

Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)

<https://www.2passeasy.com/dumps/212-89/>



NEW QUESTION 1

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

Answer: A

NEW QUESTION 2

Which of the following is an appropriate flow of the incident recovery steps?

- A. System Operation-System Restoration-System Validation-System Monitoring
- B. System Validation-System Operation-System Restoration-System Monitoring
- C. System Restoration-System Monitoring-System Validation-System Operations
- D. System Restoration-System Validation-System Operations-System Monitoring

Answer: D

NEW QUESTION 3

An incident recovery plan is a statement of actions that should be taken before, during or after an incident. Identify which of the following is NOT an objective of the incident recovery plan?

- A. Creating new business processes to maintain profitability after incident
- B. Providing a standard for testing the recovery plan
- C. Avoiding the legal liabilities arising due to incident
- D. Providing assurance that systems are reliable

Answer: A

NEW QUESTION 4

Multiple component incidents consist of a combination of two or more attacks in a system. Which of the following is not a multiple component incident?

- A. An insider intentionally deleting files from a workstation
- B. An attacker redirecting user to a malicious website and infects his system with Trojan
- C. An attacker infecting a machine to launch a DDoS attack
- D. An attacker using email with malicious code to infect internal workstation

Answer: A

NEW QUESTION 5

A threat source does not present a risk if NO vulnerability that can be exercised for a particular threat source. Identify the step in which different threat sources are defined:



- A. Identification Vulnerabilities
- B. Control analysis
- C. Threat identification
- D. System characterization

Answer: C

NEW QUESTION 6

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

Answer: A

NEW QUESTION 7

Which policy recommends controls for securing and tracking organizational resources:

- A. Access control policy
- B. Administrative security policy
- C. Acceptable use policy
- D. Asset control policy

Answer: D

NEW QUESTION 8

Except for some common roles, the roles in an IRT are distinct for every organization. Which among the following is the role played by the Incident Coordinator of an IRT?

- A. Links the appropriate technology to the incident to ensure that the foundation's offices are returned to normal operations as quickly as possible
- B. Links the groups that are affected by the incidents, such as legal, human resources, different business areas and management
- C. Applies the appropriate technology and tries to eradicate and recover from the incident
- D. Focuses on the incident and handles it from management and technical point of view

Answer: B

NEW QUESTION 9

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

Answer: A

NEW QUESTION 10

A computer virus hoax is a message warning the recipient of non-existent computer virus. The message is usually a chain e-mail that tells the recipient to forward it to every one they know. Which of the following is NOT a symptom of virus hoax message?

- A. The message prompts the end user to forward it to his / her e-mail contact list and gain monetary benefits in doing so
- B. The message from a known email id is caught by SPAM filters due to change of filter settings
- C. The message warns to delete certain files if the user does not take appropriate action
- D. The message prompts the user to install Anti-Virus

Answer: A

NEW QUESTION 10

ADAM, an employee from a multinational company, uses his company's accounts to send e-mails to a third party with their spoofed mail address. How can you categorize this type of account?

- A. Inappropriate usage incident
- B. Unauthorized access incident
- C. Network intrusion incident
- D. Denial of Service incident

Answer: A

NEW QUESTION 15

A security policy will take the form of a document or a collection of documents, depending on the situation or usage. It can become a point of reference in case a violation occurs that results in dismissal or other penalty. Which of the following is NOT true for a good security policy?

- A. It must be enforceable with security tools where appropriate and with sanctions where actual prevention is not technically feasible
- B. It must be approved by court of law after verifications of the stated terms and facts
- C. It must be implemented through system administration procedures, publishing of acceptable use guide lines or other appropriate methods
- D. It must clearly define the areas of responsibilities of the users, administrators and management

Answer: B

NEW QUESTION 18

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following helps in recognizing and separating the infected hosts from the information system?

- A. Configuring firewall to default settings
- B. Inspecting the process running on the system
- C. Browsing particular government websites
- D. Sending mails to only group of friends

Answer: B

NEW QUESTION 21

An access control policy authorized a group of users to perform a set of actions on a set of resources. Access to resources is based on necessity and if a particular job role requires the use of those resources. Which of the following is NOT a fundamental element of access control policy

- A. Action group: group of actions performed by the users on resources
- B. Development group: group of persons who develop the policy
- C. Resource group: resources controlled by the policy
- D. Access group: group of users to which the policy applies

Answer: B

NEW QUESTION 26

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

Answer: C

NEW QUESTION 30

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

Answer: C

NEW QUESTION 33

Incident management team provides support to all users in the organization that are affected by the threat or attack. The organization's internal auditor is part of the incident response team. Identify one of the responsibilities of the internal auditor as part of the incident response team:

- A. Configure information security controls
- B. Perform necessary action to block the network traffic from suspected intruder
- C. Identify and report security loopholes to the management for necessary actions
- D. Coordinate incident containment activities with the information security officer

Answer: C

NEW QUESTION 36

Based on the some statistics; what is the typical number one top incident?

