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.pass2lead.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

Which of the following is NOT one of the common techniques used to detect Insider threats:

A. Spotting an increase in their performance

B. Observing employee tardiness and unexplained absenteeism

C. Observing employee sick leaves

D. Spotting conflicts with supervisors and coworkers

Correct Answer: A

QUESTION 3

In a DDoS attack, attackers first infect multiple systems, which are then used to attack a particular target directly. Those systems are called: A. Honey Pots

B. Relays

C. Zombies

D. Handlers

Correct Answer: C

QUESTION 4

Incident Response Plan requires

A. Financial and Management support

B. Expert team composition

C. Resources

D. All the above

Correct Answer: D

QUESTION 5

A. Forensic Analysis

B. Computer Forensics

C. Forensic Readiness

D. Steganalysis

Correct Answer: B

QUESTION 6

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 7

According to the Evidence Preservation policy, a forensic investigator should make at least ..... image copies of the digital evidence.

A. One image copy

B. Two image copies

C. Three image copies

D. Four image copies

Correct Answer: B

QUESTION 8

Which of the following service(s) is provided by the CSIRT:

A. Vulnerability handling

B. Technology watch

C. Development of security tools

D. All the above

Correct Answer: D

QUESTION 9

Digital evidence plays a major role in prosecuting cyber criminals. John is a cyber-crime investigator, is asked to investigate a child pornography case. The personal computer of the criminal in question was confiscated by the county police. Which of the following evidence will lead John in his investigation?

A. SAM file

B. Web serve log

C. Routing table list

D. Web browser history

Correct Answer: D

QUESTION 10

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 11

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 12

Adam calculated the total cost of a control to protect 10,000 $ worth of data as 20,000 $. What do you advise Adam to do?

A. Apply the control

B. Not to apply the control

C. Use qualitative risk assessment

D. Use semi-qualitative risk assessment instead

Correct Answer: B

QUESTION 13

Which of the following is a risk assessment tool:

A. Nessus

B. Wireshark

C. CRAMM

D. Nmap

Correct Answer: C

QUESTION 14

Computer viruses are malicious software programs that infect computers and corrupt or delete the data on them. Identify the virus type that specifically infects Microsoft Word files?

A. Micro Virus

B. File Infector

C. Macro Virus

D. Boot Sector virus

Correct Answer: C

QUESTION 15

To whom should an information security incident be reported?

A. It should not be reported at all and it is better to resolve it internally

B. Human resources and Legal Department

C. It should be reported according to the incident reporting and handling policy

D. Chief Information Security Officer

Correct Answer: C