation:

Switch(config)# monitor session {session_number} {source {interface type/num} | {vlan vlan_ID}} [, | - | rx | tx | both]

Specifies the SPAN session number (1 through 6), the source interfaces (FastEthernet or GigabitEthernet), or VLANs (1 through 1005), and the traffic direction to be monitored.

Reference:

Configuring SPAN

QUESTION 33

Which communications protocol is used between the IDS Event Viewer and the Sensor?

- A. SNMP
- B. RDEP
- C. SSH
- D. IPSec

Answer: C

Explanation:

Configuring Secure Communications on the Sensor

You can configure the sensor to establish secure communications via Solaris IPsec or Secure Shell (SSH).

Note IPsec is supported on sensor version 2.5 or later, IDS Director version 2.2.2 or later, and CSPM version 2.3.i or later. The version 3.1 sensor can use SSH with the PIX Firewall.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/13870_01.htm#xtoci d16

QUESTION 34

Match the IDS process with its description.

Place here

processes signatures and generates alert events	place here
writes application error messages to Event Store	place here
used to block traffic on network devices	place here
communicates master blocking Sensor messages	place here
starts and stops all other IDS applications	place here

Use these

NAC	logApp
mainApp	SensorApp
ctITransSource	

Answer:

Place here

processes signatures and generates alert events	mainApp
writes application error messages to Event Store	logApp
used to block traffic on network devices	NAC
communicates master blocking Sensor messages	SensorApp
starts and stops all other IDS applications	ctITransSource

Explanation:

I used my best judgement and experience with the answers. I would advise the same with this question, because I could not find anything to backup my answers, except for NAC.

QUESTION 35

What should you do to properly add a Sensor to the IDS MC if the Sensor software version is not displayed in the drop-down list of available versions during the add process?

- A. Update IDS MC with the latest IDS signatures.
- B. Update the Sensor's software version to a version matching one in the IDS MC list.
- C. Select the Discover Settings check box to automatically discover the unlisted version.
- D. Manually enter the correct software version in the version field under the Sensor's

Identification window.

E. Use the Query Sensor option next to the version field under the Sensor's identification window to automatically discover the unlisted version.

Answer: C

Explanation:

. To retrieve sensor settings from the sensor, select the Discover Settings check box.

Note If you choose to discover settings, you may have to wait from 30 seconds to several minutes, depending upon the size and complexity of your network and its traffic.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a0080157f9d.html#79

QUESTION 36

Which information is required to add a Sensor to IDS MC if the Discover Settings check box is NOT selected?

- A. Correct IP address
- B. Correct user ID and password
- C. Correct Sensor name and SSH settings
- D. Correct user ID, password, and IP address
- E. Any legitimate values for IP address, Sensor name, user ID, and password

Answer: E

Explanation:

Step 5 Provide the information required by the Enter Sensor Information page:

- a. Enter the IP address of the sensor.
- b. Enter the NAT address of the sensor, if there is one.
- c. Enter the sensor name.
- d. To retrieve sensor settings from the sensor, select the Discover Settings check box.
Note If you choose to discover settings, you may have to wait from 30 seconds to several minutes, depending upon the size and complexity of your network and its traffic.
- e. Enter the user ID and password for Secure Shell (SSH) communications between your host and the sensor:
 - When you are using a sensor appliance, the user ID is netrangr, and the password is one that you assign.
 - When you are using an IDS module, the user ID is ciscoids, and the password is one that you assign.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a0080157f9d.html#79

QUESTION 37

Which must be configured on a Master Blocking Sensor in order to permit

communications with a Blocking Forwarding Sensor using encryption?

- A. The Blocking Forwarding Sensor's IP address.
- B. The Blocking Forwarding Sensor's SSH public key.
- C. The Allowed Hosts table must include the Blocking Forwarding Sensor.
- D. The TLS Trusted-Host table must include the Blocking Forwarding Sensor.
- E. No additional configuration is required to configure a Master Blocking Sensor.

Answer: C

Explanation:

Blocking with Multiple Sensors

Multiple sensors can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The sensor that is sending its block requests to the master blocking sensor is referred to as a "blocking forwarding sensor." On the blocking forwarding sensor, you must specify which remote host serves as the master blocking sensor. And on the master blocking sensor you must add the blocking forwarding sensors to its remote host configuration.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps5052/prod_configuration_guide09186a00800d9ddd.html#45095

QUESTION 38

What is the primary function of a Master Blocking Sensor?

- A. To serve as the central point of configuration in IDM for blocking.
- B. To serve as the central point of configuration in IDS MC for blocking.
- C. To directly communicate the blocking requests sent by other Sensors.
- D. To provide the first line of attack detection and prevention through blocking.

Answer: C

Explanation:

Multiple sensors can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The sensor that is sending its block requests to the master blocking sensor is referred to as a "blocking forwarding sensor." On the blocking forwarding sensor, you must specify which remote host serves as the master blocking sensor; on the master blocking sensor you must add the blocking forwarding sensors to its remote host configuration

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_installation_and_configuration_guide_chapter09186a008014a218.html#593675

QUESTION 39

Which is true regarding using IDS MC to upgrade a Cisco IDS Sensor?

- A. Update IDS MC prior to updating the Sensor.
- B. IDS MC can be used to update signature files only.
- C. IDS MC can be used to update service packs only.
- D. There are no special requirements for IDS MC.

Answer: D

Explanation:

To determine which version of sensor software is installed on the sensor, click Query Sensor; this action will update the information displayed by the Identification page if necessary. If you then click Apply, and the queried version is different from the current version, the configuration will be upgraded to the new version. If you click Cancel, no changes will be applied.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d985.html

QUESTION 40

Which protocol does the Monitoring Center for Security use to monitor alarms on an IDS v3.x Sensor?

- A. SSL
- B. SSH
- C. HTTP
- D. PostOffice

Answer: D

Explanation:

A sensor can monitor the services that are running on it. The sensor can generate audit events, as warnings, when a service goes down or cannot be restarted. This monitoring function, called Watchdog, helps you track the state and desired operation of your sensors. Watchdog is a feature of the postoffice service.

Watchdog checks the availability of services that are supposed to be running on the sensor and verifies that desired sensor-to-other network object communications (based on postoffice) are available. The Watchdog queries the services to see if they are operational, and if they are not, it issues warnings to the user and attempts to restart the services. You can specify the alarm levels of these warnings.

Additional postoffice settings that you can specify are the postoffice port and the heartbeat interval.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d985.html

QUESTION 41

Which best describes a protected signature parameter attribute?

- A. The default signature parameter value cannot be changed.
- B. The signature parameter value cannot be modified for custom signatures.
- C. The signature parameter value must be defined for all signatures.
- D. The signature parameter value can be modified for custom signatures only.

Answer: A

Explanation:

Protected-The protected attribute of the parameter applies only to the default signature set. When a default signature parameter is protected, its value cannot be modified meaning that the fundamental behavior of the default signature cannot be changed. For example, you can modify certain parameters (AlarmThrottle, ChokeThreshold, Unique) of default signatures, but not the underlying functionality, such as TcpFlags and Mask.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/prod_technical_reference09186a00800eea84.html

QUESTION 42

Which signature description best describes a service signature engine?

- A. Protocol analysis for layers 5, 6, and 7 applications.
- B. Inspects multiple transport protocols.
- C. Detects network reconnaissance.
- D. Identifies traffic irregularities.

Answer: A

Explanation:

SERVICE.* Engines

Use the SERVICE engines to create signatures that deal with the Layer 5+ protocol of the service. The DNS (TCP and UDP) engines support analysis of compressed messages and can fire alarms on request/reply conditions and overflows. The RPC and PORTMAP engines are fine tuned for RPC and Portmapper requests. Batch and fragmented messages are decoded and analyzed.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/prod_technical_reference09186a00800eea84.html

QUESTION 43

Which three IDS software components can be upgraded from IDS MC's Updates page?
(Choose three)

- A. IEV signatures
- B. IDS MC signatures
- C. IDS Sensor service packs

- D. IDS Sensor recovery partitions
- E. IDS Sensor version 3.x-4.x upgrades

Answer: B C E

Explanation:

Cisco Systems periodically releases updates of sensor software versions and signature release levels for its IDS Sensors (both sensor appliances and IDS modules). Two procedures are available:

- Updating IDS Sensor Software from 3.x to 4.x
- Updating IDS Sensor Software Other than from 3.x to 4.x

You should also understand the update files:

- Cisco releases its periodic updates of sensor software versions and signature release levels for its IDS Sensors in the form of update files that are compressed (.zip).

IDS MC works with these compressed files directly; you should not extract anything from them.

- There are two types of update files:

- o Service pack update files-You can identify service pack update files by their names: the letters "sp" precede the version number. When these update files are applied, they change the version number of a sensor. Service pack update files contain executable code; they affect the actual micro-engine software on the sensor. They also contain signature updates.

- o Signature update files-Signature update file names contain the letters "sig" before the version number. Signature update files contain newly released signatures but not executable code.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d985.html#894197

QUESTION 44

What are the methods for adding devices in the Management Center for IDS Sensors using the GUI interface?

