2024 Free EC-COUNCIL 212-89 Exam Files Downloaded Instantly [Q72-Q91

2024 Free EC-COUNCIL 212-89 Exam Files Downloaded Instantly Pass EC-COUNCIL 212-89 exam Dumps 100 Pass Guarantee With Latest Demo

There are advantages of Getting the ECCouncil 212-89 Certification Exam

ECIH certification will be confident and stand different from others as their skills are more trained than non-certified professionals.ECIH certification Certification provides practical experience to candidates from all the aspects to be a proficient worker in the organization.ECIH certification is distinguished among competitors. ECIH certification can give them an edge at that time easily when candidates appear for a job interview employers seek to notify something which differentiates the individual to another.ECIH certification has more useful and relevant networks that help them in setting career goals for themselves. ECIH certification networks provide them with the right career direction than non certified usually are unable to get.

QUESTION 72

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

QUESTION 73

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

QUESTION 74

Which of the following is a standard framework that provides recommendations for implementing information security controls for organizations that initiate, implement, or maintain information security management systems (ISMSs)?
* ISO/IEC 27002
* ISO/IEC 27035
* PCI DSS
* RFC 219G

ISO/IEC 27002 is a standard that provides best practice recommendations on information security controls for use by those responsible for initiating, implementing, or maintaining information security management systems (ISMSs). It covers areas such as risk assessment, human resource security, operational security, and communications security, among others, providing a framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS. ISO/IEC 27035 pertains to information security incident management, PCI DSS (Payment Card Industry Data Security Standard) deals with the security of cardholder data, and RFC 2196 is a guide for computer security incident response teams (CSIRTs), not a standard for implementing ISMSs.References:The ECIH v3 curriculum includes the study of various standards and frameworks that support information security management and governance, including ISO/IEC 27002, highlighting its role in guiding organizations in implementing effective security controls.

QUESTION 75

Bob, an incident responder at CyberTech Solutions, is investigating a cybercrime attack occurred in the client company. He acquired the evidence data, preserved it, and started performing analysis on 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.
* Vulnerability assessment phase
* Post-investigation phase
* Pre-investigation phase
* Investigation phas

QUESTION 76

Alex is an incident handler in QWERTY Company. He identified that an attacker created a backdoor inside the company’s network by installing a fake AP inside a firewall. Which of the following attack types did the attacker use?
* AP misconfiguration

* Wardriving
* Rogue access point
* Ad hoc associations

QUESTION 77

Shiela is working at night as an incident handler. During a shift, servers were affected by a massive cyberattack. After she classified and prioritized the incident, she must report the incident, obtain necessary permissions, and perform other incident response functions. What list should she check to notify other responsible personnel?
* HR log book
* Point of contact
* Email list
* Phone number list
In the context of incident handling, the “point of contact” list is essential for ensuring that Sheila, the incident handler working at night, can quickly notify the responsible personnel within the organization about the cyberattack. This list typically includes the contact information of key stakeholders and decision-makers who need to be informed about security incidents, allowing for timely communication, decision-making, and response coordination.

References:Incident Handler (ECIH v3) courses and study guides stress the importance of having a well-maintained point of contact list as part of an organization’s incident response plan to facilitate efficient and effective communication during and after cybersecurity incidents.

QUESTION 78

Rose is an incident-handler and is responsible for detecting and eliminating any kind of scanning attempts over the network by malicious threat actors. Rose uses Wire shark to sniff the network and detect any malicious activities going on.

Which of the following Wireshark filters can be used by her to detect TCP Xmas scan attempt by the attacker?
* tcp.flags.reset== 1
* tcp.flags==0X 000
* tcp.flags==0X 029
* tcp.dstport== 7

QUESTION 79

Which of the following is a volatile evidence collecting tool?
* Netstat
* HashTool
* FTK Images
* ProDiscover Forensics
Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface (and network protocol) statistics. It is considered a volatile evidence collecting tool because it gathers information that exists in the system’s memory, which is lost upon shutdown or reboot. This makes it invaluable for collecting evidence of active connections and processes that are present at the time of the incident response but does not persistently store data that can be recovered later. This contrasts with tools like FTK Imager or ProDiscover Forensics, which are used for acquiring digital evidence in a non-volatile manner, such as disk imaging, and HashTool, which is used for validating the integrity of collected digital evidence through hashing.

