

Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)

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



NEW QUESTION 1

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

Answer: B

NEW QUESTION 2

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

NEW QUESTION 3

Business continuity is defined as the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy. Identify the plan which is mandatory part of a business continuity plan?

- A. Forensics Procedure Plan
- B. Business Recovery Plan
- C. Sales and Marketing plan
- D. New business strategy plan

Answer: B

NEW QUESTION 4

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 5

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

Answer: D

NEW QUESTION 6

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following steps focus on limiting the scope and extent of an incident?

- A. Eradication
- B. Containment
- C. Identification
- D. Data collection

Answer: B

NEW QUESTION 7

Quantitative risk is the numerical determination of the probability of an adverse event and the extent of the losses due to the event. Quantitative risk is calculated as:

- A. (Probability of Loss) X (Loss)
- B. (Loss) / (Probability of Loss)
- C. (Probability of Loss) / (Loss)

D. Significant Risks X Probability of Loss X Loss

Answer: A

NEW QUESTION 8

Risk is defined as the probability of the occurrence of an incident. Risk formulation generally begins with the likeliness of an event's occurrence, the harm it may cause and is usually denoted as Risk = ?(events)X (Probability of occurrence)X?

- A. Magnitude
- B. Probability
- C. Consequences
- D. Significance

Answer: A

NEW QUESTION 9

An audit trail policy collects all audit trails such as series of records of computer events, about an operating system, application or user activities. Which of the following statements is NOT true for an audit trail policy:

- A. It helps calculating intangible losses to the organization due to incident
- B. It helps tracking individual actions and allows users to be personally accountable for their actions
- C. It helps in compliance to various regulatory laws, rules, and guidelines
- D. It helps in reconstructing the events after a problem has occurred

Answer: A

NEW QUESTION 10

When an employee is terminated from his or her job, what should be the next immediate step taken by an organization?

- A. All access rights of the employee to physical locations, networks, systems, applications and data should be disabled
- B. The organization should enforce separation of duties
- C. The access requests granted to an employee should be documented and vetted by the supervisor
- D. The organization should monitor the activities of the system administrators and privileged users who have permissions to access the sensitive information

Answer: A

NEW QUESTION 10

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 14

Risk management consists of three processes, risk assessment, mitigation and evaluation. Risk assessment determines the extent of the potential threat and the risk associated with an IT system through its SDLC. How many primary steps does NIST's risk assessment methodology involve?

- A. Twelve
- B. Four
- C. Six
- D. Nine

Answer: D

NEW QUESTION 16

Insider threats can be detected by observing concerning behaviors exhibited by insiders, such as conflicts with supervisors and coworkers, decline in performance, tardiness or unexplained absenteeism. Select the technique that helps in detecting insider threats:

- A. Correlating known patterns of suspicious and malicious behavior
- B. Protecting computer systems by implementing proper controls
- C. Making it compulsory for employees to sign a non-disclosure agreement
- D. Categorizing information according to its sensitivity and access rights

Answer: A

NEW QUESTION 21

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 23

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 24

The type of relationship between CSIRT and its constituency have an impact on the services provided by the CSIRT. Identify the level of the authority that enables members of CSIRT to undertake any necessary actions on behalf of their constituency?

- A. Full-level authority
- B. Mid-level authority
- C. Half-level authority
- D. Shared-level authority

Answer: A

NEW QUESTION 29

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

Answer: D

NEW QUESTION 33

An adversary attacks the information resources to gain undue advantage is called:

- A. Defensive Information Warfare
- B. Offensive Information Warfare
- C. Electronic Warfare
- D. Conventional Warfare

Answer: B

NEW QUESTION 36

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 39

Incidents such as DDoS that should be handled immediately may be considered as:

- A. Level One incident
- B. Level Two incident
- C. Level Three incident
- D. Level Four incident

Answer: C

NEW QUESTION 40

Incident prioritization must be based on:

- A. Potential impact
- B. Current damage
- C. Criticality of affected systems
- D. All the above

Answer: D

NEW QUESTION 44

An information security incident is

- A. Any real or suspected adverse event in relation to the security of computer systems or networks
- B. Any event that disrupts normal today's business functions
- C. Any event that breaches the availability of information assets
- D. All of the above

Answer: D

NEW QUESTION 47

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

Answer: A

NEW QUESTION 52

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 55

The left over risk after implementing a control is called:

- A. Residual risk
- B. Unaccepted risk
- C. Low risk
- D. Critical risk

Answer: A

NEW QUESTION 60

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 61

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 66

The correct sequence of Incident Response and Handling is:

- A. Incident Identification, recording, initial response, communication and containment
- B. Incident Identification, initial response, communication, recording and containment
- C. Incident Identification, communication, recording, initial response and containment
- D. Incident Identification, recording, initial response, containment and communication

Answer: A

NEW QUESTION 71

What is the best staffing model for an incident response team if current employees' expertise is very low?

