Exam : 642-532

Title : Implementing Cisco Intrusion Prevention Systems

Ver : 09.27.07

QUESTION 1:

A new IDSM2 module was installed in the Certkiller network. 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
E. None of the above

Answer: D

Explanation:
IDSM-2 provides the following capabilities or features:
- Merged switching and security into a single chassis
- 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
Reference: Cisco Press CCSP CSIDS Guide, 2nd edition page 199

QUESTION 2:

Please refer to the exhibit.
A new NM-CIDS module is being inserted into the Certkiller network. Which versions of Cisco IOS software is needed to support the NM-CIDS module?

A. 3.1 and above.
B. 4.1 and above
C. 4.0 and above
D. 2.0 and above
E. None of the 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 3:

A new Certkiller IPS sensor is being configured for inline operation. Which three steps must you perform to prepare sensor interfaces for inline operations? (Choose three)

A. Disable all interfaces except the inline pair
B. Add the inline pair to the default virtual sensor
C. Enable two interfaces for the pair
D. Disable any interfaces that are operating in promiscuous mode.
E. Create the interface pair
F. Configure an alternate TCP-reset interface.

Answer: B, C, E

Explanation:
Operating in inline interface mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service.
Not only is the inline device processing information on layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (layers 3 to 7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.
In inline interface mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.
To configure the interfaces for inline operation, you will need to create the interface pair, enable the two interfaces, and add the inline interface pair to the default sensor.
Reference: Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1, Cisco Documentation, page 5-11.

QUESTION 4:

The Certkiller security administrator is determining whether to configure a new sensor in inline or promiscuous mode. What are three differences between inline and promiscuous sensor functionality? (Choose three)

A. A sensor that is operating in inline mode can drop the packet that triggers a signature before it reaches its target, but a sensor that is operating in promiscuous mode cannot.
B. A sensor that is operating in inline mode supports more signatures than a sensor that operates in promiscuous mode.
C. Deny actions are available only to inline sensors, but blocking actions are available only to promiscuous mode sensors.
D. A sensor that is operating in promiscuous mode can perform TCP resets, but a sensor that is operating in inline mode cannot.
E. Inline operation provides more protection from Internet worms than promiscuous mode does.
F. Inline operation provides more protection from atomic attacks than promiscuous mode does.

Answer: A, E, F

Explanation:
In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance

from other networking devices, for example, routers and firewalls, to respond to an attack. While such response actions can prevent some classes of attacks, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router).
Operating in inline interface mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (layers 3 to7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.
In inline interface mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008055

QUESTION 5:

New Cisco IPS sensors are being deployed within the Certkiller network. Which of the following are appropriate installation points for a Cisco IPS sensor? (Choose two)

A. On publicly accessible servers
B. On critical network servers
C. At network entry points
D. On user desktops
E. On corporate mail servers
F. On critical network segments

Answer: C, F

Explanation:
IPS sensors are designed to be placed at Network entry points and on critical network sensors. The sensor is designed to monitor all traffic crossing a given network segment. You must consider all external network connections and remote access points you want to protect. Each of the four network entry locations includes the following:
1. Internet Connections
2. Extranets
3. Intranets
4. Remote Access
The most common sensor deployment location is between the trusted internal network and the Internet. This deployment strategy is referred to as perimeter protection and the

sensor is commonly paired with one or more firewalls to enforce security policies.
Incorrect Answers:
A, B, D, E: Cisco network based sensors are designed to be placed on network segments, not on individual hosts such as desktops or servers. Host based IDS/IPS applications should be used on these types of devices.
Reference: CCSP: Cisco Certified Security Professional Certification All-in-One Exam Guide by Robert E. Larson and Lance Cockcroft, ISBN:0072226919.

QUESTION 6:

A Cisco IPS sensor has detected a large amount of malicious activity on the Certkiller network. How does a Cisco network sensor detect malicious network activity? (Select the best answer)

A. By using a blend of intrusion detection technologies
B.
By performing in-depth analysis of the protocols that are specified in the packets that are traversing the network
C. By comparing network activity to an established profile of normal network activity
D. By using behavior-based technology that focuses on the behavior of applications

Answer: A

Explanation:
Cisco Network based IDS (NIDS) uses a blend of leading intrusion detection technologies, and provide the following benefits:
1. Comprehensive Threat Protection Multiple detection methods - Cisco uses multiple methods to accurately detect threats, including stateful pattern recognition, protocol analysis, traffic anomaly detection, and protocol anomaly detection. Additionally, Cisco IDS delivers a Layer 2 signature engine to provide protection from Address Resolution Protocol (ARP) spoofing techniques.
1. Extensive protocol monitoring All major TCP/IP protocols are monitored, including IP, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP). Cisco IDS 4.x also statefully decodes application layer protocols, such as FTP, Simple Mail Transfer Protocol (SMTP), HTTP, Domain Name System (DNS), remote-procedure call (RPC), NetBIOS, Network News Transport Protocol (NNTP), Telnet, and peer-to-peer (P2P).
1. Comprehensive attack detection Cisco has the most comprehensive detection capabilities when detecting both the exploitation activity indicative of attempts to gain access or compromise network systems and DoS activity indicative of attempts to consume bandwidth or compute resources to disrupt normal operations. Add to that its ability to detect activity indicative of attempts to probe or map your network to identify targets, such as ping sweeps and port sweeps as well as misuse activity indicative of attempts to violate corporate polic; detected by configuring the sensor to look for custom text strings in the network traffic.
1. Damage Prevention Cisco responds immediately to stop attacks that can cost you

time and money. After an attack is accurately identified and classified, the system can deny the intruder by dropping the packet, terminating the session, reconfiguring access control lists (ACLs) on routers and switches, or dynamically modifying the firewall policy. Additionally, Cisco IDS 4.x blocks source and destination port numbers as well as source and destination IP addresses.
Reference: http://s2s.ltd.uk/technology-ids.htm

QUESTION 7:

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.
E. None of the above

Answer: B

Explanation:
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.

QUESTION 8:

When designing IP blocking for the Certkiller network using different Intrusion technologies, 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.
E. None of the above

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.
Note: It is recommended that Sensors be placed at those network entry and exit points that provide sufficient intrusion detection coverage.
Reference: Cisco Secure Intrusion Detection System, Cisco Press, page 467

QUESTION 9:

Many hackers use Denial of Service attacks in conjunction with a specific attack. Why would an attacker saturate the network with noise while simultaneously launching an attack?

A. It causes the Cisco IDS to fire multiple false negative alarms.
B. An attack may go undetected.
C. It will have no effect on the ability of the sensor to detect attacks.
D. It will initiate asymmetric attack techniques.
E. It will force the sensors into Bypass mode so that future attacks go undetected.

Answer: B

Explanation:
Saturating the network with bogus traffic is an example of a DoS or a DDos attack. The goal of denial of service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial of service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data. The underlying purpose to a denial of service attack is to bog down a system by giving it too much information to process quickly enough. While this attack is occurring, an attacker could also attempt to perform another, specifically targeted attack.
Reference: Cisco 642-532 IPS Courseware, page 3-24

QUESTION 10:

Which of the following types of attacks is typical of an intruder who is targeting networks of systems in an effort to retrieve data or enhance their privileges within a specific network?

A. Access attack

B. Denial of Service attack
C. Man in the middle attack
D. Authorization attack
E. Reconnaissance attack
F. None of the above

Answer: A
Access Attacks:
Access is a broad term used to describe any attack that requires the intruder to gain unauthorized access to a secure system with the intent to manipulate data, elevate privileges, or simply access the system. The term "access attack" is used to describe any attempt to gain system access, perform data manipulation, or elevate privileges.
System Access Attacks:
System access is the act of gaining unauthorized access to a system for which the attacker doesn't have a user account. Hackers usually gain access to a device by running a script or a hacking tool, or exploiting a known vulnerability of an application or service running on the host.
Data Manipulation Access Attacks:
Data manipulation occurs when an intruder simply reads, copies, writes, deletes, or changes data that isn't intended to be accessible by the intruder. This could be as simple as finding a share on a Windows 9x or
NT computer, or as difficult as attempting to gain access to a credit bureau's information, or breaking into the department of motor vehicles to change a driving record.
Elevating Privileges Access Attacks:
Elevating privileges is a common type of attack. By elevating privileges an intruder can gain access to files, folders or application data that the user account was not initially granted access to. Once the hacker has gained a high-enough level of access, they can install applications, such as backdoors and Trojan horses, to allow further access and reconnaissance.
Reference: CCSP: Cisco Certified Security Professional Certification All-in-One Exam Guide

---

QUESTION 11:

What reconnaissance methods are used to discover mail 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 12:

Which of the following describes the evasive technique whereby control characters are sent to disguise an attack?

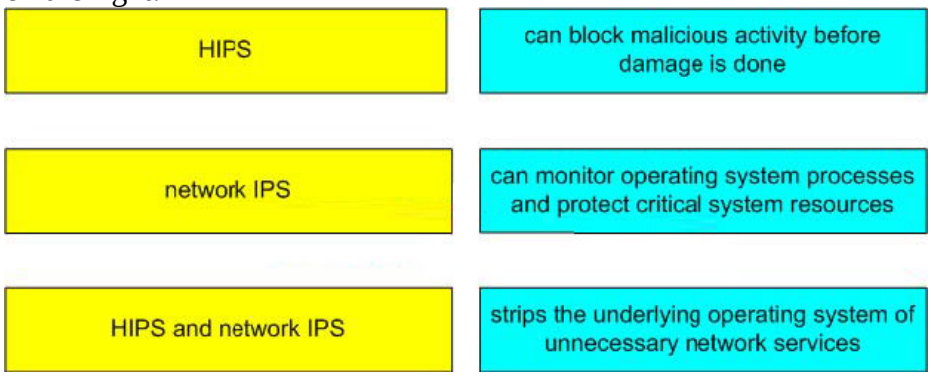
A. Flooding
B. Fragmentation
C. Obfuscation
D. Exceeding maximum transmission unit size
E. None of the above

Answer: C

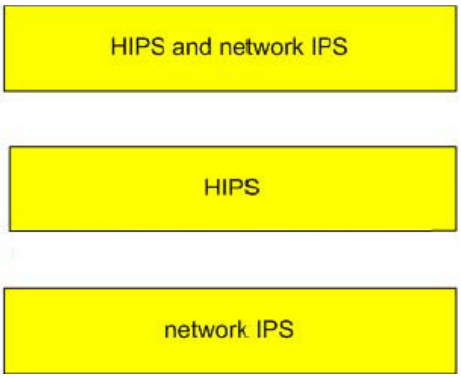
Explanation:
Intrusion Detection Systems inspect network traffic for suspect or malicious packet formats, data payloads and traffic patterns. Intrusion detection systems typically implement obfuscation defense - ensuring that suspect packets cannot easily be disguised with UTF and/or hex encoding and bypass the Intrusion Detection systems. Recently, the Code Red 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 CIDS Courseware, page 3-27

QUESTION 13:

DRAG DROP
Click and drag the security technology on the left to its corresponding description on the right.



Answer:



QUESTION 14:

New Cisco 4200 sensors were installed in the Certkiller network for network security purposes. In which three ways does a Cisco network sensor protect network devices from attacks? (Choose three)

A. It uses a blend of intrusion detection technologies to detect malicious network activity.
B. It can generate an alert when it detects traffic that matches a set of rules that pertain to typical intrusion activity.
C. It permits or denies traffic into the protected network that is based on access lists that you create on the sensor.
D. It can take a variety of actions when it detects traffic that matches a set of rules that pertain to typical intrusion activity.
E. It uses behavior-based technology that focuses on the behavior of applications to protect network devices from known attacks and from new attacks for which there is no known signature.

Answer: A, B, D

Explanation:
The Cisco IOS IDS is as an integrated intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match the IDS signatures. Upon detection of suspicious activity, the Cisco IOS IDS responds before network security can be compromised and sends alarms to a management console. The network administrator can configure the Cisco IOS IDS to choose the appropriate response to security incidents. When packets in a session match a signature, the Cisco IOS IDS can be configured to take these actions:
1. Send an alarm to a syslog server or a centralized management interface
2. Drop the packet
3. Reset the TCP connection
Incorrect Answers:
C: This describes the basic functionality of Cisco routers. Cisco IPS devices take account the state of the connections and look for anomalies in each data transmission up to layer 7. Access lists typically only filter traffic based on layers 3 and 4.

