QUESTION 1
Which of the following types of attacks is typical of an intruder who is targeting networks of systems in an effort to retrieve data of enhance their privileges?

A. Access attack
B. Denial of Service attack
C. Man in the middle attack
D. Authorization attack
E. Reconnaissance 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 AttacksSystem 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 AttacksData 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 AttacksElevating 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
CCSP: Cisco Certified Security Professional Certification All-in-One Exam Guide
Cisco Courseware 13-6

QUESTION 2
Which of the following types of attacks would be a most probable consequence of the presence of a shared folder in a Windows operating system?

A. Denial of Service Attack
B. Access Attack
C. Authorization attack
D. Reconnaissance attack
E. 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 AttacksSystem 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 AttacksData 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 9xorNT 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
Cisco Courseware 3-6

QUESTION 3
Which of the following represents a type of exploit that involves introducing programs that install in inconspicuous back door to gain unauthorized access?

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

Answer: B

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:Cisco Courseware 2-46

QUESTION 4
Which of the following is typical of signature-based intrusion detection?

A. Signature creation is automatically defined
B. Signature match patterns of malicious activity
C. Signatures are prone to a high number of false positive alarms.
D. Signatures focus on TCP connection sequences

Answer: B
Page 65 Cisco Press CCSP CSIDS 2nd edition under Misuse Detection

---

QUESTION 5
What does an attacker require to perform a Denial of Service attack?

A. a means of network access
B. prior access to the target
C. previously installed root kit
D. username and password

Answer: A
DOS attacks are performed by flooding the network, so the only requirement is access to the network.
C, the requirement of installing tools to perform distributed attacks (whatever a root toolkit may be) is only true for DDOS attacks.
As the aim is not to gain access no usernames or passwords (D), and even no prior access to the target host (B) is required.
Page 2-28 CIDS Courseware v4.0

QUESTION 6
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 7
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 8
Which of the following statements represents a false positive alarm situation?

A. normal traffic or a benign action will not cause a signature to fire
B. offending traffic will not cause a signature to fire
C. normal traffic or a benign action will result in the signature firing
D. offending traffic causes a signature to fire

Answer: C

Explanation:
A false positive is a situation in which normal traffic or a bnign action causes the signature to fire. Consider the following scenario: a signature exists that generates alarms if any network devices' enable password is entered incorrectly. A network administrator attemts to log in to a Cisco router but mistakenly enters the wrong password. The IDS cannot distinguish between a rogue user and the network administrator, and generates an alarm.
Reference: Cisco Courseware p.3-11

QUESTION 9
What is a false negative alarm situation?

A. normal traffic does not cause a signature to fire
B. a signature is fired when offending traffic is not detected
C. normal traffic or a benign action causes the signature to fire
D. a signature is not fired when offending traffic is present

Answer: D
Cisco Courseware 3-11

QUESTION 10
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 generates 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 (Ciscopress) 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 11
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 generates 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 12
Which of the following is typical of profile-based, or anomaly-based, intrusion detection?

A. Normal network activity is easily defined
B. It is most applicable to environments with unpredictable traffic patterns
C. It is prone to a high number of false positive alarms
D. Signatures match patterns of malicious activity

Answer: C
Page 3-14 CSIDS Courseware under Profile-based Intrusion Detection
Prone to high number of false positives - Difficult to define "normal" activity

---

QUESTION 13
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 14
Which of the following describes the evasive technique whereby control characters are sent 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:Cisco Courseware 3-27

QUESTION 15
Which of the following represents a technique that can be used to evade intrusion detection technology?

A. man-in-the-middle
B. TCP resets
C. targeted attacks
D. obfuscation

Answer: D

Explanation:
Early intrusion detection wa easily evaded by disguising an attack by unsing special characters to conceal an attack. The term used to describe this evasive technique is obfuscation. Obfuscation is now once again becoming a popular IDS evasive technique. The following are forms of obfuscation:
1) Control characters
2) Hex representation

3) Unicode representation.
Cisco Courseware 3-27

QUESTION 16
Why would an attacker saturate the network with "noise" while simultaneously launching an attack?

A. causes the IDS to fire multiple false negative alarms
B. an attack may go undetected
C. it will have no effect on the sensor's ability to detect attacks
D. to initiate asymmetric attack techniques

Answer: B

Explanation:
By flooding the network with noise traffic and causing the IDS to capture unnecessary packets, the attacker can launch an attack that can go undetected. If the attack is detected, the IDS resources may be exhausted causing a delayed response and thus is unable to respond in a timely manner. In the figure, the attacker is sending large amounts of traffic as signified by the larger pipe. Meanwhile, the actural attack is being sent to the target host, as represented by the thin pipe that reaches the target host.
Cisco Courseware 3-24

QUESTION 17
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 18
Which of the following represents valid responses to an active attack by PIX-IDS and IOS-IDS platforms? (Choose two.)

A. initiate shunning/blocking
B. IP logging
C. drop the offending packets

D. terminate TCP sessions
E. dynamically reconfigure access control lists

Answer: C, D
Cisco Courseware 4-12 (PIX)
Cisco Courseware 4-11 (IOS)

QUESTION 19
How many sensing interfaces does the IDS-4215 support?

A. 6
B. 5
C. 4
D. 1

Answer: B

QUESTION 20
Which two Cisco IDS platforms provide integrated intrusion detection capabilities and target lower risk environments? (Choose two.)

A. IOS-IDS
B. Switch IDS module
C. PIX-IDS
D. Network appliances IDS
E. Host IDS

Answer: A, C
Cisco Courseware 4-11 (IOS)
Cisco Courseware 4-12 (PIX)

QUESTION 21
Which routers allow OIR (online insertion and removal) of NM-CIDS? Select three.

A. 3660
B. 3725
C. 3745
D. 2600XM
E. 2691

Answer: A, B, C

QUESTION 22
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 23
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 top another port.
Cisco Secure Intrusion Detection System 4 chap 5 page 3

QUESTION 24
How many sensing interfaces are supported on the NM-CIDS?

A. 1
B. 2
C. 4
D. 6
E. all router interfaces

Answer: A

QUESTION 25
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

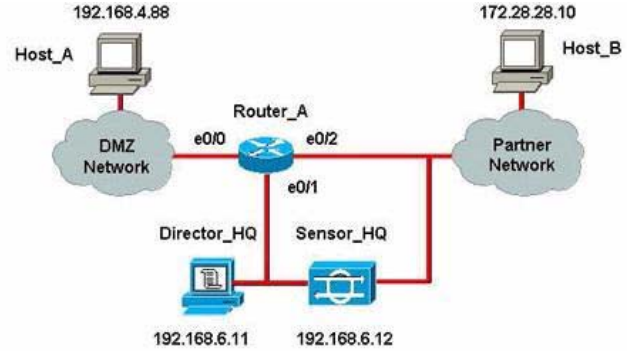
---

QUESTION 26
The new Certkiller trainee technician wants to know where the intrusion detection system sends TCP reset packets to terminate a session.What would your reply be?

A. source address of the attack packets
B. destination address of the target
C. source and destination address
D. source, destination, and IDS sensor address

Answer: C
Page 423 Cisco Press CCSP 2nd edition under Signature Response
When a specific TCP connection triggers the signature, the sensor will send TCP resets to both ends of the connection and cause it terminate.

QUESTION 27
Exhibit:



The company has decided to block using the interface connected to the Internet; the Sensor must communicate only with devices on the same network.
Which Cisco IOS router interface should the sensor use to establish an interactive session that implements blocking?

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 28
Which of the following functions can be performed remotely by means of Intrusion Detection System Device Manage? (Choose all that apply.)

A. restarting IDS services
B. initializing the Sensor configuration
C. powering down the Sensor
D. accessing the Cisco Secure Encyclopedia
E. restarting the Sensor
F. initiating a TCP reset response

Answer: A, C, E

Explanation:
Cisco IDS signature customization is now made easier through one web page. The Custom Signature configuration page presents the network security administrator with all the parameters that can be customized for a specific signature.
IDM enables the network security administrator to remotely:
1) Restart the IDS services.
2) Restart the Sensor.
3) Power down the Sensor.
Cisco Courseware 10-4

QUESTION 29
Which of the following features regarding the IDSM2 is true?

A. IDSM2 needs a separate management package
B. IDSM2 is limited to 62 signatures
C. IDSM2 can drop offending packets
D. IDSM2 makes use of the same code as the network appliance

Answer: D
Page 199 Cisco Press CCSP CSIDS 2nd edition under Key Features
IDSM-2 provides the following capabilities or features:

- Merged switching and security into a single chasis
- Ability to monitor multiple VLANs
- Does not impact switch performance
- Attacks and signatures equal to appliance sensor
- Uses the same code base of the appliance sensor
- Support for improved management techniques such as IDM

QUESTION 30
Which of the following features regarding IDSM2 is true?

A. parallels attacks and signature capabilities of the 4200 series appliances
B. supports subset of signatures available in appliance
C. support ISL trunking
D. is capable of tracking VLAN identification numbers

Answer: A

QUESTION 31
What is the maximum number of VLANs the IDSM2 is capable of handling and monitoring?

A. 100
B. 250
C. 500
D. unlimited

Answer: D
Cisco Courseware 8-4

QUESTION 32
Under which tab on IDM can you find the Signature Wizard?

A. Device
B. Config
C. Monitoring
D. Administration

Answer: B
Cisco Press CCSP Self-Study CSIDS, p 223-24

QUESTION 33
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 34
Which of the following supported client platforms are capable of communicating with aMonitoring Centerfor Security server running on a Windows-based platform?

A. Windows only
B. Windows and Linux only
C. Windows and Solaris only
D. Solaris only
E. Windows, Linux, and Solaris
F. any platform which supports Netscape Navigator v4.76 or later

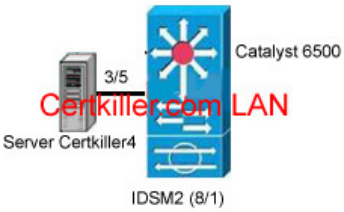
Answer: C
Page 603 Cisco Press CCSP CSIDS 2nd edition under Client Requirements
Clients need to run of the following OS:
- Windows 2000 Pro, Server, Adv. Server with Service Pack 3
- Windows XP Pro
- Solaris 2.8
Cisco Courseware 10-5

QUESTION 35
What are the two methods used to initially access the IDSM? (Choose two.)

A. Telnet to the switch
B. Telnet to the IDSM
C. By use of the IDS Device Manager GUI
D. Console cable connection to the switch
E. By use of the RDEP protocol

Answer: A, D
Since module configuration is a sub instance of normal switch configuration, every method to connect to the switch's CLI makes IDSM Module configuration possible too.
See also:
Cisco Courseware 8-13

QUESTION 36
Exhibit:



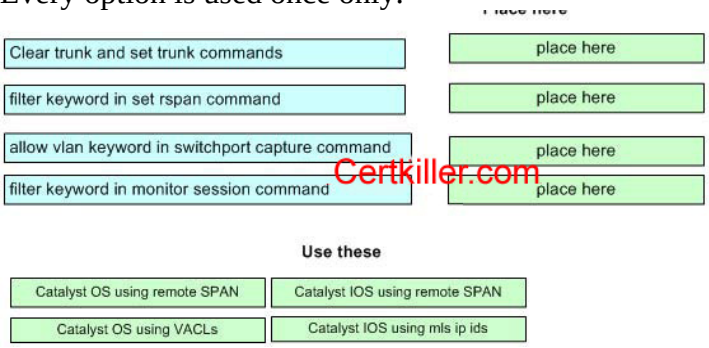
According to the exhibit, Server Certkiller 4 is in VLAN 8. The Catalyst 6500 is running Catalyst OS. Which of the following commands would you use as a configuration step if one is to permit the ISDM2 to monitor traffic sent to and from VLAN3, VLAN4, and VLAN5?

A. 6500(config)# monitor session 1 source 3-5 both
B. 6500(config)# monitor session 1 destination idsm
C. 6500(config)# monitor session 1 source vlan 3, 4, 5
D. 6500>(enable) set span 3 -5 8/1 both
E. 6500>(enable) set span source vlan-list 3 - 5 destination interface 8/1 both create

Answer: D

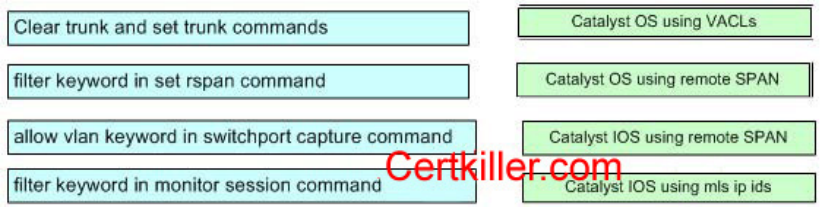
Explanation: Because of ISDM-2
Cisco Courseware 12-7

QUESTION 37
Following is a list of filtering methods followed by a list of configurations. Match the most appropriate filtering method to the capture configuration that restricts the VLANs monitored on a trunk port. Note: Every option is used once only.



Answer:

Explanation:



Clear trunk and set trunk commands -----> [Catalyst OS using VACLs]
Cisco Courseware 5-56

---
filter keyword in set rspan command ---> [Catalyst OS using remote SPAN]
Cisco Courseware 5-25
---
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]

To monitor specific VLANs when the local or RSPAN source is a trunk port, perform this task:
This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the source is a trunk port:
Router(config)# monitor session 2 filter vlan 1 - 5 , 9

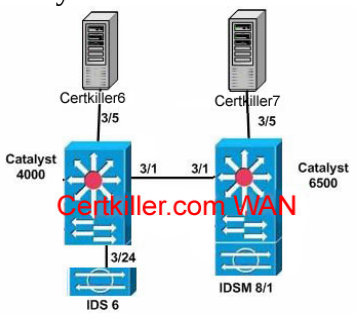
QUESTION 38
Which of the following commands are used by a Catalyst switch running Catalyst OS to block attacks, as directed by an IDS blocking Sensor?

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

Answer: E

Explanation:
Since the Catalyst is using CatOS, D is incorrect.
The proper command to define the security ACL or VACL is set security acl ip switch command
Reference: Page 147, Cisco Press CCSP 2nd Edition, Chapter 6 Capturing Network Traffic.
Cisco Courseware 5-33

QUESTION 39
Study the exhibit below carefully:



According to the exhibit Fast Ethernet connections are used to connect all switches. 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. 4000>(enable) set rspan destination 99 3/24
B. 4000>(config)# monitor session 2 destination interface fastEthernet 3/24
C. 6500(config)# remote-span 99
D. 6500>(enable) set rspan source 3/5 99 tx create
E. 4000>(enable) set rspan source vlan 99 destination interface fastEthernet 3/24

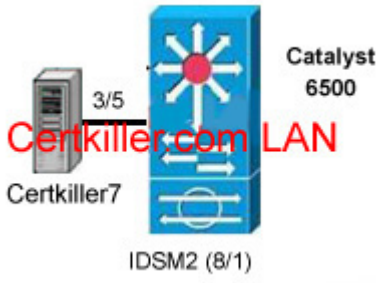
Answer: D

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
Step1	Configure RSPAN source ports. Use this command on each of the source switches participating in RSPAN.	**set rspan source**{mod/ports... | vlans... | sc0} {rspan_vlan} [rx | tx| both] [multicast {enable | disable}] [filter vlans...] [create]

Reference:Cisco Courseware 5-25

QUESTION 40
Study the exhibit below carefully:



According 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. This feature is not supported in this configuration.
D. 6500>(enable) set span source vlan-list 3- 5 destination interface 8/1 both create
E. 6500>(enable) set span 3 - 5 8/1 both

Answer: A

Explanation:
Switch(config)#monitorsession{session_number}{source{interfacetype/num}|{vlanvlan_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:Cisco Courseware 5-20

QUESTION 41
What function does themls ip ids command perform when used for traffic capture?

