PASSTCERT
QUESTION & ANSWER

Higher Quality
Better Service!

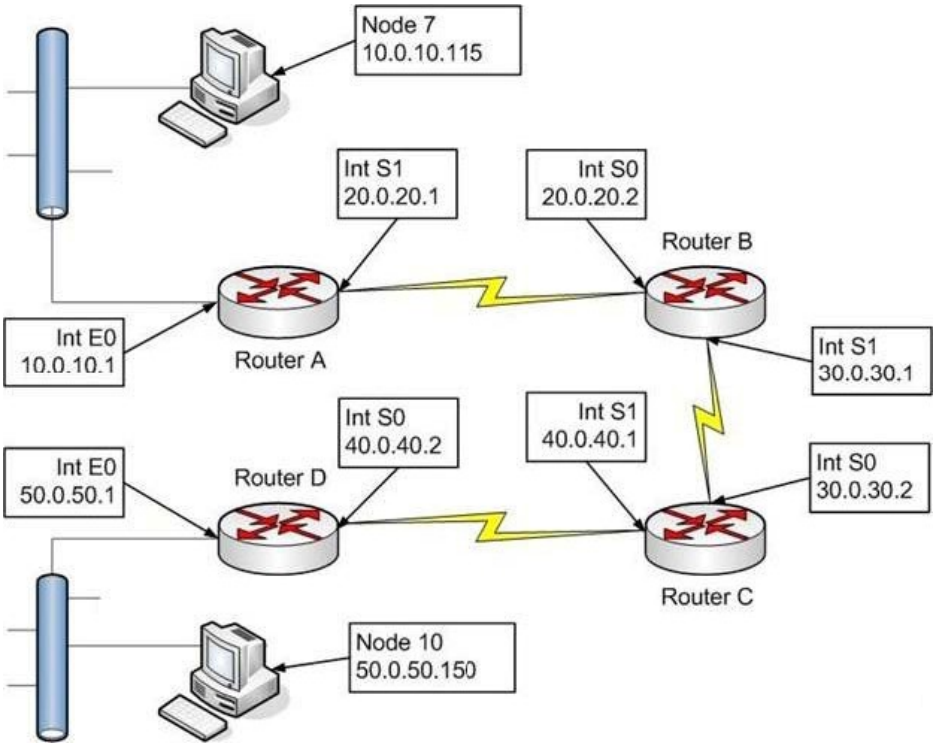
We offer free update service for one year
HTTP://WWW.PASSTCERT.COM

Exam : **SCNS_EN**

Title : SCNS SCNS Tactical Perimeter Defense

Version : Demo

1.The exhibit represents a simple routed network. Node 7 is a Windows 2000 Professional machine that establishes a TCP communication with Node 10, a Windows 2003 Server. The routers are Cisco 2500 series running IOS 11.2.
While working at Node 10, you run a packet capture. Packets received by Node 10, and sent from Node 7 will reveal which of the following combination of source IP and source Physical addresses:



A. Source IP address 10.0.10.115, Source Physical address for Node 7
B. Source IP address 50.0.50.1, Source Physical address for Node 7
C. Source IP address for Router D's Int E0, Source Physical address for Node 7
D. Source IP address 10.0.10.115, Source Physical address Router D's Int E0
E. Source IP addresses for both Nodes 7 and Router D's Int E0, Source Physical address for both Nodes 7 and Router D's Int E0.
Answer: D

2.You have implemented an IPSec policy, using only AH. You are analyzing your network traffic in Network Monitor, which of the following statements are true about your network traffic.?
A. You will not be able to view the data in the packets, as it is encrypted.
B. You will not be able to identify the upper layer protocol.
C. You will be able to view the unencrypted data in the packets.
D. You will be able to identify the encryption algorithm in use.
E. You will not be able to view the packet header.
Answer: C

3.In order to perform promiscuous mode captures using the Wireshark capture tool on a Windows Server 2003 machine, what must first be installed?
A. IPv4 stack
B. IPv6 stack

C. WinPcap
D. Nothing, it will capture by default
E. At least two network adapters
Answer: C

4.You are configuring the rules on your firewall, and need to take into consideration that some clients in the network are using automatic addressing. What is the IP address range reserved for internal use for APIPA in Microsoft networks?
A. 169.254.0.0 /4
B. 169.254.0.0 /16
C. 169.254.0.0 /8
D. 169.254.0.0 /0
E. 168.255.0.0 /16
Answer: B