- A. Manually add only
- B. Manually add or import from file
- C. Manually add or import from RME
- D. Manually add or import from security monitor
- E. Manually add or import from campus manager

Answer: A

Explanation:

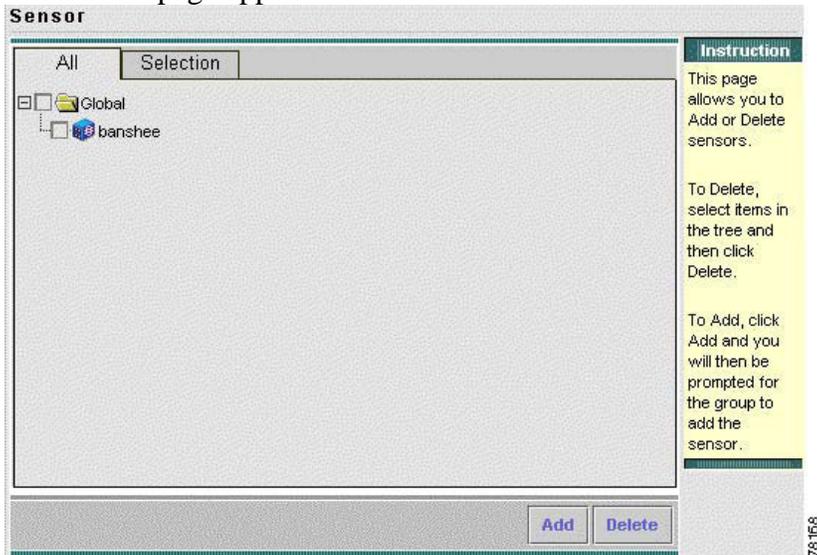
Adding Sensors to a Sensor Group

You can add a sensor to any sensor group, including the Global group.

To add a sensor to a sensor group, follow these steps:

Step 1 Select Devices > Sensor.

The Sensor page appears.



Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d972.html

QUESTION 45

Which two identify basic authentication methods for accessing a Sensor from IDS MC?
(Choose two)

- A. SSL certificates
- B. SSH public keys
- C. User account passwords
- D. Digital certificates with pre-shared keys
- E. Digital certificates with Certificate Authority

Answer: B C

Explanation:

Note SSH supports two forms of authentication: password and public key. If you have set up a public key between IDS MC and the sensor, you can use that key by selecting the Use Existing SSH keys check box. If you have not set up the key, or if you do not want to use it, leave the Use Existing SSH keys deselected, and IDS MC will use SSH password authentication.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d972.html

QUESTION 46

Match the IDS MC process with its description.

performs requested response, such as sending email	place here
generates all reports to be sent at a pre-defined time	place here
tales alarms and events and stores them in database	place here
processes event rules; request notifications	place here
manages the configuration of all IDS devices	place here

Use these

IDS_Analyzer	IDS_DeployDaemon
IDS_Notifier	IDS_Receiver
IDS_ReportScheduler	

Answer:

Place here

performs requested response, such as sending email	IDS_Analyzer
generates all reports to be sent at a pre-defined time	IDS_ReportScheduler
tales alarms and events and stores them in database	IDS_Receiver
processes event rules; request notifications	IDS_Notifier
manages the configuration of all IDS devices	IDS_DeployDaemon

Explanation:

- IDS_Analyzer-To check that the service that processes event rules and requests user-specified notifications when appropriate is running properly.
- IDS_DeployDaemon-To check that the service that manages all configuration deployments is running properly.
- IDS_Notifier-To check that the service that receives notification requests (script, email, and/or console) from other subsystems and performs the requested notification is running properly.
- IDS_Receiver-To check that the service that receives IDS and syslog events and stores them in the database is running properly.
- IDS_ReportScheduler-To check that the service that generates all scheduled reports is running properly.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_installation_guide_chapter09186a00800e42da.html

QUESTION 47

Which type of exploit involves introducing programs that install in inconspicuous back door to gain unauthorized access?

- A. File sharing
- B. Protocol weakness
- C. Trojan horse
- D. Session hijack

Answer: C

Explanation:

To gain remote access, they rely on keystroke capture software that's planted on a system, sometimes through a worm or Trojan horse disguised as a game or screen saver.

Reference:

http://www.cisco.com/en/US/netsol/ns339/ns395/ns360/ns372/net_value_proposition09186a00801b76ee.html

QUESTION 48

Exhibit:

The screenshot shows the 'Signature(s) in Group' configuration page for a sensor. The group is 'Test Sensor: Test' and the signature group is 'Reconnaissance Signatures'. The table below lists 10 signatures with their IDs, sub-IDs, descriptions, engines, and actions.

ID	Subsig ID	Signature	Engine	Enabled	Severity	Action
1	6180	1 read Attempt	SERVICE.RPC	Yes	Medium	None
2	6180	0 read Attempt	SERVICE.RPC	Yes	Medium	None
3	6102	1 RPC Dump	SERVICE.RPC	Yes	Medium	None
4	6102	0 RPC Dump	SERVICE.RPC	Yes	Medium	None
5	6061	1 DNS Intoleak	SERVICE.DNS	Yes	Medium	None
6	6061	0 DNS Intoleak	SERVICE.DNS	Yes	Medium	None
7	6052	1 DNS High Zone Xfer	SERVICE.DNS	Yes	Medium	None
8	6052	0 DNS High Zone Xfer	SERVICE.DNS	Yes	Medium	None
9	5115	6 WWW/Netcape Server with 7wp tags	SERVICE.HTTP	Yes	Medium	None
10	5115	5 WWW/Netcape Server with 7wp tags	SERVICE.HTTP	Yes	Medium	None

Refer to the exhibit. To tune a specific signature to log events when they occur, which parameter selection would display the correct panel and the capability to perform this task?

- A. Select the desired check box and click on the engine name.
- B. Click on the associated Signature ID.
- C. Select the desired check box and select the desired action from the drop down menu in the action column.
- D. Click on the desired signature name.

Answer: C

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d985.html#1227

QUESTION 49

When performing a service pack update on a Cisco IDS Sensor, which three server types are supported for retrieving the new software? (Choose three)

- A. FTP

- B. RCP
- C. NFS
- D. TFTP
- E. HTTPS

Answer: C D E

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d985.html#894166

QUESTION 50

When configuring IP logging using IDS MC, what does a value of zero (0) in the parameter field "maximum number of bytes in a log event" imply?

- A. No packets will be logged.
- B. Disabled the automatic logging feature.
- C. No limit of packets logged.
- D. Zero is an invalid setting.

Answer: A

Explanation:

ZERO-The sensor takes no action (default).

Reference:

Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1

QUESTION 51

Which command does a Cisco IOS router use to block attacks, as directed by an IDS blocking Sensor?

- A. acl
- B. shun
- C. access-list
- D. set security acl ip

Answer: C

Explanation:

If you configure the sensor for blocking, every router interface you configure the sensor to manage is controlled solely by the sensor even if no blocks are applied. The default ACL used by the sensor sets permit ip any any for controlled interfaces, and all traffic not being currently blocked is allowed through the router on the controlled interface. You should accept the ACL generated by the sensor.

If you want to change the ACL generated by the sensor, you can specify preshun or postshun ACLs by using the PreShunACL and PostShunACL tokens. The sensor allows two ACL

numbers for each interface that is controlled by device management. The PreShunACL designates ACL entries that the sensor should place in the ACL before placing any deny entries for the addresses being blocked. The PostShunACL designates ACL entries that the sensor should place after all deny entries for the address being blocked.

Note You cannot use standard named or numbered IP access lists (one that requires the standard keyword) such as the following:

```
ip access-list standard name
```

You can use a standard ACL as long as it is in this format:

```
access-list number
```

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/13870_01.htm#xtocid21

QUESTION 52

Which protocol does the Monitoring Center for Security use to monitor alarms on the IDS Sensor?

- A. SSH
- B. RDEP
- C. IDAPI
- D. PostOffice

Answer: D

Explanation:

A sensor can monitor the services that are running on it. The sensor can generate audit events, as warnings, when a service goes down or cannot be restarted. This monitoring function, called Watchdog, helps you track the state and desired operation of your sensors. Watchdog is a feature of the postoffice service.

Watchdog checks the availability of services that are supposed to be running on the sensor and verifies that desired sensor-to-other network object communications (based on postoffice) are available. The Watchdog queries the services to see if they are operational, and if they are not, it issues warnings to the user and attempts to restart the services. You can specify the alarm levels of these warnings.

Additional postoffice settings that you can specify are the postoffice port and the heartbeat interval.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d985.html

QUESTION 53

Which Sensor command archives IP log files to a remote host?

- A. ftp iplog
- B. export log
- C. copy iplog
- D. upload log

E. iplog export

Answer:

Explanation:

copy

Use the copy command to copy iplogs and configuration files.

copy [/erase] source-url destination-url

copy iplog log-id destination-url

Syntax Description

Syntax	
Description	Description
/erase	(Optional) Erases the destination file before copying. This keyword only
	applies to current-config, the backup-config is always overwritten. If this
	keyword is specified for destination current-config, the source configuration
	is applied to the system default configuration. If it is not specified for
	destination current-config, the source configuration is merged with the
	current-config.
<i>source-url</i>	The location of the source file to be copied. May be a URL or keyword.
<i>destination-</i>	The location of the destination file to be copied. May be a URL or keyword.
<i>url</i>	
<i>log-id</i>	Log id of file to copy. The log-id can be retrieved using the iplog-status

command.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_command_reference_chapter09186a008019d6d0.html

QUESTION 54

Which protocol does the IDS MC Sensors use to securely manage an IDS Sensor?

- A. SSL
- B. SSH
- C. RDEP
- D. HTTP
- E. PostOffice

Answer: B

Explanation:

Importing Communication Settings from postoffice Sensors

With postoffice-based Cisco Intrusion Detection System Sensors (sensors running sensor software version 3.x) you can discover postoffice settings directly from the device. This is accomplished using a Secure Shell (SSH) session.

SSH is a protocol for secure remote login and other secure network services over an insecure network.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3991/products_user_guide_chapter09186a008018d92b.html

QUESTION 55

Which ports will be examined if the ATOMIC.TCP signature parameter PortRangeSource is set to 0 (zero)?