E: The IPS devices require a signature to generate an alarm and have an action taken.
New attacks with no known signature will not be detected.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_white_paper09186a008010e5c8.shtml

---

QUESTION 15:

The Certkiller network has only one entry point. However, you are concerned about internal attacks. Which of the following should be utilized on the Certkiller network? (Choose three)

A. CSA Agents on corporate mail servers
B. CSA Agents on critical network servers and user desktops
C. A network sensor behind (inside) the corporate firewall
D. A network sensor in front of (outside) the corporate firewall
E. Sensor and CSA Agents that report to management and monitoring servers that are located inside the corporate firewall
F. Sensor and CSA Agents that report to management and monitoring servers that are located outside the corporate firewall

Answer: B, C, E

Explanation:
The Cisco Security Agent (CSA) provides endpoint server and desktop protection against new and emerging threats due to malicious network activity. These can be placed on any device within the enterprise, protecting the network from both internal and external threats. When concerned with threats coming from the inside network, choices B, C, and E are best.
Incorrect Answers:
A: Corporate mail servers are used to provide email services to the outside. Placing CSA agents on these servers would protect from outside threats more so than from internal attacks.
D, F: These solutions are better suited for protecting the network from external threats.

QUESTION 16:

Which of the following functions can be performed remotely by means of the Intrusion Detection System Device Manager? (Select 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
G. None of the above

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.
Reference: Cisco CIDS Courseware, page 10-4

QUESTION 17:

Your Certkiller router is hosting a NM-CIDS. This router's configuration contains an inbound ACL. Which action does this router take when it receives a packet that should be dropped, according to the inbound ACL?

A. The router forwards the packet to the NM-CIDS for inspection, then drops the packet.
B. The router drops the packet and does not forward it to the NM-CIDS for inspection.
C. The router filters the packet through the inbound ACL, tags it for drop action, and forwards the packet to the NM-CIDS. Then the router drops it if it triggers any signature, even a signature with no action configured.
D. The router filters the packet through the inbound ACL, forwards the packet to the NM-CIDS for inspection only if it is an ICMP packet, and then drops the packet.
E. None of the above.

Answer: B

Explanation:
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.
Reference:
http://www.cisco.com/en/US/products/hw/routers/ps282/prod_architecture09186a00801cf9fc.html

---

QUESTION 18:

A new IDS NM-CIDS network module was recently installed on a Certkiller router, and packets are now being inspected via this module. However, not all packets are inspected. Which two packet types are not forwarded to the NM-CIDS? (Choose two)

A. GRE encapsulation packets
B. TCP packets
C. UDP packets
D. ARP packets
E. any IP multicast packets
F. ICMP packets

Answer: A, D

Explanation:
GRE Tunnels:
The Cisco IDS software does not analyze GRE encapsulated packet. Hence if a GRE packet is received, and the incoming interface is enabled for IDS monitoring, the packet WILL NOT be forwarded to the IDS Network Module for monitoring.
If a packet is encapsulated by the router into a GRE tunnel, and the incoming interface is enabled for IDS monitoring, then the packet (before encapsulation) will be sent to the IDS Network Module.
ARP Packets:
ARP packets are handled at layer-2 and are not forwarded to the IDS Network Module.
Reference:
http://www.cisco.com/en/US/products/hw/routers/ps282/prod_architecture09186a00801cf9fc.html

---

QUESTION 19:

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
E. None of the above

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 CIDS Courseware, page 2-46

QUESTION 20:

What can intrusion detection and prevention 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/IPS system 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, Cisco Press, page 54

QUESTION 21:

The signature files on a Certkiller sensor are being updated by the security administrator. Which two statement are true about Cisco IPS signatures? (Choose two)

A. A signature is a set of rules that pertain to typical intrusion activity.
B. When network traffic matches a signature, the signature must generate an alert, but can also initiate a response action.
C. Some signatures can be triggered by the contents of a single packet.
D. Signatures trigger alerts only when they match a specific pattern of traffic.
E. You can disable signatures and later re-enable them; however, this process requires the sensing engines to rebuild their configuration, which takes time and could delay the processing of traffic.
F. You can enable and modify built-in signatures, but you cannot disable them.

Answer: A, C

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. Signatures can be triggered either by a series of packets, called compound attacks, or by a single packet. Single packet attacks are called atomic attacks; an example of this is the ping of death
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_installation_and_configuration_guide_chap

---

QUESTION 22:

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

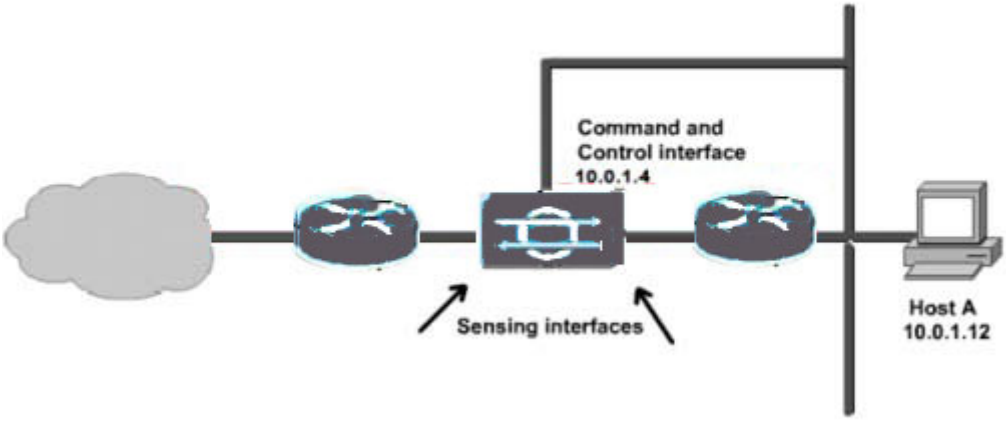
Answer: C E

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: CCSP Self-study: CSIDS Second Edition, page 438

QUESTION 23:

SIMULATION
You are the network security administrator at Certkiller .com in charge of the IPS sensors for a travel agency. Your sensors are currently deployed in promiscuous mode, but you have upgraded to IPS software 5.0 and now want to deploy in inline mode. You decide to return all signatures to heir default settings and re-tune them to maximize the benefits of your new topology. After tuning the signatures, you back up your configuration.
On the morning of May 12, 2005, your new assistant informs you that the network appears to have been under attack since you left your office at 6:00 pm the previous evening. Your assistant has tuned several signatures on the company IPS 4235 sensor in an effort to mitigate the attacks. From the assistant description of the tuning he performed, you feel sure the IPS 4235 sensor will be less, rather than more, effective in protecting your network. You decide to investigate the situation.
Your tasks are as follow:
Display all high-severity alerts that have been generated by the sensor since 6:00 pm May 11, 2005.
Verify that the only events displayed are high-severity alerts and their time-stamps are at or after 6:00 pm May 11, 2005.
Examine the tuned signature settings.
Restore the default settings to all signatures without affecting other sensor settings.
Verify that the signature settings were returned to the defaults. (While doing so, you discover that your assistant modified your allowed hosts list as well as tuning some signatures.)
Overwrite the current configuration with your backup configuration.
Display the sensor configuration again to verify the changes made by restoring from

backup.
Sensor administrator username/password: Certkiller / Certkiller 987



Answer:
Show only high events from May 11, 2005 from 6pm:
- "show events alert high 18:00 may 11 2005"
- "show config"
Reset signatures back to defaults:
- default service signature-definition sig0 (or name of signatures)
- verify with "show config"
Overwrite the current configuration with your backup config:
- "copy backup-config current-config"

QUESTION 24:

The Certkiller 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.

QUESTION 25:

The service pack file IDSk9-sp-3.1-2-S23.bin exists on the Certkiller 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: C

Explanation:
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 -l option by typing the following:
./IDSk9-sp-3.1-5-S58.bin -l
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 26:

A Certkiller 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

Explanation:
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 27:

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.

QUESTION 28:

An IDS module is being used on a Certkiller router configured with Network Address Translation. Under which circumstance would only the translated address be sent to the NM-CIDS for processing?

A. When using it outside NAT
B. When using it inside NAT
C. When using it outside PAT
D. When using it inside PAT

Answer: A

Explanation:
The Cisco IOS Software performs an input-ACL check on a packet before it processes the packet for NAT or Encryption. 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. With NAT, the only the translated IP address will be seen by the NM-CIDS for outside 1-1 address translations.
Reference:
http://www.cisco.com/en/US/products/hw/routers/ps282/prod_architecture09186a00801cf9fc.html

---

QUESTION 29:

Certkiller 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 for increased security. 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, Cisco Press, page 499

QUESTION 30:

You are the network security administrator for Certkiller . You want to create a user account for your assistant that gives the assistant the second-highest level of privileges. You want to ensure that your assistant can view all events and tune signatures.
Which role would you assign to the account for your assistant?

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

Answer: A

Explanation:
The CLI for IPS 5.0 supports four user roles: Administrator, Operator, Viewer, and Service. The privilege levels for each role are different; therefore, the menus and available commands vary for each role.
Administrators-This user role has the highest level of privileges. Administrators have unrestricted view access and can perform the following functions:
Add users and assign passwords
Enable and disable control of physical interfaces and virtual sensors
Assign physical sensing interfaces to a virtual sensor
Modify the list of hosts allowed to connect to the sensor as a configuring or viewing agent.
Modify sensor address configuration
Tune signatures
Assign configuration to a virtual sensor
Manage routers
Operators-This user role has the second highest level of privileges. Operators have unrestricted view access and can perform the following functions:
Modify their passwords
Tune signatures
Manage routers
Assign configuration to a virtual sensor
Viewers-This user role has the lowest level of privileges. Viewers can view configuration and event data and can modify their passwords.
Service-This user role does not have direct access to the CLI. Service account users are logged directly into a bash shell. Use this account for support and troubleshooting purposes only. Unauthorized modifications are not supported and will require the device to be re-imaged to guarantee proper operation. You can create only one user with the service role.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_command_reference_chapter09186a00803a

---

QUESTION 31:

A special account needs to be created via IDM so that a Certkiller sensor can be worked on by a technician. Which user account role on a Cisco IPS sensor should be specifically created in order to allow special root access for troubleshooting purposes only?

A. Operator
B. Viewer
C. Service
D. Administrator
E. None of the above

Answer: C

Explanation:

Explanation:
The CLI for IPS 5.0 supports four user roles: Administrator, Operator, Viewer, and Service. The privilege levels for each role are different; therefore, the menus and available commands vary for each role.
Administrators-This user role has the highest level of privileges. Administrators have unrestricted view access and can perform the following functions:
Add users and assign passwords
Enable and disable control of physical interfaces and virtual sensors
Assign physical sensing interfaces to a virtual sensor
Modify the list of hosts allowed to connect to the sensor as a configuring or viewing agent.
Modify sensor address configuration
Tune signatures
Assign configuration to a virtual sensor
Manage routers
Operators-This user role has the second highest level of privileges. Operators have unrestricted view access and can perform the following functions:
Modify their passwords
Tune signatures
Manage routers
Assign configuration to a virtual sensor
Viewers-This user role has the lowest level of privileges. Viewers can view configuration and event data and can modify their passwords.
Service-This user role does not have direct access to the CLI. Service account users are logged directly into a bash shell. Use this account for support and troubleshooting purposes only. Unauthorized modifications are not supported and will require the device to be re-imaged to guarantee proper operation. You can create only one user with the service role.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_command_reference_chapter09186a00803a

---

QUESTION 32:

A service account was created on a Certkiller sensor. 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.

E. None of the above

Answer: D

Explanation:
Creating the Service Account:
You should create a service account for TAC to use during troubleshooting. Although more than one user can have access to the sensor, only one user can have service privileges on a sensor. The service account is for support purposes only.
Caution:Do not make modifications to the sensor through the service account except under the direction of TAC. If you use the service account to configure the sensor, your configuration is not supported by TAC. We do not support the addition and/or running of an additional service to the operating system through the service account, because it affects the proper performance and proper functioning of the other IDS services. TAC does not support a sensor on which additional services have been added.

QUESTION 33:

The IDS MC is used to manage the Certkiller sensors. What is the Cisco IDS Management Center?

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

Answer: A

Explanation:
The Management Center for IDS Sensors is a tool with a scalable architecture for configuring Cisco network sensors, switch IDS sensors, and IDS network modules for routers using a web-based interface. The IDS MC is a web-based application that centralizes and accelerates the deployment and management of multiple IUDS sensors of IDSM.

QUESTION 34:

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

G. All of the above

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, Cisco Press, page 183

QUESTION 35:

A Certkiller IPS appliance has been configured with an interface pair. What is the purpose of an interface pair?