5.If you capture an 802.11 frame, and the ToDS bit is set to zero and the FromDS bit is set to zero, what type of WLAN is this frame a part of?
A. Mesh
B. Broadcast
C. Infrastructure
D. Hierarchical
E. Ad Hoc
Answer: E

6.There are several options available to you for your new wireless networking technologies, and you are examining how different systems function. What transmission system uses short bursts combined together as a channel?
A. Frequency Hopping Spread Spectrum (FHSS)
B. Direct Sequence Spread Spectrum (DSSS)
C. Lamar Anthell Transmission (LAT)
D. Digital Band Hopping (DBH)
E. Digital Channel Hopping (DCH)
Answer: A

7.You have just installed a new Intrusion Detection System in your network. You are concerned that there are functions this system will not be able to perform. What is a reason an IDS cannot manage hardware failures?
A. The IDS can only manage RAID 5 failures.
B. The IDS cannot be programmed to receive SNMP alert messages.
C. The IDS cannot be programmed to receive SNMP trap messages.
D. The IDS cannot be programmed to respond to hardware failures.
E. The IDS can only inform you that an event happened.
Answer: E

8.For the new Snort rules you are building, it will be required to have Snort examine inside the content of the packet. Which keyword is used to tell Snort to ignore a defined number of bytes before looking inside the packet for a content match?
A. Depth
B. Offset
C. Nocase
D. Flow_Control
E. Classtype
Answer: B

9.You have recently taken over the security of a mid-sized network. You are reviewing the current configuration of the IPTables firewall, and notice the following rule:
ipchains -A input -p TCP -d 0.0.0.0/0 12345 -j DENY
What is the function of this rule?
A. This rule for the output chain states that all incoming packets from any host to port 12345 are to be denied.
B. This rule for the input chain states that all incoming packets from any host to port 12345 are to be denied.
C. This rule for the input chain states that any TCP traffic from any address destined for any IP address and to port 12345 is to be denied.
D. This rule for the output chain states that any TCP traffic from any address destined for any IP address and to port 12345 is to be denied.
E. This rule for the input chain states that all TCP packets inbound from any network destined to any network is to be denied for ports 1, 2, 3, 4, and 5.
Answer: C

10.At a policy meeting you have been given the task of creating the firewall policy. What are the two basic positions you can take when creating the policy?
A. To deny all traffic and permit only that which is required.
B. To permit only IP traffic and filter TCP traffic
C. To permit only TCP traffic and filter IP traffic
D. To permit all traffic and deny that which is required.
E. To include your internal IP address as blocked from incoming to prevent spoofing.
Answer: A,D

11.You are planning on implementing a token-based authentication system in your network. The network currently is spread out over four floors of your building. There are plans to add three branch offices. During your research you are analyzing the different types of systems. Which of the following are the two common systems token-based authentication uses?
A. Challenge/Response
B. Random-code
C. Time-based
D. Challenge/Handshake
E. Password-Synch

Answer: A,C

12.During your review of the logs of your Cisco router, you see the following line. What is the meaning of this line?
%SYS-5-CONFIG_I: Configured from console by vty1 (172.16.10.1)
A. A normal, but noteworthy event
B. An informative message
C. A warning condition has occurred
D. A debugging message
E. An error condition has occurred
Answer: A

13.You are working on your companys IPTables Firewall; you wish to create a rule to address traffic using ports 1024 through 2048. Which of the following would you use during the creation of your rule?
A. p:1024 P:2048
B. P:1024 p2048
C. p=1024-2048
D. 1024-2048
E. 1024:2048
Answer: E

14.You are monitoring the network traffic on your Frame-Relay Internet connection. You notice a large amount of unauthorized traffic on port 21. You examine the packets, and notice there are no files being transferred. Traffic on what other port must be examined to view any file contents?
A. 20
B. 119
C. 23
D. 80
E. 2021
Answer: A

15.You are introducing a co-worker to the security systems in place in your organization. During the discussion you begin talking about the network, and how it is implemented. You mention something in RFC 791, and are asked what that is. What does RFC 791 specify the standards for?
A. IP
B. TCP
C. UDP
D. ICMP
E. Ethernet
Answer: A

16.You have been given the task of building the new wireless networks for your office, and you need to verify that your equipment will not interfere with other wireless equipment frequencies. What wireless standard allows for up to 11 Mbps transmission rates and operates in the 2.4GHz range?

