EC-Council

Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
The flow chart gives a view of different roles played by the different personnel of CSIRT. Identify the incident response personnel denoted by A, B, C, D, E, F and G.

A. A-Incident Analyst, B- Incident Coordinator, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Manager
B. A- Incident Coordinator, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Manager
C. A- Incident Coordinator, B- Constituency, C-Administrator, D-Incident Manager, E- Human Resource, FIncident Analyst, G-Public relations
D. A- Incident Manager, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Coordinator

Answer: C

NEW QUESTION 2
A computer Risk Policy is a set of ideas to be implemented to overcome the risk associated with computer security incidents. Identify the procedure that is NOT part of the computer risk policy?

A. Procedure to identify security funds to hedge risk
B. Procedure to monitor the efficiency of security controls
C. Procedure for the ongoing training of employees authorized to access the system
D. Provisions for continuing support if there is an interruption in the system or if the system crashes

Answer: C

NEW QUESTION 3
Identify the network security incident where intended authorized users are prevented from using system, network, or applications by flooding the network with high volume of traffic that consumes all existing network resources.

A. URL Manipulation
B. XSS Attack
C. SQL Injection
D. Denial of Service Attack

Answer: D

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
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 6
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 7
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. Access control policy
B. Audit trail policy
C. Logging policy
D. Documentation policy

Answer: A

NEW QUESTION 8
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 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
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 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 14
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

NEW QUESTION 15
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 21
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 25
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 29
A computer virus hoax is a message warning the recipient of non-existent computer virus. The message is usually a chain e-mail that tells the recipient to forward it to every one they know. Which of the following is NOT a symptom of virus hoax message?

A. The message prompts the end user to forward it to his / her e-mail contact list and gain monetary benefits in doing so
B. The message from a known email id is caught by SPAM filters due to change of filter settings
C. The message warns to delete certain files if the user does not take appropriate action
D. The message prompts the user to install Anti-Virus

Answer: A

NEW QUESTION 31
In which of the steps of NIST's risk assessment methodology are the boundary of the IT system, along with the resources and the information that constitute the system identified?

A. Likelihood Determination
B. Control recommendation
C. System characterization
D. Control analysis

Answer: C

NEW QUESTION 35
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

NEW QUESTION 39
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 44
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 48
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 51
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 55
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 57
An assault on system security that is derived from an intelligent threat is called:

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

Answer: C

NEW QUESTION 58
The largest number of cyber-attacks are conducted by:

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

Answer: B

NEW QUESTION 60
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 61
Incidents such as DDoS that should be handled immediately may be considered as:

A. Level One incident
B. Level Two incident
C. Level Three incident
D. Level Four incident

Answer: C

NEW QUESTION 66
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 69
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 70
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 75
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 78
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 82
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 83
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 86
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 87
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 89
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 94
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 96
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 97
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 101
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 103
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 104
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

Answer: D

NEW QUESTION 106
The very well-known free open source port, OS and service scanner and network discovery utility is called:

A. Wireshark
B. Nmap (Network Mapper)
C. Snort
D. SAINT

Answer: B

NEW QUESTION 110
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 112
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 113
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 118
_____ record(s) user's typing.

A. Spyware
B. adware
C. Virus

D. Malware

Answer: A

NEW QUESTION 120
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

Answer: B

NEW QUESTION 124
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 126
The main difference between viruses and worms is:

A. Worms require a host file to propagate while viruses don’t
B. Viruses require a host file to propagate while Worms don’t
C. Viruses don’t require user interaction; they are self-replicating malware
D. Viruses and worms are common names for the same malware

Answer: B

NEW QUESTION 131
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 132
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 134
The USB tool (depicted below) that is connected to male USB Keyboard cable and not detected by antispyware tools is most likely called:

A. Software Key Grabber
B. Hardware Keylogger
C. USB adapter
D. Anti-Keylogger

Answer: B

NEW QUESTION 139
Which of the following is NOT a digital forensic analysis tool:

A. Access Data FTK
B. EAR/ Pilar
C. Guidance Software EnCase Forensic
D. Helix

Answer: B

NEW QUESTION 141
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 145
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 147
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 152
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 157
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 162
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 165
Business Continuity planning includes other plans such as:

A. Incident/disaster recovery plan
B. Business recovery and resumption plans
C. Contingency plan
D. All the above

Answer: D

NEW QUESTION 167
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: D

NEW QUESTION 170
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 172
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 174
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 176
......

Relate Links

Contact us