A. the mls ip ids command assigns a port to receive capture traffic
B. the mls ip ids command selects all IP traffic for IDS monitoring
C. the mls ip ids command applies the IDS ACL to an interface
D. the mls ip ids command processes capture in hardware versus software
E. the mls ip ids command is used with keywords to define interesting traffic

Answer: C
Page 5-45 CSIDS Courseware under Using the mls ip ids command for Catalyst 6500 Traffic capture
1)Create an ACL to capture interesting traffic
2)Select the VLAN interface
3)Apply the ACL to the interface
4)Assign the Sensor's monitoring port as a VACL capture port
Note: The ml sip ids command is used to apply an extended IP access list to the VLAN interface.
Cisco Courseware 5-48

QUESTION 42
Study the exhibit below carefully:

According to the exhibit all switches are connected through Fast Ethernet connections. The Catalyst 4000 is running Catalyst OS . Sensor ID Certkiller is configured to send TCP resets in response to specific signatures. Which command argument in the Catalyst 4000's SPAN configuration will allow the switch to receive the TCP resets sent from Sensor ID Certkiller 3

A. rx
B. both
C. ingress
D. tcp-rst accept
E. inpkts enable
F. This feature is not supported in this configuration

Answer: E
IDS course 4.0 page 5-19 Keyworks to enable the receiving of normal inbound traffic in the SPAN destination port.

QUESTION 43
Study the exhibit below carefully:

According to the exhibit all switches are connected through Fast Ethernet connections. Server Certkiller 7 and Sensor ID Certkiller 7 are in the same VLAN.
Which of the following commands represents a valid configuration step to permit Sensor ID Certkiller 7 to monitor traffic sent from Server Certkiller 7?

A. 3500xl(config)#monitor session 1 source interface fastEthernet 0/5 tx
B. 3500xl(config-if)#port monitor fastEthernet 0/5
C. 3500xl>(enable)set span 0/5 0/24 both
D. 3500xl(config)#monitor session 1 source interface fastEthernet 0/5 rx
E. 3500xl>(enable)set span 0/24 0/5 rx create
F. No SPAN configuration is required since both devices are in the same VLAN

Answer: B
Catalyst 2900XL / 3500XL
1. port monitor [interface | vlan]
Note: D would be correct for 3550 switches, but not for 3500XL
Cisco Courseware 5-14

QUESTION 44
Which of the following represents the basic steps in the configuration of VACLs for traffic capture on a Catalyst 4000 switch running Catalyst OS. (Choose two.)

A. map the VACL to the capture port
B. assign ports to receive capture traffic
C. define an access-group for interesting traffic
D. commit the VACL to memory
E. create action clause to capture traffic

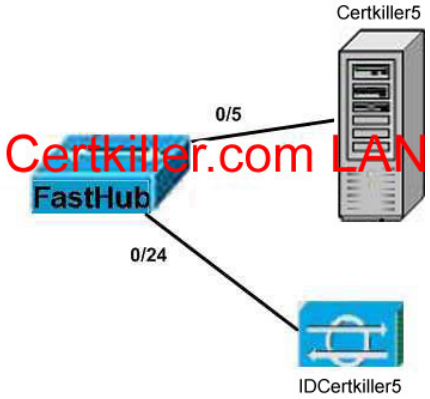
Answer: B, D
Page 146 Cisco Press CCSP Chapter 6 Capturing Network Traffic
Step 1: Define a security ACL
Step 2: Commit the VACL to memory
Step 3: Map the VACL to VLANs
Step 4: Assign the capture port
Note:Does the 4000 switch really support VACLs?

QUESTION 45
The new Certkiller trainee technician wants to know what binds the input and output of a source RSPAN session on a Catalyst 6500 switch running IOS.What would your reply be?

A. RSPAN vlan-id
B. interface number
C. SNMP ifIndex
D. single command implicitly maps inputs and outputs
E. session number

Answer: E
Cisco Courseware 5-20 (source)
Cisco Courseware 5-21 (destination)

QUESTION 46
Study the exhibit below carefully:



According to the exhibit all switches are connected through Fast Ethernet connections. Server Certkiller 5 and Sensor ID Certkiller 5 are in the same VLAN.
Which of the following commands represents a valid configuration step to permit Sensor IDS5 to monitor traffic to Server Certkiller 5?

A. fasthub(config)# monitor session 1 source interface fastEthernet 0/5 tx
B. fasthub(config)# monitor session 1 source interface fastEthernet 0/5 rx
C. fasthub(config-if)# port monitor fastEthernet 0/5
D. fasthub>(enable) set span 0/5 0/24 both
E. No SPAN configuration is required since both devices are in the same VLAN

Answer: E

Explanation:
We must agree with the conclusion that this is nonsense, but E must be the correct answer since a hub a layer 2 device meaning that it doesn't do network segmenting. All devices connected to the hub wil receive the same traffic.

QUESTION 47
Study the exhibit below carefully:

According to the exhibit all switches are connected through Fast Ethernet connections. Server Certkiller 3 is in VLAN 8. The Catalyst 4000 is running Catalyst OS. Which of the following commands represents a valid configuration step to permit IDS3 to monitor traffic sent to and from Server Certkiller 3?

A. 4000(config)# monitor session 1 source vlan 8 both
B. 4000(config)# monitor session 1 destination interface fastEthernet 3/24
C. 4000>(enable) set span 3/5 3/24 both create
D. 4000(config)# monitor session 1 source fastEthernet 3/5 destination fastEthernet 3/24 tx rx
E. 4000(config-if)# port monitor interface fastEthernet 3/5
F. This feature is not supported in this configuration

Answer: C
Cisco Courseware 5-18

QUESTION 48
Identify two basic steps in the configuration of VACLs for traffic capture on a Catalyst 6500 switch running IOS. (Choose two.)

A. Configure match clauses using the capture option.
B. Map the VLAN access map to a VLAN.
C. Use commit to save the VACL configuration.
D. Assign ports to receive capture traffic.
E. Crate VACL using the set security acl command.

Answer: B, D

Explanation:
The tasks to capture traffic using VLAN Access Control Lists (VACLs) on a Catalyst 6500 switch running IOS are as follows:
1) Configure ACLs to define interesting traffic.
2) Define a VLAN access map
3) Configure the match clause in the VLAN access map using ACLs
4) Configure the action clause in the VLAN access map using the capture option.

5) Apply the VLAN access-map to the specified VLANs
6) Select an interface.
7) Enable the capture function on the interface.
Cisco Courseware 5-38

QUESTION 49
What is a primary reason for using the mls ip ids command to capture traffic instead of VACLs?

A. higher performance due to hardware-based multilayer switching
B. CBAC is configured on the same VLAN
C. Switch is running Catalyst OS; VACLs are only supported in IOS
D. Destination capture port is an IDSM; VACLs do not support IDSM
E. mls ip ids offers more granularity for traffic capture than VACLs

Answer: B
You cannot apply VACLs to the same VLAN in which you have applied an IP inspect rule for the Cisco IDS Firewall.
(IP inspect rule is a CBAC feature -> mls ip ids can be used instead of VACLs to solve this problem)
Cisco Courseware 5-45, 5-48

QUESTION 50
Network topology exhibit:

Refer to the exhibit. All switches are connected through Fast Ethernet connections. Server Certkiller 2 is in VLAN 3.
Which command represents a valid configuration step to permit Sensor IDS1 to monitor traffic sent from Server Certkiller 2?

A. 2950(config)# monitor session 1 source interface fastEthernet 0/5 tx
B. 2950(config)# monitor session 1 source interface fastEthernet 0/5 rx
C. 2950(config)# port monitor fastEthernet 0/5
D. 2950(config)# port monitor vlan 3 Interface fastEthernet 0/24 both
E. 2950>(enable) set span 0/5 0/24 both

Answer: B
sent FROM server, RECEIVED by fastEthernet 0/5 -> rx
Cisco Courseware 5-16
Note:The reason is not

A. because you want to monitor receive traffic from the server. It is not C. because the port monitor fastEthernet 0/5command should be done in the (config-if)# mode. D and E are incorrect.

QUESTION 51
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

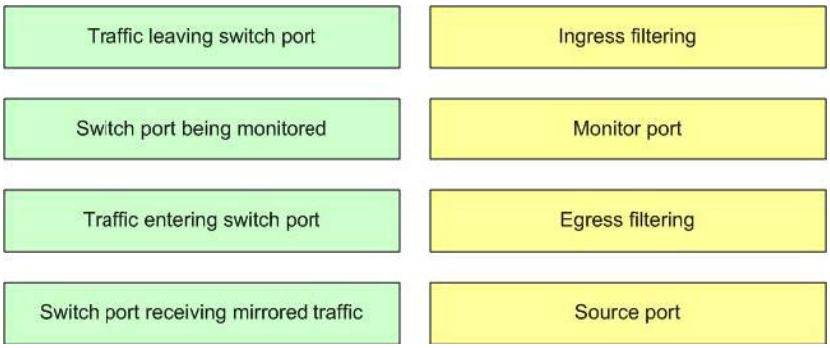
Explanation:
To create a VACL, you need to use the set security acl ip switch command. The syntax for capturing TCP traffic between a source IP address and a destination IP address is as follows:
set security aclip acl_name permit tcp src_ip_spec dest_ip_spec port capture
Reference:Cisco Secure Intrusion Detection System (Ciscopress) page 505
Cisco Secure Intrusion Detection System 4 chap 5 page 33

QUESTION 52
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?

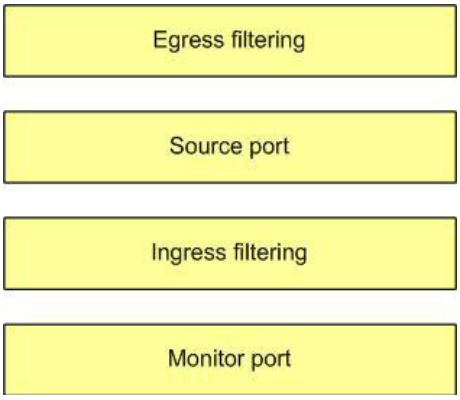
A. set trunk 9/2 199
B. clear trunk 9/2 199
C. clear trunk 9/2 1-1024
D. clear trunk 9/1 1-1024
E. set trunk 9/1 199
F. clear trunk 9/1 199

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 mpl 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 53
Match the description of the terms used when configuring SPAN



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 54
What must be done when upgrading Cisco IDS appliance models IDS-4235 or IDS-4250 from Cisco IDS v3.x?

A. swap the command and control and monitoring interfaces
B. install the spare hard-disk derive
C. BIOS upgrade
D. No special considerations are required
E. Memory upgrade

Answer: C
Page 7-16 CIDS Courseware v4.0

QUESTION 55
You are using multiple monitoring interfaces on a Sensor appliance running software version 4.1. Which four statements are true? Choose four.

A. You can have simultaneous protection of multiple network subnets, which is like having multiple Sensors in a single appliance.
B. You can use different configurations for each monitoring interface.
C. You must enable the monitoring interfaces in order fro the Sensor to monitor your networks.
D. You can enable an interface only if the interface belongs to an interface group.
E. Two interface groups, Group 0 and Group 1, are supported.
F. Multiple monitoring Interfaces can be assigned to Group 0 at any given time.

Answer: A, B, C, F
Page 9-13, 9-14 CIDS Courseware v4.0

QUESTION 56
Which sensor appliance does not support the connection of a keyboard and mouse for management?

A. 4235
B. 4250
C. 4215
D. 4250XL

Answer: C

QUESTION 57
On the IDSM-2, which logical port is used as the TCP reset port?

A. 1
B. 2
C. 7
D. 8

Answer: A

Explanation:
The IDSM2 uses four logical ports which have the following default designations:
1) Port 1 is used as the TCP reset port.
2) Port 2 is the command and control port.
3) Ports 7 and 8 are monitoring ports. One of these ports can be configured as the SPAN monitor port.

QUESTION 58
Which of the following commands will provide the basic initialization tasks in Cisco IDS?

A. configure terminal
B. sysconfig-sensor
C. set
D. setup
E. initialize

F. session

Answer: D
Page 8-8 CSIDS Courseware under IDSM2 and Switch Configuration Tasks
- Initialize the IDSM2. This includes completing the basic configuration via the setup command.

QUESTION 59
Which command will you advice the new Certkiller trainee technician to issue in order to initiate the IDSM2 system configuration dialog?

A. sysconfig-sensor
B. setup
C. configure terminal
D. session
E. initialize

Answer: B
Page 8-12 CSIDS Courseware under IDSM2 Initialization Tasks
- Execute the setup command to enter the configuration dialog
- Run the setup command and respond to its interactive prompts to complete the initial configuration

---

QUESTION 60
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 61
Which user account is used to log into the IDSM?

A. Root
B. Administrator
C. Netranger

D. Ciscoidsm
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

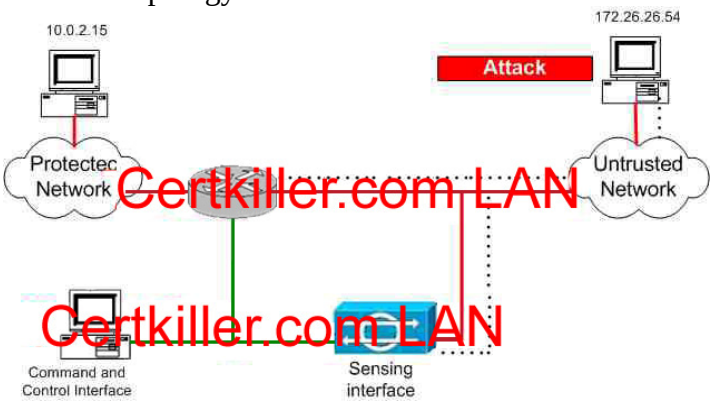
QUESTION 62
The new Certkiller trainee technician wants to know what will happen when the Sensor alarm reaches the 4GB storage limit.What would your reply be?

A. Alarms will not be written anymore
B. Alarms will be overwritten by new alarms
C. Alarms will be sent to offline event storage
D. Alarm storage size will increase dynamically

Answer: B

Explanation:
All events are stored in the Sensor eventStore. Events remain in the eventStore until they are overwritten by newer events. It takes 4 GB of newer events to overwrite an existing event.
Events can be retrieved through the Sensor's web server via RDEP communications. Management applications such as IEV and the Security Monitor use RDEP to retrieve events from the Sensor.
Cisco Courseware 9-37

QUESTION 63
Network topology exhibit/simulation

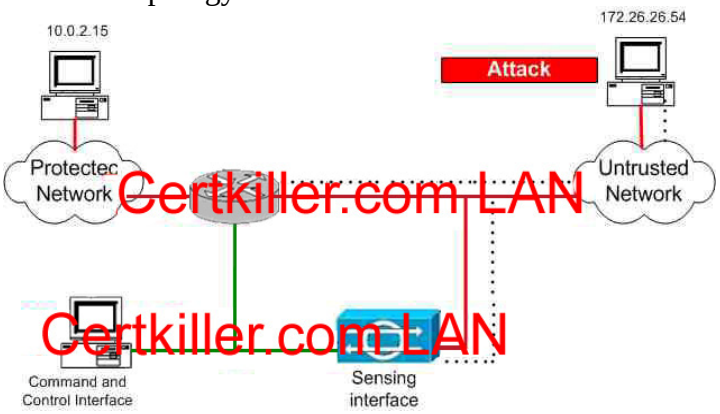


Sensor output exhibit: ***MISSING***
Note: Use the sensors command line interface to obtain information so that you can answer the question.
You are NOT expected to do any configuration.
Which of the following states would be displayed if the Sensor has established a connection to the router?

A. "State = Connected" in the Network Access Controller service's configuration mode.
B. "State = Connected" in the Network Access Controller's statistics.
C. "State = Active" in the Network Access Controller service's configuration mode.
D. "State = Active" in the Network Access Controller's statistics

Answer: D
No exact answer is provided in the course, but in the simulation look up the statistics, and you'll find the State=Active
Command:
show statistics NetworkAccess
Cisco Courseware 9-40

QUESTION 64
Network topology exhibit/simulation



Sensor output exhibit: ***MISSING***
View the signature's settings.
The signature is not configured to perform blocking.
Note: Use the sensors command line interface to obtain information so that you can answer the question.
You are NOT expected to do any configuration.
Why isn't blocking working?

A. Blocking is not enabled on the Sensor.
B. The signature is not configured for blocking.
C. The router does not exist in the Sensor's known hosts table.
D. The signature is not firing.

Answer: B

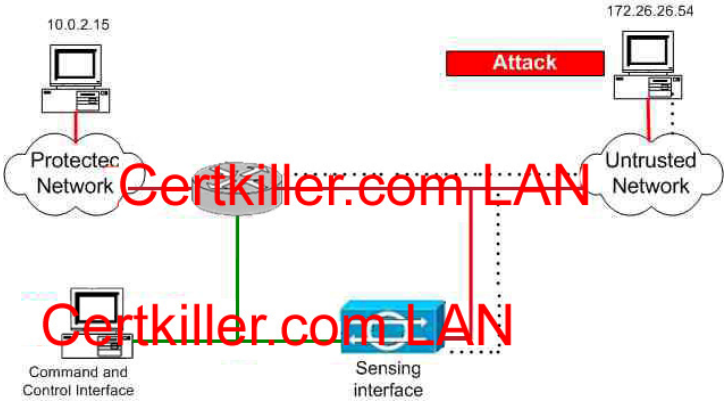
QUESTION 65
Network topology exhibit/simulation

Sensor output exhibit: ***MISSING***
The user name is Jag.
Note: Use the sensors command line interface to obtain information so that you can answer the question.
You are NOT expected to do any configuration.
What is the username the Sensor will use to log in to the router?

A. Admin
B. Certkiller
C. Lin
D. Cisco
E. Jag

Answer: E

QUESTION 66
Network topology exhibit/simulation



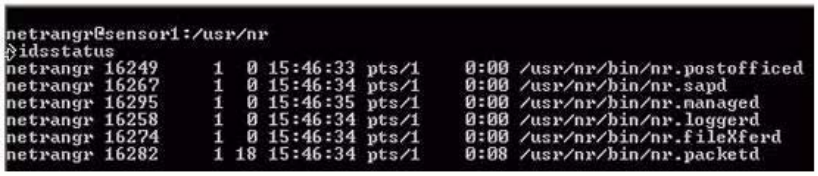
Sensor output exhibit: ***MISSING***
No ACL is configured.
Note: Use the sensors command line interface to obtain information so that you can answer the question.
You are NOT expected to do any configuration.
What pre-block ACLs are specified?

A. None
B. PreBlockACL

C. BlockingACL
D. RouterACL

Answer: A

QUESTION 67
Exhibit:



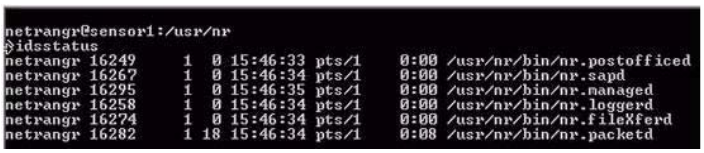
Given the output of the idsstatus Sensor command. What function is the Sensor performing? (Choose two)

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:
PostofficedThe 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.
LoggeredThe 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 68
Exhibit:



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:
PostofficedThe 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.
LoggeredThe loggerd daemon writes out sensor and error data to flat files generated by one or more of the other daemons.
fileXferdThe 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 69
Which of the following files is generated as a consequence of Sensor installation and provides information such as model and interface capabilities?

A. AE-Boot
B. BaseConfig
C. Boot.info
D. VS-Config

Answer: C

QUESTION 70
Which versions of Cisco IDS software are available on the NM-CIDS?
a. 3.1 and above.
B. 4.1 and above
C. 4.0 and above
D. 2.0 and above

Answer: B

Explanation:

Series	Devices Supported	Software
Cisco Network IDS Sensor Appliances	NRS-2E	IDS 3.0 and IDS 3.1

NRS-2FE		IDS 3.0 and IDS 3.1
NRS-TR		IDS 3.0 and IDS 3.1
NRS-SFDDI		IDS 3.0 and IDS 3.1
NRS-DFDDI		IDS 3.0 and IDS 3.1
IDS-4210		IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
IDS-4215		IDS 4.1
IDS-4220		IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
IDS-4230		IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
IDS-4235		IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
IDS-4250-TX and IDS-4250-SX		IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
IDS-4250-XL		IDS 4.0 and IDS 4.1
Cisco Switch IDS Sensor Modules	IDSM	IDSM 3.0(5) and IDSM 3.0(6)
IDSM2		IDS 4.0 and IDS 4.1
Cisco IOS Router IDS Sensor Module	NM-CIDS	IDS 4.1

QUESTION 71
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
IDS Event Viewer (IEV) .
IEV is software application provided with your sensor that enables you to analyze the alarm traffic up to 5 network sensors

---

QUESTION 72
Which of the following represents the recommended procedure when upgrading a Cisco IDS appliance which is prior to version 4.x?

A. Install the image from the IDS Management Center.
B. Install the image from the network connection.
C. Install the image from the recovery or upgrade CD.
D. Install the image from the BIOS boot diskette.

Answer: C
Page 7-17 CSIDS Courseware under Software Installation Overview
To upgrade an IDS appliance from IDS software version 3.x to version 4.0, you must install the new 4.0 image from the 4.0(1) Upgrade/RecoveryCD

QUESTION 73
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 74
Which of the following protocols is used by the IDS MC Sensors 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 CiscoIntrusionDetectionSystem 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:Cisco Courseware 6-8

QUESTION 75
Which of the following management access methods are enabled by default on the Sensor in a Cisco IDS appliance? (Choose all that apply.)

A. Telnet
B. SSH
C. https
D. IPSec
E. Postoffice

Answer: B, C
Following are the methods used to gain management access to a Sensor:
- Console port
- Monitor and Keyboard
- Telnet (Disabled by default)
- SSH (Enabled by default)
- HTTPS (Enabled by default)
Cisco Courseware 7-22, 7-23

QUESTION 76
Which user account role must you specifically create inorder to allow special root access for troubleshooting purposes only on a Cisco IDS Sensor?

A. operator
B. viewer
C. service
D. administrator
E. client

Answer: C

Explanation:
The service account is a special account that allows TAC to log into a native, operating system shell rather than a CLI shell. The purpose of the service account is not to support configuration but to support troubleshooting. to use during troubleshooting. Root access to the Sensor is only possible if you log into the service account and su to the root account.
Reference: Cisco Student Guide v4.0 p.6-13

QUESTION 77
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 78
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)#netwrokParams
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 79
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 80
Which command would you will you advice the new Certkiller trainee technician to use inorder to view the initial configuration parameters on the IDSM2?

A. show capture
B. setup
C. show running-config
D. session

Answer: B
IDS course 4.0 page 8-8 Initialize the IDSM2 this includes completing the basic configuration via the setup command.
Note:
After you enter the setup command the default settings are displayed.
(Press spacebar to continue the setup).
Cisco Courseware 7-26

QUESTION 81
Enter the Cisco IDS 4210 Sensor command used to initialize the Sensor.

Answer: sys config-sensor
Reference: Cisco Intrusion Detection System - Cisco Secure Intrusion Detection Sensor Cabling and Setup Quick Reference Guide

---

QUESTION 82
The new Certkiller trainee technician wants to know which of the following is one task that can be performed while in the interface sensing configuration mode from the Sensor CLI.What would your reply be?

A. add a sensing interface to the group
B. configure the interface's IP information0
C. disable the sensing interface
D. configure alarm setting

Answer: C

Explanation:
The interface sensing configuration mode is a third level of the CLI. It enables you to enable or disable the sensing interface.
Command: shutdown
Cisco Courseware 9-14

QUESTION 83
Which of the following qualifies to be a second level CLI mode in Cisco IDS?

A. privileged exec
B. service
C. global configuration
D. tune micro engines
E. all of the above

Answer: C
Page 9-11 CSISD Courseware under Global Configuration Mode
- Global configuration mode is the second level of the CLI

QUESTION 84
Which CLI mode allows for configuration of a Cisco IDS Sensor's interface IP information?

A. global configuration
B. Interface command-control
C. interface group
D. privileged exec

Answer: B
sensor1(config)#:interface command-control
sensor1(config)#:?
ip ... Configure IP information for the interface
Cisco Courseware 9-12

QUESTION 85
Which access method supports configuration and troubleshooting?

A. IDS event Viewer
B. Cisco ConfigMaker
C. Command Line Interface
D. Syslog

Answer: C

QUESTION 86
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:

Explanation:

Stops the Cisco IDS services
Stops the Cisco IDM service
Displays the Cisco IDS service version
Displays the Cisco IDM service status

* 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 netrangr, and issue either the nrvers 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 87
What type of user account would you need to be able to be allowed to perform all Sensor operations on a Cisco IDS Sensor?

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

Answer: D

Explanation:
User Roles
The CLI for IDS version 4.0 supports three user roles: Administrator, Operator, and Viewer. The privilege
1. Administrators-This user role has the highest level of privileges. Administrators have unrestricted view access and can perform the following functions:
2. 1. Add users and assign passwords.
2. Enable and disable control of physical interfaces and interface groups.
3. Assign physical sensing interfaces to interface groups.
4. Modify the list of hosts allowed to connect to the sensor as configuring or viewing agents.
5. Modify sensor address configuration.
6. Tune signatures.
7. Assign virtual sensor configuration to interface groups.
8. 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:
1. Modify their passwords.
Reference:Cisco Courseware 9-23

QUESTION 88
Which statement regarding the service account on an IDS Sensor is valid?

A. Only users with the administrator role can be assigned to the service account.
B. Advanced signature tuning operations can be performed through the service account.
C. The service account must be created by Cisco TAC personnel.
D. A singular user only can be assigned to the service account.

Answer: D

Explanation:
Creating the Service AccountYou 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.
CautionDo 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:Cisco Courseware 7-24

QUESTION 89
What is the default privilege level that is set when creating a user account on a Cisco IDS Sensor?

A. Viewer
B. Administrator
C. Operator
D. Anonymous
E. Guest

Answer: A
Privileges:
Allowed levels are:
1. Service
2. Administrator
3. Operator
4. Viewer
The default is Viewer.
Cisco Courseware 9-23

QUESTION 90
When setting up user accounts on a Cisco IDS Sensor. What role would you assign to provide users all viewing operations and the administrative ability to change only their own passwords?

A. operator
B. viewer
C. service
D. administrator

Answer: B
Viewers can view configuration and event data and can perform the following function:
1. Modify their password
Cisco Courseware 9-24

QUESTION 91
The new Certkiller trainee technician wants to know what the function of the "tls generate-key" command on the Cisco IDS sensor is.What would your reply be?

A. "tls generate-key" command generates a SSH host key
B. "tls generate-key" command generates a TLS host key
C. "tls generate-key" command generates X.509 certificate to present to the Certificate Authority
D. "tls generate-key" command generates a self-signed X.509 certificate

Answer: D

Page 9-33 CSIDS Courseware under Generating an X.509 Certificate
Use the tls generate-key command to generate the self-signed X.509 certificate needed by TLS

QUESTION 92
Which CLI command would permit remote network access to the IDS Sensor from network 10.1.1.0/24?

A. sensor(config)# access-list 100 permit 10.1.1.0.0.0.0.255
B. sensor(config-Host-net)# access-list 100 permit 10.1.1.0.0.0.0.255
C. sensor(config)# accessList ipAddress 10.1.1.0 netmask 255.255.255.0
D. sensor(config-Host-net)# accessList ipAddress 10.1.1.0 netmask 255.255.255.0

Answer: D
Cisco Courseware 9-31

QUESTION 93
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 94
Which of the following Sensor commands will archive IP log files to a remote host?

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

Answer: B

Explanation:

copy
Use the copy command to copy iplogs and configuration files.
copy [/erase]source-url destination-url
copy iploglog-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 over-written. 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.
source-url	The location of the source file to be copied. May be a URL or keyword.
destination-url	The location of the destination file to be copied. May be a URL or keyword.
log-id	Log id of file to copy. The log-id can be retrieved using the iplog-status command.

Reference:Cisco Courseware 12-19

QUESTION 95
The new Certkiller trainee technician wants to know what the PuTTYgen utility in IDS MC is used for. What will your reply be?

A. PuTTYgen utility is used to generate SSL certificates for IDS Sensors.
B. PuTTYgen utility is used to generate SSH public and private keys for IDS Sensors.
C. PuTTYgen utility is used to generate SSH public and private keys for IDS MC server.
D. PuTTYgen utility is used to generate SSL keys for administrative client access to IDS MC server.
E. PuTTYgen utility is used to generate shared secret keys for IDS Sensors and IDS MC server.

Answer: C

Explanation:
To use SSH keys in IDSMC or SecurityMonitor, follow these steps:
Step1 To use SSH keys in IDSMC or SecurityMonitor for Windows 2000, follow these steps:
a. Use PuttyGen to generate your keys. Instructions are available at http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html .
b. Copy the public key to the sensor's ~.ssh/authorized_keys file.

c. Save the private key. We recommend the name sensorname.key for the private key and we use it in this example.
Reference:Cisco Courseware 12-7

QUESTION 96
How would you go about successfully adding 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 the Sensor's software version to a version matching one in the IDS MC list.
B. Select the Discover Settings check box to automatically discover the unlisted version.
C. Update IDS MC with the latest IDS signatures.
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:
Page 12-5 CSIDS Course under Device - Sensor
Under the last paragraph, if the Sensor software version is not listed in the drop-down menu, it will be necessary to update the IDS MC with the latest version of IDS Signatures

---

QUESTION 97
Which of the following pieces of information is needed 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. Any legitimate values for IP address, Sensor name, user ID, and password
D. Correct Sensor name and SSH settings
E. Correct user ID, password, and IP address

Answer: C

Explanation:
Step5 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.
NoteIf 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:Cisco Courseware 12-3

QUESTION 98
Which of the following represents 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:
Cisco Courseware 12-3: Devices -> Sensor -> Add

QUESTION 99
Which of the following statements regarding Sensor group functions is valid? (Choose all that apply.)

A. Sensor groups permit signature updates to be performed in batch mode
B. Sensor groups allow configuration settings and policies to be inherited by subgroups
C. Sensor groups create administrative access domains for controlling Sensor access rights
D. Sensor groups provide a single point of configuration for parameters common to multiple Sensors
E. Sensor groups are dynamically created to separate Sensor platform types

Answer: B, D

Explanation:
The IDS MC uses a hierarchy of groups and Sensors. A group can contain Sensors, other groups, or a combination of Sensors and groups. When you start the IDS MC, you always have levels of groups and Sensors, just as a folder in Windows 2000 can contain many levels of folders and files.
The IDS MC hierarchy of groups and Sensors enables you to configure more than one Sensor at a time by configuring an entire group of Sensors simultaneously. Configuring more than one Sensor at a time in this way is possible because a Sensor can acquire settings from its parent group. A Sensor must, in fact, acquire settings from its parent group if a parent defines those settings as mandatory. A child cannot override the values for such settings.
Cisco Courseware 12-12

QUESTION 100
Which of the following options are available to add a new Sensor group? (Choose all that apply.)

A. inherit settings from the subgroup
B. copy settings from another group
C. import group from the Monitoring Center for Security
D. copy settings from the Monitoring Center for Security group
E. inherit settings from the parent group

Answer: B, E
Page 12-13 CSIDS Courseware under Devices-Sensor Group
Note: When you create subgroups, the subgroup inherits the properties of either the parent group or you may copy settings from another group to the new subgroup

---

QUESTION 101
Select the true statements regarding Sensor groups.

A. The mandatory check box exists in the context of a Sensor object to identify required configuration settings.
B. The override check box exists In the context of a Sensor Group object to prevent configuration parameters from being inherited.
C. The override check box exists in the context of a Sensor object to override settings previously flagged as mandatory.
D. By default, all Sensor subgroups inherit the configuration settings of other Sensors in the same Sensor group.
E. The mandatory check box exists in the context of a Sensor Group object to indicate that all fields in the configuration windows require values.

Answer: B, D
"A sensor must, in fact, acquire settings from the parent group, if a parent defines those settings as mandatory. A child cannot override the values for such settings."
(C) is false because of the keyword must in the statement above, so that a child cannot override values for mandatory settings.
(B) Cisco Courseware 12-15 shows the "Override" checkbox in a screenshot.
(D) Cisco Courseware 12-12 shows a screenshot with the selection key:
O Default (use parent values)
(A) and (E) are false, because "mandatory" check boxes say nothing about "requirements", but if subgroups must use the parameter or not (by overriding it):
Cisco Courseware 12-12:

QUESTION 102
You need to retrieve Sensor IP logs for analysis. Which of the following methods are available to you to accomplish this task? (Choose all that apply.)

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

Answer: A, C

Explanation:
Page 12-19 CSIDS Courseware under Automatic Logging
IP Log Files can be retrieved by the following methods
1) Use the CLI copy command to copy the IP log files to another host system using FTP or SCP.

2) Download the IP log files via IDM.
After retrieving the IP log files, you can use a network protocol analyzer to examine the data.
Not B:Archive using SCP is false, although
Copy using SCP would be true.

QUESTION 103
The new Certkiller trainee technician wants to know how automatic IP logging is enabled on Sensor.
What would your reply be?

A. It is enabled by default for all high-severity signature alarms.
B. It is enabled by default for all signatures.
C. It is enabled by default for all master signatures only.
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 signature-based 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
Cisco Courseware 12-18

QUESTION 104
Which of the following fields will you advice the new Certkiller trainee technician to populate when

creating custom signatures with IDS MC? (Choose two.)

A. SubSigID
B. signature name
C. engine description
D. engine name
E. signature string

Answer: B, D
The two required fields are Signature Name & Engine
Reference:
Cisco Courseware 14-33
Page 365 Cisco Press CCSP CSIDS 2nd edition under Creating Custom Signatures
See screenshot, fields marked with * are required.
* Signature name
* Engine

QUESTION 105
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 106
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 107
When configuring a custom signature via the IDM Signature Wizard, you must choose a signature type from one of three categories. What are those categories? Choose three.

A. HTTP signatures
B. HTTPS signatures
C. web server signatures
D. packet signatures
E. stream signatures
F. FTP server signatures

Answer: C, D, E

QUESTION 108
How do you configure the Sensor to capture the packet that triggers a signature?

A. It is always on for TCP stream signatures.
B. In the signature configuration.
C. In the signature configuration by IP address
D. Globally by IP addess

Answer: B

QUESTION 109
You are the Certkiller administrator. Which of the following actions can you configure a Cisco IDS Sensor to take a signature is fired when using IDS MC? (Choose four.)

A. log
B. alarm
C. block host
D. reset
E. trigger
F. block connection

Answer: A, C, D, F

Page 14-7 CSIDS Courseware under Signature Actions
You can configure signatures to cause the Sensor to take action when the signature is triggered by the following:
1) IP Log
2) TCP Reset
3) Block - Block Host
- Block Connection
Cisco Courseware 13-10
Cisco Courseware 14-7
Cisco Courseware 14-12 (Screenshot)

QUESTION 110
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 111
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

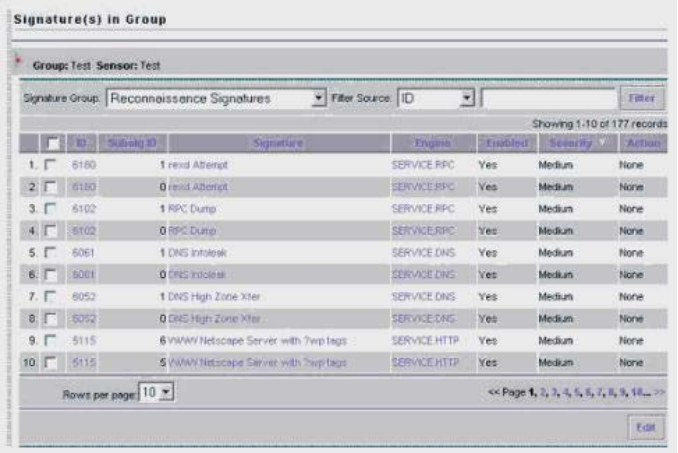
Answer: B, C, E

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 112
Study the exhibit below carefully:



According to the exhibit, which parameter selection would display the correct panel and the capability to perform a tuning of a specific signature to log events when they occur?

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#122

QUESTION 113
When customizing a signature, what would be the Alarm Throttle parameter setting if the Alarminterval parameter is also set when one is customizing a signature?

A. FireOnce
B. FireAll
C. GlobalSummarize
D. Summarize

Answer: B
FireAll is default.
AlamInterval doesn't seem to be related to AlamThrottle.
ThrottleInterval specifies the related throttle (summarization-) timer.
Cisco Courseware 13-17, 13-18

QUESTION 114
Select the three phases of sensor tuning (Choose three.)

A. Prep Phase.
B. eployment Phase
C. Setup Phase
D. Tuning Phase
E. Maintenance Phase
F. Config Phase

Answer: A, B, C

Explanation:
The following routers do not support online insertion and removal (OIR) of network modules:
Cisco2600 series
Cisco2811
Cisco2821
Cisco2851
Cisco3620
Cisco3640
CiscoMWR1941-DC

QUESTION 115
Considering the following list of signature engines, which one would you deem is the best choice when creating a custom signature when you consider a situation where 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.

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

Answer: D
TCP.STRING by using these parameters:
1. ToService (=number of the targeted port)
2. RegExString (=string of well known default password)
Reference:Cisco Courseware 13-62

QUESTION 116
Which of the following is used by a blocking Sensor inorder to manage a Cisco IOS router for shunning? (Choose two.)

A. RDEP
B. Telnet
C. SSL

D. SSH
E. serial console

Answer: B, D
Page 379 Cisco Press CCSP CSIDS 2nd edition under IP Blocking Devices-Cisco Routers
To manipulate the ACLs on the managed device, you must configure the following on your managed devices:
- Telnet access (vty) enabled
- Line password assigned to vty
- Secure Shell (SSH) access allowed from sensor (or Telnet)
- Router's enable password assigned

QUESTION 117
The new Certkiller trainee technician wants to know what the default duration for an automatic block on an IDS blocking device is.What would your reply be?

A. 1 minute
B. 10 minutes
C. 30 minutes
D. default time period is unlimited(permanent block)
E. there is no default block period, it must be configured

Answer: C
Page 15-9 CSIDS Courseware under Blocking Guidelines
Blocking duration - By default the Sensor will automatically block for 30mins

---

QUESTION 118
Which of the following Cisco IDS platforms are capable of responding to active attacks by initiating either shunning or blocking? (Choose two.)

A. PIX-IDS
B. Network appliance IDS
C. IOS-IDS
D. Switch IDS module
E. Host IDS

Answer: A, D
NAC block actions are initiated by IDS Sensors - executed by PIX and routers and featured switches.
See also Cisco Courseware 4-9, 4-10, 4-11, 4-12
Cisco Courseware 15-10

QUESTION 119
Which of the following represents the limitation for IDS Sensor blocking?

A. 10 interface/directions across all devices
B. 100 interface/directions across all devices
C. 10 interface/directions maximum per devices

D. 100 interface/directions maximum per devices
E. 10 interface (both directions) across all devices

Answer: A
Page 383 Cisco Press CCSP CSIDS 2nd edition under IP Blocking: Network Topology
A single sensor can only perform IP Blocking on a maximum of 10 interfaces across one or more managed devices
Cisco Courseware 15-3

QUESTION 120
Which of the following can a blocking Sensor utilize to manage a PIX Firewall for shunning? (Choose all that apply.)

A. RDEP
B. Telnet
C. SSLand
D. SSH
E. serial console

Answer: B, D
Page 15-7 CSIDS Courseware under Blocking Device Requirements
The blocking device must have one of the following configured:
1) Telnet enabled - Telnet access should be allowed from the sensor
2) Secure shell (SSH) enabled- SSH access should be allowedfrom the sensor

---

QUESTION 121
Which Sensor process is responsible for initialing shuns on a blocking device?

A. exec
B. NAC
C. blockd
D. shunStart
E. ACL Daemon

Answer: B

Explanation:
Network Access Controller (NAC) is used to initiate Sensor shunning on network devices.
Reference: page 120 of Ciscopress CCSP self study: CSIDS 2nd edition.
Cisco Courseware 6-4

QUESTION 122
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 123
Which of the following commands does a Cisco IOS router use to block attacks, as directed by and 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.
NoteYou cannot use standard named or numbered IP access lists (one that requires the standard keyword) such as the following:
ip access-list standardname
You can use a standard ACL as long as it is in this format:
access-listnumber
Reference:Cisco Courseware 5-46

QUESTION 124
Which of the following represents the best description of a pre-block ACL on an IDS blocking device?

A. ACL entries applied to the start of the active ACL before blocking entries applied

B. ACL applied to the internal (trusted) interface of a managed device
C. ACL applied to a managed interface prior to an attack being detected
D. ACL used to block traffic on the inbound direction of a managed interface
E. ACL used to block traffic on the external (untrusted) interface of a managed device

Answer: A
Page 15-15 CSIDS Courseware under Using Existing ACLs
The Pre-block ACL designates ACL entries that the Sensor should place in the beginning of the new ACL, before the addition of any Sensor blocking entries

---

QUESTION 125
Your Cisco router is hosting an NM-CIDS. The router's configuration contains an output ACL. Which of the following best describes the action the router takes when it receives a packet that should be dripped according to the output ACL?

A. The router drops the packet and does not forward it to the NM-CIDS.
B. The router sends the packet to the NM-CIDS for inspection, then performs output-ACL check and drops the packet.
C. If the packet is an ICMP packet, the router sends it to the NM-CIDS for inspection, then performs output ACL check and drops the packet. If the packet is not an ICMP packet, the router performs output ACL check and drops the packet.
D. The router sends the packet to the NM-CIDS check and drops the packet.

Answer: B
B seems to be the best choice, since the packet makes it into the router (no input ACL prevents this), and an IDS probably should inspect all packets that reach the router core.
Cisco Courseware 5-46
Note: The Cisco IOS Software performs an input-ACL check on a packet before it processes the packet for NAT or Encryption. As explained earlier, the IDS Network Module monitors the packet after the NAT and decryption is processed. Thus if the packet is dropped by the inbound ACL it is not forwarded to the IDS Network Module. The Cisco IOS Software performs output-ACL check after the packet is forwarded to the IDS. Hence the packet will be forwarded to the IDS even if the output ACL drops the packet

---

QUESTION 126
Your Cisco router is hosting an NM-CIDS. The router's configuration contains an inbound ACL. Which of the following best describes the action the router takes when it receives a packet that should be dropped according to the inbound ACL?

A. Router forwards packet to NM-CIDS for inspection, then drops the packet.
B. Router drops the packet and does not forward it to NM-CIDSfor inspection.
C. Router runs the packet against ACL, tags it for drop action, forwards the packet to the NM-CIDS and drops it if it triggers any signature, even a signature with no action configured.
D. Router runs packet against ACL, forwards packet to NM-CIDS for inspection, only if it is an ICMP packet , and then drops the packet.

Answer: B

QUESTION 127
Which of the following represents the best description of a post-block ACL on an IDS blocking device?

A. ACL applied to a managed interface once an attack has been detected.
B. ACL entries applied to the end of the active ACL after blocking entries.
C. ACL used to block traffic on the inbound direction of a managed interface
D. ACL used to block traffic on the internal (trusted) interface of a managed device.
E. ACL used to block traffic on the external (untrusted) interface of a managed device

Answer: B

Explanation:
If you want to change the ACL generated by the Sensor, you can specify either Pre-block or Post-block ACLs. The Pre-block ACL designates ACL entries that the Sensor should place in the beginning of the new ACL, before the addition of any Sensor blocking, deny, entries for the addresses and, or connections being blocked. The Post-block ACL designates ACL entries that the Sensor should place after the Sensor blocking entries.

QUESTION 128
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 129
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 130
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 131
The new Certkiller trainee technician wants to know which command a PIX Firewall use to block attacks, as directed by an IDS blocking Sensor. What would your reply be?

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

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:Cisco Courseware B-11

QUESTION 132
Which of the following statements regarding the IDS Sensor communications is valid?

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

Answer: A
RDEP uses HTTP and TLS/SSL to securely pass XML documents.
Cisco Courseware 4-35
RDEP mismatches the keyword "internal", but SSH (B) is definitely incorrect.
As REDP is even used to communicate between Sensors (Blocking Forwarding Sensor to Blocking Master Sensor), perhaps "internal" matches Cisco's definition?
Cisco Courseware 15-30

QUESTION 133
Which of the following statements regarding the Master Blocking Sensor communications is valid? (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 Blocking Forwarding Sensor can communicate block requests to another Blocking Forwarding Sensor.
F. A Master Blocking Sensor uses RDEP to communicate with a Blocking Forwarding Sensor.

Answer: A D, F
A: Cisco Courseware 15-7
D: Cisco Courseware 15-31
F: Although the direction "Master to Forwarding" is a little confused.
NOT B: Cisco Courseware 15-30: RDEP is used to communicate between Sensors, and
RDEP uses SSL, not SSH!
NOT C: 4.0 Sensors only support RDEP, 3.x Sensors only PostOffice -> They can't
communicate.
NOT E: Blocking Forwarding Sensors can only communicate to Masters.

QUESTION 134
You are the Certkiller administrator and have been requested to permit communications with a Blocking Forward Sensor using encryption. Which of the following will you configure on the Master Blocking Sensor in order to accomplish communications as requested?

A. Configure the Blocking Forwarding Sensor's IP address.
B. Configure the Blocking Forwarding Sensor's SSH public key.
C. Configure the Allowed Hosts table to include the Blocking Forwarding Sensor.
D. Configure the TLS Trusted-Host table to 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:Cisco Courseware 15-32

QUESTION 135
What is the primary role that a Master Blocking Sensor is responsible for?

A. The Master Blocking must serve as the central point of configuration in IDM for blocking.
B. The Master Blocking must serve as the central point of configuration in IDS MC for blocking.
C. The Master Blocking must communicate the blocking requests sent by other Sensors directly.
D. The Master Blocking must 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 its remote host configuration
Reference:Cisco Courseware 15-29

QUESTION 136
Which of the following Cisco IDS service will permit sensors to communicate with each other as well as enabling the Master Blocking Sensor capability?

A. cidWebServer
B. CtrlBlokSource
C. cidCLI
D. CtlTransSource

Answer: D
Course ver 4.0 page 6-4 CtlTransSource allows sensor to communicate control transactions with each other. This is used to enablt eh NAC's Master Blocking Capability. The NAC Network Access Controller on a Master

Blocking Sensor controls blocking on devices at the request of the NAC's running on Blocking Forwarding sensors. page 15-30 ids 4.0 uses RDEP to communicate blocking instructions.

QUESTION 137
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 fro blocking
C. to manage and distribute blocking configurations in to other "slave" Sensors
D. to directly communicate the blocking requests sent by other Sensors
E. to provide the first line of attack detection and prevention through blocking

Answer: C
Cisco Courseware 15-29, 15-30

QUESTION 138
The new Certkiller trainee technician wants to know which signature description best describes a string signature engine. What would your reply be?

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

Answer: B

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:Cisco Courseware 13-61

QUESTION 139
Which of the following statements regarding SERVICE engine signatures on a Cisco IDS Sensor is valid?

A. SERVICE engine signatures on a Cisco IDS Sensor include all general signatures
B. SERVICE engine signatures on a Cisco IDS Sensor are operating system independent

C. SERVICE engine signatures on a Cisco IDS Sensor include signatures based on network attacks.
D. SERVICE engine signatures on a Cisco IDS Sensor are categorized and tuned by operating system

Answer: B
Cisco Courseware 13-41

QUESTION 140
Which type of signature can be configured to alarm only on specific source or destination IP addresses?

A. atomic signatures
B. flood signatures
C. service signatures
D. state signatures

Answer: A
The task is simple, the simplest engine should do.
Page 13-29 CIDS Courseware v4.0

QUESTION 141
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 142
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 143
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

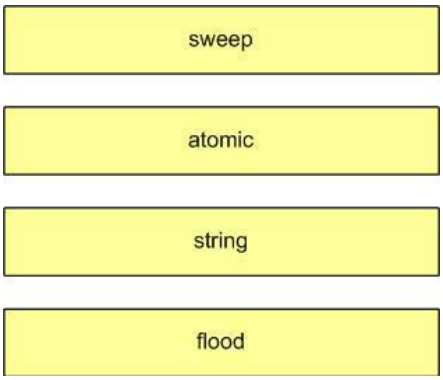
Explanation:
SWEEP.PORT.UDP - UDP connections to multiple destination ports between two nodes
Reference: Cisco Secure Intrusion Detection System Signature Engines Version 3.0

QUESTION 144
Match the Signature micro-engine usage description with the micro-engine name.

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:

Explanation:



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

QUESTION 145
Which of the following represents a type of signature engine that is characterized by single packet conditions?

A. string
B. other
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 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.
Cisco Courseware 13-14

QUESTION 146
The new Certkiller trainee technician wants to know which of the following signature engine would be the best choice when creating a signature to examine EIGRP packets, which uses protocol number 88. What will your reply be?