A. To provide load balancing
B. To provide inline monitoring
C. For multiple-subnet monitoring
D. For failover
E. For increased IPS performance
F. For SPAN source and destination-port identification

Answer: B

Explanation:
Explaining Inline Interface Mode:
You can pair interfaces on your sensor if your sensor is capable of inline monitoring. Operating in inline interface mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. An inline IPS sits in the fast-path, which allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on layers3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (layers 3 to7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.
In inline interface mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

QUESTION 36:

A new 4210 is being installed in the Certkiller LAN. 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, Cisco Press, page 98

QUESTION 37:

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:
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
Reference: CSIDS Courseware under Device - Sensor, page 12-5

QUESTION 38:

The Certkiller security administrator is setting the Bypass mode on a new IPS device. Which two statements accurately describe the software bypass mode? (Choose two)

A. When it is set to on, all Cisco IPS processing subsystems are bypassed and traffic is allowed to flow between the inline port or VLAN pairs directly.
B. When it is set to on, traffic inspection ceases without impacting network traffic.
C. The default is off.
D. If power to the sensor is lost, network traffic is not interrupted.

E. It can be used for redundancy in the event of hardware failure.
F. When it is set to off, traffic stops flowing if the sensor is down

Answer: B, F

Explanation:
To configure the sensor so that traffic continues to flow through inline pairs even when SensorApp is not running, you can enable bypass mode. Bypass mode minimizes dataflow interruptions during reconfiguration, service pack installation, or software failure. On the contrary, if the bypass mode is set to off, traffic will stop if the sensor fails as shown by the table below:
Cisco IPS Sensor Software Version 5.0 AutoBypass

AutoBypass Setting	AutoBypass Action
On	Pass traffic without first evaluating it
Off	Packets stop flowing if sensor fails
Auto	Packets continue to flow if sensor fails

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_qanda_item0900aecd80321849.shtml

---

QUESTION 39:

Which of the following identify basic authentication methods for accessing a Certkiller Sensor from the 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
F. None of the above

Answer: A C

Explanation:
SSH 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.

QUESTION 40:

Which of the following methods will you advise 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
E. SDM

Answer: B, C

Explanation:
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).

QUESTION 41:

A new IDS module was inserted into a Certkiller Catalyst switch and needs to be configured. Which command initiates the Cisco IDSM2 system-initialization dialog?

A. sysconfig-sensor
B. setup
C. configure terminal
D. session
E. initialize
F. None of the above.

Answer: B

Explanation:
Initializing the IDS Module:
After you have installed the IDS modules on your network, you can use the setup command to initially configure them.
To initially configure the IDS module, follow these steps:
Step1
Session in to the IDS module by entering the session module_number command at the prompt.
Note:
The default username and password are both cisco.
* Step2
You are prompted to change the default password.

After you change the password, the module# CONFigure prompt appears.
* Step3
Enter the setup command.
The System Configuration Dialog is displayed
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guide_chapt

---

QUESTION 42:

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
E. None of the above

Answer: D

Explanation:
Early intrusion detection was easily evaded by disguising an attack by using 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.
Reference: Cisco CIDS Courseware, page 3-27

QUESTION 43:

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
F. None of the above

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 44:

A Certkiller IPS device that has been in place for some time needs to be tuned to eliminate some false positive alerts. Which two are necessary to take into consideration when preparing to tune your sensor? (Choose two)

A. The security policy
B. The network topology
C. Which IP addresses are statically assigned, and which are DHCP addresses
D. The IP addresses of your inside gateway and outside gateway
E. Which traffic the sensor denies by default
F. The current configuration for each virtual sensor

Answer: A, B

Explanation:
Tuning and Alarm Logging:
The traffic that IPS sensors see is dependent upon the corporate security policy, as well as the network topology. For example, if the corporate security policy provides employees with open access to the Internet, then very little tuning based upon traffic type (connection signatures) can be performed on these sensors. However, if the corporate security policy is more restrictive, then tuning based upon traffic type is possible. These sensors should see few attacks, and the attack signatures can generally be left tuned at the default levels. Attacks seen here have breached the external firewall, however, or are being generated from within the internal network, and should therefore be taken seriously. Again, during incidents such as a Code Red attack, it may be necessary to tune specific signatures at a lower level in order to keep from being overwhelmed by high-priority alarms.
Reference:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801b

---

QUESTION 45:

A Certkiller sensor was placed outside of the firewall, and is detecting a large volume of web traffic because it is monitoring traffic outside the firewall. What is the most appropriate sensor tuning for this scenario?

A. Lowering the severity level of certain web signatures
B. Raising the severity level of certain web signatures

C. Disabling all web signatures
D. Disabling the Meta Event Generator
E. Retiring certain web signatures

Answer: A

Explanation:
Normally a sensor is placed on the outside of a firewall to detect the overall number and severity of attacks on a network, and to determine the effectiveness of the firewall. For sensors placed on the outside, a great deal of traffic and alerts will be seen. Cisco recommends lowering the severity level of many of the more common attacks. This will ensure that all attacks are seen and logged, but the number of high level alerts will be kept down to a reasonable level.
Incorrect Answers:
B: This will result in even more alerts, which will inundate the logs and overwhelm the security management team.
C, D, E: Although this will indeed lower the number of alerts, these solutions will also result in lowering the effectiveness of the sensor, and allowing certain events to pass into the network unmonitored and without being logged.

QUESTION 46:

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
F. None of the above

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:
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_1/idsmc11/ug/ch0

QUESTION 47:

IP log files are being sent from an existing Certkiller IPS device to a server. In which file format are these IP logs stored?

A. Microsoft Word
B. Microsoft Excel
C. Text
D. Libpcap
E. PDF

Answer: D

Explanation:
Cisco IPS devices send IP log files in the libpcap format.
You can manually configure the sensor to capture all IP traffic associated with a host you specify by IP address. You can specify how long you want the IP traffic to be logged, how many packets you want logged, and how many bytes you want logged. The sensor stops logging IP traffic at the first parameter you specify.
You can also have the sensor log IP packets every time a particular signature is fired. You can specify how long you want the sensor to log IP traffic and how many packets and bytes you want logged.
You can copy the IP logs from the sensor and have them analyzed by a tool that can read packet files in a libpcap format, such as Ethereal or tcpdump.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 48:

IP log files need to be automatically generated by a Certkiller sensor. How is automatic IP logging enabled on a sensor?

A. It is enabled by default for all signatures.
B. It is enabled by default for all master signatures only.
C. It is enabled by default for all high-severity signatures only.
D. It must be manually configured for individual signatures.
E. It is manually configured using the ip-log global configuration command.

Answer: D

Explanation:
About IP Logging
You can manually configure the sensor to capture all IP traffic associated with a host you specify by IP address. You can specify how long you want the IP traffic to be logged, how many packets you want logged, and how many bytes you want logged. The sensor

stops logging IP traffic at the first parameter you specify.
You can also have the sensor log IP packets every time a particular signature is fired.
You can specify how long you want the sensor to log IP traffic and how many packets and bytes you want logged.
Use the ip-log-packets number, ip-log-time number, and ip-log-bytes number commands to configure automatic IP logging parameters on the sensor.
The following options apply:
ip-log-packets-Identifies the number of packets you want logged.
The valid value is 0 to 65535. The default is 0.
ip-log-time-Identifies the duration you want the sensor to log packets.
The valid value is 0 to 65535 minutes. The default is 30 minutes.
ip-log-bytes -Identifies the maximum number of bytes you want logged.
The valid value is 0 to 2147483647. The default is 0.
Automatic IP logging is configured on a per signature basis or as an event action override.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 49:

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
E. None of the above

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.

QUESTION 50:

What information can the Certkiller 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:
http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a0080157f9f.htm

---

QUESTION 51:

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.
E. All of the above

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.
Reference: Cisco IDS Courseware, page 14-30

QUESTION 52:

Of the following choices, which signature description best describes a String signature engine?

A. Network reconnaissance detection
B. Regular expression-based pattern inspection for multiple transport protocols
C. Layer 5, 6, and 7 services that require protocol analysis
D. State-based, regular expression-based pattern inspection and alarm functionality for TCP streams
E. None of the above

Answer: B

Explanation:

A STRING engine is defined as a signature engine that provides regular expression-based pattern inspection and alert functionality for multiple transport protocols, including TCP, UDP, and ICMP.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_command_reference_chapter09186a00803a

---

QUESTION 53:

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

QUESTION 54:

Which type of signature engine is best suited to create a custom signature that would inspect data at Layers 5-7?

A. Atomic
B. String
C. Sweep
D. Service
E. AIC
F. None of the above

Answer: D

Explanation:
Service Engines:
SERVICE engines analyze Layer 5+ traffic between two hosts. These are 1:1 signatures that track persistent data on the STREAM (AaBb) for TCP or QUAD (AaBb) for UDP. The engines decode and interpret the Layer 5+ payload in a manner similar to the live

service. A full-service-like decode may not be necessary if the partial decode provides adequate information to inspect the signatures. The engines decode enough of the data to make the signature determinations but do not decode more than is needd; this minimizes CPU and memory load.
The purpose of the SERVICE decode is to mimic the live server's interpretation of the Layer 5+ payload. These are used primarily in the determination of signatures, as the decoded fields are compared to the signature's parameters.
Reference:
www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd80327257.shtml

---

QUESTION 55:

By manipulating the TTL on a TCP packet, an attacker could desynchronize inspection. Signature 1308 (TTL evasion) fires when the TTL for any packet in a TCP session is higher than the lowest-observed TTL for that session. Signature 1308 rewrites all TTLs to the lowest-observed TTL, and produces an alert. The Certkiller security administrator would like to have the signatures continue to modify packets inline but avoid generating alerts. How could this be done?
A. This cannot be done; an alert is always generated when a signature fires.
B. Remove the Produce Alert action from the signature.
C. Create an Event Variable.
D. Create an Event Action Override that is based on the Produce Alert action.
E. Create a custom signature with the Meta engine.

Answer: B

Explanation:
The "produce alert" action writes the event to the Event Store as an evIdsAlert, and this is enabled by default for all signatures. To configure the IPS to continue to modify packets inline for a specific signature, but not generate alerts this can be accomplished simply by removing the "produce alert" action from the specific signature.

QUESTION 56:

To ensure that all packets traversing the Certkiller network conform to RFC standards, the Normalizer engine is being used on a sensor. Which action is available only to signatures supported by the Normalizer engine?

A. Produce Verbose Alert
B. Modify Packet Inline
C. Deny Packet Inline
D. Log Pair Packets
E. Request SNMP Trap
F. Reset TCP Connection
G. All of the above

Answer: B

Explanation:
The NORMALIZER engine deals with IP fragment reassembly and TCP stream reassembly. With the NORMALIZER engine you can set limits on system resource usage, for example, the maximum number of fragments the sensor tries to track at the same time.
The "modify-packet-inline" function is a new feature from the inline normalizer engine. It scrubs the packet and corrects irregular issues such as bad checksum, out of range values, and other RFC violations.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 57:

A new sensor was installed on the Certkiller LAN. Which sensor process is used to initiate the blocking response action on this device?

A. EXEC
B. Network Access Controller
C. Blockd
D. shunStart
E. ACL Daemon

Answer: B

Explanation:
The Attack Response Controller (ARC), the blocking application on the sensor, starts and stops blocks on routers, switches, PIX. Firewalls, FWSM, and AS
A. ARC blocks the IP address on the devices it is managing. It sends the same block to all the devices it is managing, including any other master blocking sensors. ARC monitors the time for the block and removes the block after the time has expired.
Note:
ARC was formerly known as Network Access Controller. The name has been changed for IPS 5.1, although IDM still contains the term Network Access Controller.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a00804d

---

QUESTION 58:

You want to configure a new Certkiller sensor to ensure malicious attacks on the network are prevented. What would best mitigate the executable-code exploits that can perform a variety of malicious acts, such as erasing your hard drive?

A. Assigning deny actions to signatures that are controlled by the Trojan engine
B. Assigning the TCP reset action to signatures that are controlled by the Normalizer engine
C. Enabling blocking
D. Enabling Application Policy Enforcement
E. Assigning blocking actions to signatures that are controlled by the State engine
F. None of the above

Answer: A

Explanation:
Attacks or other misuses of network resources can be defined as network intrusions. Sensors that use a signature-based technology can detect network intrusions. A signature is a set of rules that your sensor uses to detect typical intrusive activity, such as 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 alert. Sensors let you modify existing signatures and define new ones. Actions can be assigned to each signature, specifying the action to take when an attack is found. For the most severe attacks such as the one described in this question, the best approach would be to configure deny actions for this signature, preventing the Trojan attack from taking place.

QUESTION 59:

When the specific signature 3116 (NetBus) is detected in the Certkiller network, you want your sensor to terminate the current packet and future packets on the TCP flow. Which action should you assign to the signature to accomplish this?

A. Request Block Connection
B. Request Block Host
C. Deny attacker Inline
D. Deny Connection Inline
E. Reset TCP Connection
F. Modify Packet Inline

Answer: D

Explanation:
The Deny connection inline action will block all packets on the TCP flow, preventing this attack signature from traversing the network. The following list describe the various event actions that can be configured:
Event Actions:
The following event action parameters belong to each signature engine:
Produce-alert-Writes an <evIdsAlert> to the Event Store.

