Vendor:EC-COUNCIL

Exam Code:212-89

Exam Name:EC-Council Certified Incident Handler

Version: Demo

QUESTION 1

Any information of probative value that is either stored or transmitted in a digital form during a computer crime is called:

A. Digital evidence

B. Computer Emails

C. Digital investigation

D. Digital Forensic Examiner

Correct Answer: A

QUESTION 2

A malicious security-breaking code that is disguised as any useful program that installs an executable programs when a file is opened and allows others to control the victim\\'s system is called:

A. Trojan

B. Worm

C. Virus

D. RootKit

Correct Answer: A

QUESTION 3

Policies are designed to protect the organizational resources on the network by establishing the set rules and procedures. Which of the following policies authorizes a group of users to perform a set of actions on a set of resources?

A. Access control policy

B. Audit trail policy

C. Logging policy

D. Documentation policy

Correct Answer: A

QUESTION 4

What is correct about Quantitative Risk Analysis:

A. It is Subjective but faster than Qualitative Risk Analysis

B. Easily automated

C. Better than Qualitative Risk Analysis

D. Uses levels and descriptive expressions

Correct Answer: B

QUESTION 5

In the Control Analysis stage of the NIST\\'s risk assessment methodology, technical and none technical control methods are classified into two categories. What are these two control categories?

A. Preventive and Detective controls

B. Detective and Disguised controls

C. Predictive and Detective controls

D. Preventive and predictive controls

Correct Answer: A

QUESTION 6

A software application in which advertising banners are displayed while the program is running that delivers ads to display pop-up windows or bars that appears on a computer screen or browser is called:

A. adware (spelled all lower case)

B. Trojan

C. RootKit

D. Virus

E. Worm

Correct Answer: A

QUESTION 7

A malware code that infects computer files, corrupts or deletes the data in them and requires a host file to propagate is called:

A. Trojan

B. Worm

C. Virus

D. RootKit

Correct Answer: C

QUESTION 8

The person who offers his formal opinion as a testimony about a computer crime incident in the court of law is known as:

A. Expert Witness

B. Incident Analyzer

C. Incident Responder

D. Evidence Documenter

Correct Answer: A

QUESTION 9

Incidents are reported in order to:

A. Provide stronger protection for systems and data

B. Deal properly with legal issues

C. Be prepared for handling future incidents

D. All the above

Correct Answer: D

QUESTION 10

Electronic evidence may reside in the following:

A. Data Files

B. Backup tapes

C. Other media sources

D. All the above

Correct Answer: D

QUESTION 11

An organization faced an information security incident where a disgruntled employee passed sensitive access control information to a competitor. The organization\\'s incident response manager, upon investigation, found that the incident must be handled within a few hours on the same day to maintain business continuity and market competitiveness. How would you categorize such information security incident?

A. High level incident

B. Middle level incident

C. Ultra-High level incident

D. Low level incident

Correct Answer: B

QUESTION 12

Which of the following incident recovery testing methods works by creating a mock disaster, like fire to identify the reaction of the procedures that are implemented to handle such situations?

A. Scenario testing

B. Facility testing

C. Live walk-through testing

D. Procedure testing

Correct Answer: D