



ECSAV10^{Q&As}

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/ecsav10.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida; They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa; She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

- A. Reciprocation
- B. Friendship/Liking
- C. Social Validation
- D. Scarcity

Correct Answer: A

QUESTION 2

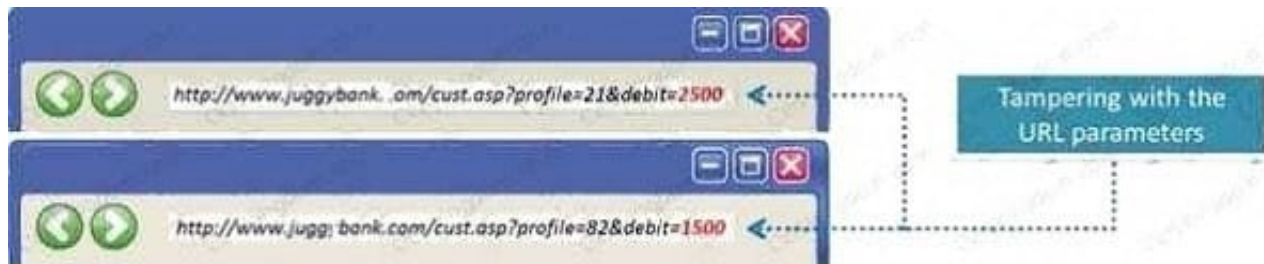
An organization recently faced a cyberattack where an attacker captured legitimate user credentials and gained access to the critical information systems. He also led other malicious hackers in gaining access to the information systems. To defend and prevent such attacks in future, the organization has decided to route all the incoming and outgoing network traffic through a centralized access proxy apart from validating user credentials. Which of the following defensive mechanisms the organization is trying to strengthen?

- A. Authentication
- B. Serialization
- C. Encryption
- D. Hashing

Correct Answer: A

QUESTION 3

The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control. This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.



What is the best way to protect web applications from parameter tampering attacks?

- A. Validating some parameters of the web application
- B. Minimizing the allowable length of parameters
- C. Using an easily guessable hashing algorithm
- D. Applying effective input field filtering parameters

Correct Answer: D

QUESTION 4

ABC Technologies, a large financial company, hired a penetration tester to do physical penetration testing.

On the first day of his assignment, the penetration tester goes to the company posing as a repairman and starts checking trash bins to collect the sensitive information.

What is the penetration tester trying to do?

- A. Trying to attempt social Engineering using phishing
- B. Trying to attempt social engineering by shoulder surfing
- C. Trying to attempt social engineering by eavesdropping
- D. Trying to attempt social engineering by dumpster diving

Correct Answer: D

QUESTION 5

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls.

(Select 2)

- A. 162



B. 160

C. 161

D. 163

Correct Answer: AC

[ECSAV10 Practice Test](#)

[ECSAV10 Exam Questions](#)

[ECSAV10 Braindumps](#)