IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **GSNA**

Title : GIAC Systems and Network Auditor

Version : Demo

1.Sarah works as a Web Developer for XYZ CORP. She is creating a Web site for her company. Sarah wants greater control over the appearance and presentation of Web pages. She wants the ability to precisely specify the display attributes and the appearance of elements on the Web pages. How will she accomplish this?
A. Use the Database Design wizard.
B. Make two templates, one for the index page and the other for all other pages.
C. Use Cascading Style Sheet (CSS).
D. Make a template and use it to create each Web page.
Answer: C

2.You work as a Network Administrator for XYZ CORP. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. You have installed a Windows Server 2008 computer. You have configured auditing on this server. The client computers of the company use the Windows XP Professional operating system. You want to audit each event that is related to a user managing an account in the user database on the computer where the auditing is configured. To accomplish the task, you have enabled the Audit account management option on the server. Which of the following events can be audited by enabling this audit option.?
A. Access to an Active Directory object
B. Change of password for a user account
C. Addition of a user account to a group
D. Creation of a user account
Answer: B,C,D

3.John works as a contract Ethical Hacker. He has recently got a project to do security checking for www.we-are-secure.com. He wants to find out the operating system of the we-are-secure server in the information gathering step. Which of the following commands will he use to accomplish the task? (Choose two)
A. nc 208.100.2.25 23
B. nmap -v -O www.we-are-secure.com
C. nc -v -n 208.100.2.25 80
D. nmap -v -O 208.100.2.25
Answer: B,D

4.You check performance logs and note that there has been a recent dramatic increase in the amount of broadcast traffic. What is this most likely to be an indicator of?
A. Misconfigured router
B. DoS attack
C. Syn flood
D. Virus
Answer: B

5.You run the wc -c file1.txt command. If this command displays any error message, you want to store the error message in the error.txt file. Which of the following commands will you use to accomplish the task?

A. wc -c file1.txt >>error.txt
B. wc -c file1.txt 1>error.txt
C. wc -c file1.txt 2>error.txt
D. wc -c file1.txt >error.txt
Answer: C

6.John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He wants to forward all the kernel messages to the remote host having IP address 192.168.0.1. Which of the following changes will he perform in the syslog.conf file to accomplish the task?
A. kern.* @192.168.0.1
B. !*.* @192.168.0.1
C. !kern.* @192.168.0.1
D. *.* @192.168.0.1
Answer: A

7.John works as a Security Professional. He is assigned a project to test the security of www.we-are-secure.com. John wants to get the information of all network connections and listening ports in the numerical form. Which of the following commands will he use?
A. netstat -e
B. netstat –r
C. netstat -s
D. netstat –an
Answer: D

8.John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to use Kismet as a wireless sniffer to sniff the Weare-secure network. Which of the following IEEE-based traffic can be sniffed with Kismet?
A. 802.11g
B. 802.11n
C. 802.11b
D. 802.11a
Answer: A,B,C,D

9.Which of the following statements about the traceroute utility are true?
A. It uses ICMP echo packets to display the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host.
B. It records the time taken for a round trip for each packet at each router.
C. It is an online tool that performs polymorphic shell code attacks.
D. It generates a buffer overflow exploit by transforming an attack shell code so that the new attack shell code cannot be recognized by any Intrusion Detection Systems.
Answer: A,B

10.George works as an office assistant in Soft Well Inc. The company uses the Windows Vista operating

system. He wants to disable a program running on a computer. Which of the following Windows Defender tools will he use to accomplish the task?
A. Allowed items
B. Quarantined items
C. Options
D. Software Explorer
Answer: D

11.You work as a Network Administrator for XYZ CORP. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks: The wireless network communication should be secured. The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps: Configure 802.1x and WEP for the wireless connections. Configure the PEAP-MS-CHAP v2 protocol for authentication. What will happen after you have taken these steps?
A. Both tasks will be accomplished.
B. The laptop users will be able to use smart cards for getting authenticated.
C. The wireless network communication will be secured.
D. None of the tasks will be accomplished.
Answer: C

12.You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to print the super block and block the group information for the filesystem present on a system. Which of the following Unix commands can you use to accomplish the task?
A. e2fsck
B. dump
C. dumpe2fs
D. e2label
Answer: C

13.Which of the following is a wireless auditing tool that is used to pinpoint the actual physical location of wireless devices in the network?
A. KisMAC
B. Ekahau
C. Kismet
D. AirSnort
Answer: B

14.Which of the following tools works both as an encryption-cracking tool and as a keylogger?
A. Magic Lantern
B. KeyGhost Keylogger
C. Alchemy Remote Executor

D. SocketShield
Answer: A

15.You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to set some terminal characteristics and environment variables. Which of the following Unix configuration files can you use to accomplish the task?
A. /etc/sysconfig/routed
B. /proc/net
C. /etc/sysconfig/network-scripts/ifcfg-interface
D. /etc/sysconfig/init
Answer: D

16.You work as a Network Auditor for XYZ CORP. The company has a Windows-based network. While auditing the company's network, you are facing problems in searching the faults and other entities that belong to it. Which of the following risks may occur due to the existence of these problems?
A. Residual risk
B. Inherent risk
C. Secondary risk
D. Detection risk
Answer: D

17.Which of the following statements are true about locating rogue access points using WLAN discovery software such as NetStumbler, Kismet, or MacStumbler if you are using a Laptop integrated with Wi-Fi compliant MiniPCI card? (Choose two)
A. These tools can determine the rogue access point even when it is attached to a wired network.
B. These tools can determine the authorization status of an access point.
C. These tools cannot detect rogue access points if the victim is using data encryption.
D. These tools detect rogue access points if the victim is using IEEE 802.11 frequency bands.
Answer: B,D

18.A Web developer with your company wants to have wireless access for contractors that come in to work on various projects. The process of getting this approved takes time. So rather than wait, he has put his own wireless router attached to one of the network ports in his department. What security risk does this present?
A. None, adding a wireless access point is a common task and not a security risk.
B. It is likely to increase network traffic and slow down network performance.
C. This circumvents network intrusion detection.
D. An unauthorized WAP is one way for hackers to get into a network.
Answer: D

19.Which of the following allows the use of multiple virtual servers using different DNS names resolved by the same IP address?
A. HTTP 1.1
B. JAVA

C. HTML
D. VPN
Answer: A

20.Which of the following is Microsoft's implementation of the file and application server for the Internet and private intranets?
A. Internet Server Service (ISS)
B. Internet Server (IS)
C. WWW Server (WWWS)
D. Internet Information Server (IIS)
Answer: D