A. SERVICE.GENERIC
B. ATOMIC.L3.IP

C. ATOMIC.IP.ROUTING
D. OTHER
E. ATOMIC.IPOPTIONS

Answer: B

Explanation:
ATOMIC.L3.IPis 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:Cisco Courseware 13-33

QUESTION 147
Given the following signature engines, which would represent the most appropriate choice when creating a intruder detecting signature that scans 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:Cisco Courseware 13-34

QUESTION 148
Which of the following signature descriptions best describes a service signature engine?

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

Answer: C

Explanation:
SERVICE.* EnginesUse 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:Cisco Courseware 13-41

QUESTION 149
Which of the following signature engines would be the most appropriate to create a custom signature that would inspect data at Layer 5 and above?

A. STRING
B. SWEEP
C. ATOMIC
D. SERVICE

Answer: D
Page 437 Cisco Press CCSP CSIDS 2nd edition under Cisco IDS Signature Engines
See: Table 13-6 Signature Engine Categories
Service: Used when services at OSI Layers 5, 6 and 7 require protocol analysis
Cisco Courseware 13-41

QUESTION 150
When creating custom signatures using the TROJAN engines, which parameter values are required?

A. protocol
B. source/destination IP addresses
C. regular expression strings
D. these signatures cannot be created

Answer: D
You cannot create custom signatures with Trojan engies.
Cisco Courseware 13-73

QUESTION 151
Which statement is true when creating custom signatures on a Cisco IDS Sensor in IDS MC?

A. All parameter fields must be entered.
B. They are automatically saved to the Sensor.
C. The default action is logging.
D. They are enabled by default.

Answer: D

Explanation:
Custom signatures are enabled by default. It is recommended to test custom signatures in a non-production environment to avoid unexpected results including network disruption.
Cisco Courseware 14-30

QUESTION 152
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 153
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: D
Microsoft Exchange Server for SMTP is based on the protocol TCP no UDP

QUESTION 154
Which of the following statements represents the most suitable description of a required signature parameter attribute?

A. The signature parameter value cannot be modified for custom signatures.
B. The default signature parameter value cannot be changed.
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
Cisco Courseware 13-16

QUESTION 155
Which of the following statements represents the best description of a protected signature parameter attribute?

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

Answer: C

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.
Note: If a parameter is protected, you cannot change it for the default signatures. You can modify it for custom signatures.
D is better than C, because it covers both, DEFAULT and CUSTOM signatures - by the word "only".
Reference:Cisco Courseware 13-16

QUESTION 156
Which of the following custom signature configurations would result in a signature to alarm on each occurrence and provide an IntervalSummary alarm if you receive 120 alarms in a 60 second time period?

A. SIG 20001 AlarmThrottle FireEvery ChokeThreshold 100 ThrottleInterval 120
B. SIG 20002 AlarmThrottle FireAll ChokeThreshold 60 ThrottleInterval 60
C. SIG 20003 AlarmThrottle FireAll ChokeThreshold 100 ThrottleInterval 60
D. SIG 20004 AlarmThrottle FireEvery ChokeThreshold 60 ThrottleInterval 120

Answer: C

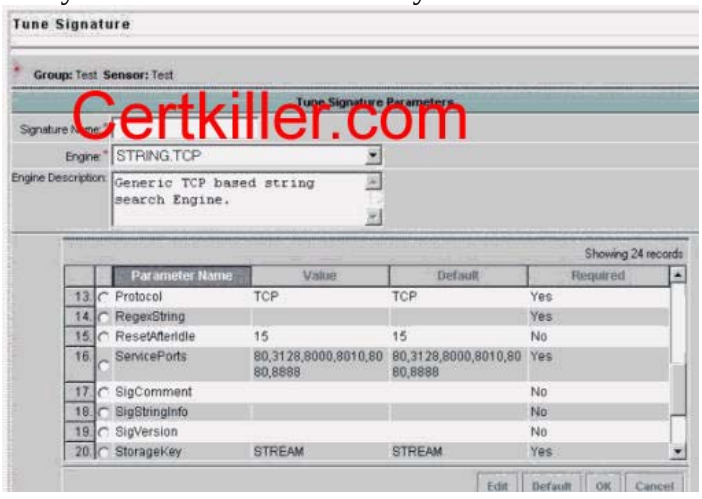
Explanation:
ThrottleInterval defines the period of time used to control alarm summarization.
AlarmThrottle is a technique which is used to limit alarm firings.
Cisco Courseware 13-18, 13-19

QUESTION 157
Which signature parameter defines the response taken when an alarm is fired?

A. Alarm Traits
B. EventAction
C. AlramAction
D. EventTraits

Answer: B
Event Action - The action to perform when an alarm is fired:
1. Log
2. Reset
3. ShunHost
4. ShunConnection
5. ZERO
Cisco Courseware 13-18

QUESTION 158
Study the exhibit below carefully:



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 of the following parameters must be configured so as to detect the desired information? (Choose all that apply.)

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

Answer: C, E

Explanation:
Both Regex and ServicePorts need to be defined for custom signatures.

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 RegexString must use to report the match.
MinMatchLength[2]	NUMBER	Yes	No	The minimum number of bytes the RegexString must match.
RegexString[3]	STRING	Yes	Yes	The Regular Expression pattern.
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. RegexStrings without repetition are fixed length and always have the same match length.
3. The RegexString 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
Cisco Courseware 14-37

QUESTION 159
Which of the following represents basic types of Cisco IDS signature parameters? (Choose all that apply.)

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

Answer: C E

Explanation:
Engine parameters have the following attributes:
1) Protected - If a parameter is protected, you cannot change if for the default signatures. You can modify it for custom signatures.
2) Required - If a parameter is required, you must define it for all signatures, both default signatures and custom signatures.
Reference:Page 438 CCSP Self-study: CSIDS Second Edition
Cisco Courseware 13-16

QUESTION 160
With the ATOMIC.TCP signature parameter PortRangeSource is set to 0 (zero), which ports will be examined?

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.
E. None of the above.

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 161
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 162
The new Certkiller trainee technician wants to know which of the following IDS software components can be upgraded from IDS MC's Updates page. What would your reply be? (Choose all that apply.)

A. IDS Sensor recovery partitions
B. IDS MC signatures
C. IDS Sensor service packs
D. IEV signatures
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:
1. 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). IDSMC works with these compressed files
2. There are two types of update files:
1. 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 contain signature updates.
2. 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:Cisco Courseware 17-5

QUESTION 163
Where should the update file be located when updating a Cisco IDS Sensor with IDS MC?

A. it should be on a SCP or FTP server
B. it should be on cisco.com
C. it should be on the FTP server only
D. it should be on the IDS MC server
E. it should be on the secure Web server

Answer: D
Requirements to install an update from the IDS MC:
The file must exist on the IDS MC at:
\Program Files\CSCOpx\MDC\etc\IDS\Updates
Cisco Courseware 17-6

QUESTION 164
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 165
You are the Certkiller administrator and need to perform 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. HTTPS
E. TFTP
F. SCP

Answer: A, D, F

Supported:
FTP (A)
HTTPS (D)
SCP (F)
HTTP
Reference:Cisco Courseware 17-6

QUESTION 166
Which of the following methods will you advice the new Certkiller trainee technician to use when upgrading the
signatures on a Cisco IDS Sensor? (Choose all that apply.)

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 IDSMC server if you want to update the IDSMC or a sensor.
*You must have access to the SecurityMonitor server if you want to update SecurityMonitor.
*If you have installed IDSMC and SecurityMonitor on the same server, you must have access to that server if you want to update the IDSMC or a sensor or SecurityMonitor.
Note:The installation of IDS software updates can be performed from supported management consoles or from the command line interface (CLI).
Only updating via IDS MC and the CLI is explained in the course.
Reference:Cisco Courseware 17-3

QUESTION 167
The new Certkiller trainee technician wants to know which IDS components require regular signature updates.What would your reply be?

A. IDS MC only
B. IEV, IDS Sensor devices, IDS MC, and Monitoring Center for Security
C. IDS Sensor devices only
D. IDS Sensor devices and IDS MC only
E. IDS MC and Monitoring Center for Security only

Answer: B
To update their NSDBs.
Cisco Courseware 17-3 Supported management consoles

QUESTION 168
Which three server types are supported retrieving the new software when performing a signature update on a Cisco IDS Sensor? (Choose all that apply.)

A. FTP
B. SCP
C. RCP
D. HTTP
E. NFS
F. TFTP

Answer: A, B, D
Page 17-6 CSIDS Courseware under Sensor Maintenance
The update file must be located and accessible on one of these types of servers:
- FTP
- HTTP/HTTPS
- SCP

QUESTION 169
Which two methods can be used to upgrade the signatures on a Cisco IDS Sensor?
(Choose two.)

A. CLI
B. IEV
C. SigUp
D. IDS MC
E. Monitoring Center for Security

Answer: A, D
Page 17-10, 17-12 CIDS Courseware v4.0

QUESTION 170
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 171
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:
INSTALLATION
To install the version 3.1(5)S58 service pack, follow these steps:
1. Download the self-extracting binary file IDSk9-sp-3.1-5-S58.bin
to a directory on the target Sensor from the following website:
http://www.cisco.com/cgi-bin/tablebuild.pl/ids3-app
CAUTION: You must preserve the original file name.
2. Log in as root on the Sensor.
3. Change directories to the location of the downloaded binary.
4. Change the binary file's attributes to an executable by typing the
following:
chmod +x IDSk9-sp-3.1-5-S58.bin
5. Execute the binary file with the -I option by typing the following:
./IDSk9-sp-3.1-5-S58.bin -I
6. Review the file output.log in /usr/nr/sp-update for any error
messages.
7. Do not remove the /usr/nr/sp-update directory. This directory is
required for uninstallation and contains backups of files replaced by
the update.

QUESTION 172
From which of the following partitions 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.
Recovering the Software Image
You can recover the software image for the IDS module if it becomes unusable. If you install a service pack on an IDS module, for example, and it is unusable after it reboots, you must reimage the IDS module from the maintenance partition.
Reference:Cisco Courseware 17-17 for the recovery of a Sensor Appliance

---

QUESTION 173
Which of the following statements regarding using IDS MC to upgrade a Cisco IDS Sensor is valid?

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

Answer: C

Explanation: Because ids mc push the upgrade to sensors.
Cisco Courseware 17-4

QUESTION 174
What will you advice the new Certkiller trainee technician to use inorder to maintain network connectivity when upgrading IDS-4220 or IDS-4230-FE Sensor appliances from Cisco IDS v3.x?

A. Swap the console and monitoring interface connections
B. Swap the console and control interface connections
C. Swapping the interface connections is not necessary
D. Swap the control and monitoring interface connections

Answer: D
Cisco Courseware 7-16 Cable swap on the 4230 Sensor
Note: ...what about 4220?
For 4220, in this list there's only a memory upgrade stated.

QUESTION 175
Upon restoring a sensor's configuration to default, which application settings are not set to default? Choose three.

A. IP address
B. netmask
C. allowed hosts
D. passwords
E. user accounts
F. time

Answer: A, B, C
Although time is not changed, time is NOT an application setting.
Cisco Courseware 17-17

QUESTION 176
What version of Cisco IDS software is required prior to upgrading to 4.1?

A. 4.0(2)S37
B. 4.0(3)S41
C. 4.0(1)S37
D. 4.0(1)S24

Answer: A
The sensor must report the version as 4.0(1)S37 or later before you can apply this minor update
http://ftp-sj.cisco.com/cisco/crypto/3DES/ciscosecure/ids/4.x/IDS-K9-min-4.1-1-S47a.readme.txt

---

QUESTION 177
Which of the following represents Sensor servlets that leverage the IDS Sensor's cidWebServer application? (Choose all that apply.)

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

Answer: B, D, F

Explanation: The correct answers can be found on pages 6-3 and 6-4 of volume 1 of the official Cisco class manuals for IDS ver 4.X. The following are Sensor servlets that leverage the IDS Sensor's cidWebServer:
* IDM
* IP log server
* Transaction server
Cisco Courseware 6-3

QUESTION 178
You are the Certkiller administrator. Which protocol would you use to communicate with the IDS MC Sensors from their desktop?

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

Answer: E

Explanation:
[client] --- HTTPS ---> [IDS MC] --- SSH ---> [IDS]
Cisco Courseware 6-8:

QUESTION 179
Which protocol is used for communication between the IDS Event Viewer and the Sensor?

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

Answer: A

Explanation:
RDEP uses the industry standard HTTPS.
1. Communications with monitoring applications - HTTPS
Reference:Cisco Courseware 6-8

QUESTION 180
You are the Certkiller administrator. Which protocol would you use to communicate with the Monitoring Center
for Security from the desktop?

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

Answer: C

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
Cisco Courseware 6-8

QUESTION 181
The new Certkiller trainee technician wants to know what types of requests can be made with a client initiated RDEP event request.What would your reply be? (Choose two.)

A. IP log

B. subscriptions
C. transaction log
D. queries
E. configuration

Answer: B, D
Page 123 Cisco Press CCSP CSIDS 2nd edition under Remote Data Exchange Protocol
The client can issue one of the following two types of event requests:
- Queries (used to retrieve events from the sensor based on a specified query)
- Subscriptions (enable a client to establish a live event feed with the sensor based on specific query criteria)

QUESTION 182
Which two classes of request and response messages are defined by RDEP? (Choose two.)

A. Event messages
B. Syslog messages
C. IP Log messages
D. PostOffice messages
E. CnC messages

Answer: A, C

Explanation:
RDEP defines the following classes of request and response messages:
1) Event messages - Include IDS alarm, status, and error messages. Monitoring applications such as IEV and the Security Monitor use RDEP's event pull model to retrieve events from the Sensor. The pull model allows the application to pull alarms at its own pace. As soon as the monitoring application connects to the Sensor and requests alarms, the alarms are returned to the monitoring application console without delay. Alarms remain on the Sensor until a 4-GB limit is reached and they are overwritten by new alarms. Since a large number of alarms can be stored on the Sensor itself, the management application can pull alarms after being disconnected for a long period of time without losing alarms.
2) IP log messages - Used by clients to retrieve IP log data from Sensors.
Cisco Courseware 6-7

QUESTION 183
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 184
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

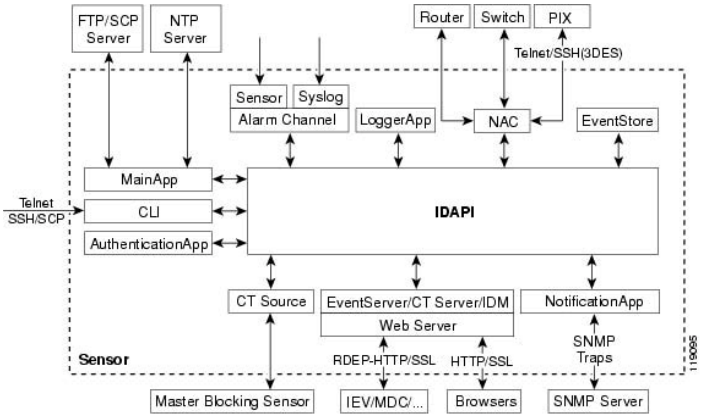
Answer: B, D
Communication infrastructure parameters:
* Sensor Host ID and Organization ID
* Sensor Host Name and Organization Name
* Sensor IP Address
* Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host ID and Organization ID
* Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host 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 185
Which of the following communication protocols does the Event Server, Transaction Server, and IPLog Server servlets use in Cisco IDS?

A. PostOffice
B. Syslog
C. RDEP
D. IDAPI
E. PIX Firewall

Answer: C

Explanation:



Cisco Courseware 6-4

QUESTION 186
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 187
The new Certkiller trainee technician wants to know which of the following applications forms part of the SensorApp process of the Cisco IDS Sensor.What would your reply be? (Choose all that apply.)

A. VirtualSensor
B. VirtualDM
C. VirtualNAC
D. VirtualEvent
E. VirtualAlarm

Answer: A, E
Page 6-5 CSIDS Courseware under Sensor App Internals
The sensorApp consists of the following:
-VirtualSensor
-VirtualAlarm

QUESTION 188
Which Cisco IDS service allows external management applications to control and configure sensors?

A. Transaction Server
B. Event Server
C. IPLog Server
D. Sensor Server

Answer: A

Explanation:
TransactionSource is an application that forwards locally initiated remote control transactions to their remote destinations using the RDEP and HTTP protocols. TransactionSource initiates either TLS or non-TLS connections and communicates remote control transactions to HTTP servers over these connections. TransactionSource must establish sufficient credentials on the remote HTTP server to execute a remote control transaction. TransactionSource establishes its credentials by presenting an identity to the HTTP server on the remote node in the form of a username/password (basic authentication). Once authenticated, the requestor is assigned a cookie containing a user authentication that must be presented with each request on that connection. Cisco Courseware 6-3

QUESTION 189
Which statement describes the Sensor's CapturePacket feature?