A. 802.11b
B. 802.11e
C. 802.11a
D. 802.11i
E. 802.11g
Answer: A

17.When performing wireless network traffic analysis, what is the type and subtype for an 802.11 authentication packet?
A. Type AA Subtype AAAA
B. Type 00 Subtype 1011
C. Type 0A Subtype 0A0A
D. Type 11 Subtype 0000
E. Type A0 Subtype A1A0
Answer: B

18.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 172.16.40.50 using any port, to any host in the 10.0.10.0/24 network using any port? A. log udp ! 172.16.40.50/32 any -> 10.0.10.0/24 any
B. log tcp ! 172.16.40.50/32 any -> 10.0.10.0/24 any
C. log udp ! 172.16.40.50/32 any <> 10.0.10.0/24 any
D. log tcp ! 172.16.40.50/32 any <> 10.0.10.0/24 any
E. log tcp ! 172.16.40.50/32 any <- 10.0.10.0/24 any
Answer: B

19.You are configuring a new IDS, running Snort, in your network. To better configure Snort, you are studying the configuration file. Which four of the following are the primary parts of the Snort configuration file?
A. Postprocessors
B. Variables
C. Preprocessors
D. Output Plug-ins
E. Rulesets
Answer: B,C,D,E

20.If you wish to create a new rule in ISA Server 2006 so that all file attachments with an .exe extension that come through the firewall are dropped, what would you select in the Toolbox to create this rule?
A. Content Type
B. User Group
C. Destination Set
D. Protocol Set
E. Extension Type

Answer: A

21.Your network traffic has increased substantially over the last year, and you are looking into your caching options for frequently visited websites. What are the two types of caching that ISA Server 2006 supports?
A. Reverse caching
B. Forward caching
C. Inverse caching
D. Recursive caching
E. Real-time caching
Answer: A,B

22.You are considering your options for a new firewall deployment. At which three layers of the OSI model does a stateful packet filtering firewall operate?
A. Presentation
B. Data Link
C. Network
D. Application
E. Transport
Answer: B,C,E

23.As you increase the layers of security in your organization, you must watch the network behaviorclosely.
How can a firewall have a negative impact on the performance of your network?
A. It can authorize sensitive information from the wrong host
B. It can block needed traffic
C. It can decrypt secure communications that were supposed to get past the firewall encrypted
D. It can restrict bandwidth based on QoS
E. It can filter packets that contain virus signatures
Answer: B

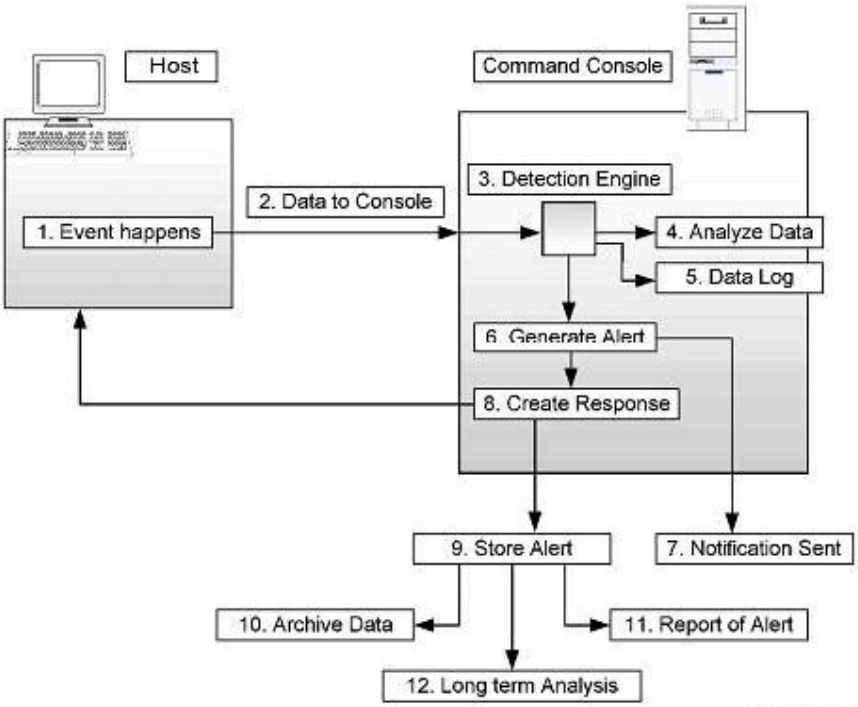
24.You are configuring a Cisco Router, and are creating Access Control Lists as part of the security of the network. When creating Wildcard Masks, which of the following rules apply?
A. If the wildcard mask bit is a 1, then do not check the corresponding bit of the IP address for a match.
B. If the wildcard mask bit is a 0, then do not check the corresponding bit of the IP address for a match.
C. If the wildcard mask bit is a 1, then do check the corresponding bit of the IP address for a match.
D. If the wildcard mask bit is a 0, then do check the corresponding bit of the IP address for a match.
E. To create a Wildcard Mask, always take the inverse of the Subnet Mask.
Answer: A,D

