

Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)

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



NEW QUESTION 1

Which of the following terms may be defined as “a measure of possible inability to achieve a goal, objective, or target within a defined security, cost plan and technical limitations that adversely affects the organization’s operation and revenues?”

- A. Risk
- B. Vulnerability
- C. Threat
- D. Incident Response

Answer: A

NEW QUESTION 2

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 3

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 4

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 5

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 6

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 7

Computer forensics is a methodical series of techniques and procedures for gathering evidence from computing equipment, various storage devices and or digital media that can be presented in a court of law in a coherent and meaningful format. Which one of the following is an appropriate flow of steps in the computer forensics process:

- A. Examination > Analysis > Preparation > Collection > Reporting
- B. Preparation > Analysis > Collection > Examination > Reporting

C. Analysis > Preparation > Collection > Reporting > Examination
D. Preparation > Collection > Examination > Analysis > Reporting

Answer: D

NEW QUESTION 8

The network perimeter should be configured in such a way that it denies all incoming and outgoing traffic/ services that are not required. Which service listed below, if blocked, can help in preventing Denial of Service attack?

- A. SAM service
- B. POP3 service
- C. SMTP service
- D. Echo service

Answer: D

NEW QUESTION 9

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 10

Which of the following incident recovery testing methods works by creating a mock disaster, like fire to identify the reaction of the procedures that are implemented to handle such situations?

- A. Scenario testing
- B. Facility testing
- C. Live walk-through testing
- D. Procedure testing

Answer: D

NEW QUESTION 10

The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the matrix, one can conclude that:

- A. If the insider's technical literacy is low and process knowledge is high, the risk posed by the threat will be insignificant.
- B. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be insignificant.
- C. If the insider's technical literacy is high and process knowledge is low, the risk posed by the threat will be high.
- D. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be high.

Answer: D

NEW QUESTION 15

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 20

Which one of the following is the correct sequence of flow of the stages in an incident response:

- A. Containment - Identification - Preparation - Recovery - Follow-up - Eradication
- B. Preparation - Identification - Containment - Eradication - Recovery - Follow-up
- C. Eradication - Containment - Identification - Preparation - Recovery - Follow-up
- D. Identification - Preparation - Containment - Recovery - Follow-up - Eradication

Answer: B

NEW QUESTION 24

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

NEW QUESTION 28

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 31

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 32

A computer forensic investigator must perform a proper investigation to protect digital evidence. During the investigation, an investigator needs to process large amounts of data using a combination of automated and manual methods. Identify the computer forensic process involved:

- A. Analysis
- B. Preparation
- C. Examination
- D. Collection

Answer: C

NEW QUESTION 34

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 39

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 44

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 46

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 48

Total cost of disruption of an incident is the sum of

- A. Tangible and Intangible costs
- B. Tangible cost only
- C. Intangible cost only
- D. Level Two and Level Three incidents cost

Answer: A

NEW QUESTION 51

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 55

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 59

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 61

Absorbing minor risks while preparing to respond to major ones is called:

- A. Risk Mitigation
- B. Risk Transfer
- C. Risk Assumption
- D. Risk Avoidance

Answer: C

NEW QUESTION 64

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 66

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 69

Which of the following is an incident tracking, reporting and handling tool:

- A. CRAMM
- B. RTIR
- C. NETSTAT
- D. EAR/ Pilar

Answer: B

NEW QUESTION 71

Removing or eliminating the root cause of the incident is called:

- A. Incident Eradication
- B. Incident Protection
- C. Incident Containment
- D. Incident Classification

Answer: A

NEW QUESTION 73

Which of the following is a correct statement about incident management, handling and response:

- A. Incident response is on the functions provided by incident handling
- B. Incident handling is on the functions provided by incident response
- C. Triage is one of the services provided by incident response
- D. Incident response is one of the services provided by triage

Answer: A

NEW QUESTION 75

Incident Response Plan requires

- A. Financial and Management support
- B. Expert team composition
- C. Resources
- D. All the above

Answer: D

NEW QUESTION 76

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 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

NEW QUESTION 84

CERT members can provide critical support services to first responders such as:

- A. Immediate assistance to victims
- B. Consolidated automated service process management platform
- C. Organizing spontaneous volunteers at a disaster site
- D. A + C

Answer: D

NEW QUESTION 85

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

NEW QUESTION 87

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 & Able
- D. nmap

Answer: B

NEW QUESTION 89

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 93

The very well-known free open source port, OS and service scanner and network discovery utility is called:

- A. Wireshark
- B. Nmap (Network Mapper)
- C. Snort
- D. SAINT

Answer: B

NEW QUESTION 97

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

Answer: C

NEW QUESTION 98

A Malicious code attack using emails is considered as:

- A. Malware based attack
- B. Email attack
- C. Inappropriate usage incident
- D. Multiple component attack

Answer: D

NEW QUESTION 103

_____ record(s) user's typing.

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

Answer: A

NEW QUESTION 107

_____ attach(es) to files

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

Answer: C

NEW QUESTION 110

A self-replicating malicious code that does not alter files but resides in active memory and duplicates itself, spreads through the infected network automatically and takes advantage of file or information transport features on the system to travel independently is called:

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

Answer: B

NEW QUESTION 114

A malicious security-breaking code that is disguised as any useful program that installs an executable programs when a file is opened and allows others to control the victim's system is called:

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

Answer: A

NEW QUESTION 119

The free utility which quickly scans Systems running Windows OS to find settings that may have been changed by spyware, malware, or other unwanted programs is called:

- A. Tripwire
- B. HijackThis
- C. Stinger
- D. F-Secure Anti-virus

Answer: B

NEW QUESTION 122

A Host is infected by worms that propagates through a vulnerable service; the sign(s) of the presence of the worm include:

- A. Decrease in network usage
- B. Established connection attempts targeted at the vulnerable services
- C. System becomes instable or crashes
- D. All the above

Answer: C

NEW QUESTION 127

Keyloggers do NOT:

- A. Run in the background
- B. Alter system files
- C. Secretly records URLs visited in browser, keystrokes, chat conversations, ...etc
- D. Send log file to attacker's email or upload it to an ftp server

Answer: B

NEW QUESTION 132

The USB tool (depicted below) that is connected to male USB Keyboard cable and not detected by antispyware tools is most likely called:



- A. Software Key Grabber
- B. Hardware Keylogger
- C. USB adapter
- D. Anti-Keylogger

Answer: B

NEW QUESTION 134

Insiders understand corporate business functions. What is the correct sequence of activities performed by Insiders to damage company assets:

- A. Gain privileged access, install malware then activate
- B. Install malware, gain privileged access, then activate
- C. Gain privileged access, activate and install malware
- D. Activate malware, gain privileged access then install malware

Answer: A

NEW QUESTION 135

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 140

Which of the following is NOT a digital forensic analysis tool:

- A. Access Data FTK
- B. EAR/ Pilar
- C. Guidance Software EnCase Forensic
- D. Helix

Answer: B

NEW QUESTION 141

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 143

The individual who recovers, analyzes, and preserves computer and related materials to be presented as evidence in a court of law and identifies the evidence, estimates the potential impact of the malicious activity on the victim, and assesses the intent and identity of the perpetrator is called:

- A. Digital Forensic Examiner
- B. Computer Forensic Investigator
- C. Computer Hacking Forensic Investigator
- D. All the above

Answer: D

NEW QUESTION 145

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 150

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 153

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 154

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 155

According to US-CERT; if an agency is unable to successfully mitigate a DOS attack it must be reported within:

- A. One (1) hour of discovery/detection if the successful attack is still ongoing
- B. Two (2) hours of discovery/detection if the successful attack is still ongoing
- C. Three (3) hours of discovery/detection if the successful attack is still ongoing
- D. Four (4) hours of discovery/detection if the successful attack is still ongoing

Answer: B

NEW QUESTION 158

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 160

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 164

The policy that defines which set of events needs to be logged in order to capture and review the important data in a timely manner is known as:

- A. Audit trail policy
 - B. Logging policy
 - C. Documentation policy
 - D. Evidence Collection policy
 - E. Distributed and communicated
 - F. Enforceable and Regularly updated
 - G. Written in simple language
 - H. All the above
- An information security policy must be:

Answer: D

NEW QUESTION 166

The most common type(s) of intellectual property is(are):

- A. Copyrights and Trademarks
- B. Patents

- C. Industrial design rights & Trade secrets
- D. All the above

Answer: D

NEW QUESTION 168

Ensuring the integrity, confidentiality and availability of electronic protected health information of a patient is known as:

- A. Gramm-Leach-Bliley Act
- B. Health Insurance Portability and Privacy Act
- C. Social Security Act
- D. Sarbanes-Oxley Act

Answer: B

NEW QUESTION 173

Bit stream image copy of the digital evidence must be performed in order to:

- A. Prevent alteration to the original disk
- B. Copy the FAT table
- C. Copy all disk sectors including slack space
- D. All the above

Answer: C

NEW QUESTION 175

A living high level document that states in writing a requirement and directions on how an agency plans to protect its information technology assets is called:

- A. Information security Policy
- B. Information security Procedure
- C. Information security Baseline
- D. Information security Standard

Answer: A

NEW QUESTION 180

.....

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