- A. Fully outsourced
- B. Partially outsourced
- C. Fully insourced
- D. All the above

Answer: A

NEW QUESTION 72

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 77

The service organization that provides 24x7 computer security incident response services to any user, company, government agency, or organization is known as:

- A. Computer Security Incident Response Team CSIRT
- B. Security Operations Center SOC
- C. Digital Forensics Examiner
- D. Vulnerability Assessor

Answer: A

NEW QUESTION 79

The main feature offered by PGP Desktop Email is:

- A. Email service during incidents
- B. End-to-end email communications
- C. End-to-end secure email service
- D. None of the above

Answer: C

NEW QUESTION 81

The typical correct sequence of activities used by CSIRT when handling a case is:

- A. Log, inform, maintain contacts, release information, follow up and reporting
- B. Log, inform, release information, maintain contacts, follow up and reporting
- C. Log, maintain contacts, inform, release information, follow up and reporting
- D. Log, maintain contacts, release information, inform, follow up and reporting

Answer: A

NEW QUESTION 82

To respond to DDoS attacks; one of the following strategies can be used:

- A. Using additional capacity to absorb attack
- B. Identifying none critical services and stopping them
- C. Shut down some services until the attack has subsided
- D. All the above

Answer: D

NEW QUESTION 84

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 87

A malware code that infects computer files, corrupts or deletes the data in them and requires a host file to propagate is called:

- A. Trojan
- B. Worm
- C. Virus
- D. RootKit

Answer: C

NEW QUESTION 90

_____ record(s) user's typing.

- A. Spyware
- B. adware
- C. Virus
- D. Malware

Answer: A

NEW QUESTION 92

Which of the following is a characteristic of adware?

- A. Gathering information
- B. Displaying popups
- C. Intimidating users
- D. Replicating

Answer: B

NEW QUESTION 97

Which of the following is NOT one of the techniques used to respond to insider threats:

- A. Placing malicious users in quarantine network, so that attack cannot be spread
- B. Preventing malicious users from accessing unclassified information
- C. Disabling the computer systems from network connection
- D. Blocking malicious user accounts

Answer: B

NEW QUESTION 99

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

Answer: B

NEW QUESTION 104

Lack of forensic readiness may result in:

- A. Loss of clients thereby damaging the organization's reputation
- B. System downtime
- C. Data manipulation, deletion, and theft
- D. All the above

Answer: D

NEW QUESTION 105

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 108

What command does a Digital Forensic Examiner use to display the list of all open ports and the associated IP addresses on a victim computer to identify the established connections on it:

- A. "arp" command
- B. "netstat -an" command

- C. “dd” command
- D. “ifconfig” command

Answer: B

NEW QUESTION 113

Any information of probative value that is either stored or transmitted in a digital form during a computer crime is called:

- A. Digital evidence
- B. Computer Emails
- C. Digital investigation
- D. Digital Forensic Examiner

Answer: A

NEW QUESTION 117

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 121

Electronic evidence may reside in the following:

- A. Data Files
- B. Backup tapes
- C. Other media sources
- D. All the above

Answer: D

NEW QUESTION 125

Incidents are reported in order to:

- A. Provide stronger protection for systems and data
- B. Deal properly with legal issues
- C. Be prepared for handling future incidents
- D. All the above

Answer: D

NEW QUESTION 130

Agencies do NOT report an information security incident is because of:

- A. Afraid of negative publicity
- B. Have full knowledge about how to handle the attack internally
- C. Do not want to pay the additional cost of reporting an incident
- D. All the above

Answer: A

NEW QUESTION 131

The process of rebuilding and restoring the computer systems affected by an incident to normal operational stage including all the processes, policies and tools is known as:

- A. Incident Management
- B. Incident Response
- C. Incident Recovery
- D. Incident Handling

Answer: C

NEW QUESTION 135

Business Continuity planning includes other plans such as:

- A. Incident/disaster recovery plan
- B. Business recovery and resumption plans
- C. Contingency plan
- D. All the above

Answer: D

NEW QUESTION 139

Business Continuity provides a planning methodology that allows continuity in business operations:

- A. Before and after a disaster
- B. Before a disaster
- C. Before, during and after a disaster
- D. During and after a disaster

Answer: C

NEW QUESTION 144

The steps followed to recover computer systems after an incident are:

- A. System restoration, validation, operation and monitoring
- B. System restoration, operation, validation, and monitoring
- C. System monitoring, validation, operation and restoration
- D. System validation, restoration, operation and monitoring

Answer: A

NEW QUESTION 145

The product of intellect that has commercial value and includes copyrights and trademarks is called:

- A. Intellectual property
- B. Trade secrets
- C. Logos
- D. Patents

Answer: A

NEW QUESTION 146

.....

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