- A. This setting will disable port inspection.
- B. This is a protected setting and cannot be set to 0 (zero).
- C. All ports destined to the source will be inspected.
- D. All ports from the source will be inspected.

Answer: D

Explanation:

ATOMIC.TCP Engine Parameters

Table A-9 lists the ATOMIC.TCP engine parameters.

Table A-9 ATOMIC.TCP Engine Parameters

Parameter Name	Data Type	Protected	Required	Description
DstPort	NUMBER (0-65535)	No	No	A single Destination Port to match.
Mask	BITSET (FIN SYN RST PSH ACK URG ZERO)	No	Yes	The mask used in TcpFlags comparison.
PortRange	NUMBER (0-2)	No	No	The destination port: Only Low Ports (1), Only High Ports (2), or All (0).
PortRangeSource	NUMBER (0-2)	No	No	The source port: Only Low Ports (1), Only High Ports (2), or All (0).
SinglePacketRegex	STRING	No	No	A regular expression to search for in a single TCP packet.
SrcPort	NUMBER (0-65535)	No	No	A single Source Port to match.
TcpFlags	BITSET (FIN SYN RST PSH ACK URG ZERO)	No	Yes	The TCP Flags to match when masked by Mask.

Reference:

Working With Signature Engines

QUESTION 56

An intruder has created a worm that targets an application running on a fixed port and attempts to gain administrator access using a well-known default password. Given these signature engines, which would be the best choice when creating a custom signature?

- A. ATOMIC.IPOPTIONS
- B. SERVICE.MSSQL
- C. SERVICE.IDENT
- D. STRING.TCP

Answer: A

QUESTION 57

Which protocol does an administrator use to communicate with the Monitoring Center for Security from the desktop?

- A. Telnet
- B. RDEP
- C. IDAPI
- D. HTTP
- E. HTTPS

Answer: E

Explanation:

To specify the communication protocol IDS Event Viewer should use when connecting to the sensor, select the Use encrypted connection (https) or Use non-encrypted connection (http) radio button.

Reference:

Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1

QUESTION 58

Which two methods can be used to upgrade the signatures on a Cisco IDS Sensor? (Choose two)

- A. IEV
- B. IDM
- C. IDS MC
- D. Monitoring Center for Security

Answer: B C

To use this procedure, you must have access to the server:

- You must have access to the IDS MC server if you want to update the IDS MC or a sensor.
- You must have access to the Security Monitor server if you want to update Security Monitor.
- If you have installed IDS MC and Security Monitor on the same server, you must have access to that server if you want to update the IDS MC or a sensor or Security Monitor.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d985.html#894197

Section B - practice questions

QUESTION 59

If you wanted to list active telnet sessions and selectively end certain ones, what commands from the list below could you use on your PIX Firewall? (Choose all that apply)

- A. show who
- B. remove session
- C. show logon
- D. end session
- E. kill
- F. whois

Answer: A, E

Explanation:

Answer

A. Show who: Shows active administrative Telnet sessions on the PIX Firewall. Cisco Secure Policy Manager does not generate this command, but the command can be supported using the Command panel on the PIX Firewall node. You can use the who command with the same results.

Answer E. kill: Terminates another Telnet session to PIX Firewall.

Reference: PIX Firewall Command Support Status

Incorrect Answers

B: remove session - is not a real command.

C: show logon - is not a real command.

D: end session - is not a real command.

F: whois - is a TCP literal name port (43 value)

QUESTION 60

If you were using the ca authenticate command, you notice that it does not save to the PIX's configuration.

Is this normal or are you making a mistake?

A. The command is not saved to the config.

B. You need to Save Run-config-

C. It saves automatically, you need to retype it.

D. To see it you need to type show cert.

Answer: A

Explanation:

The ca authenticate command is not saved to the PIX Firewall configuration. However, the public keys embedded in the received CA (and RA) certificates are saved in the configuration as part of the RSA public key record (called the "RSA public key chain").

Reference: PIX Firewall Software Version 6.3 Commands

QUESTION 61

Using the Cisco PIX and using port re-mapping, a single valid IP address can support source IP address translation for up to 64,000 active xlate objects.

This is an example of which technology?

A. PAT

B. DRE

C. SET

D. GRE

E. NAT

Answer: A

Explanation:

To allow all of the hosts access to the outside, we use Port Address Translation (PAT). If one address is specified in the global statement, that address is port translated. The PIX allows

one port translation per interface and that translation supports up to 65,535 active xlate objects to the single global address. The first 1023 are reserved.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 91

Using nat, global, static, conduit, and access-list Commands and Port Redirection on PIX

QUESTION 62

With regards to the PIX Firewall, which two terms are correct from the below list?

- A. All PIX Firewalls provide at least two interfaces, which by default, are called outside and inside.
- B. All PIX Firewalls provide at least two interfaces, which by default, are called Eth1 and Eth2.
- C. All PIX Firewalls provide at least two interfaces, which by default, are called Right and Left.
- D. All PIX Firewalls provide at least two interfaces, which by default, are called Internet and External.

Answer: A

Explanation:

With a default configuration, Ethernet0 is named outside with a security level of 0 and Ethernet1 is named inside and assigned a security level of 100.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 56

QUESTION 63

What command could you use on your PIX Firewall to view the current names and security levels for each interface?

- A. Show ifconfig
- B. Show nameif
- C. Show all
- D. Ifconfig /all

Answer: B

Explanation:

Use the show nameif command to determine which interface is being described in a message containing this variable.

Reference: Cisco PIX Firewall Software Introduction

QUESTION 64

Which TCP session reassembly configuration parameter enforces that a valid TCP session be establish before the Cisco IDS Sensor's sensing engine analyzes the traffic associated with the session?

- A. TCP open establish timeout

- B. TCP embryonic timeout
- C. TCP closed timeout
- D. TCP three way handshake
- E. TCP sequence timeout

Answer: D

Explanation:

The goal of defining these reassembly settings is to ensure that the sensor does not allocate all of its resources to datagrams that cannot be completely reconstructed, either because the sensor missed some frame transmissions or because an attack is generating random fragmented datagrams.

To specify that the sensor track only sessions for which the three-way handshake is completed, select the TCP Three Way Handshake check box.

Reference: Tuning Sensor Configurations

QUESTION 65

What can intrusion detection systems detect? (Choose three)

- A. Network misuse
- B. Network uptime
- C. Unauthorized network access
- D. Network downtime
- E. Network throughput
- F. Network abuse

Answer: A, C, F

Explanation:

An IDS is software and possibly hardware that detects attacks against your network. They detect intrusive activity that enters into your network. You can locate intrusive activity by examining network traffic, host logs, system calls, and other areas that signal an attack against your network.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 54

QUESTION 66

Which network device can be used to capture network traffic for intrusion detection systems without requiring additional configuration?

- A. Hubs
- B. Switches
- C. Network taps
- D. Router

Answer: A

Explanation: The ability to capture traffic may be inherent to a device technology or may require special features to provide this capability. For example, network hubs by their nature replicate data to all ports. Switches, on the other hand, rely on features such as port mirroring to permit the copy of specific traffic to another port.

Cisco Secure Intrusion Detection System 4 chap 5 page 3

QUESTION 67

Which VLAN ACL sends only ftp traffic to a Cisco IDS Sensor connected to a Catalyst 6500 switch?

- A. set security acl ip FTP_ACL permit udp any any eq 21
- B. set security acl ipx FTP_ACL permit ip any any capture
- C. set security acl ipx FTP_ACL permit tcp any any eq 21
- D. set security acl ip FTP_ACL permit tcp any any eq 21 capture
- E. set security acl ip FTP_ACL permit ip any any capture
- F. set security acl ip FTP_ACL permit icmp any any eq 21

Answer: D

Explanation:

To create a VACL, you need to use the set security acl ip switch command. The syntax for capturing TCP traffic between a source IP address and a destination IP address is as follows:

```
set security acl ip acl_name permit tcp src_ip_spec dest_ip_spec port capture
```

Reference: Cisco Secure Intrusion Detection System (Cisco Press) page 505

Cisco Secure Intrusion Detection System 4 chap 5 page 33

QUESTION 68

Which Cisco IDS communication infrastructure parameters are required to enable the use of IDS Device Manager to configure the Sensor? (Choose two)

- A. Sensor organization name
- B. Sensor group name
- C. IDM group name
- D. Sensor organization ID
- E. IDM organization ID

Answer: A, D

Explanation:

Communication infrastructure parameters:

Sensor Host ID and Organization ID

Sensor Host Name and Organization Name

Sensor IP Address

Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host ID and Organization ID

Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host Name and

Organization Name

Cisco Secure IDS Director or Cisco Secure PM IDS Manager workstation IP address

Reference: Cisco Secure Intrusion Detection System Sensor Configuration Note Version 2.5

QUESTION 69

A company has purchased a Cisco IDS solution that includes IDS modules. The switch group had decided not to provide the security department interactive access to the switch. What IDSM feature should be configured to provide the security department access to the IDSM command line?

- A. AAA
- B. TFTP
- C. HTTP
- D. Telnet
- E. HTTPS

Answer: D

Explanation:

The Catalyst 6000 family switch can be accessed either through a console management session or through telnet. Some switches might even support ssh access. After an interactive session is established with the switch, you must session into the ISDM line card. This is the only way to gain command-line access to the ISDM.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 499

QUESTION 70

Which network services are enabled by default on a Cisco IDS Sensor for remote management? (Choose three)

- A. SSH
- B. TFTP
- C. SNMP
- D. Telnet
- E. RSH
- F. FTP

Answer: A, D, F

Explanation:

Enter or delete the IP addresses of hosts and networks that can access the sensor via Telnet, FTP, SSH, and scp.

