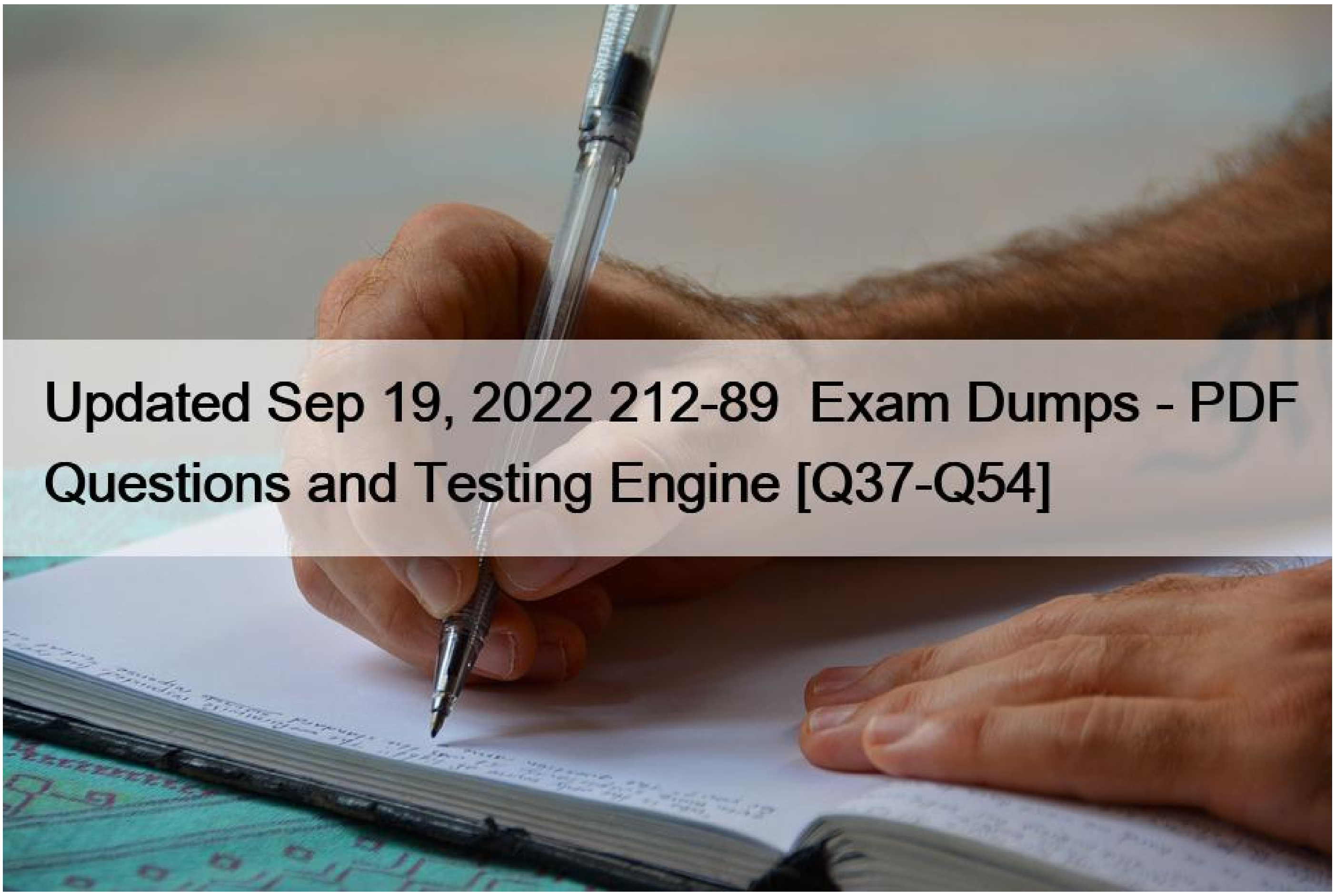
Updated Sep 19, 2022 212-89 Exam Dumps - PDF Questions and Testing Engine [Q37-Q54



Updated Sep 19, 2022 212-89 Exam Dumps - PDF Questions and Testing Engine
New (2022) EC-COUNCIL 212-89 Exam Dumps

Who Is ECIH 212-89 Test Intended for?

