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
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. Forensics Procedure Plan
B. Business Recovery Plan
C. Sales and Marketing plan
D. New business strategy plan

Answer: B

NEW QUESTION 3
Quantitative risk is the numerical determination of the probability of an adverse event and the extent of the losses due to the event. Quantitative risk is calculated as:

A. (Probability of Loss) X (Loss)
B. (Loss) / (Probability of Loss)
C. (Probability of Loss) / (Loss)
D. Significant Risks X Probability of Loss X Loss

Answer: A

NEW QUESTION 4
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 5
Computer forensics is methodical series of techniques and procedures for gathering evidence from computing equipment, various storage devices and or digital media that can be presented in a course of law in a coherent and meaningful format. Which one of the following is an appropriate flow of steps in the computer forensics process:

A. Examination> Analysis > Preparation > Collection > Reporting
B. Preparation > Analysis > Collection > Examination > Reporting
C. Analysis > Preparation > Collection > Reporting > Examination
D. Preparation > Collection > Examination > Analysis > Reporting

Answer: D

NEW QUESTION 6
Computer Forensics is the branch of forensic science in which legal evidence is found in any computer or any digital media device. Of the following, who is responsible for examining the evidence acquired and separating the useful evidence?

A. Evidence Supervisor
B. Evidence Documenter
C. Evidence Manager
D. Evidence Examiner/ Investigator

Answer: D

NEW QUESTION 7
The network perimeter should be configured in such a way that it denies all incoming and outgoing traffic/ services that are not required. Which service listed below, if blocked, can help in preventing Denial of Service attack?

A. SAM service
B. POP3 service
C. SMTP service

D. Echo service

Answer: D

NEW QUESTION 8
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 9
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

Answer: D

NEW QUESTION 10
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. Four
C. Six
D. Nine

Answer: D

NEW QUESTION 10
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 and process knowledge are high, the risk posed by the threat will be insignificant.
C. If the insider’s technical literacy is high and process knowledge is low, 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 high.

Answer: D

NEW QUESTION 12
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
Except for some common roles, the roles in an IRT are distinct for every organization. Which among the following is the role played by the Incident Coordinator of an IRT?

A. Links the appropriate technology to the incident to ensure that the foundation’s offices are returned to normal operations as quickly as possible
B. Links the groups that are affected by the incidents, such as legal, human resources, different business areas and management
C. Applies the appropriate technology and tries to eradicate and recover from the incident
D. Focuses on the incident and handles it from management and technical point of view

Answer: B

NEW QUESTION 18
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 21
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 26
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 28
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 30
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 33
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

Answer: C

NEW QUESTION 38
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

Answer: C

NEW QUESTION 40
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

Answer: D

NEW QUESTION 45
Which of the following can be considered synonymous:

A. Hazard and Threat
B. Threat and Threat Agent
C. Precaution and countermeasure
D. Vulnerability and Danger

Answer: A

NEW QUESTION 49
A payroll system has a vulnerability that cannot be exploited by current technology. Which of the following is correct about this scenario:

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

Answer: C

NEW QUESTION 54
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 59
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 63
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 67
Which of the following is a risk assessment tool:

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

Answer: C

NEW QUESTION 71
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: B

NEW QUESTION 73
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 75
Incident response team must adhere to the following:

A. Stay calm and document everything
B. Assess the situation
C. Notify appropriate personnel
D. All the above

Answer: D

NEW QUESTION 77
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 80
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 81
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 85
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 86
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 87
A Malicious code attack using emails is considered as:

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

Answer: D

NEW QUESTION 88
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 91
_____ record(s) user's typing.

A. Spyware
B. adware
C. Virus
D. Malware

Answer: A

NEW QUESTION 92
_____ attach(es) to files

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

Answer: C

NEW QUESTION 95
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 96
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 101
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 103
A software application in which advertising banners are displayed while the program is running that delivers ads to display pop-up windows or bars that appears on a computer screen or browser is called:

A. adware (spelled all lower case)
B. Trojan

C. RootKit
D. Virus
E. Worm

Answer: A

NEW QUESTION 106
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 111
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 115
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 120
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 124
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

Answer: A

NEW QUESTION 128
The correct order or sequence of the Computer Forensic processes is:

A. Preparation, analysis, examination, collection, and reporting
B. Preparation, collection, examination, analysis, and reporting
C. Preparation, examination, collection, analysis, and reporting
D. Preparation, analysis, collection, examination, and reporting

Answer: B

NEW QUESTION 130
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 133
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 136
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 141
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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 FirstTry

* 212-89 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year