Reference: Cisco Intrusion Detection System Sensor Getting Started Version 3.1

Note by 2nd Certkiller writer: I think the answers don't conform to the latest course manual. Telnet - requires an IP address that has been assigned to the command and control interface via the CLI setup command. Must be enabled to allow telnet access. Telnet is DISABLED

by default.

SSH - Requires an IP address that has been assigned to the command and control interface via the CLI setup command and uses a supported SSH client. The SSH server in the sensor is ENABLED by default.

HTTPS - Requires an IP address that has been assigned to the command and control interface via the CLI setup command and uses a supported web browser. HTTPS is ENABLED by default but can be disabled.

Cisco Secure Intrusion Detection System 4 chap 7 page 23

QUESTION 71

When does the Sensor create a new log file?

- A. Only when the Sensor is initially installed.
- B. Only when the Sensor requests it.
- C. Every time its services are restarted.
- D. Every time a local log file is used.

Answer: C

Explanation:

The sensor creates new log file every time its services are restarted. This means that every time a new configuration is pushed to the sensor, a new configuration file is created And the old file is closed and transferred to a temporary directory.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 414

QUESTION 72

Which Cisco IDSM partition must be active to install a signature update?

- A. maintenance
- B. root
- C. /usr/nr
- D. application
- E. diagnostic

Answer: D

Explanation:

Make sure that the IDSM was booted in the application (hdd:1) and not the maintenance (hdd:2) partition. Use the switch command show version module_number to display the software version currently running on the module. The application partition will show a signature update version denoted by the letter "S" followed by a number, for example, 2.5(1)S1, but the maintenance partition will not contain the signature update version, for example 2.5(0).

Reference: Catalyst 6000 Intrusion Detection System Module Installation and Configuration Note Version 3.0(5)

QUESTION 73

Which Cisco IDS software is included with a Sensor appliance?

- A. Cisco Secure Policy Manager
- B. IDS Management Center
- C. Intrusion Detection Director
- D. IDS Event Viewer

Answer: D

Explanation: The IDS Event Viewer is a Java-based application that enables you to view and manage alarms for up to three sensors. With the IDS Event Viewer you can connect to and view alarms in real time or in imported log files. You can configure filters and views to help you manage the alarms. You can also import and export event data for further analysis. The IDS Event Viewer also provides access to the Network Security Database (NSDB) for signature descriptions.

Reference: Cisco Intrusion Detection System Event Viewer Version 3.1

Note by 2nd Certkiller writer:

I am not sure about this question. The latest course manual 4, states that the IDM "is a webbased, embedded architecture configuration tool for cisco ids sensors." Cisco Secure Intrusion Detection System 4 chap 10 page 4

QUESTION 74

Exhibit:

Signature Name	Severity Level	Host ID	Org ID	SRC	DST
FTP SITE	Informational	501	500	OUT	OUT
FTP SITE	Informational	501	500	OUT	OUT

In the Cisco IDS Event Viewer, how do you display the context data associated with an event?

- A. Choose View>Context Data from the main menu.
- B. Right-click the event and choose Show Data.
- C. Choose View>Show data from the main menu.
- D. Right-click the event and choose Show Context.
- E. Choose View>Show Context from the main menu.
- F. Double-click the event.

Answer: D

Explanation:

Certain alarms may have context data associated with them. Context data provides a snapshot of the incoming and outgoing binary TCP traffic (up to a maximum of 256-bytes in both directions) that preceded the triggering of the signature. To view the context for an alarm, follow these steps:

Step 1 From the Alarm Information Dialog, right-click a cell in the Context column, and then select Show Context.

Step 2 Scroll to view the context associated with this alarm.

Reference: Cisco Intrusion Detection System Event Viewer Version 3.1

Also see Cisco Secure Intrusion Detection System 4 chap 10 page 20

QUESTION 75

When designing IP blocking, why should you consider entry points?

- A. They provide different avenues for the attacker to attack your networks.
- B. They prevent all denial of service attacks.
- C. They are considered critical hosts and should not be blocked.
- D. They provide a method for the Sensor to route through the subnet to the managed router.

Answer: A

Explanation:

Today's networks have several entry points to provide reliability, redundancy, and resilience. These entry points also represent different avenues for the attacker to attack your network. You must identify all the entry points into your network and decide whether they need to also participate in IP blocking.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 467

Cisco Secure Intrusion Detection System 4 chap 15 page 8

Note: It is recommended that Sensors be placed at those network entry and exit points that provide sufficient intrusion detection coverage. Cisco Secure Intrusion Detection System 4 chap 4 page 37

QUESTION 76

Which type of ACL is allowed when implementing the Cisco IDS IP blocking feature pre-shun ACLs?

- A. Named IP extended
- B. Named IP standard
- C. Numbered IPX standard
- D. Numbered IPX extended
- E. Named IPX extended

Answer: A

Explanation: A pre-block and post-block ACL must be an extended IP ACL, named or

unnumbered. They should be configured on the device Sensor block is configured for that interface/direction Cisco Secure Intrusion Detection System 4 chap 15 page 15

QUESTION 77

Which of the following commands let you view, change, enable, or disable the use of a service or protocol through the PIX Firewall?

- A. fixing protocol
- B. set firewall
- C. fixup protocol
- D. change -all fix

Answer: C

Explanation:

The fixup protocol commands let you view, change, enable, or disable the use of a service or protocol through the PIX Firewall. The ports you specify are those that the PIX Firewall listens at for each respective service.

Reference: Cisco PIX Firewall Command Reference, Version 6.3

Note: In Appendix B of the Cisco Secure Intrusion Detection System 4 Fixup protocol is not talked about.

QUESTION 78

Debugging a PIX is what you want to do to resolve a problem. What command would you use to display the current state of tracing?

- A. show debug
- B. debug all
- C. all on debug
- D. debug crypto

Answer: A

Explanation:

The debug command lets you view debug information. The show debug command displays the current state of tracing. You can debug the contents of network layer protocol packets with the debug packet command

Reference: Cisco PIX Firewall Command Reference, Version 6.3

. Note: in Appendix B of the Cisco Secure Intrusion Detection System 4 Debugging is not talked about.

QUESTION 79

RIP uses a port to establish communications. If you were to block it with your Firewall, what port would you be concerned about?

- A. Port 345

- A. e0/2
- B. e0/0
- C. e1/0
- D. e0/1
- E. e1/1

Answer: D

The Sensor is on the same network, so that means the only possibly answer is the Ethernet01 interface. Ethernet0/2 is using a different network address and Ethernet0/0 is using a DMZ network.

Note: What is being talked about here is a Network Tap. " A network tap is a device used to split full-duplex traffic flows into a single traffic flows that can be aggregated at a switch device. The network tap has four connectors

Two input connectors - traffic from a device

Two output connectors- traffic exiting the tap"

Cisco Secure Intrusion Detection System 4 chap 5 page 7

QUESTION 82

An ACL policy violation signature has been created on a Cisco IDS Sensor. The Sensor is configured to receive policy violations from a Cisco IOS router.

What configurations must exist on the router? (Choose two)

- A. Logs permit ACL entries
- B. Logs deny ACL entries
- C. Sends SNMP traps to the Sensor
- D. Sends Syslog messages to the Sensor
- E. Sends SNMP traps to the Director
- F. Sends syslog messages to the Director

Answer: B, F

Explanation:

The Sensor can be configured to create an alarm when it detects a policy violation from the syslog generated by a Cisco router. A policy violation is generated by a Cisco router when a packet fails to pass a designated Access Control List. Security data from Sensor and Cisco routers, including policy violations, is monitored and maintained on the Director.

Reference: Cisco Secure Intrusion Detection System Overview

QUESTION 83

A Cisco IDS Sensor has been configured to detect attempts to extract the password file from Windows 2000 systems. During a security posture assessment, the consultants attempted to extract the password files from three Windows 2000 servers.

This activity was detected by the Sensor.

What situation has this activity caused?

- A. True negative

- B. True positive
- C. False negative
- D. False positive

Answer: B

Explanation:

True positive - is when an IDS generates an alarm for known intrusive activity.

False negative - is when an IDS fails to generate an alarm for known intrusive activity.

False positive - is when an IDS generates an alarm for normal user activity.

Reference: Cisco Secure Intrusion Detection System (Cisco Press) page 55 & 58

Note: True positive - A situation in which a signature is fired properly when offending traffic is detected. An attack is detected as expected. - Cisco Secure Intrusion Detection System 4 chap 3 page 12

QUESTION 84

What Cisco IDS Sensor secure shell operation enables a network security administrator to remove hosts from the list of those previously connected to devices?

- A. Generate new Sensor SSH keys.
- B. Generate new Director SSH keys.
- C. Manage the Sensor's known hosts file.
- D. Manage the Director's known hosts file.

Answer: C

Explanation: Access to the probe is determined by a ACL but note in chap 12 the MC deals with SSH key generation.

Sensor#config t

Sensor#(Config)#service host

Sensor#(config-host)networkParams

Sensor#(config-host-net) accesslist ip address 10.0.2.0 netmask 255.255.255.0 ----adds an entire network to the access list

Cisco Secure Intrusion Detection System 4 chap 9 page 31

QUESTION 85

Which user account is used to log into the IDSM?

- A. Root
- B. Administrator
- C. Netranger
- D. Ciscoism
- E. Ciscoids

Answer: E

Explanation:

The default user login user name for the Cisco IDS Module is Ciscoids, and the default password is attack.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 680

Note: This was correct in the older course however it is not right according to 4 but the answers given don't match what is listed in the course manual.

