Vendor:EC-COUNCIL

Exam Code:ECSS

Exam Name:EC-Council Certified Security Specialist Practice Test

Version: Demo

QUESTION 1

You work as a system administrator for BlueSkwer.com. You have just finished installing and configuring a new laptop for the CEO. The laptop has Windows 7 operating system. You have just deployed a secure wireless network in the company. Alex, the CEO, wants you to connect his laptop to the wireless network. What will you open to start the process of connecting to a wireless network?

A. Network and Sharing Center

B. Appearance and Personalization

C. System and Security

D. Devices and Printers

Correct Answer: A

QUESTION 2

Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the following techniques is Sam using?

Each correct answer represents a part of the solution. Choose all that apply.

A. Text Semagrams

B. Perceptual masking

C. Linguistic steganography

D. Technical steganography

Correct Answer: AC

QUESTION 3

Who among the following are security experts who specialize in penetration testing and other testing methodologies to ensure that their company\\'s information systems are secure?

Each correct answer represents a complete solution. Choose all that apply.

A. Black hat hackers

B. Script Kiddies

C. White hat hackers

D. Ethical hackers

Correct Answer: CD

QUESTION 4

Which of the following is the most important resource associated with any digital forensic investigations process?

A. Human talent

B. Forensic software

C. Human experience

D. Forensic tools

Correct Answer: A

QUESTION 5

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest domain-based network. The company has recently provided fifty laptops to its sales team members. You are required to configure an 802.11 wireless network for the laptops. The sales team members must be able to use their data placed at a server in a cabled network. The planned network should be able to handle the threat of unauthorized access and data interception by an unauthorized user. You are also required to prevent the sales team members from communicating directly to one another. Which of the following actions will you perform to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Implement the open system authentication for the wireless network.

B. Implement the IEEE 802.1X authentication for the wireless network.

C. Configure the wireless network to use WEP encryption for the data transmitted over a wireless network.

D. Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only.

E. Using group policies, configure the network to allow the wireless computers to connect to the ad hoc networks only.

Correct Answer: BCD

QUESTION 6

Which of the following needs to be documented to preserve evidences for presentation in court?

A. Incident response policy

B. Account lockout policy

C. Separation of duties

D. Chain of custody

Correct Answer: D

QUESTION 7

Which of the following terms is used for the process of securing a system or a device on a network infrastructure?

A. Hardening

B. Authentication

C. Cryptography

D. Sanitization

Correct Answer: A

QUESTION 8

Which of the following protocols of the TCP/IP suite is used in the application layer of the OSI model?

A. DCAP

B. OSPF

C. ARP

D. Telnet

Correct Answer: D

QUESTION 9

Peter works as a professional Computer Hacking Forensic Investigator for eLaw-Suit law firm. He is working on a case of a cyber crime. Peter knows that the good investigative report should not only communicate the relevant facts, but also present expert opinion. This report should not include the cases in which the expert acted as a lay witness. Which of the following type of witnesses is a lay witness?

A. One who observes an event.

B. One with special knowledge of the subject about which he or she is testifying.

C. One who can give a firsthand account of something seen, heard, or experienced.

D. One who is not qualified as an expert witness.

Correct Answer: D

QUESTION 10

Which of the following agencies is responsible for handling computer crimes in the United States?

A. The FBI only

B. The Federal Bureau of Investigation (FBI) and the Secret Service

C. The Central Intelligence Agency (CIA)

D. The National Security Agency (NSA)

Correct Answer: B

QUESTION 11

Which of the following attacks is used by attackers to access a company\\'s internal network through its remote access system?

A. Trojan horse

B. Land attack

C. War dialer

D. Denial-of-Service (DoS) attack

Correct Answer: C

QUESTION 12

Which of the following types of attacks cannot be prevented by technical measures only?

A. Brute force

B. Ping flood attack

C. Smurf DoS

D. Social engineering

Correct Answer: D