25.The CEO of your company has just issued a statement that the network must be more secure right away. You have discussed several options with the Chief Security Officer and the Chief Technology Officer. The results of your discussion are to implement IPSec. What are the two prime functions of IPSec that you can let the CEO know will be addressed with the implementation?

A. Ensure data corruptibility
B. Ensure data integrity
C. Ensure data availability
D. Ensure data security
E. Ensure data deliverability
Answer: B,D

26.As per the specifications of RFC 1191: Path MTU Discovery, MTUs have been defined so that transmitted datagram will not unnecessarily become fragmented when traveling across different types of physical media. You are going to run several packet captures to be sure there are no out of spec packets on your network. According to these specifications what are the absolute minimum and maximum MTUs?
A. 1492 Bytes and 1500 Bytes respectively
B. 68 Bytes and 65535 Bytes respectively
C. 512 Bytes and 1500 Bytes respectively
D. 512 bits and 1500 bits respectively
E. 512 bits per second and 1500 bits per second respectively
Answer: B

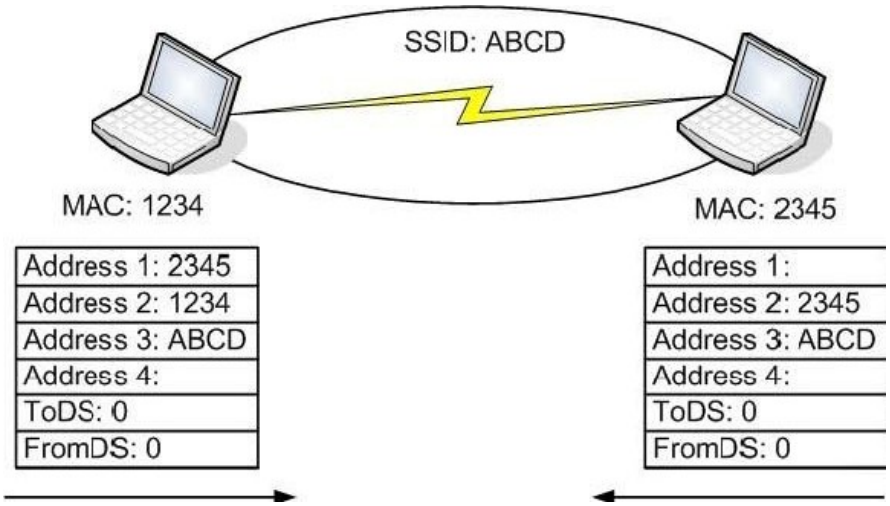
27.What step in the process of Intrusion Detection as shown in the exhibit would determine if given alerts were part of a bigger intrusion, or would help discover infrequent attacks?



A. 5
B. 9
C. 12
D. 10

E. 4
Answer: C

28.In the image, there are two nodes communicating directly, without an access point. In the packet on the right side of the image, the Address 1 field is blank. If this packet is going to the other computer, what is the value that must be filled in this blank address field?



A. 2345
B. 1234
C. ABCD
D. <null>
E. ABCD-1234
Answer: B

29.During a training presentation, that you are delivering, you are asked how wireless networks function, compared to the OSI Model. What two layers of the OSI Model are addressed by the 802.11 standards? A. Physical
B. Data Link
C. Network
D. Transport
E. Session
Answer: A,B

30.You have configured Snort to run on your SuSe Linux machine, and you are currently making the configuration changes to your MySQL database. What is the result of running the following command at the mysql prompt?
source /usr/share/doc/packages/snort/schemas/create_mysql;
A. This command tells MySQL to connect to the /usr directory when source files are required for Snort rules.
B. This command tells MySQL that the source files for Snort are located in the /usr directory.
C. This command tells MySQL where to place the Snort capture files in the database.
D. This command tells MySQL to populate the database using the fields provided by Snort.
E. This command tells MySQL where to find the source data for connecting to Snort.

Answer: D