Produce-verbose-alert-Includes an encoded dump (possibly truncated) of the offending packet in the evIdsAlert.
Deny-attacker-inline -Does not transmit this packet and future packets from the attacker address for a specified period of time (inline only).
Deny-connection-inline -Does not transmit this packet and future packets on the TCP Flow (inline only).
Deny-packet-inline-Does not transmit this packet.
Log-attacker-packets-Starts IP logging of packets containing the attacker address (inline only).
Log-pair-packets-Starts IP logging of packets containing the attacker-victim address pair.
Log-victim-packets-Starts IP logging of packets containing the victim address.
Request-block-connection-Requests Network Access Controller to block this connection.
Request-block-host-Requests Network Access Controller to block this attacker host.
Request-snmp-trap-Sends request to NotificationApp to perform SNMP action.
Reset-tcp-connection-Sends TCP resets to hijack and terminate the TCP flow.
Modify-packet-inline-Modifies packet contents (inline only).
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 60:

The Certkiller security administrator is trying to calculate a numerical value on the importance of individual alerts. What is a configurable weight that is associated with the perceived importance of a network asset?

A. Risk Rating
B. Parameter value
C. Target Value Rating
D. Severity level
E. Storage key
F. Rate parameter

Answer: C

Explanation:
The Target Value Rating is a main component of determining the Risk rating, and is used to place a relative value on the importance of a device.
In contrast to simplistic alert rating models that are commonly used in the industry, Cisco IPS Version 5.0 Sensor Software delivers unique Risk Ratings that are assigned to alerts generated from IPS (Intrusion Prevention Systems) sensors. The intent of this risk rating is to provide the user withan indication of the relative risk of the traffic or offending host continuing to access the user's network. This rating can be used either to illuminate the events that require immediate administrator attention in the classic intrusion detection system (IDS) promiscuous mode, or to provide a means fordeveloping risk-oriented event action policies when the sensor is employed in the inline intrusion protection system

(IPS) mode.
The risk rating is realized as an integer value in the range from 0 to 100. The higher the value, the greater the security risk of the trigger event for theassociated alert. The risk rating is a calculated number that has four primary components-Alert Severity Rating (ASR), Signature Fidelity Rating (SFR), Attack Relevancy Rating (ARR), and Target Value Rating (TVR).
The Risk Rating is calculated using the following formula:

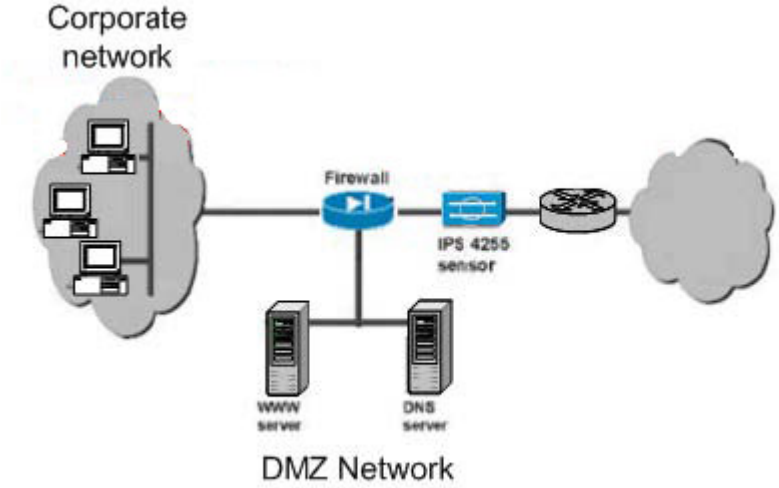
$$RR = \frac{Fidelity * Severity * Target\text{-}Value\text{-}Rating}{100 * 100 * 100}$$

Signature Fidelity Rating (SFR) = Relative measure of the accuracy of the signature (predefined); 0-100 Set by Cisco Systems, Inc.
Alert Severity Rating (ASR) = Relative result or damage if the attack succeeds (predefined); 25-Information, 50-Low, 75-Medium, 100-High
Target Value Rating (TVR) = Value used to change the risk rating higher or lower based on the target of the attact (user defined);
75-Low Asset Value , 100-Medium Asset value , 150-High Asset Value, 200-Mission Critical Asset Value
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_white_paper0900aecd80191021.shtml

---

QUESTION 61:

The Certkiller Corporate network is displayed in the following exhibit:



Refer to the exhibit shown above. You want your inline Cisco IPS 4255 sensor to drop packets that pose the most severe risk to your network, especially to the servers on your DMZ. Which two should you use to accomplish your goal in the most time-efficient manner? (Choose two)

A. Use an Event Action Filter
B. Modify the Signature Fidelity Rating
C. Adjust the Alert Severity

D. Configure an Event Action Override
E. Modify the Application Policy
F. Adjust the Target Value Rating

Answer: D, F

Explanation:
Since this server is deemed to be more important than other elements on the same IP network, the security administrator should use target value ratings to assign this server a higher level of importance. Cisco defines the TLV Rating as:
Target Value Rating-A weight associated with the perceived value of the target.
TVR is a user-configurable value that identifies the importance of a network asset (through its IP address). You can develop a security policy that is more stringent for valuable corporate resources and looser for less important resources. For example, you could assign a TVR to the company web server that is higher than the TVR you assign to a desktop node. In this example, attacks against the company web server have a higher RR than attacks against the desktop node.
Finally, event action overrides should be configured to prevent and drop attacks aimed at the server. Event action overrides are a way to add event actions globally without having to configure each signature individually. Each event action has an associated RR range. If a signature event occurs and the RR for that event falls within the range for an event action, that action is added to the event. You can configure event action filters to remove specific actions from an event or to discard an entire event and prevent further processing by the sensor. You can use event action variables that you defined to group addresses for your filters.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 62:

The Certkiller security administrator is determining the risk rating for specific events. Which three values are used to calculate the risk rating for an event? (Choose three)

A. Alert Severity Rating
B. Signature Fidelity Rating
C. Target Value Rating
D. Target Fidelity Rating
E. Reply Ration
F. Rate
G. Cost Metric

Answer: A, B, C

Explanation:

The risk rating is realized as an integer value in the range from 0 to 100. The higher the value, the greater the security risk of the trigger event for theassociated alert. The risk rating is a calculated number that has three primary components-Alert Severity Rating (ASR), Signature Fidelity Rating (SFR), and Target Value Rating (TVR).
The Risk Rating is calculated using the following formula:

$$RR = \frac{Fidelity * Severity * Target\text{-}Value\text{-}Rating}{100 * 100 * 100}$$

Signature Fidelity Rating (SFR) = Relative measure of the accuracy of the signature (predefined); 0-100 Set by Cisco Systems, Inc.
Alert Severity Rating (ASR) = Relative result or damage if the attack succeeds (predefined); 25-Information, 50-Low, 75-Medium, 100-High
Target Value Rating (TVR) = Value used to change the risk rating higher or lower based on the target of the attact (user defined);
75-Low Asset Value , 100-Medium Asset value , 150-High Asset Value, 200-Mission Critical Asset Value
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_white_paper0900aecd80191021.shtml

---

QUESTION 63:

In a Certkiller IPS device, both the AIC engine and the Application Policy Enforcement features are enabled. In which of the scenarios listed below are these feature needed?

A. You think some users with operator privileges have been misusing their privileges. You want the sensor to detect this activity and revoke authentication privileges.
B. You think users on your network are disguising the use of file-sharing applications by tunneling the traffic through port 80. You want your sensor to identify and stop this activity.
C. You have been experiencing attacks on your voice gateways. You want to implement advanced VOIP protection.
D. You believe that hackers are evading the Cisco IPS. You want the sensor to eradicate anomalies in the IP and TCP layers that allow an IPS to be avoided.

Answer: B

Explanation:
Cisco IPS Version 5.0 Sensor detects and prevents covert channel tunneling through Port 80. For example, a request message can be inspected that indicates traffic is being tunneled through Web ports using the application GoTomypc. Similarly, users can easily disguise the use of file sharing applications such as Kazaa by tunneling the traffic through Port 80. These types of activities can be accurately identified and subsequently stopped.
The AIC and Application policy enforcement feature provides deep analysis and control of a broad set of applications, including control of peer-to-peer, instant messaging (IM),

and tunneled applications over Port 80. This allows the user to make policy decisions concerning various traffic types and Multipurpose Internet Mail Extensions (MIME) types to help ensure that malicious traffic is disallowed from traversing the network.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_data_sheet0900aecd801eeea5.html

---

QUESTION 64:

A Custom signature needs to be created in a Certkiller sensor. Under which tab in the Cisco IDM can you find the Custom Signature Wizard?

A. Device
B. Configuration
C. Monitoring
D. Administration
E. None of the above

Answer: B

Explanation:
The Custom Signature Wizard guides you through a step-by-step process for creating custom signatures. There are two possible sequences-using a signature engine to create your custom signature or creating the custom signature without a signature engine.
The Custom Signature Wizard provides a step-by-step procedure for configuring custom signatures.
Using the IDM, the first step to create custom signatures using the Custom Signature Wizard is:
Step1
Click Configuration> Signature Definition> Custom Signature Wizard.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a00803e

---

QUESTION 65:

A new Certkiller sensor is generating a great deal of false positive alerts on the web servers. Which two actions will help to reduce the amount of these false positives? (Choose two)

A. Create a policy that denies attackers inline and filters alerts for events with high Risk Ratings.
B. Lower the severity level of signatures that are generating the false positives.
C. Lower the fidelity ratings of signatures that are generating the false positives.
D. Raise the Target Value Ratings for your web servers.
E. Create a filter that filters out any alerts whose target address is that of one of your web servers.

Answer: A, D

Explanation:
The Target Value Rating (TVR) is a user-configurable value that identifies the importance of a network asset (through its IP address). You can develop a security policy that is more stringent for valuable corporate resources and looser for less important resources. For example, you could assign a TVR to the company web server that is higher than the TVR you assign to a desktop node. In this example, attacks against the company web server have a higher RR than attacks against the desktop node. Raising the TVR and creating a policy that filters for the events associated with a high Risk Rating would reduce the number of overall false positive alerts for the web server.
Incorrect Answers:
B: The Alert Severity Rating (ASR) = Relative result or damage if the attack succeeds (predefined); 25-Information, 50-Low, 75-Medium, 100-High. This value will only affect the severity of the alert, not the total number of alerts.
C: The Signature Fidelity Rating (SFR) = Relative measure of the accuracy of the signature (predefined); 0-100 Set by Cisco. Lowering this value would most likely result in more false positive alerts.
D: This will eliminate all of the alerts for attacks aimed at the web servers, including real attacks. This would fundamentally defeat the purpose of using an IPS device to monitor the web servers in the first place.

QUESTION 66:

Newly installed sensors need to be configured to send SNMP traps to the Certkiller NOC. Which two tasks must you complete in Cisco IDM to configure the sensor to allow an SNMP network management station to obtain the sensor's health and welfare information? (Choose two)

A. From the SNMP General Configuration panel, configure the SNMP agent parameters.
B. From the SNMP Traps Configuration panel, enable SNMP Traps and SNMP Gets/Sets.
C. From the SNMP Traps Configuration panel, enable SNMP Traps.
D. From the SNMP General Configuration panel, enable SNMP Gets/Sets.
E. From the SNMP Traps Configuration panel, enabled SNMP Traps and SNMP Get-Responses.

Answer: A, D

Explanation:
Use the SNMP General Configuration panel to configure the sensor to use SNMP.
The following fields and buttons are found on the SNMP General Configuration panel.
Field Descriptions:
Enable SNMP Gets/Sets-If selected, allows SNMP gets and sets.
SNMP Agent Parameters-Configures the parameters for SNMP agent.

Read-Only Community String-Identifies the community string for read-only access.
Read-Write Community String-Identifies the community string for read and write access.
Sensor Contact-Identifies the contact person, contact point, or both for the sensor.
Sensor Location-Identifies the location of the sensor.
Sensor Agent Port-Identifies the IP port of the sensor.
The default is 161.
Sensor Agent Protocol-Identifies the IP protocol of the sensor.
The default is UDP.
To set the general SNMP parameters, follow these steps:
Step1
Log in to IDM using an account with administrator privileges.
Step2
Click Configuration> SNMP> SNMP General Configuration.
The SNMP General Configuration panel appears.
Step3
Select Enable SNMP Gets/Sets to enable SNMP so that the SNMP management workstation can issue requests to the sensor SNMP agent.
Step4
Configure the SNMP agent parameters:
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a00804c

---

QUESTION 67:

What information can the Certkiller 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 (Cisco Press) page 446

QUESTION 68:

A new Certkiller IPS appliance needs to be configured to have the inline sensor deny attackers inline when events occur that have a Risk Ratings over 85. Which two actions will accomplish this? (Choose two)

A. Create Target Value Ratings of 85 to 100.
B. Create an Event Variable for the protected network.
C. Enable Event Action Overrides.
D. Create an Event Action Filter, and assign the Risk Rating range of 85 to 100 to the filter.
E. Enable Event Action Filters.
F. Assign the Risk Rating range of 85 to 100 to the Deny Attacker Inline event action.