"Log in to the IDSM2 using the default username CISCO and the Password CISCO" - Cisco Secure Intrusion Detection System 4 chap 8 page 12

"The sensor allows you to create multiple local user accounts. The default username and password is cisco. You are required to change the default password the first time you log on."

- Cisco Secure Intrusion Detection System 4 chap 7 page 24

QUESTION 86

Which Cisco IDS software update file can be installed on a IDS-4210 Sensor?

- A. IDSMk9-sp-3.0-3-S10.exe
- B. IDSMk9-sp-3.0-3-S10.bin
- C. IDSMk9-sig-3.0-3-S10.exe
- D. IDSk9-sp-3.1-2-S24.exe
- E. IDSk9-sp-3.1-2-S24.bin
- F. IDSk9-sig-3.1-2-S24.exe

Answer: E

Explanation: D is not the correct answer. I have an example in the course guide 4 that show the.bin is correct. Also supported in appendix C-17 (bin-this is the executable files directory. It includes all of the cisco IDS services, programs, and functions)

IDS-k9-sp-4.0-2-s42.rpm.pkg - executable file that contains signature or service pack update.

This is not an option but it is shown on 17-8

Sensor(config)#upgrade

ftp://cisco@192.168.1.1/ids-k9-sp4.0-2-s29.bin - Installs the IDS-k9-sp-4.0-2-s29.bin from the ftp server's root directory at IP address 192.168.1.1 with user name of cisco

- Cisco Secure Intrusion Detection System 4 chap 17 page 10

QUESTION 87

Exhibit:

```
netrangr@sensor1:/usr/nr
#idsstatus
netrangr 16249    1 0 15:46:33 pts/1    0:00 /usr/nr/bin/nr.postofficed
netrangr 16267    1 0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.sapd
netrangr 16295    1 0 15:46:35 pts/1    0:00 /usr/nr/bin/nr.managed
netrangr 16258    1 0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.loggerd
netrangr 16274    1 0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.fileXferd
netrangr 16282    1 18 15:46:34 pts/1    0:08 /usr/nr/bin/nr.packetd
```

Given the output of the idsstatus Sensor command. What function is the Sensor performing? (Choose two)

- A. Not logging alarms, commands, and errors.
- B. Performing IP blocking.

- C. Not capturing network traffic.
- D. Logging alarms, commands, and errors.
- E. Not performing IP blocking.

Answer: B, D

Explanation:

Postofficed The postofficed daemon serves as the communication vehicle for the entire Cisco IDS product

Sapd - The sapd daemon is a user-configurable scheduler that controls database loading and archival of old event and IP session logs.

Managed - The managed daemon is responsible for managing and monitoring network devices (routers and packet filters). For example, when packetd identifies that a certain type of attack should be shunned, it sends a shun command to managed via the post office facility.

Logged - The loggerd daemon writes out sensor and error data to flat files generated by one or more of the other daemons.

fileXferd The fileXferd daemon is used for file transfer between Sensors and Directors. It is used to transport configuration files between Directors and Sensors.

Packetd - The packetd daemon interprets and responds to all of the events it detects on the monitored subnet.

Reference: Cisco Secure IDS Internal Architecture

QUESTION 88

What is the Cisco IDS Management Center?

- A. Web-based interface for managing and configuring multiple sensors.
- B. Command-line interface for managing and configuring multiple sensors.
- C. Web-based interface for managing and configuring a single sensor.
- D. Command-line interface for managing and configuring a single sensor.

Answer: A

Explanation:

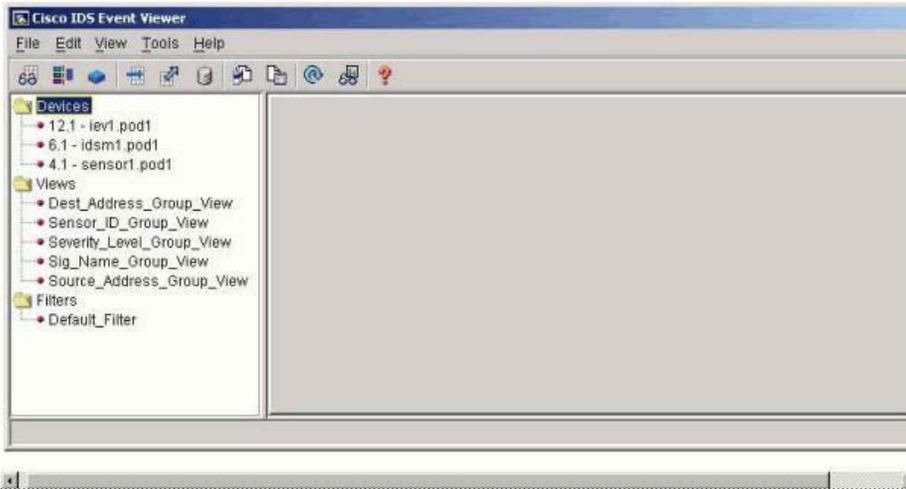
The Management Center for IDS Sensors is a tool with a scalable architecture for configuring Cisco network sensors, switch IDS sensors, and IDS network modules for routers. Uses a web-based interface.

Reference: CiscoWorks Management Center for IDS Sensors Datasheet

Note: What is the IDS MC? The IDS MC is a web-based application that centralizes and accelerates the deployment and management of multiple IUDS sensors of IDSM. IDS MC is a component of the VMS bundle. - Cisco Secure Intrusion Detection System 4 chap 11 page 3

QUESTION 89

Exhibit:



After 1EV has been configured to receive alarms from Sensors, how do you display the alarms in the Cisco IDS Event Viewer? (Choose all that apply)

- A. Right-click Dest_Address_Group_View and choose View.
- B. Double-click Dest_Address_Group_View
- C. Right-click Dest_Address_Group_View and choose Display.
- D. Right-click Sig_Name_Group_View and choose View.
- E. Right-click Sig_Name_Group_View and choose Display.
- F. Double-click Sig_Name_Group_View

Answer: B, F

Explanation:

Right-click a row in the Expanded Details Dialog, and then select View Alarms.

Result: The Alarm Information Dialog appears.

-or-

Double-click the cell containing the alarms you want to view in the Total Alarm Count column. Result: The Alarm Information Dialog appears.

Reference: Cisco IDS Sensor Software - Cisco Intrusion Detection System Event Viewer Version 3.1

Note: To view the alarm information, right-click the alarm in the Expanded Details Dialog window and choose View Alarms. The alarm Information Dialog window displays each event and the associated alarm data, such as Signature Name, Source address, and Destination address. - Cisco Secure Intrusion Detection System 4 chap 10 page 19

QUESTION 90

Which Cisco IDS Sensor configuration parameter affects the source and destination values included in an IDS alarm event?

- A. Data source
- B. IP fragment reassembly
- C. External network definition
- D. Internal network definition

- E. TCP reassembly
- F. Sensor IP address

Answer: D

Explanation:

You can use the source and destination location to alter your response to specific alarms. Traffic coming from a system within your network to another internal host that generates an alarm may be acceptable, whereas, you might consider this same traffic, originating from an external host or the Internet, totally unacceptable.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 183

QUESTION 91

Which TCP session reassembly configuration parameter enforces that a valid TCP session be establish before the Cisco IDS Sensor's sensing engine analyzes the traffic associated with the session?

- A. TCP open establish timeout
- B. TCP embryonic timeout
- C. TCP closed timeout
- D. TCP three way handshake
- E. TCP sequence timeout

Answer: D

Explanation:

Select the TCP three way handshake if you want the sensor to tack only those sessions for which the three-way handshake is completed. The other options for reassembly are:

No reassembly

Loose reassembly

Strict reassembly

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 419

QUESTION 92

Which common command are you going to use to clear the contents of the translation slots when needed?

- A. clear xlate
- B. clear translate
- C. clear all
- D. show translate

Answer: A

Explanation:

The xlate command allows you to show or clear the contents of the translation (xlate) slots.

show xlate, clear xlate

Reference: Cisco Secure PIX Firewall (Ciscopress) page 77

QUESTION 93

When working on your PIX, you would like to view the network states of local hosts. What command could you use?

- A. local host all
- B. show local-host
- C. show host all
- D. show local remote
- E. show set local

Answer: B

Explanation:

The show local-host command assists you in characterizing your "normal" load on a statically translated host, both before and after setting limits.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 171

QUESTION 94

If you wanted to enable access to a higher security level interface from a lower level interface what could you do?

- A. Set the conduit to 0/1.
- B. Use the static and access-list commands.
- C. Set the Eth1/0 interface to auto.
- D. Use the nat and global commands.

Answer: B

Explanation:

Two things are required for traffic to flow from a lower security to a higher security interface: a static translation and a conduit or an access list to permit the desired traffic.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 55

QUESTION 95

A company has a requirement to create a custom signature that detects BGP packets traversing the network.

Which Cisco IDS signature micro-engine can be used to create this signature?

- A. Atomic.TCP
- B. Atomic.L3.IP
- C. Sweep.Port.TCP
- D. Atomic.IPOptions

Answer: B

Explanation:

The following are Atomic.L3.IP parameters:

MaxProto-defines the maximum IP protocol number, after which the signature fires

MinProto-Defines the minimum IP protocol number, after which the signature fires

isRFC1918-Defines whether the packet is from RFC 1918 address pool

-Cisco Secure Intrusion Detection System 4 chap 13 page 13

BGP is a layer 3 routing protocol. Atomic.L3.IP will detect layer 3 IP alarms

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 628

QUESTION 96

A Cisco IDS Sensor has been configured to detect attempts to extract the password file from Windows 2000 systems. During a security assessment, the consultants attempted to extract the password files from three Windows 2000 servers. This activity was not detected by the Sensor.

