Vendor: GIAC

Exam Code: GSNA

Exam Name: GIAC Systems and Network Auditor

Version: DEMO

QUESTION NO: 1

Sarah works as a Web Developer for X 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 6

John works as a Network Administrator for P 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

QUESTION NO: 7

John works as a Security Professional. He is assigned a project to test the security of www.weare-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

QUESTION NO: 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 We-are-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

QUESTION NO: 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

QUESTION NO: 10

George works as an office assistant in S 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