EC1-349$^{\text{Q\&As}}$

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee

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

https://www.geekcert.com/ec1-349.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

A. Security Administrator

B. Network Administrator

C. Director of Information Technology

D. Director of Administration

Correct Answer: B

QUESTION 2

Paul\\'s company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Fuzzing

B. Tailgating

C. Backtrapping

D. Man trap attack

Correct Answer: B

QUESTION 3

The Electronic Serial Number (ESN) is a unique __________ recorded on a secure chip in a mobile phone by the manufacturer.

A. 16-bit identifier

B. 24-bit identifier

C. 32-bit identifier

D. 64-bit identifier

Correct Answer: C

QUESTION 4

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as other members of your team collect it. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

A. All forms should be placed in an approved secure container because they are now primary evidence in the case

B. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file

C. All forms should be placed in the report file because they are now primary evidence in the case

D. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container

Correct Answer: D

QUESTION 5

Identify the attack from following sequence of actions? Step 1: A user logs in to a trusted site and creates a new session Step 2: The trusted site stores a session identifier for the session in a cookie in the web browser Step 3: The user is tricked to visit a malicious site Step 4: the malicious site sends a request from the user\\'s browser using his session cookie

A. Web Application Denial-of-Service (DoS) Attack

B. Cross-Site Scripting (XSS) Attacks

C. Cross-Site Request Forgery (CSRF) Attack

D. Hidden Field Manipulation Attack

Correct Answer: C