Latest Version: 6

Question: 1

You are creating the User Account section of your organizational security policy. From the following options, select the questions
to use for the formation of this section?

A. Are users allowed to make copies of any operating system files (including, but not limited to /etc/passwd or the SAM)?
B. Who in the organization has the right to approve the request for new user accounts?
C. Are users allowed to have multiple accounts on a computer?
D. Are users allowed to share their user account with coworkers?
E. Are users required to use password-protected screensavers?
F. Are users allowed to modify files they do not own, but have write abilities?

Answer: BCD

Question: 2

You are examining a packet from an unknown host that was trying to ping one of your protected servers and notice that the packets it sent had an IPLen of 20 byes and DgmLen set to 60 bytes. What type of operating system should you believe this packet came from?

A. Linux
B. SCO
C. Windows
D. Mac OSX
E. Netware

Answer: C

Question: 3

You have found a user in your organization who has managed to gain access to a system that this user was not granted the right to
use. This user has just provided you with a working example of which of the following?

A. Intrusion
B. Misuse
C. Intrusion detection
D. Misuse detection

E. Anomaly detection

Answer: A

Question: 4

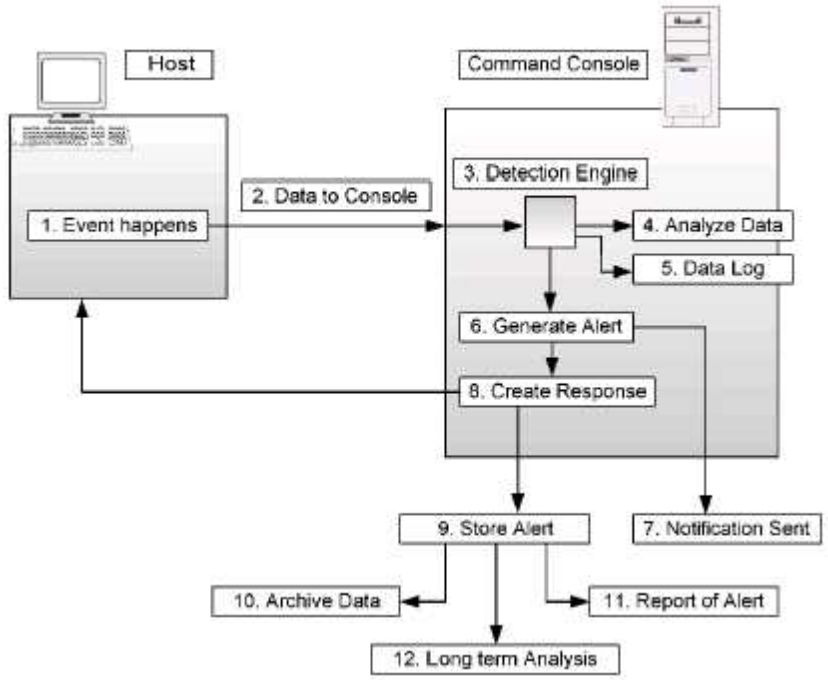
You are configuring your new IDS machine, where you have recently installed Snort. While you are working with this machine, you wish to create some basic rules to test the ability to log traffic as you desire. Which of the following Snort rules will log any tcp traffic from any host other than 172164050 using any port, to any host in the 100100/24 network using any port?

A. log udp ! 172164050/32 any -> 100100/24 any
B. log tcp ! 172164050/32 any -> 100100/24 any
C. log udp ! 172164050/32 any <> 100100/24 any
D. log tcp ! 172164050/32 any <> 100100/24 any
E. log tcp ! 172164050/32 any <- 100100/24 any

Answer: B

Question: 5

What step in the process of Intrusion Detection as shown in the exhibit would determine if given alerts were part of a bigger intrusion, or would help discover infrequent attacks?



A. 5

B. 9
C. 12
D. 10
E. 4

Answer: C

Question: 6

You are reviewing your company's IPChains Firewall and see the command (minus the quotes) " ! 101010216" as part of a rule, what does this mean?

A. Traffic destined for host 101010216 is exempt from filtering
B. Traffic originating from host 101010216 is exempt from filtering
C. Any host except 101010216
D. Only host 101010216
E. Traffic destined for 101010216 gets sent to the input filter.
F. Traffic originating from 101010216 gets sent to the input filter

Answer: C

Question: 7

You have just installed a new firewall and explained the benefits to your CEO. Next you are asked what some of the limitations of the firewall are. Which of the following are issues where a firewall cannot help
to secure the network?

A. Poor Security Policy
B. Increased ability to enforce policies
C. End node virus control
D. Increased ability to enforce policies
E. Social Engineering

Answer: ACE

Question: 8

You have been chosen to manage the new security system that is to be implemented next month in your network. You are determining the type of access control to use. What are the two types of Access Control that may be implemented in a network?

