Vendor:EC-COUNCIL

Exam Code:312-49V8

Exam Name: Computer Hacking Forensic Investigator Exam

Version: Demo

QUESTION 1

Which of the following is not correct when documenting an electronic crime scene?

A. Document the physical scene, such as the position of the mouse and the location of components near the system

B. Document related electronic components that are difficult to find

C. Record the condition of the computer system, storage media, electronic devices and conventional evidence, including power status of the computer

D. Write down the color of shirt and pant the suspect was wearing

Correct Answer: D

QUESTION 2

Web applications provide an Interface between end users and web servers through a set of web pages that are generated at the server-end or contain script code to be executed dynamically within the client Web browser.

A. True

B. False

Correct Answer: A

QUESTION 3

Subscriber Identity Module (SIM) is a removable component that contains essential information about the subscriber. Its main function entails authenticating the user of the cell phone to the network to gain access to subscribed services. SIM contains a 20-digit long Integrated Circuit Card identification (ICCID) number, identify the issuer identifier Number from the ICCID below.

A. 89

B. 44

C. 245252

D. 001451548

Correct Answer: C

QUESTION 4

Computer security logs contain information about the events occurring within an organization\\'s systems and networks. Which of the following security logs contains Logs of network and host-based security software?

A. Operating System (OS) logs

B. Application logs

C. Security software logs

D. Audit logs

Correct Answer: C

QUESTION 5

International Mobile Equipment Identifier (IMEI) is a 15-dlgit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

A. Type Allocation Code (TAC)

B. Device Origin Code (DOC)

C. Manufacturer identification Code (MIC)

D. Integrated Circuit Code (ICC)

Correct Answer: A

QUESTION 6

How do you define Technical Steganography?

A. Steganography that uses physical or chemical means to hide the existence of a message

B. Steganography that utilizes written natural language to hide the message in the carrier in some non-obvious ways

C. Steganography that utilizes written JAVA language to hide the message in the carrier in some non-obvious ways

D. Steganography that utilizes visual symbols or signs to hide secret messages

Correct Answer: A

QUESTION 7

What is cold boot (hard boot)?

A. It is the process of starting a computer from a powered-down or off state

B. It is the process of restarting a computer that is already turned on through the operating system

C. It is the process of shutting down a computer from a powered-on or on state

D. It is the process of restarting a computer that is already in sleep mode

Correct Answer: A

QUESTION 8

Which one of the following is not a consideration in a forensic readiness planning checklist?

A. Define the business states that need digital evidence

B. Identify the potential evidence available

C. Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner

D. Take permission from all employees of the organization

Correct Answer: D

QUESTION 9

In which step of the computer forensics investigation methodology would you run MD5 checksum on the evidence?

A. Obtain search warrant

B. Evaluate and secure the scene

C. Collect the evidence

D. Acquire the data

Correct Answer: D

QUESTION 10

Operating System logs are most beneficial for Identifying or Investigating suspicious activities involving a particular host. Which of the following Operating System logs contains information about operational actions performed by OS components?

A. Event logs

B. Audit logs

C. Firewall logs

D. IDS logs

Correct Answer: A

QUESTION 11

Which of the following Wi-Fi chalking methods refers to drawing symbols in public places to advertise open Wi-Fi networks?

A. WarWalking

B. WarFlying

C. WarChalking

D. WarDhving

Correct Answer: C

QUESTION 12

Attacker uses vulnerabilities in the authentication or session management functions such as exposed accounts, session IDs, logout, password management, timeouts, remember me. secret question, account update etc. to impersonate users, if a user simply closes the browser without logging out from sites accessed through a public computer, attacker can use the same browser later and exploit the user\\'s privileges. Which of the following vulnerability/exploitation is referred above?

A. Session ID in URLs

B. Timeout Exploitation

C. I/O exploitation

D. Password Exploitation

Correct Answer: B