References:EC-Council’s ECIH v3 materials include discussions on the importance of volatile and non-volatile evidence, emphasizing tools like Netstat for their role in the immediate collection

QUESTION 80

You are talking to a colleague who Is deciding what information they should include in their organization’s logs to help with security auditing. Which of the following items should you tell them to NOT log?
* Timestamp
* Session ID
* Source IP eddross
* userid

Logging User IDs (D) can pose privacy concerns and may conflict with regulations such as the General Data Protection Regulation (GDPR), which emphasizes the protection of personal data and privacy. Therefore, while logging details such as Timestamps, Session IDs, and Source IP addresses are essential for security auditing to track when events occur, who is initiating sessions, and from where, care must be taken with User IDs. The handling of personally identifiable information (PII) must comply with privacy laws and organizational policies to safeguard individual privacy rights.

References:Security best practices and compliance frameworks discussed in the ECIH v3 certification guide incident handlers on what information should and should not be logged, emphasizing the need to balance security auditing requirements with privacy and regulatory obligations.

QUESTION 81

Nervous Nat often sends emails with screenshots of what he thinks are serious incidents, but they always tum out to be false positives. Today, he sends another screenshot, suspecting a nation-state attack. As usual, you go through your list of questions, check your resources for information to determine whether the screenshot shows a real attack, and determine the condition of your network.

Which step of IR did you just perform?
* Recovery
* Detection and analysis (or identification)
* Remediation
* Preparation

QUESTION 82

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

QUESTION 83

Bob, an incident responder at CyberTech Solutions, is investigating a cybercrime attack occurred in the client company. He acquired the evidence data, preserved it, and started performing analysis on 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.
* Vulnerability assessment phase

* Post-investigation phase
* Pre-investigation phase
* Investigation phas

Bob is in the Investigation phase of the forensic investigation process. This phase involves the detailed examination and analysis of the collected evidence to identify the source of the crime and the perpetrator behind the incident. It is a crucial step that follows the acquisition and preservation of evidence, where the incident responder applies various techniques and methodologies to analyze the evidentiary data. This analysis aims to uncover how the cybercrime was committed, trace the activities of the culprit, and gather actionable intelligence to support legal actions and prevent future incidents.References:The ECIH v3 certification materials discuss the stages of a forensic investigation, emphasizing the investigation phase as the point at which the incident responder analyzes evidence to draw conclusions about the incident’s specifics.

QUESTION 84

A colleague wants to minimize their security responsibility because they are in a small organization. They are evaluating a new application that is offered in different forms. Which form would result in the least amount of responsibility for the colleague?

* On-prom installation
* saaS
* laaS
* PaaS

Software as a Service (SaaS) offers the least amount of security responsibility for the end-user or organization, as the service provider manages the underlying infrastructure, software maintenance, security patching, and updates. Choosing a SaaS application means the colleague’s organization would not be responsible for the physical servers, operating systems, or the application’s security configurations, making it the best option for minimizing their security responsibilities.

References:In the Certified Incident Handler (ECIH v3) course materials, the various cloud service models (IaaS, PaaS, SaaS) are discussed with a focus on their implications for security responsibilities and management.

QUESTION 85

Which of the following are malicious software programs that infect computers and corruptor delete the data on them?

* Trojans
* Worms
* Spyware
* Virus

QUESTION 86

Nervous Nat often sends emails with screenshots of what he thinks are serious incidents, but they always turn out to be false positives. Today, he sends another screenshot, suspecting a nation-state attack. As usual, you go through your list of questions, check your resources for information to determine whether the screenshot shows a real attack, and determine the condition of your network. Which step of IR did you just perform?

* Recovery
* Preparation
* Remediation
* Detection anc analysis (or identification)

QUESTION 87

Adam is an incident handler who intends to use DBCC LOG command to analyze a database and retrieve the active transaction log files for the specified database. The syntax of DBCC LOG command is DBCC LOG(,), where the output parameter specifies the

level of information an incident handler wants to retrieve. If Adam wants to retrieve the full information on each operation along with the hex dump of a current transaction row, which of the following output parameters should Adam use?
* 2
* 3
* 4
* 1
The DBCC LOG command is used in SQL Server environments to analyze the transaction log files of a database. It provides insights into the transactions that have occurred, which is crucial for forensic analysis in the event of an incident. The syntaxDBCC LOG(<database_name>, <output_level>)allows an incident handler to specify the level of detail they wish to retrieve from the log files. When an incident handler like Adam requires the full information on each operation along with the hex dump of the current transaction row, the output parameter should be set to 4. This level of output is the most verbose, providing comprehensive details about each transaction, including a hex dump which is essential for a deep forensic analysis. It helps in understanding the exact changes made by transactions, which can be pivotal in investigating incidents involving data manipulation or other unauthorized database activities.

