DUMPSBOSS.

EC Council Certified Incident Handler (ECIH v3)

ECCouncil 212-89

Version Demo

Total Demo Questions: 10

Total Premium Questions: 163

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Incident response team must adhere to the following:

A. Stay calm and document everything

B. Assess the situation

C. Notify appropriate personnel

D. All the above

ANSWER: D

QUESTION NO: 2

An active vulnerability scanner featuring high speed discovery, configuration auditing, asset profiling, sensitive data discovery, and vulnerability analysis is called:

A. Nessus

B. CyberCop

C. EtherApe

D. nmap

ANSWER: A

QUESTION NO: 3

To recover, analyze, and preserve computer and related materials in such a way that it can be presented as evidence in a court of law and identify the evidence in short time, estimate the potential impact of the malicious activity on the victim, and assess the intent and identity of the perpetrator is known as:

A. Computer Forensics

B. Digital Forensic Analysis

C. Forensic Readiness

D. Digital Forensic Examiner

ANSWER: B

QUESTION NO: 4

The role that applies appropriate technology and tries to eradicate and recover from the incident is known as:

A. Incident Manager

B. Incident Analyst

C. Incident Handler

D. Incident coordinator

ANSWER: B

QUESTION NO: 5

Performing Vulnerability Assessment is an example of a:

A. Incident Response

B. Incident Handling

C. Pre-Incident Preparation

D. Post Incident Management

ANSWER: C

QUESTION NO: 6

In a qualitative risk analysis, risk is calculated in terms of:

A. (Attack Success + Criticality) –(Countermeasures)

B. Asset criticality assessment – (Risks and Associated Risk Levels)

C. Probability of Loss X Loss

D. (Countermeasures + Magnitude of Impact) – (Reports from prior risk assessments)

ANSWER: C

QUESTION NO: 7

If the loss anticipated is greater than the agreed upon threshold; the organization will:

A. Accept the risk

B. Mitigate the risk

C. Accept the risk but after management approval

D. Do nothing

ANSWER: B

QUESTION NO: 8

Identify a standard national process which establishes a set of activities, general tasks and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site.

A. NIASAP

B. NIAAAP

C. NIPACP

D. NIACAP

ANSWER: D

QUESTION NO: 9

The goal of incident response is to handle the incident in a way that minimizes damage and reduces recovery time and cost. Which of the following does NOT constitute a goal of incident response?

A. Dealing with human resources department and various employee conflict behaviors.

B. Using information gathered during incident handling to prepare for handling future incidents in a better way and to provide stronger protection for systems and data.

C. Helping personal to recover quickly and efficiently from security incidents, minimizing loss or theft and disruption of services.

D. Dealing properly with legal issues that may arise during incidents.

ANSWER: A

QUESTION NO: 10

According to the Fourth Amendment of USA PATRIOT Act of 2001; if a search does NOT violate a person’s “reasonable” or “legitimate” expectation of privacy then it is considered:

A. Constitutional/ Legitimate

B. Illegal/ illegitimate

C. Unethical

D. None of the above

ANSWER: A