- A. Phishing
- B. Policy violation
- C. Un-authorized access
- D. Malware

Answer: A

NEW QUESTION 38

An assault on system security that is derived from an intelligent threat is called:

- A. Threat Agent
- B. Vulnerability
- C. Attack
- D. Risk

Answer: C

NEW QUESTION 43

The IDS and IPS system logs indicating an unusual deviation from typical network traffic flows; this is called:

- A. A Precursor
- B. An Indication
- C. A Proactive
- D. A Reactive

Answer: B

NEW QUESTION 45

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

NEW QUESTION 46

In NIST risk assessment/ methodology; the process of identifying the boundaries of an IT system along with the resources and information that constitute the system is known as:

- A. Asset Identification
- B. System characterization
- C. Asset valuation
- D. System classification

Answer: B

NEW QUESTION 47

Performing Vulnerability Assessment is an example of a:

- A. Incident Response
- B. Incident Handling
- C. Pre-Incident Preparation
- D. Post Incident Management

Answer: C

NEW QUESTION 52

The correct sequence of incident management process is:

- A. Prepare, protect, triage, detect and respond
- B. Prepare, protect, detect, triage and respond
- C. Prepare, detect, protect, triage and respond
- D. Prepare, protect, detect, respond and triage

Answer: B

NEW QUESTION 54

The region where the CSIRT is bound to serve and what does it and give service to is known as:

- A. Consistency
- B. Confidentiality
- C. Constituency
- D. None of the above

Answer: C

NEW QUESTION 56

The open source TCP/IP network intrusion prevention and detection system (IDS/IPS), uses a rule-driven language, performs real-time traffic analysis and packet logging is known as:

- A. Snort
- B. Wireshark
- C. Nessus
- D. SAINT

Answer: A

NEW QUESTION 61

_____ attach(es) to files

- A. adware
- B. Spyware
- C. Viruses
- D. Worms

Answer: C

NEW QUESTION 63

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

Answer: A

NEW QUESTION 65

Authorized users with privileged access who misuse the corporate informational assets and directly affects the confidentiality, integrity, and availability of the assets are known as:

- A. Outsider threats
- B. Social Engineers
- C. Insider threats
- D. Zombies

Answer: C

NEW QUESTION 70

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

Answer: C

NEW QUESTION 74

What command does a Digital Forensic Examiner use to display the list of all IP addresses and their associated MAC addresses on a victim computer to identify the machines that were communicating with it:

- A. “arp” command
- B. “netstat –an” command
- C. “dd” command
- D. “ifconfig” command

Answer: A

NEW QUESTION 79

Digital evidence must:

- A. Be Authentic, complete and reliable
- B. Not prove the attackers actions
- C. Be Volatile
- D. Cast doubt on the authenticity and veracity of the evidence

Answer: A

NEW QUESTION 82

The correct order or sequence of the Computer Forensic processes is:

- A. Preparation, analysis, examination, collection, and reporting
- B. Preparation, collection, examination, analysis, and reporting
- C. Preparation, examination, collection, analysis, and reporting
- D. Preparation, analysis, collection, examination, and reporting

Answer: B

NEW QUESTION 85

A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format is called:

- A. Forensic Analysis
- B. Computer Forensics
- C. Forensic Readiness
- D. Steganalysis

Answer: B

NEW QUESTION 90

Incident may be reported using/ by:

- A. Phone call
- B. Facsimile (Fax)
- C. Email or on-line Web form
- D. All the above

Answer: D

NEW QUESTION 93

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 212-89 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 212-89 Product From:

<https://www.2passeasy.com/dumps/212-89/>

Money Back Guarantee

212-89 Practice Exam Features:

- * 212-89 Questions and Answers Updated Frequently
- * 212-89 Practice Questions Verified by Expert Senior Certified Staff
- * 212-89 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 212-89 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year