References:EC-Council’s Certified Incident Handler (ECIH v3) program emphasizes the importance of understanding and utilizing various tools and commands for forensic analysis, including how to use the DBCC LOG command for transaction log analysis in SQL Server environments.

QUESTION 88

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:
* Computer Forensics
* Digital Forensic Analysis
* Forensic Readiness
* Digital Forensic Policy

QUESTION 89

Auser downloaded what appears to be genuine software. Unknown to her, when she installed the application, it executed code that provided an unauthorized remote attacker access to her computer. What type of malicious threat displays this characteristic?
* Backdoor
* Trojan
* Spyware
* Virus
The scenario described is characteristic of a Trojan. A Trojan is a type of malware that disguises itself as legitimate software but performs malicious actions once installed. Unlike viruses, which can replicate themselves, or worms, which can spread across networks on theirown, Trojans rely on the guise of legitimacy to trick users into initiating their execution. In this case, the user believed they were downloading and installing genuine software, but the reality was that the application contained a Trojan. The malicious code executed upon installation provided unauthorized remote access to the user’s computer, which could be used by an attacker to control the system, steal data, install additional malware, or carry out other malicious activities.

Trojans can come in many forms and can be used to achieve a wide range of malicious objectives, making them a versatile and dangerous type of cyber threat. The deceptive nature of Trojans, exploiting the trust users have in what appears to be legitimate software, is what makes them particularly effective and widespread.

References:The ECIH v3 curriculum from EC-Council thoroughly covers different types of malware, including Trojans, and emphasizes understanding their behavior, methods of infection, and strategies for prevention and response.

QUESTION 90

Shall y, an incident handler, works for a company named Texas Pvt.Ltd.based in Florida. She was asked to work on an incident response plan. As part of the plan, she decided to enhance and improve the security infrastructure of the enterprise. She incorporated a security strategy that allows security professionals to use several protection layers throughout their information system. Owing to multiple-layer protection, this security strategy assists in preventing direct attacks against the organization’s information system as a break in one layer only leads the attacker to the next layer.

Which of the following security strategies did Shall y incorporate in the incident response plan?
* Defense-in-depth
* Three-way handshake
* Covert channels
* Exponential back off algorithm

QUESTION 91

Elizabeth, who works for OBC organization as an incident responder, is assessing the risks to the organizational security. As part of the assessment process, she is calculating the probability of a threat source exploiting an existing system vulnerability. Which of the following risk assessment steps is Elizabeth currently in?
* Vulnerability identification
* Impact analysis
* Likelihood analysis
* System characterization

In the risk assessment process, calculating the probability that a threat source will exploit an existing system vulnerability is known as likelihood analysis. This step involves evaluating how probable it is that the organization’s vulnerabilities can be exploited by potential threats, considering various factors such as the nature of the vulnerability, the presence and capability of threat actors, and the effectiveness of current controls. Elizabeth’s task of assessing the probability of exploitation is crucial for understanding the risk level associated with different vulnerabilities and for prioritizing risk mitigation efforts based on the likelihood of occurrence.

References:The Certified Incident Handler (ECIH v3) program by EC-Council includes detailed discussions on risk assessment methodologies, where likelihood analysis is highlighted as a key component in evaluating risks to organizational security.

The ECIH v2 certification is an important credential for IT security professionals who are involved in incident handling and response. EC Council Certified Incident Handler (ECIH v3) certification demonstrates that the candidate has the knowledge, skills, and abilities to effectively manage and respond to security incidents. It also provides employers with a way to evaluate the skills of their IT security staff, and to ensure that they have the necessary expertise to protect their organization's critical assets.

Read Online 212-89 Test Practice Test Questions Exam Dumps: https://www.dumpleader.com/212-89_exam.html]