Free Questions for CFA-001 by ebraindumps

Shared by Luna on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

Options:

A- Unvalidated input

B- Parameter/form tampering

C- Directory traversal

D- Security misconfiguration

Answer:

C

Question 2

Which of the following is the certifying body of forensics labs that investigate criminal cases by analyzing evidence?

Options:

A- The American Society of Crime Laboratory Directors (ASCLD)

B- International Society of Forensics Laboratory (ISFL)

C- The American Forensics Laboratory Society (AFLS)

D- The American Forensics Laboratory for Computer Forensics (AFLCF)

Answer:

A

Question 3

Question Type: MultipleChoice

Billy, a computer forensics expert, has recovered a large number of DBX files during forensic investigation of a laptop. Which of the following email clients he can use to analyze the DBX files?

Options:

A- Microsoft Outlook

B- Microsoft Outlook Express

C- Mozilla Thunderoird

D- Eudora

Answer:

B

Question 4

Question Type: MultipleChoice

How do you define Technical Steganography?

Options:

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

Answer:

A

Question 5

Question Type: MultipleChoice

An attack vector is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome.

Options:

A- True

B- False

Answer:

A

Question 6

Question Type: MultipleChoice

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.

Options:

A- True

B- False

Answer:

A

Question 7

Question Type: MultipleChoice

The need for computer forensics is highlighted by an exponential increase in the number of cybercrimes and litigations where large organizations were involved. Computer forensics plays an important role in tracking the cyber criminals. The main role of computer forensics is to:

Options:

A- Maximize the investigative potential by maximizing the costs

B- Harden organization perimeter security

C- Document monitoring processes of employees of the organization

D- Extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court

Answer:

D

Question 8

Question Type: **MultipleChoice**

What is static executable file analysis?

Options:

A- It is a process that consists of collecting information about and from an executable file without actually launching the file under any circumstances

B- It is a process that consists of collecting information about and from an executable file by launching the file under any circumstances

C- It is a process that consists of collecting information about and from an executable file without actually launching an executable file in a controlled and monitored environment

D- It is a process that consists of collecting information about and from an executable file by launching an executable file in a controlled and monitored environment

Answer:

A

Question 9

Question Type: MultipleChoice

Ever-changing advancement or mobile devices increases the complexity of mobile device examinations. Which or the following is an appropriate action for the mobile forensic investigation?

Options:

A- To avoid unwanted interaction with devices found on the scene, turn on any wireless interfaces such as Bluetooth and Wi-Fi radios

B- Do not wear gloves while handling cell phone evidence to maintain integrity of physical evidence

C- If the device's display is ON. the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons

D- If the phone is in a cradle or connected to a PC with a cable, then unplug the device from the computer

Answer:

C

Question 10

Question Type: **MultipleChoice**

What is a first sector ("sector zero") of a hard disk?

Options:

A- Master boot record

B- System boot record

C- Secondary boot record

D- Hard disk boot record

Answer:

A

Question 11

Question Type: **MultipleChoice**

A mobile operating system is the operating system that operates a mobile device like a mobile phone, smartphone, PDA, etc. It determines the functions and features available on mobile devices such as keyboards, applications, email, text messaging, etc. Which of the following mobile operating systems is free and open source?

Options:

A- Web OS

B- Android

C- Apple IOS

D- Symbian OS

Answer:

B