Answer: C, F

Explanation:
Calculating the Risk Rating:
An RR is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network. The calculation takes into account the value of the network asset being attacked (for example, a particular server), so it is configured on a per-signature basis (ASR and SFR) and on a per-server basis (TVR). RRs let you prioritize alerts that need your attention. These RR factors take into consideration the severity of the attack if it succeeds, the fidelity of the signature, and the overall value of the target host to you.
You can add an event action override to change the actions associated with an event based on the RR of that event. Event action overrides are a way to add event actions globally without having to configure each signature individually. Each event action has an associated RR range. If a signature event occurs and the RR for that event falls within the range for an event action, that action is added to the event. For example, if you want any event with an RR of 85 or more to generate an SNMP trap, you can set the RR range for Request SNMP Trap to 85-100. If you do not want to use action overrides, you can disable the entire event action override component.
Event action rules are a group of settings you configure for the event action processing component of the sensor. These rules dictate the actions the sensor performs when an event occurs.
The event action processing component is responsible for the following functions:
Calculating the risk rating
Adding event action overrides
Filtering event action
Executing the resulting event action
Summarizing and aggregating events
Maintaining a list of denied attackers
The "deny attacker inline" event action function does not transmit this packet and future packets originating from the attacker address for a specified period of time (inline mode

only). After the RR range has been created, it can be applied to the Deny Attacker Inline event action.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 69:

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:
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.
Note: Archive using SCP is false, although Copy using SCP would be true.

QUESTION 70:

The following output was seen on a Certkiller IPS device:

```
evIdsAlert: eventId=1111114419743472090 severity=high
vendor=Cisco
  originator:
    hostId: sensor1
    appName: sensorApp
    appInstanceId: 340
  time: 2005/03/21 10:47:53 2005/03/21 10:47:53 UTC
  signature: description=SYN23 id=60000
version=custom
    subsigId: 0
    sigDetails: My Sig Info
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.10.10
      port: 2151
    target:
      addr: locality=IN 10.0.1.50
      port: 23
  actions:
    deniedPacket: true
    deniedFlow: true
  riskRatioValue: 90
  interface: vlan
  protocol: tcp

evIdsAlert: eventId=1111100779743472268 severity=high
vendor=Cisco
  originator:
    hostId: sensor1
    appName: sensorApp
    appInstanceId: 340
  time: 2005/03/21 13:04:41 2005/03/21 13:04:41 UTC
  signature: description=ICMP Echo Request id=2004
version=81
    subsigId: 0
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.10.10
    target:
      addr: locality=IN 0.0.0.0
  summary: final=true initialAlert=0
summaryType=Regular 6
  alertDetails: Regular Summary: 6 events this interval ;
  riskRatingValue: 100
  interface: fe0_1
```

Refer to the exhibit shown above. You notice these alerts and other with some of the same attributes on your sensor when you arrive at work one morning. What is an appropriate action to take?

A. Set Bypass mode to off for Sensor1.
B. Lower the target Value Ratings for hosts on your internal network.
C. Lower the Alert Severity level of signatures 2004 and 60000.
D. Create an Active Host Block.
E. Activate all retired signatures.

Answer: D

Explanation:
The output shown above is the result of a "show events" command, and shows two separate alert instances. Both of them were initiated by a device with IP address 192.168.10.10, so an active host block should be created for this specific device to stop it from continuing to attack the network.
Use the Active Host Blocks panel to configure and manage blocking of hosts.
An active host block denies traffic from a specific host permanently (until you remove the block) or for a specified amount of time. You can base the block on a connection by specifying the destination IP address and the destination protocol and port.
An active host block is defined by its source IP address. If you add a block with the same source IP address as an existing block, the new block overwrites the old block.
If you specify an amount of time for the block, the value must be in the range of 1 to 70560 minutes (49 days). If you do not specify a time, the host block remains in effect until the sensor is rebooted or the block is deleted.

QUESTION 71:

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 72:

One of the Certkiller IPS devices is configured as a Master Blocking Sensor. What is

the primary function of a Master Blocking Sensor?

A. To serve as the central point of configuration in the Cisco IDM for blocking.
B. To serve as the central point of configuration in the Cisco IDS MC for blocking.
C. To manage and distribute blocking configurations 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.
F. All of the above

Answer: D

Explanation:
Two sensors cannot control blocking on the same device. If this situation is needed, configure one sensor as the master blocking sensor to manage the devices and the other sensors can forward their block requests to the master blocking sensor. Multiple sensors (blocking forwarding sensors) can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The master blocking sensor is the Network Access Controller running on a sensor that controls blocking on one or more devices on behalf of one or more other sensors. The Network Access Controller on a master blocking sensor controls blocking on devices at the request of the Network Access Controllers running on other sensors.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 73:

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

sensor. And on the master blocking sensor you must add the blocking forwarding sensors to its remote host configuration.

QUESTION 74:

A Certkiller sensor is acting as the Master Blocking Sensor. 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 as the master blocking sensor; on the master blocking sensor you must add the blocking forwarding sensors to its remote host configuration.

QUESTION 75:

Some of the Certkiller users on the network are disguising the use of file-sharing applications by tunneling the traffic through port 80. How can you configure your sensor to identify and stop users from performing this activity?

A. Enable all signatures in the Service HTTP engine.
B. Assign the Deny Packet Inline action to all signatures in the Service HTTP engine.
C. Enable HTTP Application Policy and enable the Alarm on Non-HTTP Traffic signature.
D. Enable all signatures in the Service HTTP engine. Then create an Event Action Override that adds the Deny Packet Inline action to events triggered by these signatures if the traffic originates from your corporate network.
E. Enable the Alarm on the Non-HTTP Traffic signature. Then create an Event Action Override that adds the Deny Packet Inline action to events triggered by the signature if the traffic originates from your corporate network.
F. None of the above.

Answer: C

Explanation:
Cisco IOS HTTP Application Policy Overview:
HTTP uses port 80 to transport Internet web services, which are commonly used on the network and rarely challenged with regards to their legitimacy and conformance to standards. Because port 80 traffic is typically allowed through the network without being challenged, many application developers are leveraging HTTP traffic as an alternative transport protocol in which to enable their application to travel through or even bypass the firewall.
Cisco IPS Version 5.0 Sensor detects and prevents covert channel tunneling through Port 80. For example, a request message can be inspected that indicates traffic is being tunneled through Web ports using the application GoTomypc. Similarly, users can easily disguise the use of file sharing applications such as Kazaa by tunneling the traffic through Port 80. These types of activities can be accurately identified and subsequently stopped.
The AIC and Application policy enforcement feature provides deep analysis and control of a broad set of applications, including control of peer-to-peer, instant messaging (IM), and tunneled applications over Port 80. This allows the user to make policy decisions concerning various traffic types and Multipurpose Internet Mail Extensions (MIME) types to help ensure that malicious traffic is disallowed from traversing the network. By enabling the HTTP policy and alarming on non-HTTP traffic, you will be able to view and optionally block all applications other than HTTP that uses port 80.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_data_sheet0900aecd801eeea5.html

---

QUESTION 76:

The Certkiller security administrator is viewing the alert logs. What is the "hostid" entry in a Cisco IPS alert?

A. The blocking device that blocked the attack
B. The globally unique identifier for the attacker
C. The sensor that originated the alert
D. The IP address of the attacked host
E. The IP address of the attacker
F. None of the above.

Answer: C

Explanation:
The "hostid" entry seen in an IPS alert is the name or IP address of the sensor that originated the alert. Following is an example:
sensor#@ show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
originator:
hostId: CK2

appName: cidwebserver
appInstanceId: 12075
time: 2003/01/07 04:41:45 2003/01/07 04:41:45 UTC
errorMessage: name=errWarning received fatal alert: certificate_unknown
In this example, the sensor called " CK2 " generated the alert shown above.

QUESTION 77:

The Certkiller security administrator wants to view the events generated by a sensor. Which three are types of events that are generated by a Cisco sensor? (Choose three)

A. evIdsAlert: intrusion detection alerts
B. evError: application errors
C. evStatus: status changes, such as software upgrade, that are being completed
D. evLog: IP logging requests
E. evAlert: system failure warnings
F. evSNMP: notification of data retrievals by an NMS

Answer: B, C, E

Explanation:
IPS Events:
IPS applications generate IPS events to report the occurrence of some stimulus. The events are the data, such as the alerts generated by SensorApp or errors generated by any application. Events are stored in a local database known as the Event Store.
There are five types of events:
<evAlert>-Alert event messages that report when a signature is triggered by network activity.
<evStatus>-Status event messages that report the status and actions of the IPS applications.
<evError>- Error event messages that report errors that occurred while attempting response actions.
<evLogTransaction>-Log transaction messages that report the control transactions processed by each sensor application.
<evShunRqst>-Block request messages that report when ARC issues a block request.
You can view the status and error messages using the CLI, IDM, and ASDM.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008055

QUESTION 78:

A Large number of false negatives were discovered on the Certkiller LAN after a new sensor was installed. 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 a signature to fire.
D. A signature is not fired when offending traffic is present.
E. None of the above

Answer: D

Explanation:
Some legitimate network activity, such as virus scanning, can appear to be an attack on your network. When legitimate network activity is reported as an attack, that report is called a false positive. More generally, a false positive can be defined as the interpretation of an instance of legitimate and expected network activity as an attack because that activity meets criteria that were specified to identify an attack prior to the occurrence of the attack. You can decrease the number of false positives by tuning your sensor signatures.
Tuning your sensor signatures can also help you solve another problem. You can decrease the number of false negatives by tuning your sensor signatures. A false negative can be defined as an attack that was not detected.
Reference:
http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a0080104f0f.htm

---

QUESTION 79:

A Cisco IDS Sensor has been configured to detect attempts to extract the password file from the Certkiller 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 best defines this activity?

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 - an IDS fails to generates an alarm for known intrusive activity.
False positive - an IDS generates an alarm for normal user activity.
Note: True positive -A situation in which a signature is fired properly when offending traffic is detected. In other words, an attack is detected as expected.
Reference: Cisco Secure Intrusion Detection System (Cisco Press) page 55 & 58

QUESTION 80:

A Cisco IDS Sensor has been configured to detect attempts to extract the password file from the Certkiller 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 best defines this activity?

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

Answer: A
False negative - When an IDS fails to generates an alarm for known intrusive activity.
False positive - When an IDS generates an alarm for normal user activity.
True positive - When an IDS generates an alarm for known intrusive activity.
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
Reference: Cisco Secure Intrusion Detection System, Cisco Press, page 55 & 58

QUESTION 81:

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
E. Simple

Answer: C
Signature Structure
Signature implementations deal with packet headers and packet payloads. The structure of the signatures deals with the number of packets that must be examined to trigger an alarm. Two types of signature structures exist and these are as follows:
Atomic
Composite
Atomic Structure
Some attacks can be detected by matching IP header information (context based) or string information contained in a single IP packet (content based). Any signatures that can be matched with a single packet fall into the atomic category. Because atomic signatures examine individual packets, there's no need to collect or store state information.
An example of an atomic signature is the SYN-FIN signature (signature ID 3041).

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

QUESTION 82:

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
E. None of the above

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.

QUESTION 83:

Which of the following statements represents a false positive alarm situation?

A. Normal traffic or a benign action which will not cause a signature to fire
B. Offending traffic which will not cause a signature to fire
C. Normal traffic or a benign action which will result in the signature firing
D. Offending traffic which 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 CIDS Courseware, page 3-11

QUESTION 84:

The signature files need to be updated on the Certkiller sensors. When performing a signature update on a Cisco IDS Sensor, which three server types are supported for retrieving the new software? (Choose three)

A. FTP
B. SCP
C. RCP
D. FS
E. TFTP
F. HTTP
G. Telnet

Answer: A, B, F

Explanation:
To update the signature files, you can use the following transport protocols: FTP, or HTTPS, SCP, HTTP.
The following URL types are supported:
ftp:-Source URL for File Transfer Protocol network server.
The syntax for this prefix is:
ftp://username@location/relativeDirectory/filename
or
ftp://username@location//absoluteDirectory/filename.
https:-Source URL for web server.
The syntax for this prefix is https://username@location/directory/filename.
scp:-Source URL for the Secure Copy Protocol network server.
The syntax for this prefix is:
scp://username@]location/relativeDirectory/filename
or
scp://username@location/absoluteDirectory/filename.
http:-Source URL for web server.
The syntax for this prefix is:
http://username@location/directory/filename.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/module_installation_and_configuration_guides_chap

QUESTION 85:

You want to configure a new Certkiller sensor to automatically download and install updates. Which four tasks must you complete in the Cisco IDM to have the sensor automatically look for and install signature and service pack updates? (Choose four)

A.
Specify whether the sensor should look for an update file on Cisco.com or on a local server.
B. Enter you Cisco.com username and password.
C. Enter the IP address of the remote server that contains the updates.
D. Select the protocol that is used for transferring the file.
E. Enter the path to the update file.
F. Schedule the updates.