This exam is designed for the individuals who work as incident handlers, penetration testers, risk assessment administrators, cyber forensic investigators, system administrators, firewall administrators, IT professionals, IT managers, etc. Those who want to pursue their career in incident response and handling can also apply for this certification exam as it will enhance your skills and abilities to perform tasks in the ECIH sector.

Recommended Revision Books

Now, let's focus on the must-have revision books that Amazon kindly proffers: EC Council Certified Incident Handler A Complete Guide - 2021 Edition Now, let's talk about this 2021 material **by the Art of Service - EC Council Certified Incident Handler Publishing.** Unlike many revision books that you will want to purchase to study for 212-89, this guide takes your training a notch higher by emphasizing the skills you should know in practical environments. Particularly, it provides the skills you need to define, design, create and implement a process that solves challenging security incidents. By studying using this revision material, you will understand how to diagnose and manage bothersome security incidents, implement the best practices & policies that are geared towards the organization's overall objectives, and integrate the latest concepts and processes into actual practice in line with the stipulated guidelines. Be ready to spend at least $100 to validate your skills using this material. **Practice Questions & Answers EC Council Certified Incident Handler (ECIH V2): ECCouncil 212-89**This is the ultimate solution if you are looking for valid and updated ECIH exam dumps and practice test questions for the actual 212-89 evaluation. **Phil Scott** has done an impressive job in putting together the latest question bank for the ECIH 212-89 exam using this book, with the help of which you will not only memorize the test details but also understand the crucial information you need to master regarding the latest updates. Get your copy from Amazon at only $14 and improve your knowledge as you prepare for the final test. **EC Council Certified Incident Handler Complete Guide - 2020 Edition**This is the definitive guide to the ECIH 212-89 exam covering all the concepts necessary. It costs about $90 from Amazon. Throughout this book, important questions are asked and detailed answers are given. For instance, what should you know to complete a successful operation? How should you perform a response exercise? Does your company have an official computer incident response plan? And most importantly, how do you protect your organization's systems from security incidents and maintain high-quality services every time? The author, **Gerardus Blokdyk**, uses his years of experience to craft a series of informative questions covering all aspects of the ECIH designation. There's no doubt any candidate will find this tool helpful in his/her certification prep journey, taking into consideration the detailed account it gives to all the topic areas. All in all, every purchase comes with the following tools: - A valid current edition of this book in PDF format;- An Excel dashboard for self-assessment;- Detailed ECIH checklists;- Highly informative project management checklists.

NEW QUESTION 37

Which of the following is NOT a digital forensic analysis tool:
* Access Data FTK
* EAR/ Pilar
* Guidance Software EnCase Forensic
* Helix

NEW QUESTION 38

The service organization that provides 24&#215;7 computer security incident response services to any user, company, government agency, or organization is known as:
* Computer Security Incident Response Team CSIRT
* Security Operations Center SOC
* Digital Forensics Examiner
* Vulnerability Assessor

NEW QUESTION 39

Incidents are reported in order to:
* Provide stronger protection for systems and data
* Deal properly with legal issues
* Be prepared for handling future incidents
* All the above

NEW QUESTION 40

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?
* Incident recording
* Reporting
* Containment
* Identification

NEW QUESTION 41

Which of the following incident recovery testing methods works by creating a mock disaster, like fire to identify

the reaction of the procedures that are implemented to handle such situations?
* Scenario testing
* Facility testing
* Live walk-through testing
* Procedure testing

NEW QUESTION 42

The policy that defines which set of events needs to be logged in order to capture and review the important

data in a timely manner is known as:
* Audit trail policy
* Logging policy
* Documentation policy
* Evidence Collection policy

NEW QUESTION 43

Digital evidence must:
* Be Authentic, complete and reliable
* Not prove the attackers actions
* Be Volatile
* Cast doubt on the authenticity and veracity of the evidence

NEW QUESTION 44

Insiders understand corporate business functions. What is the correct sequence of activities performed by

Insiders to damage company assets:
* Gain privileged access, install malware then activate
* Install malware, gain privileged access, then activate
* Gain privileged access, activate and install malware
* Activate malware, gain privileged access then install malware

NEW QUESTION 45

An insider threat response plan help san organization minimize the damage caused by malicious insiders.

One of the approaches to mitigate these threats is setting up controls from the human resources department.

Which of the following guidelines can the human resources department use?
* Monitor and secure the organization&#8217;s physical environment.
* Disable the default administrative account to ensure accountability.
* Access granted to users should be documented and vetted by a supervisor.
* Implement a person-to-person rule to secure the backup process and physical media.

NEW QUESTION 46

A computer virus hoax is a message warning the recipient of an on-existent computer virus threat. The message is usually a chain e-mail that tells the recipient to forward it to everyone they know.

Which of the following is not a symptom of virus hoax message?
* The message warns to delete certain files if the user does not take appropriate action
* The message from a known email id is caught by SPAM filters due to change in filter settings
* The message prompts the end user to forward it to his/her email contact list and gain monetary benefits in doing so
* The message prompts the user to install Anti-virus

NEW QUESTION 47

Bob, an incident responder at CyberTech Solutions, is investigating a cybercrime attack that occurred in the client company. He acquired the evidence data, preserved it, and started performing analysis on the acquired evidentiary data to identify the source of the crime and the culprit behind the incident. Identify the forensic investigation phase in which Bob is currently in.
* Post-investigation phase
* Pre-investigation phase
* Vulnerability assessment phase
* Investigation phase

NEW QUESTION 48

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?
* An insider intentionally deleting files from a workstation
* An attacker redirecting user to a malicious website and infects his system with Trojan
* An attacker infecting a machine to launch a DDoS attack
* An attacker using email with malicious code to infect internal workstation

NEW QUESTION 49

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:
* Trojans
* Zombies
* Spyware
* Worms

NEW QUESTION 50

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?
* Links the appropriate technology to the incident to ensure that the foundation&#8217;s offices are returned to normal operations as quickly as possible
* Links the groups that are affected by the incidents, such as legal, human resources, different business areas and management
* Applies the appropriate technology and tries to eradicate and recover from the incident
* Focuses on the incident and handles it from management and technical point of view

NEW QUESTION 51

Malicious downloads that result from malicious office documents being manipulated are caused by which of the following?
* Impersonation
* Click jacking
* Macro abuse
* Registry key manipulation

NEW QUESTION 52

Farheen is an incident responder at reputed IT Firm based in Florida. Farheen was asked to investigate a recent cybercrime faced by the organization. As part of this process, she collected static data from a victim system. She used dd, a command line tool, to perform forensic duplication to obtain an NTFS image of the original disk. She created a sector-by-sector mirror imaging of the disk and saved the output image file as image.dd. Identify the static data collection process step performed by Farheen while collecting static data.
* Physical presentation
* Administrative consideration
* System preservation
* Comparison

NEW QUESTION 53

Which of the following is an attack that occurs when a malicious program causes a user&#8217;s browser to perform man unwanted action on a trusted site for which the user is currently authenticated?
* Insecure direct object references
* SQL injection
* Cross-site request forgery
* Cross-site scripting

NEW QUESTION 54

One of the goals of CSIRT is to manage security problems by taking a certain approach towards the customers&#8217; 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:
* Interactive approach
* Introductive approach
* Proactive approach
* Qualitative approach

Career Path

If you want to pursue your career beyond the EC-Council ECIH certification, there are many paths that you can choose from. First of all, you can become a Licensed Security Consultant. In this case, you can opt for the EC-Council Licensed Penetration Tester (LPT) certificate. Alternatively, you can go for the trainer path. Then you should apply for the Certified EC-Council Instructor (CEI)

program.
If your goal is to become a multidisciplinary expert, earning the Computer Hacking Forensics Investigator (CHFI) or Certified Application Security Engineer (CASE) certifications will be an ideal choice for you. Finally, you can consider attaining a master's cybersecurity degree. For this purpose, go for the EC-Council University Master of Security Sciences (MSS) program. By obtaining the ECIH certificate, you have already automatically earned 3 credits for this degree.

Updated Verified Pass 212-89 Exam - Real Questions and Answers: https://www.dumpsmaterials.com/212-89-real-torrent.html]