A. It is used for TCP streams only. And contains only the Layer 5 data of the TCP stream and a limited number of bytes.
B. It provides a snapshot of the TCP traffic that preceded the triggering of the signature.
C. It captures packets that follow the trigger packet.
D. It captures the actual packet that triggered a signature.

Answer: D

QUESTION 190
The Sensor has a CapturePacket feature which enables it to capture the packet that triggered a signature. Which four statements are true about this feature? Choose four.

A. It captures a limited number of bytes
B. The captured packet can be viewed in the command line interface (CLI) as raw hexadecimal data.
C. The captured packet can be viewed in tIDS Event Viewer (IEV) if Ethereal is installed on the same system as IEV.
D. It contains only Layer 5 data of a TCP stream.
E. It contains the entire frame.
F. It is enabled for each signature individually.

Answer: B, C, E, F

QUESTION 191
Which network services are enabled by default on a Cisco IDS Sensor for remote management? (Choose all that apply)

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

Answer: A, F

Explanation:
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
Note:For IDS Sensor Version 4.0 the Telnet is disabled by default since it is insecure. Instead SSH is used.

QUESTION 192
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 193
Which Cisco IDS service must be running if a Sensor is capturing network traffic?

A. Managed
B. Captured
C. Snifferd
D. Packetd
E. Trafficd

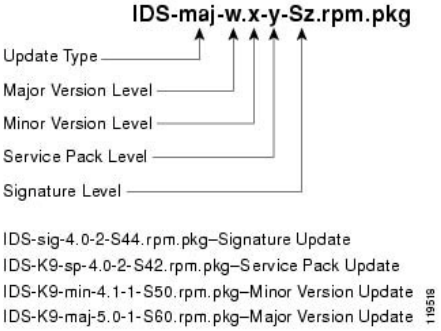
Answer: D

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 194
What can be determined about a Cisco IDS update file named IDS-K9-sp-4.1-2-S40.zip?
A. It is a Sensor software patch: signature version is 4.1; IDS version is 4.0.
B. It is a Sensor service pack: signature version is 40; IDS version is 4.1.2.
C. It is an IDS MC service pack; signature version is 40; IDS version is 4.1.
D. It is a Sensor signature patch; signature version is 4.0; IDS version is 4.1
E. It is an IDS MC software patch; signature version is 4.1; IDS version is 4.0.

Answer: C

Explanation:



Cisco Courseware 17-8

QUESTION 195
You are the Certkiller administrator and need to get detailed signature and vulnerability information. Which feature of IDS Event Viewer will provide this information to you?

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:Cisco Courseware 10-8

QUESTION 196
Which of the following represents one method of communication between IDS Event Viewer and the IDS device?

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

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
Cisco Courseware 10-13

QUESTION 197
The new Certkiller trainee technician wants to know how IDS devices are added into IDS Event Viewer. What would your reply be?

A. IDS devices are discovered by IEV by default.
B. IDS devices initiate a connection request to IEV.
C. IDS devices must manually be 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
Cisco Courseware 10-13

QUESTION 198
Where will you advice the new Certkiller trainee technician to install the Intrusion Detection System

Device Manager?

A. on a web server with supported operating systems
B. on a Cisco IDS Sensor running version 3.1 and higher
C. on a Cisco IOS router with IOS version 12.2.(2)T and higher running IDS software
D. on a Cisco PIX Firewall version 6.3 and higher running IDS software

Answer: B
CiscoPress CSIDS Self-Study Second Edition Earl Carter
Page 227 è IDS Device Manager and Certification
You access the IDM through a web server that is running on your sensor

---

QUESTION 199
How are IDS device added into IDS Even 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

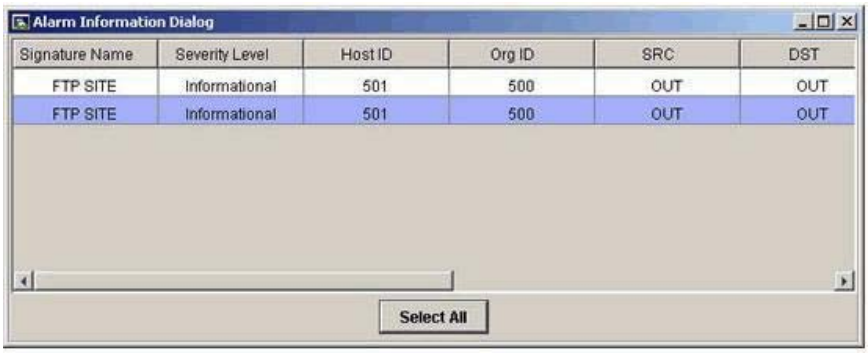
Answer: C
Add IDS Devices:
Start the IEV
Choose: File->New->Device
Cisco Courseware 10-13

QUESTION 200
Which of the following statements are true about a trigger packet captured by sensor? (Choose two)

A. It can be viewed in CLI as raw hexadecimal data.
B. It can be viewed in IEV if ethereal is installed on the same system as IEV.
C. It contains only layer 5 data of a TCP stream.
D. It contains a limited number of bytes.

Answer: A, B

QUESTION 201
Exhibit:



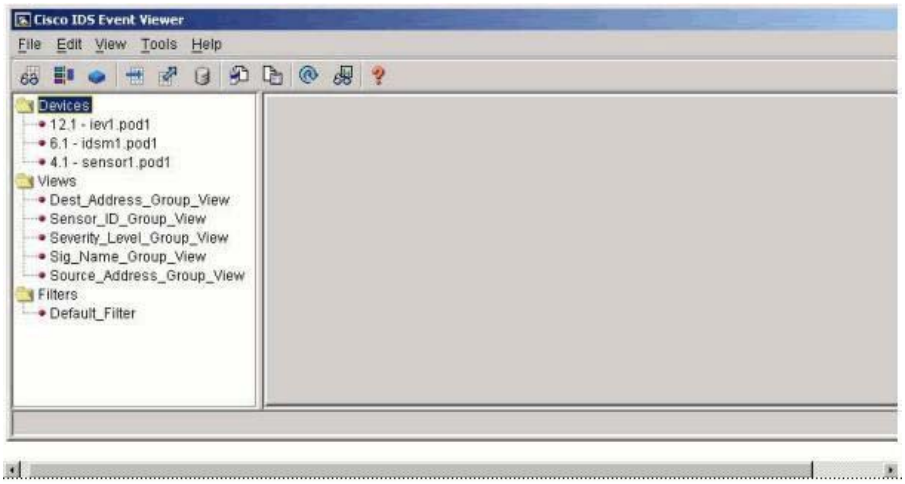
In the Cisco IDS Event Viewer, how do you display the context data associated with an event?

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 202
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 203
Which methods are available inMonitoring Center for Security to populate the device database?

A. manual entry only
B. import from IDS MC only
C. manual entry and import from IDS MC only
D. manual entry, import from IDS MC, and import from Resource Manager Essentials only
E. manual entry, import from IDS MC, and import from Resource Manager Essentials, and import from text file.

Answer: C
Page 16-28 & 16-29 CSIDS Courseware under Add IOS IDS Device and Import Devices

---

QUESTION 204
How is the certificate information obtained when choosing an encrypted protocol with IDS Event Viewer?

A. It is generated on the IEV host
B. It is obtained from the Certificate Authority
C. It is obtained from the Cisco IDS Sensor
D. HTTPS does not need a certificate

Answer: C

Explanation:
The information you provide in the Device Properties panel should match the settings you entered during the initial configuration of the Sensor. If you have set up a user account with Viewer access for the IEV, specify the username and password for that account.
Reference: Cisco Courseware p.10-13

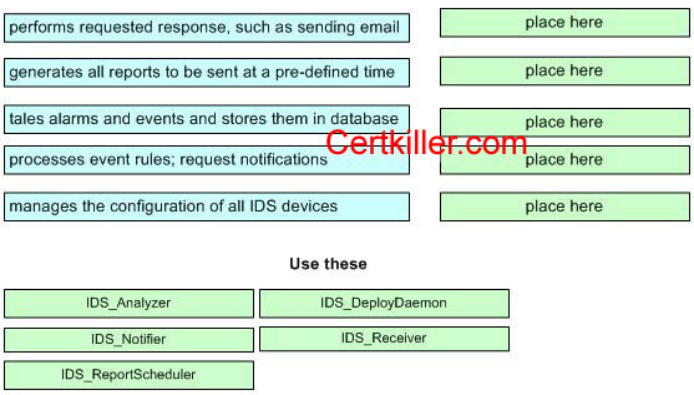
QUESTION 205
When enabling time schedules for archival of events with IDS Event Viewer. Which three options are available? (Choose three.)

A. every N minutes
B. every N MB
C. every N hours
D. every N KB
E. every day at same time
F. every week on same day and time

Answer: A, C, E

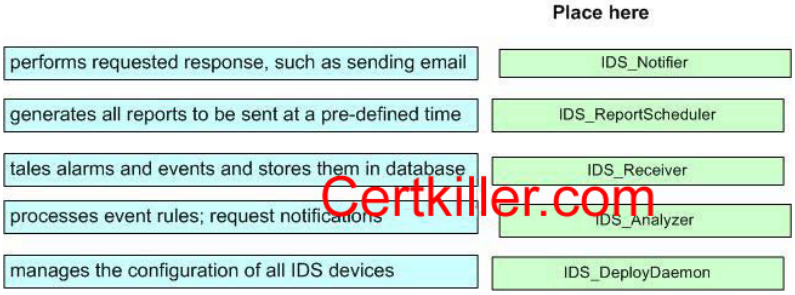
Explanation:
The time schedule for the archiving events feature must be enabled. The time schedule options are as follows:
1) Every N Minutes - From the Minute(s) drop-down menu choose how many minutes until the next data archival occurs.
2) Every N Hour - From the Hour(s) drop-down menu choose how many hours until the next data archival occurs.
3) Every day at time - From the Every day at time drop- down menu choose the specific time the data archival occurs every day.
Cisco Courseware 10-46

QUESTION 206
Following is a list of descriptions and IDS MC processes. Match the IDS MC process with its description.



Answer:

Explanation:



1. IDS_Analyzer-To check that the service that processes event rules and requests user-specified notifications when appropriate is running properly.
2. IDS_DeployDaemon-To check that the service that manages all configuration deployments is running properly.
3. IDS_Notifier-To check that the service that receives notification requests (script, e-mail, and/or console) from other subsystems and performs the requested notification is running properly.
4. IDS_Receiver-To check that the service that receives IDS and syslog events and stores them in the database is running properly.
5. IDS_ReportScheduler-To check that the service that generates all scheduled reports is running properly.
Reference:Cisco Courseware 11-12

QUESTION 207
Which of the following represents the default URL address for accessing the IDS MC application on a server with the IP address 172.l19.222.100?

A. http://172.19.222.100
B. https://172.19.222.100
C. https://172.19.222.100:443
D. http://172.19.222.100:1741
E. https://172.19.222.100:1741

Answer: D
Page 11-23 CSIDS Courseware under Getting Started
You must log in to CiscoWorks to navigate in the IDS MC
Open a browser and point to the IP address of the CiscoWorks Machine with port number 1741

QUESTION 208
What is the Cisco IDS ManagementCenter?

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 209
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 210
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 211
In the Cisco IDS Management Center, what workflow steps must you perform to push configuration files to a Sensor?

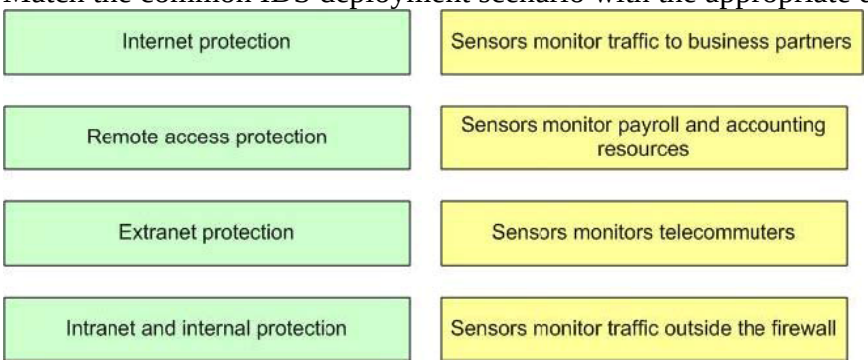
A. Configure, load, submit
B. Generate, approve, deploy
C. Generate, submit, approve
D. Load, submit, approve

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 IDSMC
Reference: Generating, Approving, and Deploying Configuration Files

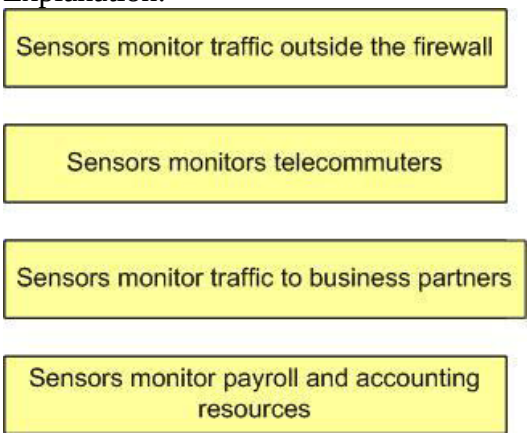
---

QUESTION 212
Match the common IDS deployment scenario with the appropriate description.



Answer:

Explanation:



Reference: Cisco IOS Intrusion Detection System Software App Overview

---

QUESTION 213
What is the default username/password that you will need to use when accessing and administrating the IDS MC server?

A. cisco/cisco
B. admin/cisco
C. admin/admin
D. administrator/cisco
E. administrator/attack

Answer: C
Cisco Courseware Lab 11-4

QUESTION 214
Which CiscoWorks user role provides administrative access for performing all IDS MC operations?

A. root
B. administrator
C. service account
D. system administrator
E. network administrator

Answer: D

Explanation:
The five types of user authorization roles are as follows:
1) Help Desk - Read-only for the entire system.
2) Approver - Read-only for the entire system and includes approval privileges for configuration changes.
3) Network Operator - Read-only for the entire system, generates reports, and includes configuration deployment privileges.
4) Network Administrator - Read-only for the entire system and includes privileges to edit devices and device groups.
5) System Administrator - Capable of performing all operations.
Page 11-24 CIDS Courseware v4.0

QUESTION 215
What does the password represent in the Sensor's identification window when one uses SSH in IDS MC for Sensor access?

A. It represents the passphrase to access the Sensor's public key
B. It represents the passphrase to access the Sensor's private key
C. It represents the password of user account to access the Sensor
D. It represents the passphrase to access the IDS MC server's private key
E. It represents the password of user account to access the IDS MC server

Answer: B
The sensors private key is stored on the server (12-7) using the sensor's hostname as the key filename.
The sensor's public key is being copied to the sensor (12-8).
Reference:Cisco Courseware 12-3

QUESTION 216
Which IDS MC utility is used to create the IDS MC public key for SSH communications to the Sensor?

A. ssh
B. pulty
C. sshgen

D. keygen
E. puttygen

Answer: E

Explanation:
This document explains how to use the Key generator for PuTTY (PuTTYgen) to generate Secure Shell (SSH) authorized keys and RSA authentication for use on Cisco Secure Intrusion Detection System (IDS). The primary issue when you establish SSH authorized keys is that only the older RSA1 key format is acceptable. This means that you need to tell your key generator to create an RSA1 key, and you must restrict the SSH client to use the SSH1 protocol.
Cisco Courseware 12-6

QUESTION 217
Which of the following identify basic authentication methods for accessing a Sensor from IDS MC? (Choose all that apply.)

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

Answer: A C

Explanation:
NoteSSH supports two forms of authentication: password and public key. If you have set up a public key between IDSMC 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 IDSMC will use SSH password authentication.
Reference:Cisco Courseware 12-3
Password (or Passphrase if using existing SSH keys)

QUESTION 218
Which of the following CLI commands will you advice the new Certkiller trainee technician to use in orderto configure the IDS MC public key on the Sensor?

A. copy
B. putty
C. puttygen
D. ssh generate-key
E. ssh authorized-key

Answer: E
IDS course 4.0 page 12-8 sensor1(config)#ssh authorized-key 0 ....

