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

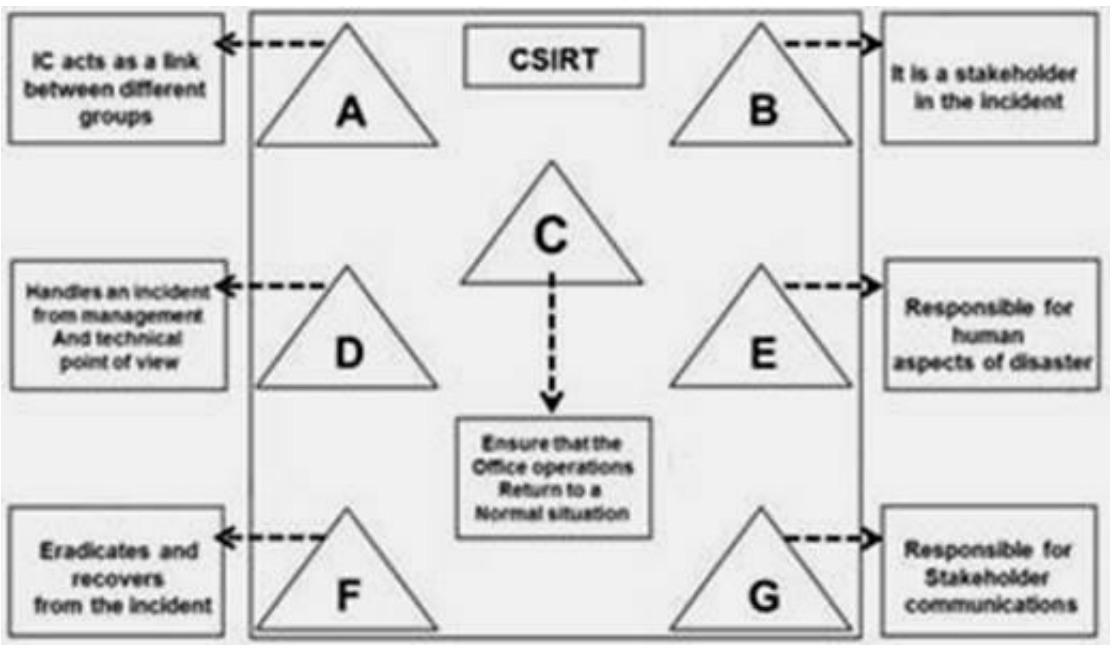
Answer: B

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
The flow chart gives a view of different roles played by the different personnel of CSIRT. Identify the incident response personnel denoted by A, B, C, D, E, F and G.



A. A-Incident Analyst, B- Incident Coordinator, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Manager
B. A- Incident Coordinator, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Manager
C. A- Incident Coordinator, B- Constituency, C-Administrator, D-Incident Manager, E- Human Resource, FIncident Analyst, G-Public relations
D. A- Incident Manager, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Coordinator

Answer: C

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
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 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
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 8
Computer Forensics is the branch of forensic science in which legal evidence is found in any computer or any digital media device. Of the following, who is responsible for examining the evidence acquired and separating the useful evidence?

A. Evidence Supervisor
B. Evidence Documenter
C. Evidence Manager
D. Evidence Examiner/ Investigator

Answer: D

NEW QUESTION 9
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 10
A US Federal agency network was the target of a DoS attack that prevented and impaired the normal authorized functionality of the networks. According to agency's reporting timeframe guidelines, this incident
should be reported within two (2) HOURS of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity. Which incident category of the US Federal Agency does this incident belong to?

A. CAT 5
B. CAT 1
C. CAT 2
D. CAT 6

Answer: C

NEW QUESTION 10
US-CERT and Federal civilian agencies use the reporting timeframe criteria in the federal agency reporting categorization. What is the timeframe required to report an incident under the CAT 4 Federal Agency category?

A. Weekly
B. Within four (4) hours of discovery/detection if the successful attack is still ongoing and agency is unable to successfully mitigate activity
C. Within two (2) hours of discovery/detection
D. Monthly

Answer: A

NEW QUESTION 15
Policies are designed to protect the organizational resources on the network by establishing the set rules and procedures. Which of the following policies authorizes a group of users to perform a set of actions on a set of resources?

