

**100%** Money Back  
**Guarantee**

**Vendor:**EC-COUNCIL

**Exam Code:**ECSS

**Exam Name:**EC-Council Certified Security Specialist  
Practice Test

**Version:**Demo

### QUESTION 1

Fill in the blank with the appropriate layer name of the OSI model.

Secure Socket Layer (SSL) operates at the \_\_\_\_\_ layer of the OSI model.

Correct Answer: transport

---

### QUESTION 2

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack. Which of the following logs will you review to accomplish the task?

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

- A. Web server logs
- B. Event logs
- C. Program logs
- D. System logs

Correct Answer: BCD

---

### QUESTION 3

Which two security components should you implement on the sales personnel portable computers to increase security?

(Click the Exhibit button on the toolbar to see the case study.)

Each correct answer represents a complete solution. Choose two.

- A. Encrypting File System (EFS)
- B. L2TP over IPSec
- C. PPTP
- D. Remote access policy
- E. Remote Authentication Dial-In User Service (RADIUS)

Correct Answer: AB

---

### QUESTION 4

Which of the following Trojans opens a very large number of Web browser windows?

- A. Backdoor.Zagaban
- B. Wmpscfgs.exe
- C. Back Orifice
- D. JS.WindowsBomb

Correct Answer: D

---

#### QUESTION 5

Andrew, a bachelor student of Faulkner University, creates a gmail account. He uses '\\Faulkner\\' as the password for the gmail account. After a few days, he starts receiving a lot of e-mails stating that his gmail account has been hacked. He also finds that some of his important mails have been deleted by someone. Which of the following methods has the attacker used to crack Andrew\\'s password?

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

- A. Brute force attack
- B. Dictionary-based attack
- C. Rainbow attack
- D. Zero-day attack
- E. Password guessing
- F. Social engineering
- G. Denial-of-service (DoS) attack
- H. Buffer-overflow attack

Correct Answer: ABCEF

---

#### QUESTION 6

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 7

Sam, a bank employee, develops a program and uploads it to the bank's server. He deducts \$1 a month from the account of every customer using the program. Probably no account holder will notice this type of illegal debit, but Sam will make a good amount of money every month. Which of the following types of cybercrime is Sam performing?

- A. Salami attack
- B. Web jacking
- C. Web defacement
- D. Data diddling

Correct Answer: A

---

#### QUESTION 8

Which of the following statements are true about firewalking?

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

- A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.
- B. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
- C. Firewalking works on the UDP packets.
- D. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.

Correct Answer: ABD

---

#### QUESTION 9

Which of the following networks relies on the tunneling protocol?

- A. Wide Area Network (WAN)
- B. Virtual Private Network (VPN)
- C. Local Area Network (LAN)

D. Wireless Network

Correct Answer: B

---

#### QUESTION 10

You work as a Network Administrator for Tech Perfect Inc. The company requires a secure wireless network. To provide security, you are configuring ISA Server 2006 as a firewall. While configuring ISA Server 2006, which of the following is NOT necessary?

- A. Defining how ISA Server would cache Web contents
- B. Defining ISA Server network configuration
- C. Setting up of monitoring on ISA Server
- D. Configuration of VPN access

Correct Answer: D

---

#### QUESTION 11

Which of the following programs is used to monitor the keystrokes that a user types on a specific computer's keyboard?

- A. Keylogger
- B. Ettercap
- C. THC-Hydra
- D. Brutus

Correct Answer: A

---

#### QUESTION 12

Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions that is available to the Internet. Which of the following security threats may occur if DMZ protocol attacks are performed? Each correct answer represents a complete solution. Choose all that apply.

- A. The attacker can exploit any protocol used to go into the internal network or intranet of the company.
- B. The attacker can gain access to the Web server in a DMZ and exploit the database.
- C. The attacker can perform a Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.

D. The attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.

Correct Answer: ABC