

# EC-Council

## Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)



#### 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

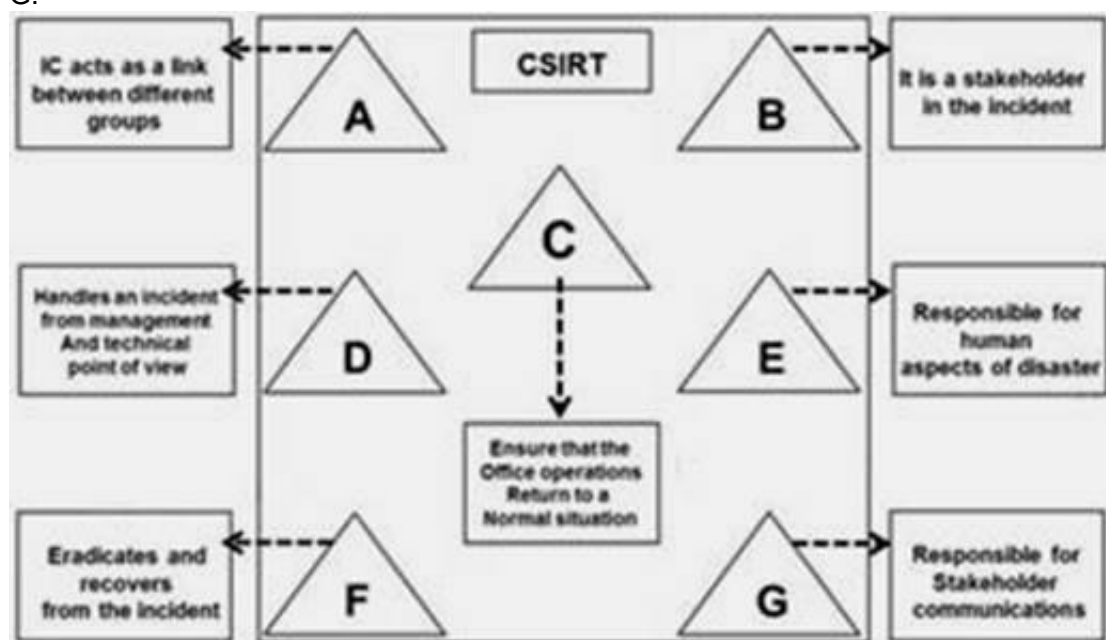
The goal of incident response is to handle the incident in a way that minimizes damage and reduces recovery time and cost. Which of the following does NOT constitute a goal of incident response?

- 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

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 6

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 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

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 10

Identify a standard national process which establishes a set of activities, general tasks and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site.

- A. NIASAP
- B. NIAAAP
- C. NIPACP
- D. NIACAP

**Answer:** D

#### 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 13

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 16**

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 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**

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 33**

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 38**

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 40**

A risk mitigation strategy determines the circumstances under which an action has to be taken to minimize and overcome risks. Identify the risk mitigation strategy that focuses on minimizing the probability of risk and losses by searching for vulnerabilities in the system and appropriate controls:

- A. Risk Assumption
- B. Research and acknowledgment
- C. Risk limitation
- D. Risk absorption

**Answer:** B

**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 44**

The largest number of cyber-attacks are conducted by:

- A. Insiders
- B. Outsiders
- C. Business partners
- D. Suppliers

**Answer:** B

**NEW QUESTION 48**

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 53**

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 58**

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 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 62**

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 66**

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 70

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 71

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

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 79

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 83

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 86

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 89

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 93**

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 98**

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 103**

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 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**

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 110**

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 112**

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 113**

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 116**

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 117**

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 122**

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 125**

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 128**

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 132**

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 134**

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 139**

.....

## 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](#)**