# EC-COUNCIL.212-89.v2022-02-19.q72

| | |
|---|---|
| **Exam Code:** | 212-89 |
| **Exam Name:** | EC Council Certified Incident Handler (ECIH v3) |
| **Certification Provider:** | EC-COUNCIL |
| **Free Question Number:** | 72 |
| **Version:** | v2022-02-19 |
| **# of views:** | 3444 |
| **# of Questions views:** | 720 |
| https://www.freepdfdumps.com/EC-COUNCIL.212-89.v2022-02-19.q72.html | |

**NEW QUESTION: 1**
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.** Dealing properly with legal issues that may arise during incidents.
**D.** Helping personal to recover quickly and efficiently from security incidents, minimizing loss or theft and disruption of services.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 2**
Total cost of disruption of an incident is the sum of
**A.** Tangible and Intangible costs
**B.** Level Two and Level Three incidents cost
**C.** Intangible cost only
**D.** Tangible cost only
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 3**
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 is high and process knowledge is low, the risk posed by the threat will be
high.
**C.** If the insider's technical literacy and process knowledge are high, 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
insignificant.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 4**
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.** Incident investigation
**B.** Eradication
**C.** Incident recording
**D.** Containment
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 5**
The main feature offered by PGP Desktop Email is:
**A.** End-to-end secure email service
**B.** End-to-end email communications
**C.** None of the above
**D.** Email service during incidents
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 6**
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: (SHOW ANSWER)**

**NEW QUESTION: 7**
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: (SHOW ANSWER)**

**NEW QUESTION: 8**
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.** Wireshark
**B.** Nessus
**C.** SAINT
**D.** Snort
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 9**
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.** Lost productivity damage
**D.** Psychological damage
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 10**
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
**B.** Business Continuity Plan

**C.** Contingency Planning
**D.** Disaster Planning
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 11**
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.** Spyware
**B.** Zombies
**C.** Worms
**D.** Trojans
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 12**
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.** Development group: group of persons who develop the policy
**B.** Resource group: resources controlled by the policy
**C.** Action group: group of actions performed by the users on resources
**D.** Access group: group of users to which the policy applies
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 13**
A Host is infected by worms that propagates through a vulnerable service; the sign(s) of the presence of the worm include:
**A.** Established connection attempts targeted at the vulnerable services
**B.** Decrease in network usage
**C.** System becomes instable or crashes
**D.** All the above
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 14**
Which of the following is a risk assessment tool:
**A.** Nessus
**B.** Wireshark
**C.** Nmap
**D.** CRAMM
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 15**
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: (SHOW ANSWER)**
Explanation

**NEW QUESTION: 16**
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: (SHOW ANSWER)**



**NEW QUESTION: 17**
Performing Vulnerability Assessment is an example of a:
**A.** Incident Response
**B.** Pre-Incident Preparation
**C.** Incident Handling
**D.** Post Incident Management
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 18**

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.** Zombies
**B.** Trojans
**C.** Spyware
**D.** Worms
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 19**
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.** NIACAP
**D.** NIPACP
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 20**
The correct sequence of Incident Response and Handling is:
**A.** Incident Identification, initial response, communication, recording and containment
**B.** Incident Identification, recording, initial response, communication and containment
**C.** Incident Identification, recording, initial response, containment and communication
**D.** Incident Identification, communication, recording, initial response and containment
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 21**
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.** Worm
**B.** RootKit
**C.** Trojan
**D.** Virus
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 22**
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.** Half-level authority
**B.** Shared-level authority
**C.** Mid-level authority
**D.** Full-level authority
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 23**
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.** Denial of Service attack
**B.** Man in the Middle attack
**C.** Session Hijacking attack
**D.** SQL injection attack
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 24**
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.** Facility testing
**B.** Scenario testing
**C.** Live walk-through testing
**D.** Procedure testing
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 25**
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 attacker infecting a machine to launch a DDoS attack
**B.** An attacker using email with malicious code to infect internal workstation
**C.** An insider intentionally deleting files from a workstation
**D.** An attacker redirecting user to a malicious website and infects his system with Trojan
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 26**

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.** Reporting

**B.** Incident recording

**C.** Identification

**D.** Containment

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 27**

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.** Providing a standard for testing the recovery plan

**B.** Creating new business processes to maintain profitability after incident

**C.** Providing assurance that systems are reliable

**D.** Avoiding the legal liabilities arising due to incident

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 28**

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.** Digital Forensic Policy

**B.** Computer Forensics

**C.** Digital Forensic Analysis

**D.** Forensic Readiness

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 29**

The role that applies appropriate technology and tries to eradicate and recover from the incident is known as:

**A.** Incident Analyst

**B.** Incident Handler

**C.** Incident coordinator

**D.** Incident Manager

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 30**

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 (LEAVE A REPLY)**

**NEW QUESTION: 31**
Authorized users with privileged access who misuse the corporate informational assets and directly affects the confidentiality, integrity, and availability of the assets are known as:
**A.** Zombies
**B.** Social Engineers
**C.** Outsider threats
**D.** Insider threats
**Answer: D (LEAVE A REPLY)**



**NEW QUESTION: 32**
Insiders understand corporate business functions. What is the correct sequence of activities performed by
Insiders to damage company assets:
**A.** Activate malware, gain privileged access then install malware
**B.** Gain privileged access, activate and install malware
**C.** Install malware, gain privileged access, then activate
**D.** Gain privileged access, install malware then activate
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 33**
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: (SHOW ANSWER)**
Explanation/Reference:

**NEW QUESTION: 34**
An information security incident is
**A.** Any event that disrupts normal today's business functions
**B.** All of the above
**C.** Any real or suspected adverse event in relation to the security of computer systems or networks
**D.** Any event that breaches the availability of information assets
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 35**
The sign of incident that may happen in the future is called:
**A.** A Reactive
**B.** A Proactive
**C.** A Precursor
**D.** An Indication
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 36**
Business Continuity provides a planning methodology that allows continuity in business operations:
**A.** During and after a disaster
**B.** Before and after a disaster
**C.** Before, during and after a disaster
**D.** Before a disaster
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 37**
To respond to DDoS attacks; one of the following strategies can be used:
**A.** All the above
**B.** Shut down some services until the attack has subsided
**C.** Using additional capacity to absorb attack
**D.** Identifying none critical services and stopping them
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 38**
Which of the following is NOT a digital forensic analysis tool:
**A.** Helix
**B.** Guidance Software EnCase Forensic
**C.** EAR/ Pilar
**D.** Access Data FTK
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 39**
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.** SQL injection attack
**B.** Denial of Service attack
**C.** Session Hijacking attack
**D.** Man in the Middle attack
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 40**
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.** Evidence Collection policy
**B.** Documentation policy
**C.** Logging policy
**D.** Audit trail policy
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 41**
When an employee is terminated from his or her job, what should be the next immediate step taken by an organization?
**A.** The organization should enforce separation of duties
**B.** All access rights of the employee to physical locations, networks, systems, applications and data should be disabled
**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: (SHOW ANSWER)**

**NEW QUESTION: 42**
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 (LEAVE A REPLY)**
Explanation/Reference:

**NEW QUESTION: 43**
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.** Evidence Collection policy
**C.** Documentation policy
**D.** Logging policy
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 44**
The largest number of cyber-attacks are conducted by:
**A.** Suppliers
**B.** Insiders
**C.** Business partners
**D.** Outsiders
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 45**
Insiders understand corporate business functions. What is the correct sequence of activities performed by Insiders to damage company assets:
**A.** Gain privileged access, activate and install malware
**B.** Activate malware, gain privileged access then install malware
**C.** Gain privileged access, install malware then activate
**D.** Install malware, gain privileged access, then activate
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 46**
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 in compliance to various regulatory laws, rules,and guidelines
**C.** It helps tracking individual actions and allows users to be personally accountable for their actions
**D.** It helps in reconstructing the events after a problem has occurred
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 47**
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 (LEAVE A REPLY)**
Explanation/Reference:

**NEW QUESTION: 48**
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.** Stinger
**B.** F-Secure Anti-virus
**C.** Tripwire
**D.** HijackThis
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 49**
Which of the following is a correct statement about incident management, handling and response:
**A.** Incident response is one of the services provided by triage
**B.** Triage is one of the services provided by incident response
**C.** Incident handling is on the functions provided by incident response
**D.** Incident response is on the functions provided by incident handling
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 50**
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.** Coordinate incident containment activities with the information security officer

**B.** Identify and report security loopholes to the management for necessary actions

**C.** Configure information security controls

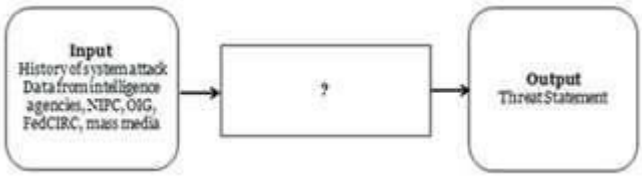
**D.** Perform necessary action to block the network traffic from suspected intruder