A. Regulatory Access Control
B. Mandatory Access Control
C. Discretionary Access Control
D. Centralized Access Control
E. Distributed Access Control

Answer: BC

Question: 9

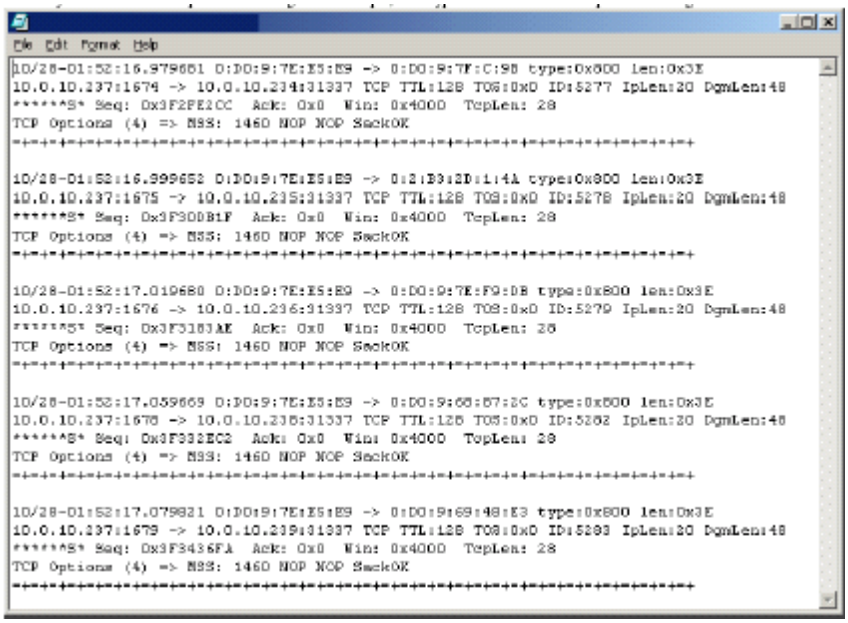
To manage the risk analysis of your organization you must first identify the method of analysis to use. Which of the following organizations defines the current standards of risk analysis methodologies?

A. NIST
B. CERT
C. F-ICRC
D. NBS
E. NSA

Answer: A

Question: 10

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



A. Trojan Horse Scan
B. Back Orifice Scan
C. NetBus Scan
D. Port Scan
E. Ping Sweep

Answer: B

Question: 11

Which of the following defines the security policy to be used for securing communications between the VPN Client and Server?

A. Encapsulating Delimiters
B. Security Authentications
C. Encapsulating Security Payload
D. Security Associations
E. Authentication Header

Answer: D

Question: 12

After a meeting between the IT department leaders and a security consultant, they decide to implement a new IDS in your network. You are later asked to explain to your team the type of IDS that is going to be implemented. Which of the following best describes the centralized design of a Host-Based IDS?

A. In a Centralized design, sensors (also called agents) are placed on each key host throughout the network analyzing the network traffic for intrusion indicators. Once an incident is identified the sensor notifies the command console.
B. In a Centralized design, the agents is on the single command console as the one that performs the analysis. There is a significant advantage to this method. The intrusion data can be monitored in realtime.
C. In a Centralized design, the IDS uses what are known as agents (also called sensors). These agents are in fact small programs running on the hosts that are programmed to detect network traffic intrusions. They communicate with the command console, or a
central computer controlling the IDS.
D. In a Centralized design, sensors are installed in key positions throughout the network, and they all report to the command console. The sensors in this case, are full detection engines that have the ability to sniff network packets, analyze for known signatures, and notify the console with an alert if an intrusion is detected.
E. In a Centralized design, the data is gathered and sent from the host to a centralized location. There is no significant performance drop on the hosts because the agents simply gather information and send

them elsewhere for analysis. However, due to the nature of the design, there is no possibility of realtime detection and response.

Answer: E

Question: 13

You are reviewing the IDS logs and during your analysis you notice a user account that had attempted to log on to your network ten times one night between 3 and 4 AM. This is quite different from the normal pattern of this user account, as this user is only in the office from 8AM to 6PM. Had your IDS detected this anomaly, which of the following types of detection best describes this event?

A. External Intrusion
B. Internal Intrusion
C. Misuse Detection
D. Behavioral Use Detection
E. Hybrid Intrusion Attempt

Answer: D

Question: 14

You have finished configuration of your ISA server and are in the section where you secure the actual server itself. Of the three options presented to you, which of the following answer best describes the Limited Services option?

A. A Firewall that is a domain controller or an infrastructure server
B. A Firewall that is a stand-alone firewall
C. A Firewall that is a database server or an application server
D. A Firewall that is a stand-alone web server
E. A Firewall that is a domain controller and a web server

Answer: A

Question: 15

You have been given the task of installing a new firewall system for your network. You are analyzing the different implementation
options. Which of the following best describes a Screened Host?

A. This is when one device is configured to run as a packet filter, granting or denying access based on the content of the headers.

B. This is when a packet is received on one interface and sent out another interface.
C. This is when a device has been configured with more than one network interface, and is running proxy
software to forward packets back and forth between the interfaces.
D. This is when the device reads only the session layer and higher headers to grant or deny access to the packet.
E. This is when the network is protected by multiple devices, one running as a proxy server and another as a packet filter. The packet
filter only accepting connections from the proxy server.

Answer: E