212-89.74q

Number: 212-89
Passing Score: 800
Time Limit: 120 min

212-89

EC Council Certified Incident Handler (ECIH v2)

Exam A

QUESTION 1

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

When an employee is terminated from his or her job, what should be the next immediate step taken by an organization?

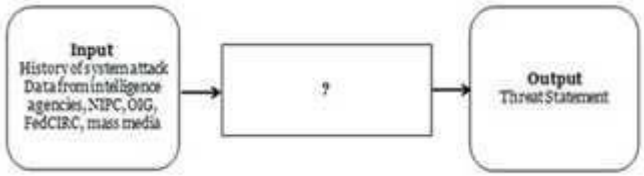
A. All access rights of the employee to physical locations, networks, systems, applications and data should be disabled

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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

Correct Answer: D

Section: (none)
Explanation
Explanation/Reference:

QUESTION 10
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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. FourC. Six
D. Nine

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
One of the goals of CSIRT is to manage security problems by taking a certain approach towards the customers' security vulnerabilities and by responding effectively to potential information security incidents. Identify the incident response approach that focuses on developing the infrastructure and security processes before the occurrence or detection of an event or any incident:

A. Interactive approach
B. Introductive approach

C. Proactive approach
D. Qualitative approach

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

Based on the some statistics; what is the typical number one top incident?

A. Phishing
B. Policy violation
C. Un-authorized access
D. Malware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
An assault on system security that is derived from an intelligent threat is called:

A. Threat Agent
B. Vulnerability
C. Attack
D. Risk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
The largest number of cyber-attacks are conducted by:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
The sign of incident that may happen in the future is called:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 29
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Incident prioritization must be based on:

A. Potential impact
B. Current damage
C. Criticality of affected systems
D. All the above

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
The program that helps to train people to be better prepared to respond to emergency situations in their communities is known as:

A. Community Emergency Response Team (CERT)
B. Incident Response Team (IRT)
C. Security Incident Response Team (SIRT)
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 42
CSIRT can be implemented at:

A. Internal enterprise level
B. National, government and military level
C. Vendor level
D. All the above

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
The typical correct sequence of activities used by CSIRT when handling a case is:

A. Log, inform, maintain contacts, release information, follow up and reporting
B. Log, inform, release information, maintain contacts, follow up and reporting
C. Log, maintain contacts, inform, release information, follow up and reporting
D. Log, maintain contacts, release information, inform, follow up and reporting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51

A Malicious code attack using emails is considered as:

A. Malware based attack
B. Email attack
C. Inappropriate usage incident
D. Multiple component attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
_____ record(s) user's typing.

Spyware
B. adware
C. Virus
D. Malware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following is a characteristic of adware?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
_____ attach(es) to files

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

Correct Answer: C

A.

Section: (none)
Explanation
Explanation/Reference:

QUESTION 57
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59

The message that is received and requires an urgent action and it prompts the recipient to delete certain files or forward it to others is called:

An Adware

B. Mail bomb
C. A Virus Hoax
D. Spear Phishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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

A.

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64

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:

“arp” command
B. “netstat –an” command

A.
C. “dd” command
D. “ifconfig” command

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69

Electronic evidence may reside in the following:

Data Files
B. Backup tapes

A.
C. Other media sources
D. All the above

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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

Correct Answer: D
Section: (none)
QUESTION 72

Explanation

Explanation/Reference:
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Incident may be reported using/ by:

A. Phone call

B. Facsimile (Fax) C. Email or on-line Web form
D. All the above

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: