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 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 2
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 3
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 4
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 5
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

Answer: A

NEW QUESTION 6
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 7
Computer viruses are malicious software programs that infect computers and corrupt or delete the data on them. Identify the virus type that specifically infects Microsoft Word files?

A. Micro Virus
B. File Infector
C. Macro Virus
D. Boot Sector virus

Answer: C

NEW QUESTION 8
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 9
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 10
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 10
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 13
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 14
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 16
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 19
The correct sequence of Incident Response and Handling is:

A. Incident Identification, recording, initial response, communication and containment
B. Incident Identification, initial response, communication, recording and containment
C. Incident Identification, communication, recording, initial response and containment
D. Incident Identification, recording, initial response, containment and communication

Answer: A

NEW QUESTION 22
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 25
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 30
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

Answer: A

NEW QUESTION 31
Incident Response Plan requires

A. Financial and Management support
B. Expert team composition
C. Resources
D. All the above

Answer: D

NEW QUESTION 34
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 35
CSIRT can be implemented at:

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

Answer: D

NEW QUESTION 38
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

Answer: C

NEW QUESTION 41
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 45
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 47
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 51
The Malicious code that is installed on the computer without user's knowledge to acquire information from the user's machine and send it to the attacker who can access it remotely is called:

A. Spyware
B. Logic Bomb
C. Trojan
D. Worm

Answer: A

NEW QUESTION 53
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 57
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 61
Which of the following is NOT one of the common techniques used to detect Insider threats:

A. Spotting an increase in their performance
B. Observing employee tardiness and unexplained absenteeism
C. Observing employee sick leaves
D. Spotting conflicts with supervisors and coworkers

Answer: A

NEW QUESTION 66
Which of the following is NOT one of the techniques used to respond to insider threats:

A. Placing malicious users in quarantine network, so that attack cannot be spread
B. Preventing malicious users from accessing unclassified information
C. Disabling the computer systems from network connection
D. Blocking malicious user accounts

Answer: B

NEW QUESTION 68
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 72
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 77
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 80
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 83
Insiders may be:

A. Ignorant employees
B. Carless administrators
C. Disgruntled staff members
D. All the above

Answer: D

NEW QUESTION 84
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

Answer: B

NEW QUESTION 89
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 92
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 93
Electronic evidence may reside in the following:

A. Data Files
B. Backup tapes
C. Other media sources
D. All the above

Answer: D

NEW QUESTION 94
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 96
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 98
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 102
The steps followed to recover computer systems after an incident are:

A. System restoration, validation, operation and monitoring
B. System restoration, operation, validation, and monitoring
C. System monitoring, validation, operation and restoration
D. System validation, restoration, operation and monitoring

Answer: A

NEW QUESTION 106

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 107
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. Constitutional/ Legitimate
B. Illegal/ illegitimate
C. Unethical
D. None of the above

Answer: A

NEW QUESTION 109
......

Relate Links

100% Pass Your 212-89 Exam with Exambible Prep Materials

https://www.exambible.com/212-89-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/