QUESTION 219
Study the exhibit below carefully:

According to the exhibit depicting the RDEP properties of a Sensor in IDS MC: Which of the following statements will be valid if the web server port value changed from its current value? (Choose all that apply.)

A. IEV must use this new port value to retrieve IDS events
B. The web server port must be manually changed on the Sensor to match the new value
C. IDS MC must use this new port value to configure the Sensor
D. Clients accessing the IDS MC must specify the new port value in the browser URL
E. Clients accessing IDM on the Sensor must specify the new port value in the brower URL

Answer: A, C
Cisco Courseware 12-15

QUESTION 220
Which Sensor user account must be used to configure the IDS MC's SSH key on the Sensor to permit SSH communications between the IDS MC and a Sensor?

A. any administrator account
B. Sensor's service account only
C. username specified in the Sensor's identification settings in the IDS MC
D. administrator account cisco only
E. Sensor administrator account defined in the IDS MC SSH session

Answer: C

Explanation:
There is no direct answer provided in the course, but probably it can be derived from the following statement in:
Cisco Courseware 12-9 SSH Key test:
Auto-login username... Enter the username with which you logged in and created the session.
- If logging in with the same username is required for testing, the same requirements should apply for the login via IDS MC.

QUESTION 221
Which of the following represents a valid statement regarding the "Use Existing SSH keys" option in the Sensor's identification windows in IDS MC?

A. The option increases security of Sensor communications by replacing username or password authentication with SSH authentication.
B. If selected, the option specifies that IDS MC should use existing keys instead of prompting for new keys.

C. If not selected, the option specifies that IDS MC will dynamically generate new keys to securely communicate with the Sensor.
D. The option increases security of Sensor communications by requiring the use of both username/password and SSH authentication.
E. The option increases performance, but decreases security of Sensor communications by replacing username and password authentication with a single pre-shared key.

Answer: A
Reference Cisco Press CCSP 2nd Edition, Chapter 10 Page 290, Last Paragraph

---

QUESTION 222
The new Certkiller trainee technician wants to know what version of SSH is used by the Sensor for IDS MC access.What would your reply be?

A. SSH1
B. SSH2
C. SSH3
D. SSH1 or SSH2
E. SSH2 or SSH3

Answer: A
Page 294 Cisco Press CCSP 2nd Edition under Sensor Configuration
Although you can connect to the sensor using both RSA (SSH version 1) and DSA (SSH version 2), the sensor communicates with other devices using only RSA keys (SSH version 1)

QUESTION 223
Exhibit:

What is the purpose of the NAT address field in the graphic?

A. Informs Monitoring Center for Security which address to use in order to access an IDS device located behind

a NAT device
B. Informs the IDS device which address to use in order to send alarms to Monitoring Center for Security when separated by a NAT device
C. Specifies to Monitoring Center for Security the true address of an IDS device located behind a NAT device
D. Identifies the IP address of a NAT device that separates Monitoring Center for Security from the IDS device
E. Informs the IDS device which address to use when sending TCP resets to offending traffic when a NAT device separates the IDS device from Internet traffic

Answer: A
IDS MC uses the NAT or Pubic IP address to connect to the Sensor which uses the Private key in case where the Sensor
is using the NAT.
CiscoPress CSIDS Self-Study Second Edition Earl Carter, Page 287

QUESTION 224
What does a value of zero (0) in the parameter field "maximum number of bytes in a log event" imply when you are configuring IP logging using IDS MC?

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

Answer: C

Explanation:
Page 420 Cisco Press CCSP 2nd Edition under IP Logging parameters in IDS MC
See Screenshot diagram, it is stated 'Maximum number of packets in a log event (0 implies no limit)
Cisco Courseware 12-20

QUESTION 225
Which protocol does theMonitoring Center for Security use to monitor alarms on a Cisco IOS router?

A. SSL
B. SSH
C. RDEP
D. Syslog
E. Not supported

Answer: D

QUESTION 226
Which of the following represents aprotocol used by the Monitoring Center for Security 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 PIXFirewall or Cisco IDS Host Sensor
PIXFirewalls and Cisco IDS Host Sensors use syslog messages to communicate with SecurityMonitor.
You do not have to add syslog devices because SecurityMonitor 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 SecurityMonitor.
Reference:Cisco Courseware 16-34

QUESTION 227
The new Certkiller trainee technician wants to know which protocol the Monitoring Center for Security use to monitor alarms on an IDS v3.x Sensor. What would your reply be?

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:Cisco Courseware 16-27

QUESTION 228
Which of the following statements regarding installation prerequisites for the IDS MC and MonitoringCenterfor Security is valid? (Choose two.)

A. The monitoring Center for Security can be installed without the IDS MC.
B. The monitoring Center for Security must be installed before the IDS MC.
C. The IDS MC must be installed before the MonitoringCenterfor Security.
D. The IDS MC can be installed without the Monitoring Center for Security.
E. The monitoring Center for Security and the IDS MC must be installed at the same time.

F. None of the above.

Answer: A, D
Page 581 Cisco Press CCSP CSIDS 2nd edition under Enterprise IDSManagement
Under 3rd Note: If you want to install only IDS MC or the Security Monitor, you can choose Custom Installation and specify which component you want to install
Note:
See the requirement lists for the software installations:
Cisco Courseware 11-5 (IDS MC)
Cisco Courseware 16-6 (Security Monitor)
And the Screenshot on Cisco Courseware 11-12

QUESTION 229
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 230
The new Certkiller trainee technician wants to know which IDS device types can appear under the Monitoring Center for Security's Monitor>Connections display. What would your reply be?

A. RDEP devices only
B. PostOffice devices only
C. RDEP and PostOffice devices only
D. IOS and PIX Firewall devices only
E. PostOffice, IOS, and PIX Firewall devices only
F. RDEP, PostOffice, IOS, and PIX Firewall devices

Answer: C
Page 16-32 CSIDS Courseware under Monitor-Connections
For RDEP and PostOffice devices, you can check the status of these connections using Monitor>Connections
Note: IOS and PIX devices are sending their messages via syslog -> connectionless.

QUESTION 231
Which three main categories of information can be monitored usingMonitoring Center for Security?

(Choose three.)

A. events
B. sensors
C. statistics
D. signatures
E. connections
F. notifications

Answer: A, C, E

Explanation:
You can monitor information about the devices that you have added to Security Monitor. This information falls into the following three categories:
1) Connections
2) Statistics
3) Events
Cisco Courseware 16-33

QUESTION 232
Which of the following will identify possible actions for an event rule in theMonitoring Center for Security? (Choose three.)

A. notify via Email
B. execute a Script
C. log to IP Logger
D. block IP Address
E. notify via Syslog
F. log a Console Notification Event

Answer: A, B, F
Page 617 Cisco Press CCSP CSIDS 2nd edition under Event Notification
Each rule can perform one or more of the following actions:
- Notification via email
- Log a console notification event
- Execute a script
Cisco Courseware 16-41

QUESTION 233
Which of the following specify the graphing options in theMonitoring Center for Security's Event Viewer? (Choose all that apply.)

A. by group
B. by parent
C. by time
D. by child

E. by Sensor
F. by address

Answer: C, D
Page 16-58 CSIDS Courseware under Event-Viewer - Creating Graph
Two types of graphs:
- By Child (Displays child events across the X-axis of the graph and the number of occurrences along the Y-axis)
number of occurrences)

QUESTION 234
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 235
Which of the following protocols is used by the Monitoring Center for Security to monitor alarms on the IDS Sensor?

A. SSH
B. RDEP
C. IDAPI
D. PostOffice
E. SSL

Answer: B

Explanation:
A) SSH Wrong
B) RDEP only for the IDS appliance Version 4.x
C) IDAPI Wrong
D) Post Office only for the IDS appliance Version 3.x

E) SSL Wrong .
The test is not specifying the version 3.X that means version 4.X the right answer is B
CiscoPress CSIDS Self-Study Second Edition Earl Cater
Page 607, 608 and 610

QUESTION 236
Which of the following protocols is utilized by theMonitoring Center for Security use to monitor alarms on an IDS v3.x Sensor?

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

Answer: E
Implicit hints: Instead of the password for the sensor, the passphrase to the locally stored private key is to be entered to the input-field (12-3).
As, if you use the input-field for the passphrase, no longer provide a password, username/password authentication must have been replaced.
Page 16-26 CSIDS Courseware under PostOffice Devices-Add
Security Monitor can receive events from Cisco IDS version 3.x sensors
Cisco Courseware 12-6

QUESTION 237
Which of the following protocols is utilized by theMonitoring Center for Security to monitor alarms on an IDS Sensor?

A. SSH
B. RDEP
C. XML
D. SSL
E. IDAPI
F. PostOffice

Answer: B

Explanation:
Devices using RDEP to communicate with SecurityMonitor and SecurityAgent MC servers can show the following one of the following statuses:
Connected TLS-A secure connection has been established.
Connected non-TLS-(RDEP devices only) A connection that does not use Transport Layer Security (TLS) has been established.
Not Connected-A connection with the devices has not been established

---

QUESTION 238
Which protocol does theMonitoring Center for Security use to monitor alarms on an IDS v3x Sensor?

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

Answer: E
Page 16-27 CIDS Courseware v4.0

QUESTION 239
Which three parameters, in addition to its IP address, are required byMonitoring Center for Security in orderfor it to receive alarms from an IDS Sensor device? (Choose three.)

A. Org ID
B. HostID
C. Username
D. Org Name
E. Password
F. Web Server port

Answer: A, B, D
The required parameters to enter are:
- IP Address
- Device Name
- Host ID
- OrgName
- Org ID
- Port
- Heartbeat

Note:...only required if running an IDS software version earlier than 4.0 (PostOffice).
Page 612 Cisco Press CCSP CSIDS 2nd edition under Adding IOS Devices
Cisco Courseware 16-14

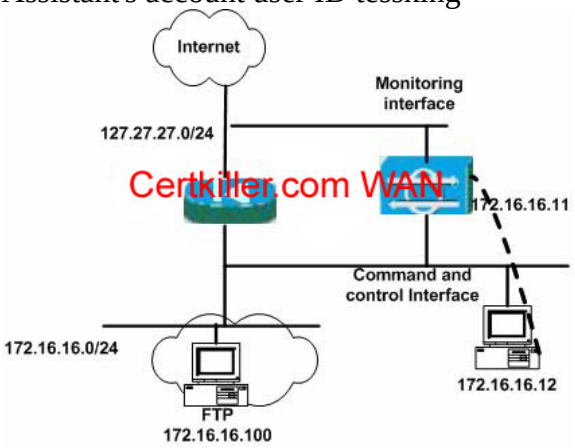
QUESTION 240
Which three specify the predefined rules for database maintenance in theMonitoring Center for Security? (Choose three.)

A. default pruning
B. default IP log pruning
C. default SNMP pruning
D. default Syslog
E. default audit log pruning
F. default SQL database pruning

Answer: A, D, E

Explanation:
The Security Monitor enables you to launch a notification, trigger a script, or sent an e-mail when a database rule is triggered. These database rules can be triggered when the Security Monitor database reaches a certain size, a number of events happen, or on a daily basis.
The Security Monitor comes with three predefined rules for database maintenance:
1) Default pruning - Default pruning for alarm tables when the database reaches 2,000,000 total events.
2) Default Syslog pruning - Default pruning for Syslog tables when a database reaches 2,000,000 total events.
3) Default audit log pruning - Default pruning for audit log pruning performed on a daily basis.
Reference: CSIDS Student Guide v4.0 p.16-63
Cisco Courseware 16-63

QUESTION 241
You have recently been employed by Certkiller and have inspected the configuration of Certkiller 's IDS-4215 Sensor. You then decide to modify access on user accounts and return some of the system's parameters to a known baseline through 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, Jack King, 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 accomplish these tasks successfully.
CISCO IDS Parameters Settings
Sensor administrator username/password Certkiller / Certkiller 1636
FTP server address 172.16.16.100
FTP username/password admin/password2
FTP upload directory / Certkiller 5287
Backup file name /backup-cfg
Assistant's account user ID tessking



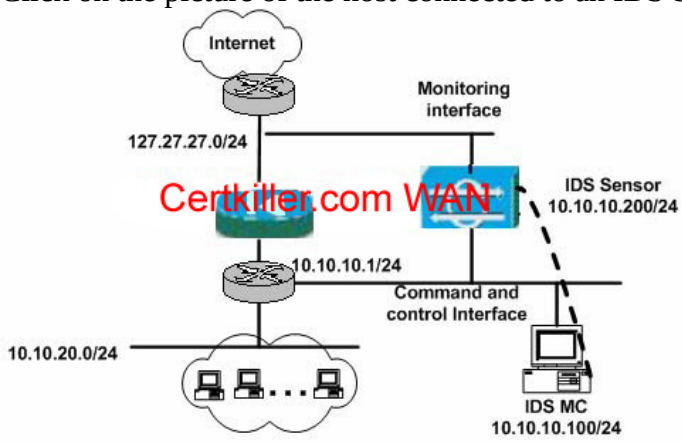
Click on the picture of the host connected to an IDS Sensor by a serial console cable.

Answer:

Explanation:
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 tessking operator
5. sensor(config)#service virtual-sensor-configuration virtualSensor
6. sensor(config-vsc)#reset-signatures service-http all
Reference for Reset Signatures
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_command_reference_chapter09186a00801471c9.ht

---

QUESTION 242
You are a network security at Certkiller Inc. Certkiller is installing new Cisco IDS Sensors. You have to configure the new Sensors to permit remote access from trusted hosts exclusively. 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. Due to this being a new installation, you must remove the default allowed network address. Note: Verify your configuration setting prior to saving, and then save your configuration when finished.
Cisco IDS Parameters Settings
Sensor operator username/password operator/ Certkiller 1636
Sensor administrator username/password admin/ Certkiller 1636
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.



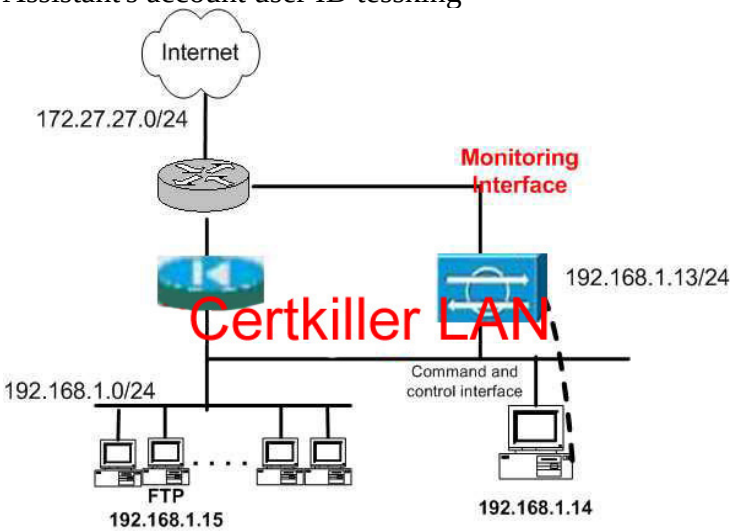
Answer:

Explanation:

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)Add ony the IDS MC to the access-list (as per question)
sensor(config-Host-net)# accessList ipAddress 10.10.10.100
g)Verify the change
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: 10.10.10.100
netmask: 255.255.255.255 <defaulted>
h)Exit network parameters configuration mode
sensor(config-Host-net)# exit
sensor(config-Host)#
i)Exit configure host mode
sensor(config-Host)#exit
Apply Changes:?[yes]
Press Enter to apply the changes
Reference:Cisco Courseware, nearly the same shown in LAB 7-4

QUESTION 243
You work as a security technician at Certkiller .com. You have reviewed the configuration of Certkiller 's Cisco IDS-4235 Sensor. You have decided 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 account and access privileges
3)Delete the service account
4)Reduce the access rights of your assistant, Jack King, from operator access to one that can only monitor IDS events.
5)Return all STRING TCP signatures to their default settings
Use the Information in the following table to complete these tasks
Cisco IDS Parameters Settings
Sensor administrator username/password Certkiller / Certkiller 1914
FTP server address 192.168.1.15
FTP username/password tkoperator/ Certkiller
FTP upload directory /ids4235
Backup file name backup-config
Assistant's account user ID tessking



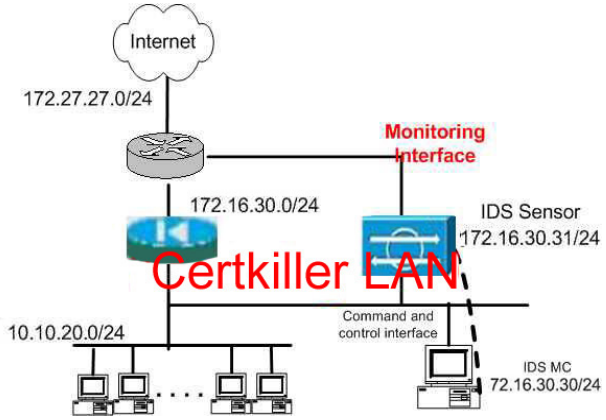
Assignment: Click on the picture of the host connected to an IDS Sensor by a serial console cable shown in the diagram as a dotted line. Select the Cisco Terminal Option and make the appropriate configuration tasks.

