Vendor:EC-COUNCIL

Exam Code:212-89

Exam Name:EC-Council Certified Incident Handler

Version: Demo

QUESTION 1

Preventing the incident from spreading and limiting the scope of the incident is known as:

A. Incident Eradication

B. Incident Protection

C. Incident Containment

D. Incident Classification

Correct Answer: C

QUESTION 2

Identify the network security incident where intended authorized users are prevented from using system, network, or applications by flooding the network with high volume of traffic that consumes all existing network resources.

A. URL Manipulation

B. XSS Attack

C. SQL Injection

D. Denial of Service Attack

Correct Answer: D

QUESTION 3

Which of the following can be considered synonymous:

A. Hazard and Threat

B. Threat and Threat Agent

C. Precaution and countermeasure

D. Vulnerability and Danger

Correct Answer: A

QUESTION 4

Which of the following is NOT one of the Computer Forensic types:

A. USB Forensics

B. Email Forensics

C. Forensic Archaeology

D. Image Forensics

Correct Answer: C

QUESTION 5

Which is the incorrect statement about Anti-keyloggers scanners: A. Detect already installed Keyloggers in victim machines

B. Run in stealthy mode to record victims online activity

C. Software tools

Correct Answer: B

QUESTION 6

Installing a password cracking tool, downloading pornography material, sending emails to colleagues which irritates them and hosting unauthorized websites on the company\\'s computer are considered:

A. Network based attacks

B. Unauthorized access attacks

C. Malware attacks

D. Inappropriate usage incidents

Correct Answer: D

QUESTION 7

The state of incident response preparedness that enables an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation is called:

A. Computer Forensics

B. Digital Forensic Analysis

C. Forensic Readiness

D. Digital Forensic Policy

Correct Answer: C

QUESTION 8

Which of the following is a risk assessment tool:

A. Nessus

B. Wireshark

C. CRAMM

D. Nmap

Correct Answer: C

QUESTION 9

Which of the following terms may be defined as "a measure of possible inability to achieve a goal, objective, or target within a defined security, cost plan and technical limitations that adversely affects the organization\\'s operation and revenues?

A. Risk

B. Vulnerability

C. Threat

D. Incident Response

Correct Answer: A

QUESTION 10

An incident is analyzed for its nature, intensity and its effects on the network and systems. Which stage of the incident response and handling process involves auditing the system and network log files?

A. Incident recording

B. Reporting

C. Containment

D. Identification

Correct Answer: D

QUESTION 11

A distributed Denial of Service (DDoS) attack is a more common type of DoS Attack, where a single system is targeted by a large number of infected machines over the Internet. In a DDoS attack, attackers first infect multiple systems which are known as:

A. Trojans

B. Zombies

C. Spyware

D. Worms

Correct Answer: B

QUESTION 12

Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?

A. To restore the original site, tests systems to prevent the incident and terminates operations

B. To define the notification procedures, damage assessments and offers the plan activation

C. To provide the introduction and detailed concept of the contingency plan

D. To provide a sequence of recovery activities with the help of recovery procedures

Correct Answer: A