Exam : **SC0-411**

Title : Hardening the Infrastructure

Version : DEMO

1.If an attacker uses a program that sends thousands of email messages to every user of the network, some of them with over 50MB attachments. What are the possible consequences to the email server in the network?

A. Server hard disk can fill to capacity
B. Client hard disks can fill to capacity
C. Server can completely crash
D. Network bandwidth can be used up
E. Clients cannot receive new email messages
Answer: AC

2.You have recently installed an Apache Web server on a Red Hat Linux machine. When you return from lunch, you find that a colleague has made a few configuration changes. One thing you notice is a .htpasswd file. What is the function of this file?

A. It is a copy of the /etc/passwd file for Web access
B. It is a copy of the etc/shadow file for Web access
C. It is a listing of all anonymous users to the Web server
D. It is a listing of http users and passwords for authentication
E. It is a database file that can be pulled remotely via a web interface to identify currently logged in users.
Answer: D

3.In order to perform promiscuous mode captures using the Ethereal capture tool on a Windows 2000 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.In a TCP Header, what is the function of the first sixteen bits?

A. To define the type
B. To define the IP Version
C. To define the destination port number
D. To define the upper layer protocol
E. To define the source port number
Answer: E

5.You are configuring the IP addressing for your network. One of the subnets has

been defined with addresses already. You run ifconfig on a host and determine that it has an address of 172.18.32.54 with a mask of 255.255.254.0. What is the network ID to which this host belongs?

A. 172.18.0.0
B. 0.0.32.0
C. 172.0.0.0
D. 172.18.32.32
E. 172.18.32.0
Answer: E

6.You are configuring the Access Lists for your new Cisco Router. The following are the commands that are entered into the router for the list configuration.
Router(config)#access-list 145 deny tcp any 10.10.0.0 0.0.255.255 eq 80
Router(config)#access-list 145 deny tcp any 10.10.0.0 0.0.255.255 eq 119
Router(config)#access-list 145 permit ip any any
Router(config)#interface Serial 0
Router(config-if)#ip access-group 145 in
Router(config-if)#interface Ethernet 0
Router(config-if)# ip access-group 145 in
Router(config-if)#interface Ethernet 1
Router(config-if)# ip access-group 145 in
Router(config-if)#interface Ethernet 2
Router(config-if)# ip access-group 145 in
Based on this configuration, and using the exhibit, select the answers that identify what the list will accomplish.

A. Permit network 10.10.10.0 to access NNTP on the Internet
B. Permit network 10.10.10.0 to access NNTP on network 10.10.11.0
C. Permit network 10.10.10.0 to access NNTP on network 10.10.12.0
D. Deny network 10.10.10.0 to access Internet WWW sites
E. Permit network 10.10.10.0 to access Internet WWW sites
Answer: AE

7.You are configuring the dial up options in your Windows 2000 network. While you do so, you are studying the configuration options available to you. You notice the term RADIUS used often during your research. What does RADIUS provide?

A. RADIUS is used to define the implementation method of Kerberos in a network.
B. RADIUS is used to define the implementation method of PKI in a network.
C. RADIUS is used to define the implementation method of Biometrics in a network.
D. RADIUS is a standard that provides authorization, authentication, identification, and accounting services.
E. RADIUS is a standard that defines the methods used to secure the connections

between a dialup client and a dialup server.
Answer: D

8.You are in the process of securing several new machines on your Windows 2000 network. To help with the process Microsoft has defined a set of Security Templates to use in various situations. Which of the following best describes the Basic Security Template?

A. This template is provided as a way to reverse the implementation of different Windows 2000 security settings, except for user rights.
B. This template is provided so that Local Users have ideal security settings, while Power Users have settings that are compatible with NT 4 Users.
C. This template is provided to implement suggested security settings for all security areas, except for the following: files, folders, and Registry keys.
D. This template is provided to create the maximum level of security for network traffic between Windows 2000 clients.
E. This template is provided to allow for an administrator to run legacy applications on a DC.
Answer: A

9.The exhibit shows a router with three interfaces E0, E1 and S0. Interfaces E0 and E1 are connected to internal networks 192.168.10.0 and 192.168.20.0 respectively and interface S0 is connected to the Internet.
The objective is to allow two hosts, 192.168.20.16 and 192.168.10.7 access to the Internet while all other hosts are to be denied Internet access. All hosts on network 192.168.10.0 and 192.168.20.0 must be allowed to access resources on both internal networks. From the following, select all the access list statements that are required to make this possible.

A. access-list 53 permit 192.168.20.16 0.0.0.0
B. access-list 80 permit 192.168.20.16 0.0.0.0
C. access-list 53 deny 0.0.0.0 255.255.255.255
D. access-list 80 permit 192.168.10.7 0.0.0.0
E. int S0, ip access-group 53 out
F. int S0, ip access-group 80 out
Answer: BDF

10.Which of the following fields are found in a user account's line in the /etc/passwd file?