Answer:

Explanation:
login: Certkiller
password: Certkiller 1914
sensor#
1.sensor# copy current-config ftp://tkoperator@192.168.1.15/ids4235/backup-config
password: Certkiller
2.sensor# show user all
3.sensor# config terminal
sensor(config)#nousername service
4.sensor(config)#privilege user tessking viewer

5.sensor(config)#service virtual-sensor-configuration virtualSensor
sensor(config-vsc)#reset-signatures string.tcp

QUESTION 244
You work as network security administrator at the Certkiller .com office inWashington DC. Certkiller is now installing new Cisco IDS Sensors and you are responsible to configure them to permit remote access only from trusted hosts. Perform this task on one of the Sensors using the CLI (Command Line Interface). Refer to the following information and network topology exhibit to permit access from the IDS MC management station only to the Sensor.
Note: Since this is a new installation, you will also need to remove the default allowed network address. Verify your configuration settings prior to saving, and the save your configuration when finished.
Cisco IDS Paramaters Settings
Sensor operator username/password Certkiller op/ Certkiller 1918
Sensor administrator username/password Certkiller admin/ Certkiller 1918
Sensor IP address: 192.168.1.50/24
Default allowed network address: 10.0.0.0/8

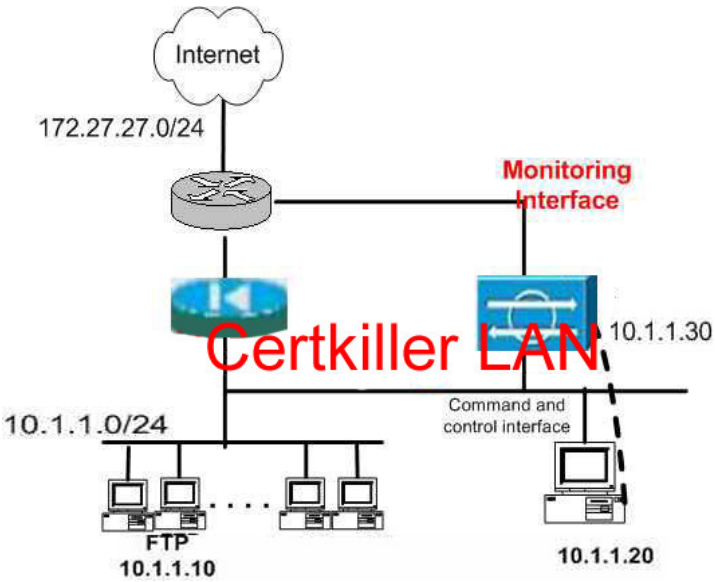


Task: Click on the picture of the host connected to an IDS Sensor by a serial console cable shown in the diagram as a dotted line. Select the Cisco Terminal Option and make the appropriate configuration tasks.

Answer:

Explanation:
sensor#configure terminal
sensor(config)#service host (Enters Host Configuration mode)
sensor(config-Host)#networkParams (Enter Network Parameters Configuration mode)
sensor(config-Host-net)# no accessList ipAddress 10.0.0.0 netmask 255.0.0.0 (Removes the default allowed network address)
sensor(config-Host-net)# accessList ipAddress192.168.1.51 (Allows only the IDS MC to access the Sensor)
sensor(config-Host-net)# show settings (Verify changes)
sensor(config-Host-net)# exit (Exits Network Parameters Configuration mode)
sensor(config-Host)# exit (Exits Configure Host mode)
Apply Changes:?[yes]: (Press Enter to apply the changes)

QUESTION 245
Exhibit/simulation:



Certkiller .com has recently hired you as a security administrator at theirToronto office. You are required to increase the security on one of Certkiller 's Cisco IDS-4250 Sensors.
After examining the current configuration you intend to modify access on user accounts and return some of the system's parameters to a known baseline by performing the following steps:
A)Use a remote FTP server to create a backup of the running configuration
B)Confirm existing accounts and access privileges
C)Delete the service account
D)Give your trainee Jack King, the daughter of the Certkiller CEO, increased access rights. Jack's access rights should be increased from viewer access to one that can monitor and tune IDS, however Jack should not be granted excessive access.
E)To default settings returned to all ATOMIC L3 IP signatures.
The information in the following table should be used:

Cisco IDS Parameters	**Settings**
Sensor administrator username/password	Certkiller / Certkiller abc
FTP server address	10.1.1.10
FTP username/password	Certkiller admin/tessking

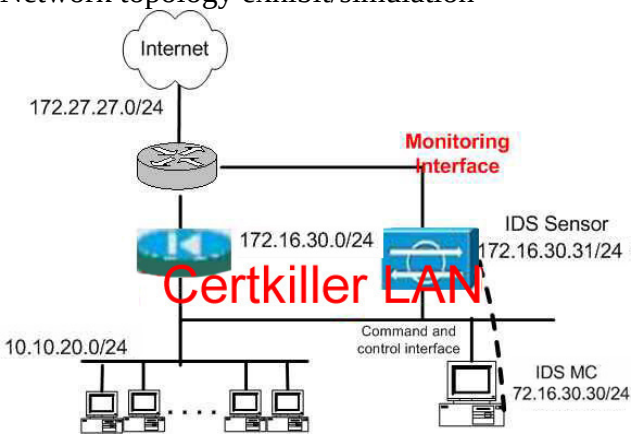
Assignment: Click on the picture of the host connected to an IDS Sensor by a serial console cable shown in the diagram as a dotted line. Select the Cisco Terminal Option and make the appropriate configuration tasks.

Answer:

Explanation:
login: Certkiller
password: Certkiller abc
sensor#
1.sensor# copy current-config ftp:// Certkiller admin@10.1.1.10/ Certkiller 5287/backup-cfg
password: tessking
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 tessking operator
5. sensor(config)#service virtual-sensor-configuration virtualSensor
6. sensor(config-vsc)#reset-signatures ATOMIC.L3.TCP

QUESTION 246
Network topology exhibit/simulation



You work as a network security administrator at Certkiller .com. Certkiller is now installing new Cisco IDS Sensors. You are required to configure these new Sensors so that they allow remote access only from hosts that are trusted. You must execute this task on of the IDS Sensors using the CLI (Command Line Interface). Use the information below and the network topology exhibit.
Permit access from IDS MC management station only to the sensor.
NOTICE: As this is a new installation, you must also remove the default allowed network address.
You are also required to verify your configuration settings before you save them. When you have saved the configuration you are finished.

Cisco IDS Parameters	**Settings**
Sensor operator username/password	Certkiller operator/ Certkiller 789
Sensor administrator username password	Certkiller admin/ Certkiller 789
Sensor IP address	172.16.30.31/24
Default allowed network address	10.0.0.0/8

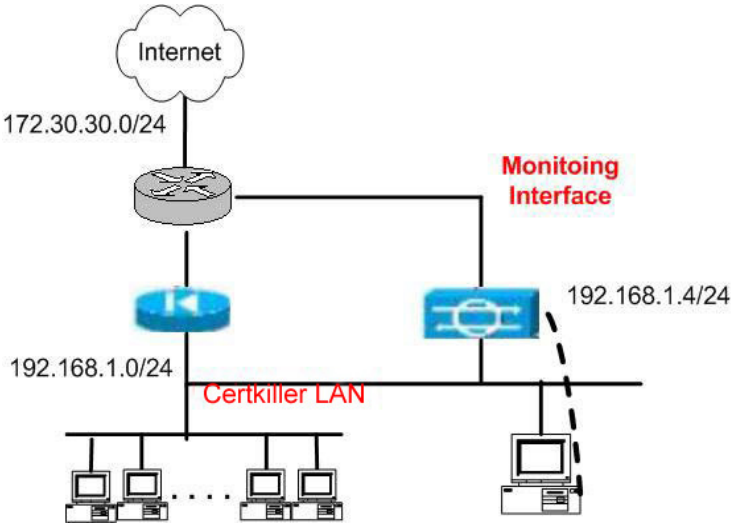
Assignment: Click on the picture of the host connected to an IDS Sensor by a serial console cable shown in the diagram as a dotted line. Select the Cisco Terminal Option and make the appropriate configuration tasks.

Answer:

Explanation:
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)Add ony the IDS MC to the access-list (as per question)
sensor(config-Host-net)# accessList ipAddress 10.10.10.100
g)Verify the change
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: 10.10.10.100
netmask: 255.255.255.255 <defaulted>
h)Exit network parameters configuration mode
sensor(config-Host-net)# exit
sensor(config-Host)#
i)Exit configure host mode
sensor(config-Host)#exit
Apply Changes:?[yes]
Press Enter to apply the changes

QUESTION 247
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 Paramaters Settings
Sensor Host ID 4
Sensor Organization ID 27
Sensor Host Name sensor27
Sensor Organization Name HQ



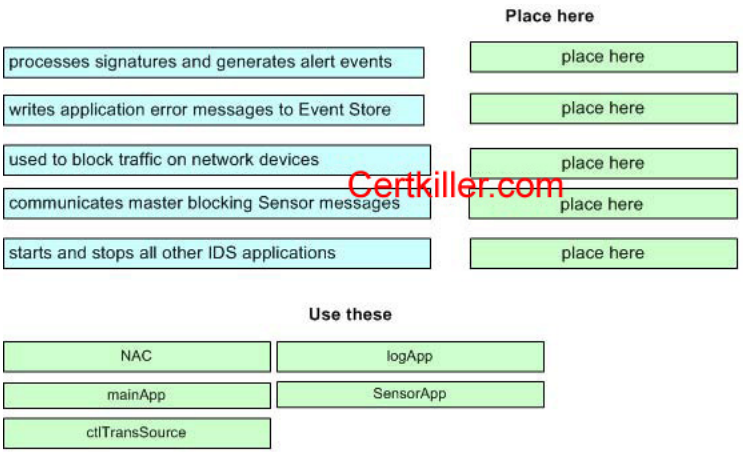
Assignment: Click on the picture of the host connected to an IDS Sensor by a serial console cable shown in the diagram as a dotted line. Select the Cisco Terminal Option and make the appropriate configuration tasks.
Sensor IP address 192.168.1.4/24
IDS Manager Host ID 4
IDS Manager Host Organization ID 27
IDS Manager Host Name sensor 27
IDS Manager Organizaiton Name HQ
IDS Manager IP Address 192.168.1.12/24
Note:The rout account password is " Certkiller "

Answer:

Explanation:
(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 248
Following is a list of descriptions and IDS processes. Match the IDS process with its description.



Answer:

Explanation:

Reference:Cisco Courseware 6-4

QUESTION 249
Starting and stopping all IDS applications is the task of which of the following Cisco IDS application servlets?

A. sensorApp
B. mainApp
C. cidCLI
D. IDM servlet

Answer: B

Explanation:
Correct description, but wrong options choused.MainApp is started by the operating system. It starts the applications in
the following sequence:
1.
Read and validate contents of dynamic and static configurations.
2.
Write dynamic configuration data to system files to make sure the two representations of data are in sync (for example, the IP address in the dynamic configuration must match the system network files).
3.

Create the shared system components-EventStore and IDAPI.
4.
Open status event subscription.
5.
Start the IDS applications (the order is specified in the static configuration).
6.
Wait for an initialization status event from each application.
If after waiting 60 seconds all status events have not been received, MainApp generates an error event identifying all applications that did not start.
7.
Close status event subscription.
8.
Start the upgrade scheduler.
9.
Register for control transaction requests, and service them as received.
Schedule, download, and install software upgrades.
Page 119 Cisco Press CCSP CSIDS 2nd edition under mainApp
The mainApp handles starting and stopping all the other Cisco IDS applications

---

QUESTION 250
What role would you assign to permit users all viewing operations and the administrative ability to change only their own passwords when setting up user accounts on a Cisco IDS Sensor?

A. operator
B. viewer
C. service
D. guest
E. administrator

Answer: B

Explanation:
Viewer - A user that can perform all viewing operations such as viewing events and viewing some configuration files. The only administrative option available to users with the viewer role is setting their own password.
Reference: Cisco Courseware p.6-12.

QUESTION 251
The NM-CIDS is directly connected to the router's backplane via which interface? Choose two.

A. the internal 100-Mbps Fast Ethernet port on the NM-CIDS
B. the external 100-Mbps Fast Ethernet port on the router
C. the internal 100-Mbps Fast Ethernet port on the router
D. the external 100-Mbps Fast Ethernet port on the NM-CIDS

Answer: A, C

QUESTION 252
Which types of packets are not forwarded to the NM-CIDS? (Choose two.)

A. GRE encapsulated packets
B. TCP packets
C. UDP packets
D. ARP packets

Answer: A, D

QUESTION 253
How many megabits per second can the NM-CIDS monitor?

A. 10mbps
B. 100mbps
C. 45mbps
D. 80mbps

Answer: B

QUESTION 254
Under what circumstance would only the untranslated inside source be sent to the NM-CIDS for processing?

A. When using outside NAT
B. When using intside NAT
C. When using outside PAT
D. When using intside PAT

Answer: A

QUESTION 255
What is the maximum number of command and control interfaces on an IDS Sensor appliance?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: A

QUESTION 256
Which Cisco IOS command is used to enable the forwarding of packets from the router to the NM-CIDS?

A. ip cef
B. ip inspect
C. service-module
D. ip cef linecard ipc memory

Answer: A

QUESTION 257
Select the true statement regarding Sensor groups.

A. The mandatory check box exists in the context of a Sensor object to identify required configuration settings.
B. The override check box exists in the context of a Sensor Group object to prevent configuration parameters from being inherited.
C. The override check box exists in the context of a Sensor object to override settings previously flagged as mandatory.
D. By default, all Sensor subgroups inherit the configuration settings of other Sensors in the same Sensor group.
E. The mandatory check box exists in the context of a Sensor Group object to indicate that all fields in the configuration window requires values.

Answer: B

QUESTION 258
IDS MC version 2.0 communicates with a sensor using which two methods? Choose two.

A. HTTP
B. SSH
C. RDEP
D. Telnet
E. FTP

Answer: B, C

QUESTION 259
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 PIXFirewall. Cisco Secure Policy Manager does not generate this command, but the command can be supported using the Command panel on the PIXFirewall node. You can use the who command with the same results.
AnswerE. kill: Terminates another Telnet session to PIXFirewall.
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 260
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 PIXFirewall 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 261
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 262
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 263
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 264
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 PIXFirewall. The ports you specify are those that the PIXFirewall 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 265
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 packetcommand
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 266
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
B. Port 345
C. Port 520
D. Port 354

Answer: C

Explanation:
Port 520 is the Routing Information Protocol port.
Reference: Cisco PIX Firewall Software - Introduction
Note: Rip is not talked about in this manner in the course manual 4

QUESTION 267
Exhibit:

If you were looking at the back of your PIX firewall and saw the following plate, what model of PIX would you be working on?

A. 501
B. 506
C. 515
D. 1100

Answer: C
Reference: Cisco Secure PIX Firewall

QUESTION 268
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 269
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 270
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 271
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 272
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 273
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 PIXFirewall Adaptive Security Algorithm that then permits connections from one PIXFirewall network interface to access hosts on another.
Reference: Cisco PIX Firewall Command Reference, Version 6.3

QUESTION 274
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 PIXFirewall 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 275
What port would you be concerned about if you were worried bout 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 276
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 277
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 PIXFirewall. 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 278
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
PIXFirewall supports the following TCP/IP protocols and applications:
*Address Resolution Protocol (ARP)
*Archie
*BerkeleyStandard Distribution (BSD)-rcmds
*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