



## **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

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 3

A computer Risk Policy is a set of ideas to be implemented to overcome the risk associated with computer security incidents. Identify the procedure that is NOT part of the computer risk policy?

- A. Procedure to identify security funds to hedge risk
- B. Procedure to monitor the efficiency of security controls
- C. Procedure for the ongoing training of employees authorized to access the system
- D. Provisions for continuing support if there is an interruption in the system or if the system crashes

**Answer:** C

#### NEW QUESTION 4

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 5

Identify the malicious program that is masked as a genuine harmless program and gives the attacker unrestricted access to the user’s information and system. These programs may unleash dangerous programs that may erase the unsuspecting user’s disk and send the victim’s credit card numbers and passwords to a stranger.

- A. Cookie tracker
- B. Worm
- C. Trojan
- D. Virus

**Answer:** C

#### 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

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 8

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 9

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 10

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 10

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 12

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 16

In which of the steps of NIST's risk assessment methodology are the boundary of the IT system, along with the resources and the information that constitute the system identified?

- A. Likelihood Determination
- B. Control recommendation
- C. System characterization
- D. Control analysis

**Answer:** C

#### 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 24

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 27

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 31

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 35

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 37

A payroll system has a vulnerability that cannot be exploited by current technology. Which of the following is correct about this scenario:

- A. The risk must be urgently mitigated
- B. The risk must be transferred immediately
- C. The risk is not present at this time
- D. The risk is accepted

**Answer: C**

#### NEW QUESTION 42

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 44

Which of the following is a risk assessment tool:

- A. Nessus
- B. Wireshark
- C. CRAMM
- D. Nmap

**Answer:** C

#### NEW QUESTION 46

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 50

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 51

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 56

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 59

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 64

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 68

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 73**

Installing a password cracking tool, downloading pornography material, sending emails to colleagues which irritates them and hosting unauthorized websites on the company's computer are considered:

- A. Network based attacks
- B. Unauthorized access attacks
- C. Malware attacks
- D. Inappropriate usage incidents

**Answer:** D

**NEW QUESTION 77**

Changing the web server contents, Accessing the workstation using a false ID and Copying sensitive data without authorization are examples of:

- A. DDoS attacks
- B. Unauthorized access attacks
- C. Malware attacks
- D. Social Engineering attacks

**Answer:** B

**NEW QUESTION 78**

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 80**

They type of attack that prevents the authorized users to access networks, systems, or applications by exhausting the network resources and sending illegal requests to an application is known as:

- A. Session Hijacking attack
- B. Denial of Service attack
- C. Man in the Middle attack
- D. SQL injection attack

**Answer:** B

**NEW QUESTION 83**

\_\_\_\_\_ attach(es) to files

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

**Answer:** C

**NEW QUESTION 85**

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 87**

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 89

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 92

A software application in which advertising banners are displayed while the program is running that delivers ads to display pop-up windows or bars that appears on a computer screen or browser is called:

- A. adware (spelled all lower case)
- B. Trojan
- C. RootKit
- D. Virus
- E. Worm

**Answer:** A

#### NEW QUESTION 93

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 94

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 98

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 102

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 107

Spyware tool used to record malicious user's computer activities and keyboard strokes is called:



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

**Answer:** B

#### NEW QUESTION 108

Insiders may be:

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

**Answer:** D

#### NEW QUESTION 110

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 112

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 115

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 120

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 121

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 123

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 124

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 127

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 132

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

**Answer:** D

#### NEW QUESTION 134

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 137

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 139

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 144

According to the Evidence Preservation policy, a forensic investigator should make at least ..... image copies of the digital evidence.

- A. One image copy
- B. Two image copies

- C. Three image copies
- D. Four image copies

**Answer:** B

**NEW QUESTION 149**

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 151**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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 First Try
- \* 212-89 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 212-89 Practice Test Here](#)**