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 51**

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.** Control analysis

**B.** Threat identification

**C.** Identification Vulnerabilities

**D.** System characterization

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 52**

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

**A.** A + C

**B.** Consolidated automated service process management platform

**C.** Immediate assistance to victims

**D.** Organizing spontaneous volunteers at a disaster site

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 53**

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.** Logging policy

**B.** Audit trail policy

**C.** Documentation policy

**D.** Access control policy

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 54**

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 and process knowledge are high, the risk posed by the threat will be high.
**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 low and process knowledge is high, the risk posed by the threat will be insignificant.
**D.** If the insider's technical literacy is high and process knowledge is low, the risk posed by the threat will be high.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 55**
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 (LEAVE A REPLY)**
Explanation

**NEW QUESTION: 56**
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.** Steganalysis
**D.** Forensic Readiness
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 57**
The free, open source, TCP/IP protocol analyzer, sniffer and packet capturing utility standard across many industries and educational institutions is known as:
**A.** Wireshark
**B.** Cain & Able
**C.** Snort

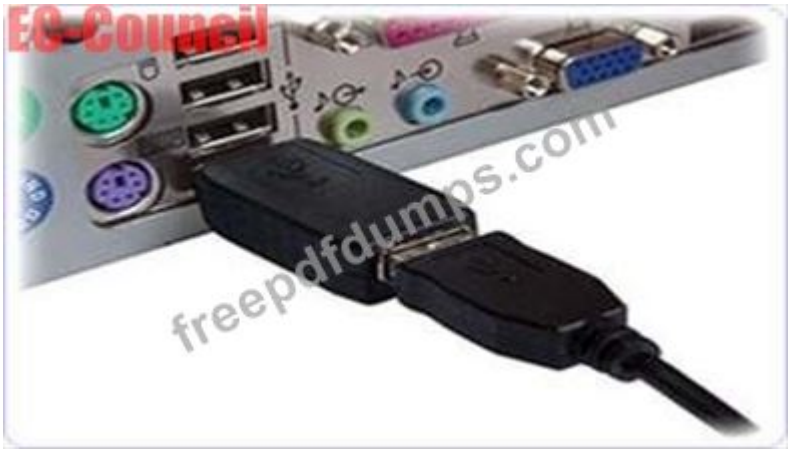
**D.** nmap
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 58**
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.** Research and acknowledgment
**B.** Risk absorption
**C.** Risk Assumption
**D.** Risk limitation
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 59**
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.** Low level incident
**B.** High level incident
**C.** Ultra-High level incident
**D.** Middle level incident
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 60**
Incident Response Plan requires
**A.** Financial and Management support
**B.** Resources
**C.** Expert team composition
**D.** All the above
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 61**
The USB tool (depicted below) that is connected to male USB Keyboard cable and not detected by anti-
spyware tools is most likely called:




**A.** Software Key Grabber
**B.** Hardware Keylogger
**C.** USB adapter
**D.** Anti-Keylogger
**Answer: (SHOW ANSWER)**
Explanation



**NEW QUESTION: 62**
Which of the following is a characteristic of adware?
**A.** Replicating
**B.** Gathering information
**C.** Intimidating users
**D.** Displaying popups
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 63**
Based on the some statistics; what is the typical number one top incident?
**A.** Phishing
**B.** Policy violation
**C.** Malware
**D.** Un-authorized access
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 64**
The correct order or sequence of the Computer Forensic processes is:
**A.** Preparation, analysis, collection, examination, and reporting
**B.** Preparation, collection, examination, analysis, and reporting
**C.** Preparation, analysis, examination, collection, and reporting
**D.** Preparation, examination, collection, analysis, and reporting
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 65**
Insiders may be:
**A.** Ignorant employees
**B.** Disgruntled staff members
**C.** All the above
**D.** Carless administrators
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 66**
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 Standard
**B.** Information security Policy
**C.** Information security Procedure
**D.** Information security Baseline
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 67**
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.** Unethical
**B.** None of the above
**C.** Illegal/ illegitimate
**D.** Constitutional/ Legitimate
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 68**
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.** New business strategy plan
**B.** Business Recovery Plan

**C.** Forensics Procedure Plan
**D.** Sales and Marketing plan
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 69**
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 (LEAVE A REPLY)**

**NEW QUESTION: 70**
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.** Threat
**B.** Incident Response
**C.** Vulnerability
**D.** Risk
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 71**
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 (LEAVE A REPLY)**
Explanation

**NEW QUESTION: 72**
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 Documenter
**B.** Evidence Examiner/ Investigator
**C.** Evidence Supervisor
**D.** Evidence Manager
**Answer: (SHOW ANSWER)**