Answer: C, D, E, F

Explanation:
You can configure the sensor to look for new upgrade files in your upgrade directory automatically.
You must download the software upgrade from Cisco.com and copy it to the upgrade directory before the sensor can poll for automatic upgrades.
Auto-upgrade Command and Options:
Use the auto-upgrade-option enabled command in the service host submode to configure automatic upgrades.
Using the auto-upgrade Command
To schedule automatic upgrades, follow these steps:
Step1
Log in to the CLI using an account with administrator privileges.
Step2
Configure the sensor to automatically look for new upgrades in your upgrade directory.
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# auto-upgrade-option enabled
Step3
Specify the scheduling:
a.
For calendar scheduling, which starts upgrades at specific times on specific day:
sensor(config-hos-ena)# schedule-option calendar-schedule
sensor(config-hos-ena-cal# days-of-week sunday
sensor(config-hos-ena-cal# times-of-day 12:00:00
b.
For periodic scheduling, which starts upgrades at specific periodic intervals:
sensor(config-hos-ena)# schedule-option periodic-schedule
sensor(config-hos-ena-per)# interval 24
sensor(config-hos-ena-per)# start-time 13:00:00
Step4
Specify the IP address of the file server:
sensor(config-hos-ena-per)# exit
sensor(config-hos-ena)# ip-address 10.1.1.1
Step5
Specify the directory where the upgrade files are located on the file server:

sensor(config-hos-ena)# directory /tftpboot/update/5.0_dummy_updates
Step6
Specify the username for authentication on the file server:
sensor(config-hos-ena)# user-name tester
Step7
Specify the password of the user:
sensor(config-hos-ena)# password
Enter password[]: ******
Re-enter password: ******
Step8
Specify the file server protocol:
sensor(config-hos-ena)# file-copy-protocol ftp
Step9
Verify the settings:
sensor(config-hos-ena)# show settings
enabled
schedule-option
periodic-schedule
start-time: 13:00:00
interval: 24 hours
ip-address: 10.1.1.1
directory: /tftpboot/update/5.0_dummy_updates
user-name: tester
password: <hidden>
file-copy-protocol: ftp default: scp
sensor(config-hos-ena)#
Step10
Exit auto upgrade submode:
sensor(config-hos-ena)# exit
sensor(config-hos)# exit
Apply Changes:?[yes]:
Step11
Press Enter to apply the changes or type no to discard them.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 86:

You want a new Certkiller sensor to automatically update signature and service pack files. Which statement is true about using the Cisco IDM to configure automatic signature and service pack updates?

A. You access the Automatic Update panel from the IDM Monitoring tab.
B. You must select the Enable Auto Update check box in the Auto Update panel in order to configure automatic updates.

C. You can schedule updates to occur daily, the sensor checks for updates at 12:00 a.m. each day.
D. If you configure updates to occur daily, the sensor checks for updates at 12:00 a.m. each day.
E. You must enter you Cisco.com username and password.

Answer: B

Explanation:
Configuring Automatic Updates:
You can configure automatic service pack and signature updates, so that when service pack and signature updates are loaded on a central FTP or SCP server, they are downloaded and applied to your sensor.
To configure automatic updates, follow these steps:
Step1
Select Configuration> Auto Update.
The Auto Update page appears.
Step2
Select the Enable Auto Update check box to enable automatic updates.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/module_installation_and_configuration_guides_chap

---

QUESTION 87:

A new image needs to be applied to a Certkiller 4240 sensor. Which two statements are true about applying a system image file to a Cisco IPS 4240 sensor? (Choose two)

A. The system image file contains a sys identifier.
B. The same system-image file can be applied to any sensor platform.
C. The system image has an rpm.pkg extension.
D. You can use ROMMON to use the TFTP facility to copy the system image onto the sensor.
E. You can apply the system image by using the Cisco IDS version 5.0(1) Recovery CD-ROM

Answer: A, D

Explanation:
Installing the IPS-4240 and IPS-4255 System Image:
You can install the IPS-4240 and IPS-4255 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.
The complete installation procedure for the 4240 and the 4255 is described in the reference link below.
Incorrect Answers:

B: The images are platform specific.
C: The system image has an .img extension. The .pkg extensions are used for upgrading the system image only.
E: You can use the recovery/upgrade CD on appliances that have a CD-ROM, such as the IDS-4210, IDS-4235, and IDS-4250. This procedure is not supported on the 4240.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 88:

You want to configure a new Certkiller sensor to automatically download and install updates. Which two protocols can be used for automatic signature and service pack updates? (Choose two)

A. SCP
B. SSH
C. FTP
D. HTTP
E. HTTPS

Answer: A, C

Explanation:
Configuring Automatic Updates:
You can configure automatic service pack and signature updates, so that when service pack and signature updates are loaded on a central FTP or SCP server, they are downloaded and applied to your sensor. Although SCP, FTP, HTTP, and HTTPS can be used to manually download and install updates, only SCP and FTP are supported for automatic updates.
Note:
The sensor cannot automatically download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP or SCP server, and then configure the sensor to download them from the FTP or SCP server. After you download an update from Cisco.com, you must take steps to ensure the integrity of the downloaded file while it resides on your FTP or SCP server.
To configure automatic updates, follow these steps:
Step1:
Select Configuration> Auto Update.
The Auto Update page appears.
Step2:
Select the Enable Auto Update check box to enable automatic updates.
Step3:
In the IP Address field, enter the IP address of the server to poll for updates.
Step4:
In the Directory field, enter the path to the directory on the server where the updates are

located (1 to 128 characters).
Step5:
In the Username field, enter the username to use when logging in to the server (1 to 16 characters).
Step6:
In the Password field, enter the username password on the server (1 to 16 characters).
Step7:
In the File Copy Protocol list box, select either SCP or FTP.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/module_installation_and_configuration_guides_chap

---

QUESTION 89:

The Certkiller security administrator needs to reset the signature settings back to the default values. Which command resets all signature settings back to the factory defaults?

A. default signatures
B. reset signatures
C. default service signature-definitions
D. default service virtual-sensor
E. None of the above

Answer: C

Explanation:
To enter configuration menus for various sensor services, use the service command in global configuration mode. Use the default form of the command to reset the entire configuration for the application back to factory defaults.
Syntax:
service { authentication | analysis-engine | event-action-rules name| host | interface | logger | network-access | notification | signature-definition name | ssh-known-hosts | trusted-certificate | web-server }
default service { authentication | analysis-engine | host | interface | logger | network-access | notification | ssh-known-hosts | trusted-certificate | web-server }
Syntax Description:

authentication	Configures the order of methods that should be used to authenticate users.
analysis-engine	Configures the global analysis engine parameters. This configuration lets you create virtual sensors and assign signature definitions, event action rules, and sensing interfaces to virtual sensors.
event-action-rules	Configures the parameters for an event action rules configuration. This configuration replaces the 4.X alarm channel configuration.
host	Configures the system clock settings, upgrades, and IP access list.
interface-config	Configures the physical interfaces and inline interface pairs.
logger	Configures debug levels.
network-access	Configures parameters relating to network access controller.
notification	Configures the notification application.
signature-definition	Configures the parameters for a signature definition configuration.

Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_command_reference_chapter09186a00803a

---

QUESTION 90:

The Certkiller IPS sensors are being upgraded to 5.0. To use the upgrade command to retain the sensor configuration when upgrading to Cisco IPS software version 5.0, which version of Cisco IDS software must the sensor be running prior to upgrade?

A. 3.5
B. 4.0
C. 4.1
D. 4.2
E. 4.9

Answer: C

Explanation:
Upgrading Cisco IPS Software from 4.1 to 5.0:
The minimum required version for upgrading to 5.0 is 4.1(1). The upgrade from Cisco 4.1 to 5.0 is available as a download from Cisco.com.
After downloading the 5.0 upgrade file, refer to the accompanying Readme for the procedure for installing the 5.0 upgrade file using the upgrade command.
If you install an upgrade on your sensor and the sensor is unusable after it reboots, you must reimage your sensor. Upgrading a sensor from any Cisco IDS version before 4.1 also requires you to use the recover command or the recovery/upgrade CD.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

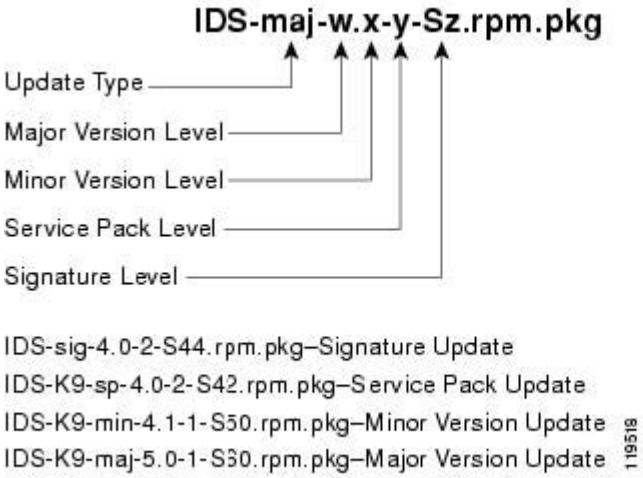
QUESTION 91:

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:



QUESTION 92:

Which command can be used to retrieve Cisco Product Evolution Program (PEP) unique device identifier (UDI) information to help you manage certified hardware versions within the Certkiller network?

A. show tech-support
B. display
C. show pep
D. show udi
E. show inventory
F. show version
G. show hardware

Answer: E

Explanation:

The Unique Device Identifier Retrieval feature provides the ability to retrieve and display the Unique Device Identifier (UDI) information from any Cisco product that has electronically stored such identity information.
The show inventory command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).
The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." This is the identifier that one would use to order an exact replacement part.
The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.
The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.
The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.
Use the show inventory command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.
Example:
Certkiller 1# show inventory
NAME: "Chassis", DESCR: "12008/GRP chassis"
PID: GSR8/40 , VID: V01, SN: 63915640
NAME: "slot 0", DESCR: "GRP"
PID: GRP-B , VID: V01, SN: CAB021300R5
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d6d.html

---

QUESTION 93:

Updates need to be installed on an existing Certkiller IPS sensor. Which statement is true about automatic signature and service pack updates?

A. The sensor can automatically download service pack and signature updates from Cisco.com.
B. The sensor can download signature and service pack updates only from an FTP or HTTP server.
C. You must download service pack and signature updates from Cisco.com to a locally accessible server before they can be automatically applied to your sensor.
D. When you configure automatic updates, the sensor checks Cisco.com for updates hourly.
E. If multiple signature or service pack updates are available when the sensor checks for an update, the sensor installs the first update it detects.

Answer: C

Explanation:
Applying Service Pack and Signature Updates:
The sensor cannot download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.
The following FTP servers are supported for service pack and signature updates:
Sambar FTP Server Version 5.0 (win32).
Web-mail Microsoft FTP Service Version 5.0 (win32).
Serv-U FTP-Server v2.5h for WinSock (win32).
Solaris 2.8.
HP-UX (HP-UX qdir-5 B.10.20 A 9000/715).
Windows 2000 (Microsoft ftp server version 5.0).
Windows NT 4.0 (Microsoft ftp server version 3.0).
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/module_installation_and_configuration_guides_chap

---

QUESTION 94:

A license for a Certkiller sensor running 5.0 is needed. For which purpose is a sensor license needed?

A. For Cisco IDM functionality
B. For signature updates
C. To enable all sensor operations
D. For service pack updates
E. For failover configurations
F. For remote management

Answer: B

Explanation:
You can find major and minor version updates, signature updates, service pack updates, system and recovery files, firmware upgrades, and readmes at Downloads on Cisco.com.
Signature updates are posted to Cisco.com approximately every week, more often if needed. Service packs are posted to Cisco.com as needed. Major and minor version updates are also posted periodically.
You must have an active IPS maintenance contract and a Cisco.com password to download updates. Beginning with 5.0, you must have a license to apply signature updates.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 95:

The Certkiller security administrator wants to view live traffic going through a specific interface on a sensor. Which command displays live traffic traversing interface FastEthernet0/0?

A. show interfaces FatEthernet0/0 | include real-time
B. show traffic FastEthernet0/0
C. packet capture FastEthernet0/0
D. packet display FastEthernet0/0
E. physical-interface FastEthernet0/0
F. traffic display FastEthernet0/0

Answer: D

Explanation:
To display or capture live traffic on an interface, use the packet command in privileged EXEC mode. Use the display option to dump live traffic or a previously captured file output directly to the screen. Use the capture option to capture the libpcap output into a local file. There is only one local file storage location; subsequent capture requests overwrite the existing file.
Example:
The following example displays the live traffic occurring on fastethernet 0/0:
CKSENSOR# packet display fastethernet0/0
Warning This command will cause significant performance degradation.
Executing command: tethereal -i fastethernet0/0
0.000000 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=56
0.000262 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470
Ack=2972370007
Win=9184 Len=0
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_command_reference_chapter09186a00803a

QUESTION 96:

How would you copy packets that have been captured from the data interfaces to a location off the Cisco IDS or IPS sensor, such as one of the Certkiller FTP servers?

A. Use the copy command with the packet-file keyword.
B. Use the copy command with the capture keyword.
C. Press Ctrl-C when the capture is complete and paste the capture to your local host.
D. Use the packet display command
E. None of the above

Answer: A

Explanation:
Use the copy packet-file destination-url command to copy the packet file from the IDS or an IPS sensor to an FTP or SCP server for saving or further analysis with another tool, such as Ethereal or tcpdump.
To copy packets files to an FTP or SCP server, follow these steps:
Step1:
Log in to the CLI using an account with administrator privileges.
Step2:
Copy the packet-file to an FTP or SCP server:
CKSENSOR# copy packet-file scp://ckuser@164.10.12.20/work/
Password: *********
packet-file 100% 1670 0.0KB/s 00:00
CKSENSOR#
Step3:
View the packet file with Ethereal or tcpdump.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 97:

The Certkiller security administrator wants to view the events that occurred on a sensor. Which statement is true about viewing sensor events?

A. You can view events from the CLI, but you cannot filter them.
B. You can use the Events panel in the Cisco IDM to filter and view events.
C. In the Cisco IDM, you can filter events based on type or time but not both.
D. The Cisco IDM does not limit the number of events that you can view at one time.
E. To view events with high- and medium-severity levels in the Cisco IDM, you must select only the High check box from the Show alert events check boxes.

Answer: B

Explanation:
The Events panel lets you filter and view event data. You can filter events based on type, time, or both. By default all alert and error events are displayed for the past one hour. You can access these events by clicking View.
When you click View, IDM defines a time range for the events if you have not already configured one. If you do not specify an end time of the range, it is defined as the moment you clicked View.
To prevent system errors when retrieving large numbers of events from the sensor, IDM limits the number of events you can view at one time (the maximum number of rows per page is 500). You can click Back and Next to view more events.
Reference:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a00804c

---

QUESTION 98:

A Certkiller 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. Choose 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. Rebooting the sensor may also be necessary.
Reference:
http://www.cisco.com/en/US/partner/products/sw/secursw/ps2113/prod_release_note09186a00801a00ac.html

---

QUESTION 99:

You are using multiple monitoring interfaces on a new Certkiller sensor appliance running software version 5.0. Which statement is true regarding this sensor?

A. You can have the simultaneous protection of multiple network subnets, which is like having multiple sensors in a single appliance.
B. You can se different sensing configurations for each monitoring interface.
C. You can enable an interface only if the interface belongs to an interface group.
D. Multiple monitoring interfaces can be assigned to Group 0 at any given time.
E. All interfaces must operate in a single mode; you cannot mix inline- and promiscuous-mode operations.
F. All of the above

Answer: A

Explanation:
The following is one of the frequently asked questions taken from Cisco IPS Sensor Software Version 5.0 FAQ documents:
Q. Can a single Cisco IPS device deliver IPS services to multiple subnets on the network?

A. Yes. Multiple monitoring interfaces on a sensor can be paired up such that each interface pair will be capable of supporting a single instance ofIPS services. For example, a sensor that supports four monitoring interfaces can simultaneously deliver IPS services to two network subnets.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_qanda_item0900aecd801e6a99.shtml

---

QUESTION 100:

You would like to examine all high-severity alert events generated by specific Certkiller sensor since 1:00 a.m. January 1, 2005. Which command should you use to accomplish this?

A. show events high 1:00 jan 1 2005
B. show events alert
C. show events high
D. show events alert high 1:00 jan 1 2005
E. None of the above

Answer: D

Explanation:
Enter the following command to display alarm events since a specified time for a specified alert level:
show events alert level hh:mm month day year
For example, show events alert high 10:00 September 22 2002 displays all high severity events since 10:00 am September 22, 2002.
The show events command displays the requested event types beginning at the requested start time. If no start time is entered, the selected events are displayed beginning at the current time. If no event types are entered, all events are displayed. Events are displayed as a live feed. You can cancel the live feed by the pressing CTRL-C.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_command_reference_chapter09186a008014

QUESTION 101:

A new log file was created on a Certkiller sensor. When does a 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.
E. All of the above.

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, Cisco Press, page 414

QUESTION 102:

While logged in to a Certkiller IPS device you want to see the statistics for one of the Fast Ethernet interfaces. Which command displays the statistics for Fast Ethernet interface 0/1?

A. show interfaces FastEthernet0/1
B. show interface int1
C. show statistics FastEthernet0/1
D. show statistics virtual-sensor
E. packet capture FastEthernet0/1
F. show statistics event-store

Answer: A

Explanation:
To display statistics for all system interfaces on the IPS, use the show interfaces command in privileged EXEC mode. This command displays show interfaces management, show interfaces fastethernet, and show interface gigabitethernet.
showinterfaces [clear]
showinterfaces {fastethernet | gigabitethernet | management } [slot/port]
Syntax Description:

clear	Clears the diagnostics.
fastethernet	Displays the statistics for the FastEthernet interface(s).
gigabitethernet	Displays the statistics for the GigabitEthernet interface(s).
management	Displays the statistics for the Management interface(s). **Note** Only platforms with external ports marked as Management support this keyword. The management interface for the remaining platforms is displayed in the **show interfaces** output based on the interface type, normally FastEthernet.
slot/port	Refer to the appropriate hardware manual for slot and port information.

Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_command_reference_chapter09186a00803a

---

QUESTION 103:

Which command provides a snapshot of the current internal state of a sensor service, enabling you to check the status of automatic upgrades and NTP?

A. show settings
B. show statistics
C. show statistics host
D. show service statistics
E. show ntp
F. show inventory

Answer: C

Explanation:
In IPS 5.0, you cannot apply an incorrect NTP configuration, such as an invalid NTP key value or ID, to the sensor. If you try to apply an incorrect configuration, you receive an error message. To verify the NTP configuration, use the show statistics host command to gather sensor statistics. The NTP statistics section provides NTP statistics including feedback on sensor synchronization with the NTP server.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_chapter09186a008045

QUESTION 104:

Given the following signature engines, which would represent the most appropriate choice when creating an 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
E. None of the above

Answer: A

Explanation:

ATOMIC.TCP Engine Parameters

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

Table A-9 ATOMIC.TCP Engine Parameters

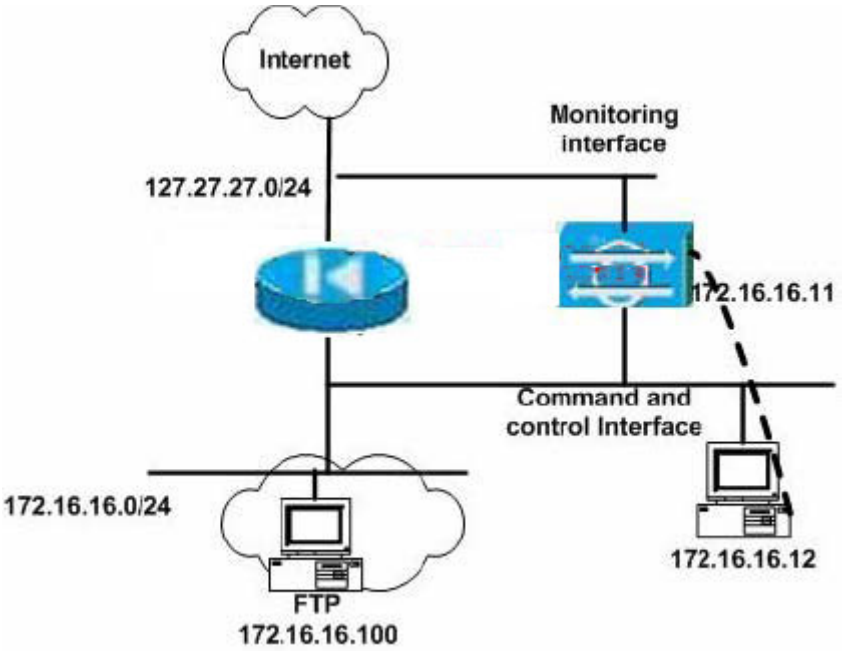
Parameter Name	Data Type	Protected	Required	Description
DstPort	NUMBER (0–65535)	No	No	A single Destination Port to match.
Mask	BITSET (FIN SYN RST PSH ACK URG ZERO)	No	Yes	The mask used in TcpFlags comparison.
PortRange	NUMBER (0–2)	No	No	The destination port: Only Low Ports (1), Only High Ports (2), 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 IDS Courseware, page 13-34

QUESTION 105:

SIMULATION
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, Certkiller, from administrative access to one that can only monitor IDS events and tune IDS signatures.
5) Return all SERVICE HTTP signatures to their default settings.
Use the information in the following table to 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 Certkiller



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

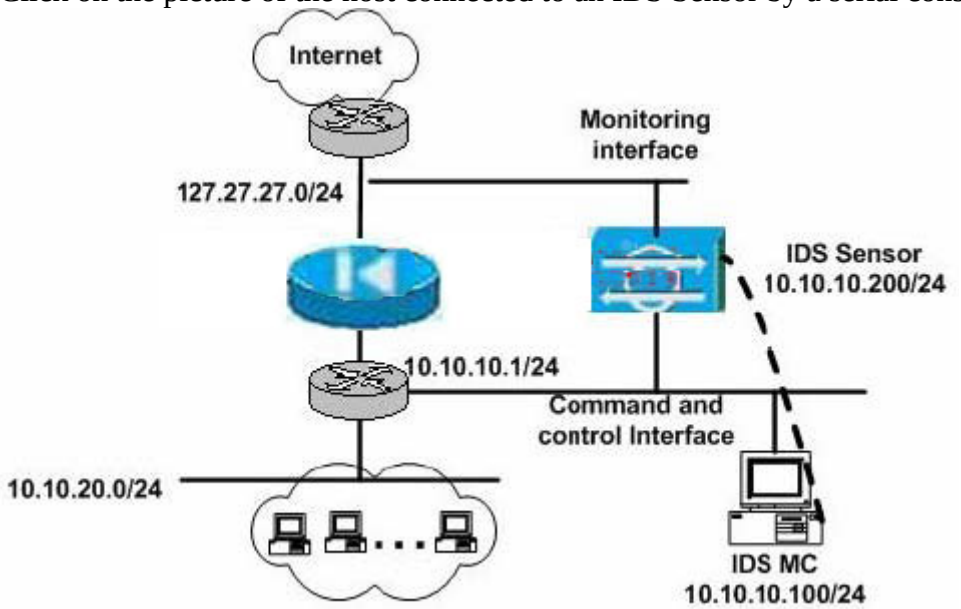
Answer:

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# configterminal
sensor(config)#no username service (service is the username for service account)
4.sensor(config)# privilege user Certkiller operator
5. sensor(config)#service virtual-sensor-configuration virtualSensor
6. sensor(config-vsc)#reset-signatures service-http all
Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_command_reference_chapter09186a008014

QUESTION 106:

SIMULATION
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:

