Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)

https://www.2passeasy.com/dumps/212-89/

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
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 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
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 6
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 7
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 tracking individual actions and allows users to be personally accountable for their actions
C. It helps in compliance to various regulatory laws, rules,and guidelines

D. It helps in reconstructing the events after a problem has occurred

Answer: A

NEW QUESTION 8
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

Answer: A

NEW QUESTION 9
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 10
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 10
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 12
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 14
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 16
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 17
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

Answer: A

NEW QUESTION 21
Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?

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

Answer: A

NEW QUESTION 23
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 25
Which one of the following is the correct sequence of flow of the stages in an incident response:

A. Containment - Identification - Preparation - Recovery - Follow-up - Eradication
B. Preparation - Identification - Containment - Eradication - Recovery - Follow-up
C. Eradication - Containment - Identification - Preparation - Recovery - Follow-up
D. Identification - Preparation - Containment - Recovery - Follow-up - Eradication

Answer: B

NEW QUESTION 26
Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues. Which of the following documents helps in protecting evidence from physical or logical damage:

A. Network and host log records
B. Chain-of-Custody
C. Forensic analysis report
D. Chain-of-Precedence

Answer: B

NEW QUESTION 29

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 34
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 35
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 38
Digital evidence plays a major role in prosecuting cyber criminals. John is a cyber-crime investigator, is asked to investigate a child pornography case. The personal computer of the criminal in question was confiscated by the county police. Which of the following evidence will lead John in his investigation?

A. SAM file
B. Web serve log
C. Routing table list
D. Web browser history

Answer: D

NEW QUESTION 43
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 45
Which of the following incidents are reported under CAT -5 federal agency category?

A. Exercise/ Network Defense Testing
B. Malicious code
C. Scans/ probes/ Attempted Access
D. Denial of Service DoS

Answer: C

NEW QUESTION 49
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 52

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

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

Answer: A

NEW QUESTION 54
The IDS and IPS system logs indicating an unusual deviation from typical network traffic flows; this is called:

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

Answer: B

NEW QUESTION 56
The sign of incident that may happen in the future is called:

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

Answer: A

NEW QUESTION 58
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 63
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 64
Overall Likelihood rating of a Threat to Exploit a Vulnerability is driven by :

A. Threat-source motivation and capability
B. Nature of the vulnerability
C. Existence and effectiveness of the current controls
D. All the above

Answer: D

NEW QUESTION 68
Absorbing minor risks while preparing to respond to major ones is called:

A. Risk Mitigation
B. Risk Transfer
C. Risk Assumption
D. Risk Avoidance

Answer: C

NEW QUESTION 69
The left over risk after implementing a control is called:

A. Residual risk
B. Unaccepted risk
C. Low risk

D. Critical risk

Answer: A

NEW QUESTION 70
What is correct about Quantitative Risk Analysis:

A. It is Subjective but faster than Qualitative Risk Analysis
B. Easily automated
C. Better than Qualitative Risk Analysis
D. Uses levels and descriptive expressions

Answer: B

NEW QUESTION 71
Preventing the incident from spreading and limiting the scope of the incident is known as:

A. Incident Eradication
B. Incident Protection
C. Incident Containment
D. Incident Classification

Answer: C

NEW QUESTION 74
What is the best staffing model for an incident response team if current employees’ expertise is very low?

A. Fully outsourced
B. Partially outsourced
C. Fully insourced
D. All the above

Answer: A

NEW QUESTION 77
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 79
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 82
The service organization that provides 24x7 computer security incident response services to any user, company, government agency, or organization is known as:

A. Computer Security Incident Response Team CSIRT
B. Security Operations Center SOC
C. Digital Forensics Examiner
D. Vulnerability Assessor

Answer: A

NEW QUESTION 87
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 92
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 94
The role that applies appropriate technology and tries to eradicate and recover from the incident is known as:

A. Incident Manager
B. Incident Analyst
C. Incident Handler
D. Incident coordinator

Answer: B

NEW QUESTION 98
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 103
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

Answer: A

NEW QUESTION 104
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

Answer: A

NEW QUESTION 109
Common name(s) for CSIRT is(are)

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

Answer: D

NEW QUESTION 114
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 119
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 120
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 123
______ attach(es) to files

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

Answer: C

NEW QUESTION 126
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 127
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:

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

Answer: C

NEW QUESTION 130
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 134
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 135
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 138
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. Outsider threats
B. Social Engineers
C. Insider threats
D. Zombies

Answer: C

NEW QUESTION 140
Keyloggers do NOT:

A. Run in the background
B. Alter system files
C. Secretly records URLs visited in browser, keystrokes, chat conversations, ...etc
D. Send log file to attacker's email or upload it to an ftp server

Answer: B

NEW QUESTION 142
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 145
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 150
Spyware tool used to record malicious user's computer activities and keyboard stokes is called:

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

Answer: B

NEW QUESTION 151
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 153
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 157
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

Answer: A

NEW QUESTION 161
The individual who recovers, analyzes, and preserves computer and related materials to be presented as evidence in a court of law and identifies the evidence, estimates the potential impact of the malicious activity on the victim, and assesses the intent and identity of the perpetrator is called:

A. Digital Forensic Examiner
B. Computer Forensic Investigator
C. Computer Hacking Forensic Investigator
D. All the above

Answer: D

NEW QUESTION 162
Any information of probative value that is either stored or transmitted in a digital form during a computer crime is called:

A. Digital evidence
B. Computer Emails
C. Digital investigation
D. Digital Forensic Examiner

Answer: A

NEW QUESTION 165
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 169
The person who offers his formal opinion as a testimony about a computer crime incident in the court of law is known as:

A. Expert Witness
B. Incident Analyzer
C. Incident Responder
D. Evidence Documenter

Answer: A

NEW QUESTION 171
Incidents are reported in order to:

A. Provide stronger protection for systems and data
B. Deal properly with legal issues
C. Be prepared for handling future incidents
D. All the above

Answer: D

NEW QUESTION 173
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 177
Agencies do NOT report an information security incident is because of:

A. Afraid of negative publicity
B. Have full knowledge about how to handle the attack internally
C. Do not want to pay the additional cost of reporting an incident
D. All the above

Answer: A

NEW QUESTION 178
Incident may be reported using/ by:

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

Answer: D

NEW QUESTION 179
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 181
Business Continuity provides a planning methodology that allows continuity in business operations:

A. Before and after a disaster
B. Before a disaster
C. Before, during and after a disaster
D. During and after a disaster

Answer: C

NEW QUESTION 185
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 188
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 193
Bit stream image copy of the digital evidence must be performed in order to:

A. Prevent alteration to the original disk
B. Copy the FAT table
C. Copy all disk sectors including slack space
D. All the above

Answer: C

NEW QUESTION 194
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 198

......