What situation has this activity caused?

- A. False negative
- B. False positive
- C. True positive
- D. True negative

Answer: A

False negative - is when an IDS fails to generate an alarm for known intrusive activity.

False positive - is when an IDS generates an alarm for normal user activity.

True positive - is when an IDS generates an alarm for known intrusive activity.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 55 & 58

Note: A situation in which a signature is not fired when offending traffic is detected. An actual attack is not detected -Cisco Secure Intrusion Detection System 4 chap 3 page 11

QUESTION 97

A company has installed an IDSM into a Catalyst 6509 switch in slot 9. The network security architect has designed a solution that requires the IDSM monitor traffic only from VLAN 199.

Which Catalyst OS commands are used to achieve this configuration?

- A. set trunk 9/2 199
- B. clear trunk 9/2 199
- C. clear trunk 9/2 1-1024
- D. clear trunk 9/1 1-1024
- E. set trunk 9/1 199
- F. clear trunk 9/1 199

Answer: D, E

Reference: Cisco Catalyst 5000 Series Switches - Switch and ROM Monitor

Commands; Release 6.2

Note: In the new course we think the answer would be this

Router(config)#interface vlan <vlan_number> - creates or access the vlan interface specified

Router(config)# interface vlan 401

Router(config-if)#mlp ip ids <acl_name> - applies an IP acl to the vlan interface

The mlp ip ids command is used to apply an extended ip access list to the vlan interface

-Cisco Secure Intrusion Detection System 4 chap 5 page 48

QUESTION 98

How many interactive login sessions to the IDSM are allowed?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: A

Note: In the IDSM chapter I did not come across anything that stated this. In fact there is not much listed in the IDSM chapter. The main thrust was that it uses the same code as the ver4 sensors so it works the same except for some alterations.. Cisco Secure Intrusion Detection System 4 chap 4

QUESTION 99

The Cisco IDS Sensor service pack file IDSk9-sp-3.1-2-S23.bin exists on the Sensor.

Which command installs the service pack on the Sensor?

- A. IDSk9-sp-3.1-2-S23 -install
- B. IDSk9-sp-3.1-2-S23.bin -install
- C. IDSk9-sp-3.1-2-S23.bin -i
- D. IDSk9-sp-3.1-2-S23.bin -l
- E. IDSk9-sp-3.1-2-S23-bin -apply
- F. IDSk9-sp-3.1-2-S23 -apply

Answer: E

Explanation:

Valid Service Pack upgrade

idsm(config)# apply ftp://user@10.0.0.1//IDSMk9-sp-3.0-3-S10.exe

Reference: Cisco Intrusion Detection System - Upgrading the Intrusion Detection System Module

I am not sure about answer D. I really cant find anything that supports it. In the new course the command is update. I think that the answer may be E using the apply command as shown in the explanation.

QUESTION 100

Which network management product is used to deploy configurations to groups of IDS

devices?

- A. IDM
- B. IDS Management Center
- C. Security Monitoring
- D. IEV

Answer: B

Explanation:

The Management Center for IDS Sensors is a tool with a scalable architecture for configuring Cisco network sensors, switch IDS sensors, and IDS network modules for routers. Uses a web-based interface.

Reference: CiscoWorks Management Center for IDS Sensors

QUESTION 101

A hospital's security policy states that any e-mail messages with the words SSN or Social Security must be detected by the IDS Sensor.

Which Cisco IDS signature micro-engine should be used to create the signature?

- A. Atomic.TCP
- B. Atomic.UDP
- C. String.ICMP
- D. String.TCP
- E. String.UDP

Answer: E (or D)

Note: I am not sure why the original person who answered this question picked tcp but I think that most email is delivered via tcp. However he/she is correct in that it is a string signature. Off hand I have a slight doubt if most email is delivered via UDP or TCP. If you think that most email is UDP pick E if you don't then stay with the given answer.

ICMP is wrong.

Atomic is one packet and wrong.

The course manual does not give examples of String signatures.

Cisco Secure Intrusion Detection System 4 chap 13 page 41

QUESTION 102

What information can a network security administrator specify in a Cisco IDS exclude signature filter? (Choose two)

- A. Signature name
- B. Signature ID
- C. Signature action
- D. Signature severity level
- E. Sub-signature ID
- F. Source port

Answer: B, E

Explanation:

When defining a simple filter, you need to configure the following fields:

Signature

Subsignature

IP address

Network Mask

Address Role

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 446

QUESTION 103

Which common command are you going to use to clear the contents of the translation slots when needed?

- A. clear xlate
- B. remove session
- C. show logon
- D. end session
- E. kill
- F. whois

Answer: A

The xlate command allows you to show or clear the contents of the translation (xlate) slots.

show xlate, clear xlate

Reference: Cisco Secure PIX Firewall (Ciscopress) page 77

QUESTION 104

If you wanted to view the conduit command statements in the configuration and the number of times (hit count) an element has been matched during a conduit command search, what command would you type on the PIX Firewall?

- A. show con -all
- B. show config
- C. show conduit
- D. conduit /all

Answer: C

Explanation:

To look at the configured conduits, use the show conduit command.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 89

QUESTION 105

In PIX Terminology, what exactly is a Conduit?

- A. It routes data from one interface to another.
- B. The Conduit is where the data travels on the Bus.
- C. It controls what QoS the packets get when going through Eth1.
- D. Controls connections between external and internal networks.

Answer: D

Explanation:

the conduit command functions by creating an exception to the PIX Firewall Adaptive Security Algorithm that then permits connections from one PIX Firewall network interface to access hosts on another.

Reference: Cisco PIX Firewall Command Reference, Version 6.3

QUESTION 106

Which value can be assigned to define the Cisco IDS 4210 Sensor's sensing interface?

- A. Auto
- B. Detect
- C. Probe
- D. Sniffing
- E. Select

Answer: D

Explanation:

An individual sensor contains two separate interfaces. The sensor used on of the interfaces to passively sniff all the network packets by placing the interface in Promiscuous mode. The sensor uses the other network interface for command and control traffic.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 98

QUESTION 107

The network administrator has informed the security administrator that the average number of packets per seconds is 400.

Which Sensor selection factor should the security administrator take into consideration?

- A. Sensor processor speed
- B. Server performance
- C. Network throughput
- D. Intrusion detection analysis performance.

Answer: D

Explanation:

Real-time monitoring of network packets, which involves packet capture and analysis

Reference: Cisco IDS Sensor Software - Cisco Secure Intrusion Detection System Overview

QUESTION 108

Which Cisco IDS communication infrastructure parameters are required to enable the use of the IDS Device Manager to configure the Sensor? (Choose two)

- A. IEV IP address
- B. Sensor IP address
- C. IDM IP address
- D. Sensor host name
- E. IEV host name
- F. IDM host name

Answer: B, D

Communication infrastructure parameters:

Sensor Host ID and Organization ID

Sensor Host Name and Organization Name

Sensor IP Address

Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host ID and Organization ID

Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host Name and Organization Name

Cisco Secure IDS Director or Cisco Secure PM IDS Manager workstation IP address

Reference: Cisco Secure Intrusion Detection System Sensor Configuration Note Version 2.5

QUESTION 109

Which management access methods require that an IP address be assigned to a Cisco IDS Sensor? (Choose three)

- A. IDS Device Manager
- B. IDS Event Viewer
- C. Remote Shell
- D. Secure Shell
- E. Telnet
- F. Trivial File Transfer Protocol

Answer: A, D, E

Explanation:

Enter or delete the IP addresses of hosts and networks that can access the sensor via Telnet, FTP, SSH, and scp.

Reference: Cisco Intrusion Detection System Sensor Getting Started Version 3.1

QUESTION 110

Exhibit:

```
netrangr@sensor1:/usr/nr
#idsstatus
netrangr 16249      1 0 15:46:33 pts/1    0:00 /usr/nr/bin/nr.postofficed
netrangr 16267      1 0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.sapd
netrangr 16295      1 0 15:46:35 pts/1    0:00 /usr/nr/bin/nr.managed
netrangr 16258      1 0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.loggerd
netrangr 16274      1 0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.fileXferd
netrangr 16282      1 18 15:46:34 pts/1    0:08 /usr/nr/bin/nr.packetd
```

Given the output of the idsstatus Sensor command, what function is the Sensor performing?

- A. Capturing network traffic.
- B. Not performing IP blocking.
- C. Not logging alarms, errors, and commands.
- D. Generating e-mails for alarms.
- E. Not capturing network traffic.
- F. Loading alarms into a user database.

Answer: A

Explanation:

Postofficed The postofficed daemon serves as the communication vehicle for the entire Cisco IDS product

Sapd - The sapd daemon is a user-configurable scheduler that controls database loading and archival of old event and IP session logs.

Managed - The managed daemon is responsible for managing and monitoring network devices (routers and packet filters). For example, when packetd identifies that a certain type of attack should be shunned, it sends a shun command to managed via the post office facility.

Loggerd The loggerd daemon writes out sensor and error data to flat files generated by one or more of the other daemons.

fileXferd The fileXferd daemon is used for file transfer between Sensors and Directors. It is used to transport configuration files between Directors and Sensors.

Packetd - The packetd daemon interprets and responds to all of the events it detects on the monitored subnet.

Reference: Cisco Secure IDS Internal Architecture

QUESTION 111

What Cisco IDS software is included with a Sensor appliance? (Choose two)

- A. IDS Management Center
- B. IDS Device Manager
- C. Intrusion Detection Director
- D. Cisco Secure Policy Manager
- E. IDS Event Viewer

Answer: B, E

Explanation: The Cisco IDS Device Manager and IDS Event Viewer, both delivered through

Cisco IDS software version 3.1, are part of Cisco's multi-tiered management strategy addressing the administrative needs of e-business security. The IDS Device Manager enables easy, remote IDS sensor configuration with a high degree of customization, minimizing the occurrence of false positives. The event monitoring capabilities delivered via the IDS Event Viewer let customers collect, correlate, and analyze event data for rapid detection and response to unauthorized network activity.

Reference: Cisco Addresses Intrusion Protection with new IDS Solutions

QUESTION 112

A Cisco IDS Sensor is capturing large volumes of network traffic. Which Cisco IDS Sensor status alarm is an indication that the Sensor is being overwhelmed?

- A. Daemon down
- B. Route down
- C. No traffic
- D. Captured packet count
- E. Missed packet count
- F. Network saturated

Answer: E

Explanation: Problem: sensorApp does not respond after hours of being seriously oversubscribed. All system memory, including SWAP, is exhausted when a 700 Mbps traffic feed is sent to the 250 Mbps appliance 4235 over several hours.

Symptom: The CLI show version command may say "AnalysisEngine Not Running" or control transactions will timeout with error about sensorApp not responding. You will see 993 missed packet alarms before the unresponsive state (if that alarm is Enabled).

Workaround: 1) Do not seriously oversubscribe the sensor. Chose the right appliance for your network segment and partition the traffic accordingly. 2) If sensorApp (aka AnalysisEngine) is listed as Not Running or is not responsive, issue a RESET command on the CLI. Do this after examining the traffic feed and adjusting the feed to the sensor so it is within the rating for the specific appliance

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2113/prod_release_note09186a00801a00ac.html

QUESTION 113

Which PIX Command will allow the PIX Firewall to authenticate its certification authority (CA) by obtaining the CA's self-signed certificate, which contains the CA's public key?

- A. ca lock /all
- B. show auth
- C. Set ca auth
- D. ca authenticate

Answer: D

Explanation: The ca authenticate command allows the PIX Firewall to authenticate its certification authority (CA) by obtaining the CA's self-signed certificate, which contains the CA's public key.

Reference: Cisco PIX Firewall Command Reference, Version 6.3

QUESTION 114

What port would you be concerned about if you were worried about DNS Zone Transfers while protecting your infrastructure with a PIX?

- A. UDP 12
- B. UDP 53
- C. TCP 62
- D. UDP 45

Answer: B

Explanation:

Triggers on normal DNS zone transfers, in which the source port is 53.

Reference: Cisco IOS Intrusion Detection System Signature List

QUESTION 115

If you wanted to show the running configuration of a PIX firewall, what command would you use?

- A. Show Running-Config
- B. Write terminal
- C. Show Config
- D. Show pix

Answer: B

Explanation:

Write terminal displays current configuration on the terminal.

Reference: Cisco PIX Firewall Command Reference, Version 6.3

QUESTION 116

Which Cisco IDS signatures are affected by the Sensor's level of traffic logging value?

- A. String signatures
- B. HTTP signatures
- C. TCP connection signatures
- D. FTP connection signatures
- E. ICMP signatures

Answer: C

Explanation:

Connection signatures are user-configurable attack signatures based on the transport-layer protocol (TCP or UDP) and port number of the packets being monitored

Reference: Sensor Signatures

QUESTION 117

An anonymous person has posted a tool on a public website that can cause Cisco DSL routers to reboot.

What term describes how this tool is used to leverage the weakness in the Cisco DSL routers?

- A. Vulnerability
- B. Exploit
- C. Rootkit
- D. Exposure

Answer: B

Explanation:

Exploits activity-Indicative of someone attempting to gain access or compromise systems on your network, such as Back Orifice, failed login attempts, and TCP hijacking

Reference: Cisco Intrusion Detection System - Cisco Secure Intrusion Detection System

QUESTION 118

A university's security policy states that network devices must be managed using secure communication methods.

Which Cisco IDS Sensor services must be disabled to meet this requirement? (Choose two)

- A. SSH
- B. Telnet
- C. TFTP
- D. SNMP
- E. FTP
- F. RSH

Answer: B, E

Explanation: The Sensor always provides secure shell services (including scp). Increase the security of the Sensor by disabling two services that allow clear text password authentication: Telnet and FTP. For maximum security disable both.

Reference: Cisco IDS Sensor Software - Cisco Intrusion Detection System Sensor Configuration Note Version 3.1

QUESTION 119

A company policy states that IDS Sensors can be managed only by authorized management workstations. The management workstations exist on the 192.168.21.0/24 network.

Which address must the network security administrator add to the Cisco IDS Sensor's network access control list?

- A. 192.168.21.
- B. 192.168.21
- C. 192.168.
- D. 192.168
- E. 192.168.21.0.
- F. 192.168.21.0

Answer: F

Explanation: I am not sure the difference between E and F except for an extra dot (which is wrong)

Actually the original answer is A 192.168.21. which is wrong as far as version 4 of the course manual is concerned. I think this answer was wrong. Acls you must put all aspects of the 4 octets in. I think the correct was the 192.168.21.0 the original had 192.168.21. - nothing in the fourth octet

```
Sensor#config t
```

```
Sensor(config)# service host
```

```
Sensor(config-Host)#networkParams
```

```
Sensor(config-Host-net) accesslist ipAddress 10.0.2.0 netmask 255.255.255.0 - adds an entire network to the access list.
```

Cisco Secure Intrusion Detection System 4 chap 13 page 41

QUESTION 120

A Cisco IDS Sensor has been configured to perform IP Blocking. Which Cisco IDS service must be running on the Sensor?

- A. Logged
- B. Eventd
- C. Blocked
- D. Managed
- E. Shunned

Answer: D

Explanation:

Managed - The managed daemon is responsible for managing and monitoring network devices (routers and packet filters). For example, when packetd identifies that a certain type of attack should be shunned, it sends a shun command to managed via the post office facility.

Reference: Cisco Secure IDS Internal Architecture

QUESTION 121

In the Cisco IDS Management Center, what workflow steps must you perform to push configuration files to a Sensor?

- A. Configure, load, submit
- B. Generate, approve, deploy
- C. Generate, submit, approve
- D. Load, submit, approve

Answer: B

Explanation:

The Workflow tab is where you can generate, approve, and deploy configuration files for the sensors that you want to manage with your installation of IDS MC

Reference: Generating, Approving, and Deploying Configuration Files

QUESTION 122

A company has a custom client-server application that communicates on UDP ports 6000-7000.

Which Cisco IDS signature micro-engine can be used to detect attempts to locate the servers?

- A. Atomic.IPOptions
- B. Sweep.RPC
- C. Sweep.Net.UDP
- D. Sweep.Port.UDP
- E. String.Net.UDP
- F. String.Port.UDP

Answer: D

Explanation:

SWEEP.PORT.UDP - UDP connections to multiple destination ports between two nodes

Reference: Cisco Secure Intrusion Detection System Signature Engines Version 3.0

QUESTION 123

Which command(s) from the list below generates RSA key pairs for your PIX Firewall?

- A. rsa set ca
- B. ca generate rsa
- C. ca rsa config
- D. config rsa

Answer: B

Explanation:

The ca generate rsa command generates RSA key pairs for your PIX Firewall. RSA keys are generated in pairs-one public RSA key and one private RSA key

Reference: Cisco PIX Firewall Command Reference, Version 6.3

QUESTION 124

Cisco PIX will support which protocols listed below?

- A. PIX Supports all listed here.
- B. File Transfer Protocol (FTP)
- C. Domain Name System (DNS)
- D. Bootstrap Protocol (BOOTP)
- E. Generic Route Encapsulation (GRE)

Answer: A

Explanation:

Supported Protocols and Applications

PIX Firewall supports the following TCP/IP protocols and applications:

- Address Resolution Protocol (ARP)
- Archie
- Berkeley Standard Distribution (BSD)-rcmnds
- Bootstrap Protocol (BOOTP)
- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- generic routing encapsulation (GRE)
- Gopher
- HyperText Transport Protocol (HTTP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP)
- NetBIOS over IP (Microsoft Networking)
- Point-to-Point Tunneling Protocol (PPTP)
- Simple Network Management Protocol (SNMP)
- Sitara Networks Protocol (SNP)
- SQL*Net (Oracle client/server protocol)
- Sun Remote Procedure Call (RPC) services, including Network File System (NFS)
- Telnet
- Transmission Control Protocol (TCP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)
- RFC 1700

Reference: Cisco PIX Firewall Software - TCP/IP Reference Information

QUESTION 125

Which type of ACL is allowed when implementing the Cisco IDS IP blocking feature using post-shun ACLs?

- A. Numbered IP extended
- B. Named IPX extended
- C. Numbered IP standard
- D. Numbered IPX standard

Answer: A

Explanation: Extended ACLs enable you to create fine-tuned filtering policies.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 464

QUESTION 126

What reconnaissance methods are used to discover servers running SMTP and SNMP?
(Choose two)

- A. TCP scans for port 25
- B. UDP scans for port 25
- C. UDP scans for port 161
- D. ICMP sweeps for port 25
- E. ICMP sweeps for port 161

Answer: A, C

Explanation:

If the public SMTP server were compromised, a hacker might try to attack the internal mail server over TCP port 25, which is permitted to allow mail transfer between the two hosts. SNMP is a network management protocol that can be used to retrieve information from a network device (commonly referred to as read-only access) or to remotely configure parameters on the device (commonly referred to as read-write access). SNMP agents listen on UDP port 161.

Reference: SAFE Blueprint for Small, Midsize, and Remote-User Networks

QUESTION 127

An attacker has launched an attack against a web server by requesting a web page using the Unicode representation for the slash character in the URL.
What IDS evasive technique is the attacker using?

