



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

Which of the following terms may be defined as “a measure of possible inability to achieve a goal, objective, or target within a defined security, cost plan and technical limitations that adversely affects the organization’s operation and revenues?”

- A. Risk
- B. Vulnerability
- C. Threat
- D. Incident Response

Answer: A

NEW QUESTION 2

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 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

An incident recovery plan is a statement of actions that should be taken before, during or after an incident. Identify which of the following is NOT an objective of the incident recovery plan?

- A. Creating new business processes to maintain profitability after incident
- B. Providing a standard for testing the recovery plan
- C. Avoiding the legal liabilities arising due to incident
- D. Providing assurance that systems are reliable

Answer: A

NEW QUESTION 5

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 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

Answer: C

NEW QUESTION 7

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 8

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 9

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 10

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 10

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 12

If the loss anticipated is greater than the agreed upon threshold; the organization will:

- A. Accept the risk
- B. Mitigate the risk
- C. Accept the risk but after management approval
- D. Do nothing

Answer: B

NEW QUESTION 14

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 18

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 20

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 23

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 24

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 25

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 28

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 32

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 35

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

Answer: A

NEW QUESTION 39

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 40

_____ record(s) user's typing.

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

Answer: A

NEW QUESTION 41

_____ attach(es) to files

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

Answer: C

NEW QUESTION 44

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 46

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 51

Which of the following may be considered as insider threat(s):

- A. An employee having no clashes with supervisors and coworkers
- B. Disgruntled system administrators
- C. An employee who gets an annual 7% salary raise
- D. An employee with an insignificant technical literacy and business process knowledge

Answer: B

NEW QUESTION 55

Lack of forensic readiness may result in:

- A. Loss of clients thereby damaging the organization's reputation
- B. System downtime
- C. Data manipulation, deletion, and theft
- D. All the above

Answer: D

NEW QUESTION 56

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 59

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 60

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 61

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 64

.....

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/>