A. Access control policy
B. Audit trail policy
C. Logging policy
D. Documentation policy

Answer: A

NEW QUESTION 16
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 18
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 21
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 25
An incident is analyzed for its nature, intensity and its effects on the network and systems. Which stage of the incident response and handling process involves auditing the system and network log files?

A. Incident recording
B. Reporting
C. Containment
D. Identification

Answer: D

NEW QUESTION 30
Which among the following CERTs is an Internet provider to higher education institutions and various other research institutions in the Netherlands and deals with all cases related to computer security incidents in which a customer is involved either as a victim or as a suspect?

A. NET-CERT
B. DFN-CERT
C. Funet CERT
D. SURFnet-CERT

Answer: D

NEW QUESTION 31
One of the main objectives of incident management is to prevent incidents and attacks by tightening the physical security of the system or infrastructure. According to CERT's incident management process, which stage focuses on implementing infrastructure improvements resulting from postmortem reviews or other process improvement mechanisms?

A. Protection
B. Preparation
C. Detection
D. Triage

Answer: A

NEW QUESTION 36
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 is compulsory for employees to sign a none disclosure agreement
D. Categorizing information according to its sensitivity and access rights

Answer: A

NEW QUESTION 38
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 43
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 47
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 52
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 56
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 57
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 60
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 61
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 62
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 67
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 72
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 76
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 80
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 85
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 86
What is correct about Quantitative Risk Analysis:

A. It is Subjective but faster than Qualitative Risk Analysis
B. Easily automated
C. Better than Qualitative Risk Analysis
D. Uses levels and descriptive expressions

Answer: B

NEW QUESTION 90
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 93
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

Answer: C

NEW QUESTION 95
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 98
Incident response team must adhere to the following:

A. Stay calm and document everything
B. Assess the situation
C. Notify appropriate personnel
D. All the above

Answer: D

NEW QUESTION 100
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 101
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 102

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 104
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 105
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 106
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 110
_____ record(s) user's typing.

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

Answer: A

NEW QUESTION 112
Which of the following is a characteristic of adware?

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

Answer: B

NEW QUESTION 113
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 117
The main difference between viruses and worms is:

A. Worms require a host file to propagate while viruses don't
B. Viruses require a host file to propagate while Worms don't

C. Viruses don’t require user interaction; they are self-replicating malware
D. Viruses and worms are common names for the same malware

Answer: B

NEW QUESTION 119
The sign(s) of the presence of malicious code on a host infected by a virus which is delivered via e-mail could be:

A. Antivirus software detects the infected files
B. Increase in the number of e-mails sent and received
C. System files become inaccessible
D. All the above

Answer: D

NEW QUESTION 120
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 121
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 125
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 130
Spyware tool used to record malicious user’s computer activities and keyboard stokes is called:

A. adware
B. Keylogger
C. Rootkit
D. Firewall

Answer: B

NEW QUESTION 134
Which of the following may be considered as insider threat(s):

A. An employee having no clashes with supervisors and coworkers
B. Disgruntled system administrators
C. An employee who gets an annual 7% salary raise
D. An employee with an insignificant technical literacy and business process knowledge

Answer: B

NEW QUESTION 137
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 138
The Linux command used to make binary copies of computer media and as a disk imaging tool if given a raw disk device as its input is:

A. “dd” command
B. “netstat” command
C. “nslookup” command
D. “find” command

Answer: A

NEW QUESTION 139
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 141
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

Answer: B

NEW QUESTION 142
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 146
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 148
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 152
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 154
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 156
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 158
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 & handling policy
D. Chief Information Security Officer

Answer: C

NEW QUESTION 159
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 160
Which test is conducted to determine the incident recovery procedures effectiveness?

A. Live walk-throughs of procedures
B. Scenario testing
C. Department-level test
D. Facility-level test

Answer: A

NEW QUESTION 162
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 163
The ability of an agency 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 is known as:

A. Business Continuity Plan
B. Business Continuity
C. Disaster Planning
D. Contingency Planning

Answer: B

NEW QUESTION 167
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 168
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 169
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 171
According to the Fourth Amendment of USA PATRIOT Act of 2001; if a search does NOT violate a person's "reasonable" or "legitimate" expectation of privacy then it is considered:

A. Constitutional/ Legitimate
B. Illegal/ illegitimate
C. Unethical
D. None of the above

Answer: A

NEW QUESTION 175
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 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