- A. Encryption
- B. Fragmentation
- C. Flooding
- D. Obfuscation
- E. Saturation

Answer: D

Explanation: Intrusion detection systems typically implement obfuscation defense - ensuring

that suspect packets cannot easily be disguised with UTF and/or hex encoding and bypass the Intrusion Detection systems.

Reference: Cisco Intrusion Detection System - Cisco Security Advisory: Cisco Secure Intrusion Detection System Signature Obfuscation Vulnerability

QUESTION 128

What methods can be used to access the IDSM command line? (Choose two)

- A. Telnet
- B. Monitor and keyboard
- C. IDS Device Manager
- D. IDS Event Viewer
- E. Session command
- F. IDS Management Center

Answer: A, E

Explanation:

The Catalyst 6000 family switch can be accessed either through a console management session or through telnet.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 498

QUESTION 129

Which Cisco IDS service must be running if a Sensor is capturing network traffic?

- A. Managed
- B. Captured
- C. Snifferd
- D. Packetd
- E. Traffid

Answer: D

Explanation:

Packetd - The packetd daemon interprets and responds to all of the events it detects on the monitored subnet.

Reference: Cisco Secure IDS Internal Architecture

QUESTION 130

What network devices does Security Monitoring Center monitor? (Choose three)

- A. Cisco VPN Concentrators
- B. Cisco IDS Sensors
- C. Cisco Host IDS software
- D. Cisco PIX Firewalls
- E. Cisco Catalyst switches

F. Cisco Secure Access Control server

Answer: B, C, D

Explanation: You can use Event Viewer to view real-time and historical events. Events include IDS alerts (generated by network-based and host-based sensors, IOS devices, and PIX devices), syslog messages, and audit logs. This section contains the following topics:

QUESTION 131

What security management product allows IDS Sensor to be grouped for management?

- A. CSPM
- B. IDS MC
- C. IDM
- D. IEV

Answer: B

Explanation:

The CiscoWorks Management Center for IDS Sensors is management software for the configuration of network IDS, switch IDS sensors and IDS network modules for routers.

Reference: CiscoWorks Management Center for IDS Sensors

QUESTION 132

What information can a network security administrator specify in a Cisco IDS signature filter? (Choose three)

- A. Source port
- B. Source address
- C. Destination address
- D. Destination port
- E. Signature ID

Answer: B, C, E

Explanation: A filter is defined by specifying the signature, the source address, and the destination address and whether it is an inclusive or exclusive filter.

Reference: CiscoWorks Management Center for IDS Sensors - Tuning Sensor Configurations

QUESTION 133

Match the Signature micro-engine usage description with the micro-engine name.

643-531

Detect network reconnaissance	flood
Used for single packet conditions	sweep
Used for character pattern matching	string
Detect attempts to cause denial of service	atomic

Answer:

sweep
atomic
string
flood

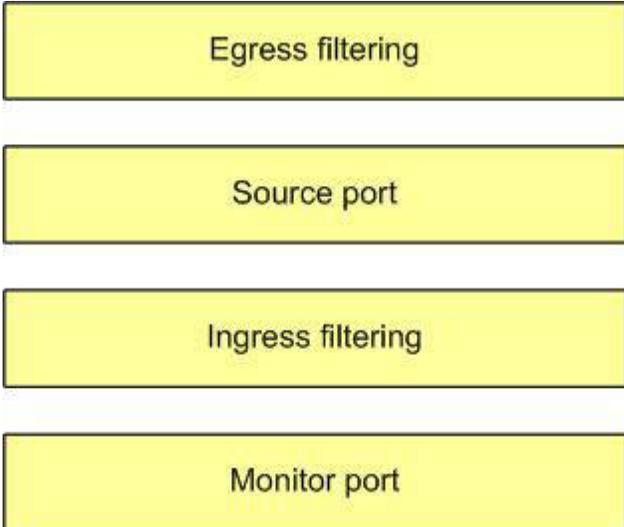
Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 628-629

QUESTION 134

Match the description of the terms used when configuring SPAN

Traffic leaving switch port	Ingress filtering
Switch port being monitored	Monitor port
Traffic entering switch port	Egress filtering
Switch port receiving mirrored traffic	Source port

Answer:



Explanation:

Ingress SPAN copies network traffic received by the source ports for analysis at the destination port.

Egress SPAN copies network traffic transmitted from the source ports for analysis at the destination port.

A source port is a switch port monitored for network traffic analysis. The traffic through the source ports can be categorized as ingress, egress, or both.

A destination port (also called a monitor port) is a switch port where SPAN sends packets for analysis.

Reference: Cisco Catalyst 6500 Series Switches - Configuring SPAN and RSPAN

QUESTION 135

Enter the Cisco IDB 4210 Sensor command used to initialize the Sensor.

Answer: sysconfig-sensor

Reference: Cisco Intrusion Detection System - Cisco Secure Intrusion Detection Sensor Cabling and Setup Quick Reference Guide

QUESTION 136

Match the Cisco IDS Sensor command with its function.

idsstop	Displays the Cisco IDM service status
cidServer stop	Stops the Cisco IDS services
idsvers	Stops the Cisco IDM service
cidServer version	Displays the Cisco IDS service version

Answer:

Stops the Cisco IDS services

Stops the Cisco IDM service

Displays the Cisco IDS service version

Displays the Cisco IDM service status

Explanation:

idsstop - Executing this script stops the Cisco IDS daemons.

cidServer stop - If you are troubleshooting an issue with TAC and you need to stop and start the server, enter the following commands

idsvers - To verify the installation of the S10 signature pack, Telnet to the Sensor, log on as netranger, and issue either the nervers or the idsvers command.

cidServer version - If you are having difficulty connecting to the sensor via the IDS Device Manager, SSH or Telnet to the sensor and type the cidServer version command to check the version and status of the sensor (whether it is running):

Reference: Cisco Secure Intrusion Detection System Internal Architecture

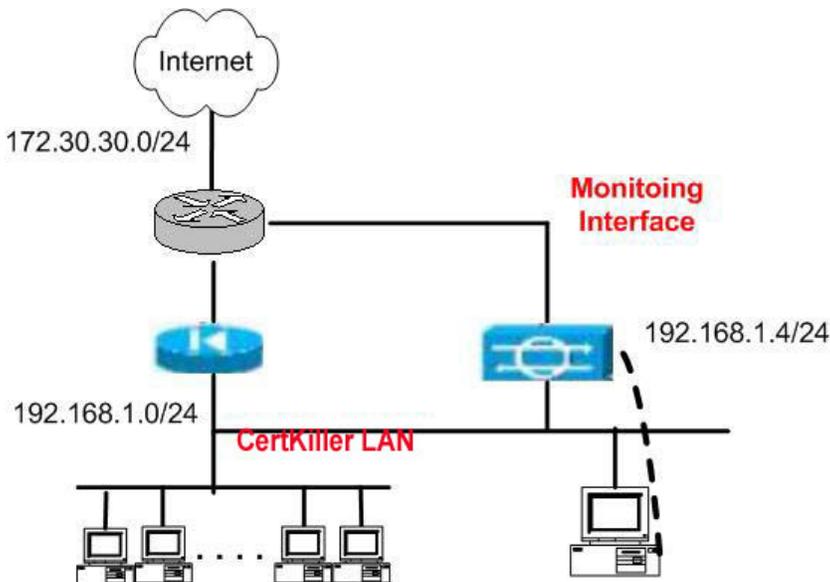
Cisco IDS Sensor Software - Cisco Intrusion Detection System Sensor Getting Started Version 3.1

Updating IDS Appliance Signatures and Troubleshooting Basic Communication

QUESTION 137

Certkiller International has decided to deploy a Cisco IDS solution. They have purchased a Cisco IOS 4235 Sensor which has never been configured. You will have to configure and initialize the Sensor to communicate with the Cisco IDS Director using the information listed in the following table:

Cisco IDS Parameters	Settings
Sensor Host ID	4
Sensor Organization ID	27
Sensor Host Name sensor	27
Sensor Organization Name	HQ



Assignment: Click on the picture of the host connected to an IDS Sensor by a serial console cable shown in the diagram as a dotted line. Select the Cisco Terminal Option and make the appropriate configuration tasks.

Sensor IP address 192.168.1.4/24

IDS Manager Host ID 4

IDS Manager Host Organization ID 27

IDS Manager Host Name sensor 27

IDS Manager Organization Name HQ

IDS Manager IP Address 192.168.1.12/24

Note: The root account password is " Certkiller "

Answer:

(Click on the host connected to the IDS Sensor)

Type: sysconfig-sensor

Select option 6 to access the Communications

Infrastructure screen, type "y" to enter in the information. Enter information for A, B, C, D, and E

A. Sensor host ID - 4

B. Sensor Organization ID - 27

C. Sensor host name - sensor 27

D. Sensor organization name - HQ

E. Sensor IP address - 192.168.1.4/24

Type "y" to use the IDS Device Manager.

Note: Use the sensor settings, not the director settings.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/13872_01.htm

Pages 6-12.

QUESTION 138

Match the common IDS deployment scenario with the appropriate description.

643-531

Internet protection	Sensors monitor traffic to business partners
Remote access protection	Sensors monitor payroll and accounting resources
Extranet protection	Sensors monitors telecommuters
Intranet and internal protection	Sensors monitor traffic outside the firewall

Answer:

Sensors monitor traffic outside the firewall

Sensors monitors telecommuters

Sensors monitor traffic to business partners

Sensors monitor payroll and accounting resources

Reference: Cisco IOS Intrusion Detection System Software App Overview