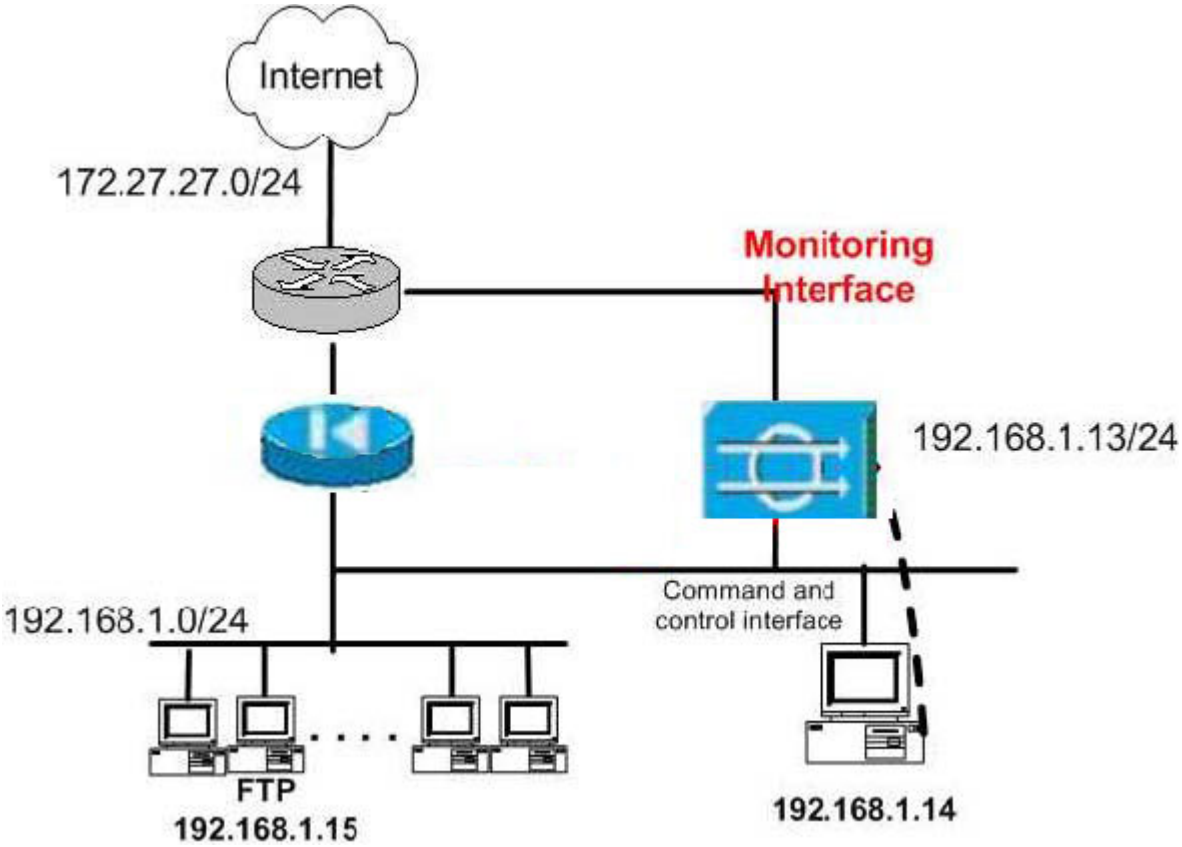
Explanation:
a. Enter configure terminal mode:
sensor# configure terminal
b. Enter host configuration mode:
sensor(config)# service host
c. Enter network parameters configuration mode:
sensor(config-Host)# networkParams

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
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 642-531 Courseware, nearly the same shown in LAB 7-4

QUESTION 107:

SIMULATION
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, Certkiller, 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 ckoperator/ Certkiller
FTP upload directory /ids4235
Backup file name backup-config
Assistant's account user ID Certkiller



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.

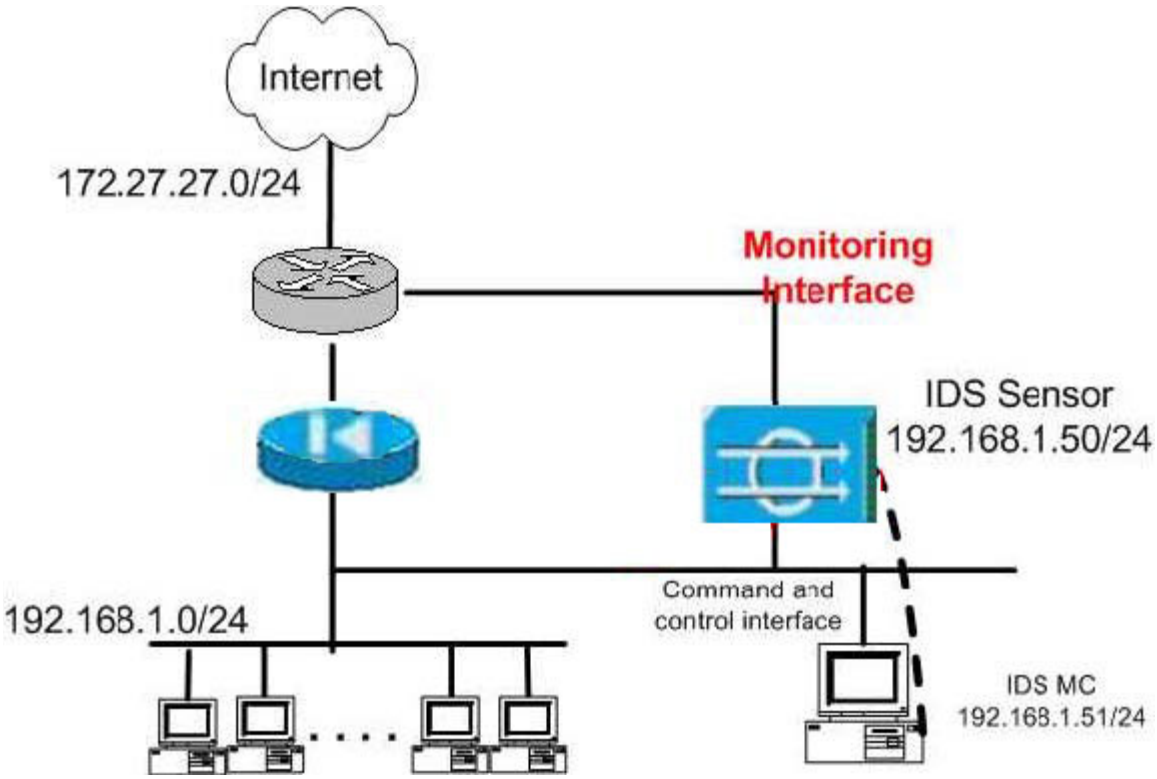
Answer:

Explanation:
login: Certkiller
password: Certkiller 1914
sensor#
1. sensor# copy current-config ftp://ckoperator@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 Certkiller viewer
5. sensor(config)#service virtual-sensor-configuration virtualSensor
sensor(config-vsc)#reset-signatures string.tcp

QUESTION 108:

SIMULATION
You work as network security administrator at the Certkiller .com office in Washington 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

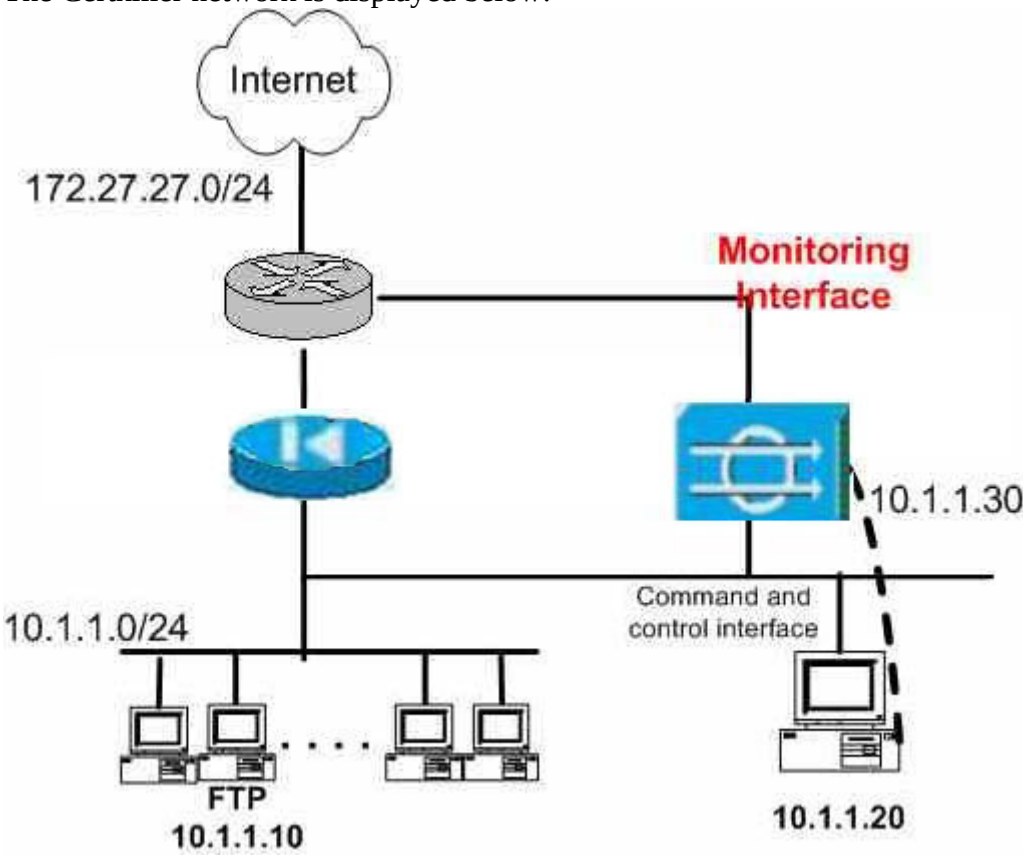
make the appropriate configuration tasks.

Answer:

Explanation:
sensor#configureterminal
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 109:

SIMULATION
The Certkiller network is displayed below:



Certkiller .com has recently hired you as a security administrator at their Toronto 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 Certkiller, 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/certkillerabc
FTP server address	10.1.1.10
FTP username/password	certkilleradmin/certkiller

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.

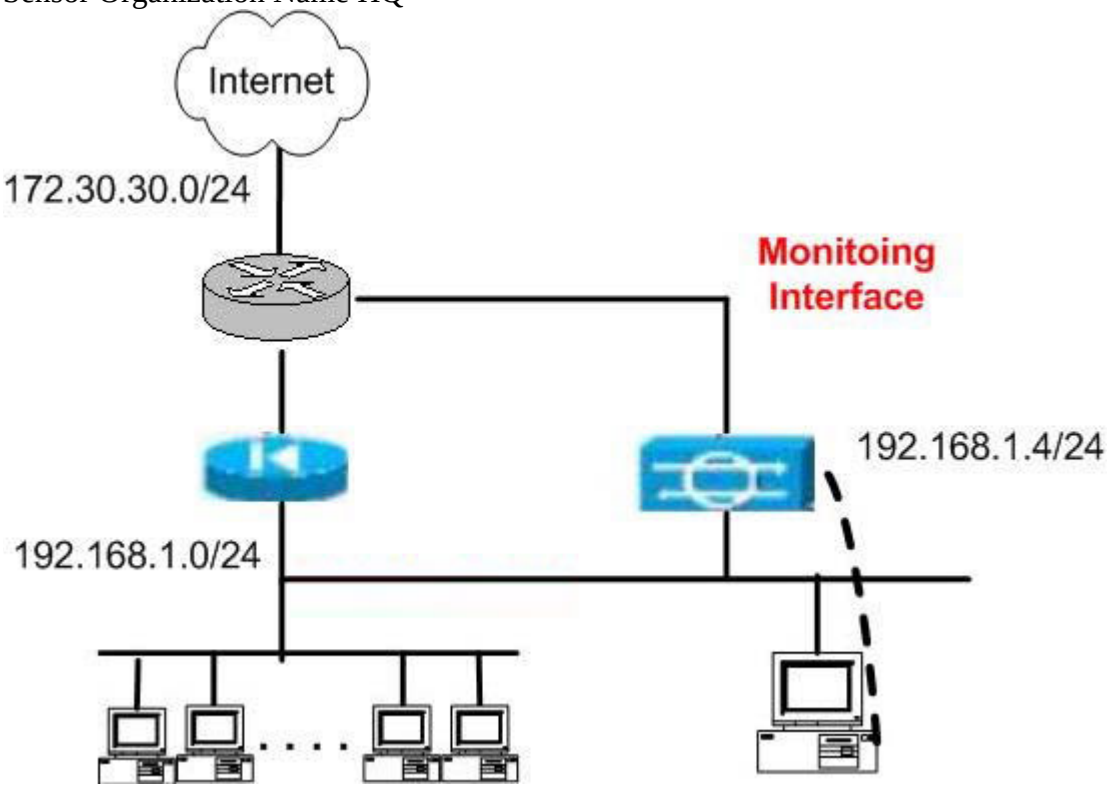
Answer:

Explanation:
login: Certkiller
password: Certkiller abc
sensor#
1.sensor# copy current-config
ftp:// Certkiller admin@10.1.1.10/ Certkiller 5287/backup-cfg
password: Certkiller
2. sensor# show user all
3. sensor# configterminal
sensor(config)#no username service (service is the username for service account)
4.sensor(config)# privilege user Certkiller operator
5. sensor(config)#service virtual-sensor-configuration virtualSensor
6. sensor(config-vsc)#reset-signatures ATOMIC.L3.TCP

QUESTION 110:

SIMULATION
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