EC-Council

Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)

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
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 3
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 4
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 5
Computer forensics is 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 course 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 6
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 7
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 8
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 9
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 10
Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?

A. To restore the original site, tests systems to prevent the incident and terminates operations
B. To define the notification procedures, damage assessments and offers the plan activation
C. To provide the introduction and detailed concept of the contingency plan
D. To provide a sequence of recovery activities with the help of recovery procedures

Answer: A

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 14
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 18
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 20
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 25
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 28
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 29
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 30
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
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 35
An estimation of the expected losses after an incident helps organization in prioritizing and formulating their incident response. The cost of an incident can be categorized as a tangible and intangible cost. Identify the tangible cost associated with virus outbreak?

A. Loss of goodwill
B. Damage to corporate reputation
C. Psychological damage
D. Lost productivity damage

Answer: D

NEW QUESTION 39
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 42
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 47
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 49
The sign of incident that may happen in the future is called:

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

Answer: A

NEW QUESTION 53
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 58
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 61
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 62
Overall Likelihood rating of a Threat to Exploit a Vulnerability is driven by :

A. Threat-source motivation and capability
B. Nature of the vulnerability

C. Existence and effectiveness of the current controls
D. All the above

Answer: D

NEW QUESTION 63
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 68
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

Answer: B

NEW QUESTION 69
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 71
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 76
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 81
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 84
Incident Response Plan requires

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

Answer: D

NEW QUESTION 85
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 88
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 90
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

Answer: D

NEW QUESTION 92
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 94
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 97
Common name(s) for CSIRT is(are)

A. Incident Handling Team (IHT)
B. Incident Response Team (IRT)
C. Security Incident Response Team (SIRT)
D. All the above

Answer: D

NEW QUESTION 99
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 100
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 102
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 103
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 104
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 105
_____ 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
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 115
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
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 122
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 124
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 126
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 128
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 133
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 138

Insiders may be:

A. Ignorant employees
B. Carless administrators
C. Disgruntled staff members
D. All the above

Answer: D

NEW QUESTION 143
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 144
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 148
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 150
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 153
Which of the following is NOT one of the Computer Forensic types:

A. USB Forensics
B. Email Forensics
C. Forensic Archaeology
D. Image Forensics

Answer: C

NEW QUESTION 157
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 158
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 162
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 167
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 171
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 172
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 policyAn information security policy must be:
E. Distributed and communicated
F. Enforceable and Regularly updated
G. Written in simple language
H. All the above

Answer: D

NEW QUESTION 173
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 175
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 176
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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