212-89 Q&As

EC-Council Certified Incident Handler

Pass EC-COUNCIL 212-89 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/212-89.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

The data on the affected system must be backed up so that it can be retrieved if it is damaged during incident response. The system backup can also be used for further investigations of the incident. Identify the stage of the incident response and handling process in which complete backup of the infected system is carried out?

A. Containment

B. Eradication

C. Incident recording

D. Incident investigation

Correct Answer: A

QUESTION 2

The free, open source, TCP/IP protocol analyzer, sniffer and packet capturing utility standard across many industries and educational institutions is known as:

A. Snort

B. Wireshark

C. Cain and Able

D. nmap

Correct Answer: B

QUESTION 3

Which of the following incidents are reported under CAT -5 federal agency category?

A. Exercise/ Network Defense Testing

B. Malicious code

C. Scans/ probes/ Attempted Access

D. Denial of Service DoS

Correct Answer: C

QUESTION 4

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

Correct Answer: B

QUESTION 5

Incident Response Plan requires

A. Financial and Management support

B. Expert team composition

C. Resources

D. All the above

Correct Answer: D