A. The User Identifier assigned to the user account
B. The home directory used by the user account
C. The number of days since the user account password was changed
D. The full name for the user account

E. The number of days until the user account's password must change
Answer: ABD

11.When a new user account is created in Linux, what values are assigned?
A. Shell_GID
B. SetGID
C. SetUID
D. UID
E. GID
Answer: DE

12.You are creating the contingency plan, and are trying to take into consideration as many of the disasters as you can think of. Which of the following are examples of technological disasters?

A. Hurricane
B. Terrorism
C. Tornado
D. Virus
E. Trojan Horse
Answer: BDE

13.One way to find out more about a company's infrastructure layout is to send email to a non-existent user of the target organization. When this email bounces back as undeliverable, you can read the message source. Which of the following pieces of information can be derived from the returned message source?

A. Target company's email server's hostname.
B. Target company's email server's public IP address.
C. Target company's internal IP addressing scheme.
D. Target company's email server's application name and version, if provided.
E. Target company's employees' email addresses.
Answer: ABD

14.You work for a mid sized ISP on the West Coast of the United Kingdom. Recently you have noticed that there are an increasing number of attacks on the Internet routers used in the company. The routers are physically secured well, so you can be somewhat confident the attacks are all remote. Which of the following are legitimate threats the routers are facing, under this situation?

A. Damaged Cables
B. False Data Injection
C. Social Engineering
D. Unauthorized Remote Access

E. Denial of Service
Answer: BDE

15.In order to add to your layered defense, you wish to implement some security configurations on your router. If you wish to have the router work on blocking TCP SYN attacks, what do you add to the end of an ACL statement?

A. The IP addresses for allowed networks
B. The port range of allowed applications
C. The word Established
D. The word Log
E. The string: no service udp-small-servers
Answer: C

16.If you are looking for plain-text ASCII characters in the payload of a packet you capture using Network Monitor, which Pane will provide you this information?

A. Summary Pane
B. Packet Pane
C. Collection Pane
D. Hex Pane
E. Detail Pane
Answer: D

17.In order to properly manage the network traffic in your organization, you need a complete understanding of protocols and networking models. In regards to the 7-layer OSI model, what is the function of the Transport Layer?

A. The Transport layer allows two applications on different computers to establish, use, and end a session. This layer establishes dialog control between the two computers in a session, regulating which side transmits, plus when and how long it transmits.
B. The Transport layer manages logical addresses. It also determines the route from the source to the destination computer and manages traffic problems, such as routing, and controlling the congestion of data packets.
C. The Transport layer packages raw bits from the Physical (Layer 1) layer into frames (structured packets for data). Physical addressing (as opposed to network or logical addressing) defines how devices are addressed at the data link layer. This layer is responsible for transferring frames from one computer to another, without errors. After sending a frame, it waits for an acknowledgment from the receiving computer.
D. The Transport layer transmits bits from one computer to another and regulates the transmission of a stream of bits over a physical medium. For example, this layer defines how the cable is attached to the network adapter and what transmission technique is used to send data over the cable.
E. The Transport layer handles error recognition and recovery. It also repackages long

messages, when necessary, into small packets for transmission and, at the receiving end, rebuilds packets into the original message. The corresponding Transport layer at the receiving end also sends receipt acknowledgments.
Answer: E

18.Which of the following is implemented in an IPv6 environment, which helps to increase security?

A. EFS
B. IPsec
C. Caching
D. S/MIME
E. Destination and Source Address Encryption
Answer: B

19.You wish to add a new group to your Linux system. The group is called SCNP_Admins, and is to be given a Group Identifier of 1024. What is the correct command to add this new group?

A. addgroup SCNP_Admins -id 1024
B. groupadd -g 1024 SCNP_Admins
C. addgroup SCNP_Admins id/1024
D. groupadd id/1024 g/SCNP_Admins
E. groupadd g/1024 SCNP_Admins
Answer: B

20.You have recently hired an assistant to help you with managing the security of your network. You are currently running an all Windows environment, and are describing NTFS permission issues. You are using some demonstration files to help with your discussion. You have two NTFS partitions, C:\ and D:\ There is a test file, C:\DIR1\test.txt that is currently set so that only Administrators have Full Control. If you move this file to the C:\DIR2 folder, what will the permissions be for this file?

A. The file will have the same permissions as D:\DIR2
B. The file permissions will remain the same
C. The file permissions will be lost
D. The file permissions will convert to Everyone - Full Control
E. The permissions will be set to whatever the CREATOR OWNER permissions are for the D:\ partition
Answer: B

21.If you wish to change the permissions of a parent directory in your Linux system, and want the permissions to be changed on the files and subdirectories in the parent directory to be the same, what switch must you use?

A. -G
B. -R
C. -P
D. -S
E. -F
Answer: B

22.You are reviewing the Xinetd configuration file for the ftp service. If the following line found in this file, what is the line's function?
redirect = 192.168.10.1 3456

A. That only 192.168.10.1 can make ftp requests
B. That only hosts in the 192.168.10.0/24 network can make ftp requests
C. That only 3456 connections are allowed to the ftp service on 192.168.10.1
D. That the overall Xinetd configuration has redirect lines in it
E. That the ftp service is redirected to IP 192.168.10.1 on port 3456
Answer: E

23.You are creating the contingency plan for the network in hospital where you just started working. The network has about 300 PCs, about 50 Servers, and is interconnected into some of the critical patient systems for monitoring purposes. What is the appropriate level of backup power for this type of network?

A. Building Generator
B. Personal UPS
C. Alternative Fuel-Cell Technology
D. Server Rack UPS
E. Electrical Company
Answer: A

24.In the last few days, users have reported to you that they have each received two emails from an unknown source with file attachments. Fortunately the users have listened to your training and no one has run the attached program. You study the attachment on an isolated computer and find that it is a program that is designed to execute a payload when the system clock registers 10:10 PM on February 29. Which of the following best identifies the type of program is the attachment?

A. Mail Bomb
B. Logic Bomb
C. Polymorphic Virus
D. Stealth Virus
E. Polymorphic Trojan
Answer: B

25.What is the function of the HFNetChk tool from Microsoft?

A. To check for the current Hotfixes that are available from Microsoft
B. It is an upgrade to the Windows Update tool for checking on all updates
C. It is the tool that must be run prior to installing IIS 5.0
D. It is the tool that checks the network configuration of all web servers
E. To record what Hotfixes and service packs are running on the Windows machine
Answer: E

26.When you took over the security responsibilities at your office, you noticed there were no warning banners on any of the equipment. You have decided to create a warning login banner on your Cisco router. Which of the following shows the correct syntax for the banner creation?

A. banner login C Restricted access. Only authorized users allowed to access this device.
B. login banner C Restricted access. Only authorized users allowed to access this device.
C. banner login Restricted access. Only authorized users allowed to access this device.
D. login banner Restricted access. Only authorized users allowed to access this device.
E. banner logging C Restricted access. Only authorized users allowed to access this device. C
Answer: A

27.You are configuring a wildcard mask for the subnet 10.12.24.0 / 255.255.248.0. Which of the following is the wildcard mask to use for this subnet?

A. 0.255.255.255
B. 10.12.24.255
C. 0.0.248.0
D. 255.255.248.0
E. 0.0.7.255
Answer: E

28.In your network, you manage a mixed environment of Windows, Linux, and UNIX computers. The clients run Windows 2000 Professional and Windows NT 4.0 Workstation, while the Servers are UNIX and Linux based with custom applications. During routine administration you successfully ping several nodes in the network. During this you are running a packet capture for further analysis. When examining one of the frames you notice that the Ethernet address for the source is 1ED0.097E.E5E9 and that for the destination is 1ED0.096F.5B13. From this information you gather that:

A. They are in different networks
B. The destination address is in the 1ED0 subnet

C. The network cards are by the same manufacturer
D. The destination address is in the 1ED0.09AA subnet
E. The source and destination share the same MAC subnet
Answer: C

29.As you become more involved in the security and networking of your organization, you wish to learn the exact details of the protocols in use. It is suggested to you, by a friend, that you check the RFC for each protocol. What is an RFC?

A. An RFC is a program that has a searchable index to troubleshoot network problems.
B. An RFC is a document that discusses issues surrounding the Internet, networking technologies, and/or networking protocols.
C. An RFC is a hidden resource, which can be called up via the Windows Help file to identify details about networking protocols.
D. An RFC is a single document that details all the communications protocols and technologies used on the Internet.
E. An RFC is a single document that details all the communications protocols and technologies used on an Intranet.
Answer: B

30.In Windows 2000, there are four methods of implementing IPSec. They are:
1- Require Security
2 - Request Security
3 - Respond Only
4 - No IPSec Policy
Your network hosts many servers, and different security policies are in place in different locations in the network. The Clients and Servers in your network are configured as follows:
-You have servers numbered 1-9, which have a policy stating they require no network traffic security.
-You have servers numbered 10-19, which have a policy stating they are not required to be secure, but will encrypt network traffic if the client is able to receive it.
-You have servers numbered 20-29, which have a policy stating they are required to be secure and all network traffic they deliver must be secured.
-You have clients numbered 60-79 that are required to access secure servers 20-29.
-You have clients numbered 80-99 that are not required to access secure servers 20-29, but are required to access servers 1-9 and 10-19.
Based on the Client and Server configuration provided above, which of the following computers will implement IPSec method 2?

A. Computers numbered 1-9
B. Computers numbered 10-19
C. Computers numbered 20-29

D. Computers numbered 60-79
E. Computers numbered 80-99
Answer: B