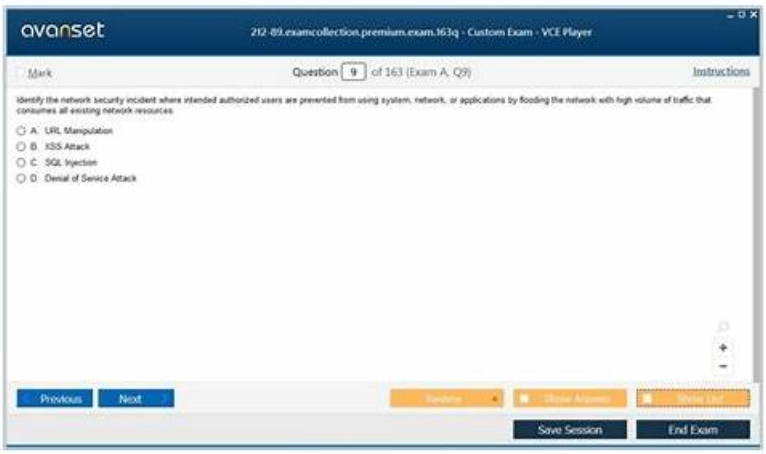
212-89 Test Vce Free - Updated 212-89 CBT



DOWNLOAD the newest PassTestking 212-89 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=152Y-dX5FpMTYRRSc9S9CDVMCRjcglR8w

After taking a bird's eye view of applicants' issues, PassTestking has decided to provide them with the real 212-89 Questions. These EC-COUNCIL 212-89 dumps pdf is according to the new and updated syllabus so they can prepare for EC Council Certified Incident Handler (ECIH v3) (212-89) certification anywhere, anytime, with ease. A team of professionals has made the product of PassTestking after much hard work with their complete potential so the candidates can prepare for EC Council Certified Incident Handler (ECIH v3) (212-89) practice test in a short time.

What Are Domains Covered by ECIH Test?

Overall, this certification exam has nine domains that have a specific weightage in the official validation. The candidates who take this exam need to master the following topics:

- Application-level incidents 8%;
- Insider threats 7%;
- Mobile & network incidents 16%;
- Email security incidents 10%;
- Incident handling and response 16%;

The ECIH certification exam is a multiple-choice exam that is administered by EC-Council. 212-89 Exam consists of 50 questions and has a duration of 120 minutes. 212-89 exam is designed to test an individual's knowledge and understanding of various cybersecurity concepts, including incident handling and response, network security, and malware analysis.

The EC-Council Certified Incident Handler (ECIH) certification is a globally recognized certification that validates an individual's knowledge and skills in incident handling and response. The ECIH certification program is designed to provide individuals with the necessary skills to detect, respond, and resolve computer security incidents in a systematic and efficient manner. EC Council Certified Incident Handler (ECIH v3) certification program is based on the latest industry standards and best practices, and is intended for professionals who are responsible for managing and responding to security incidents.

>> 212-89 Test Vce Free <<

212-89 Study Guide Practice Materials and 212-89 Actual Dumps and Torrent - PassTestking

212-89 Practice Material is from our company which made these 212-89 practice materials with accountability. And 212-89 Training Materials are efficient products. What is more, 212-89 Exam Prep is appropriate and respectable practice material. We know making progress and getting the certificate of 212-89 Training Materials will be a matter of course with the most professional experts in command of the newest and the most accurate knowledge in it. Our 212-89 exam prep has taken up a large part of market.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q78-Q83):

NEW QUESTION # 78
After a recent email attack, Harry is analyzing the incident to obtain important information related to the incident. While investigating the incident, he is trying to extract information such as sender identity, mail server, sender's IP address, location, and so on.
Which of the following tools Harry must use to perform this task?

- A. Yesware
- B. Clamwin
- C. Logly
- D. Sharp

Answer: A

Explanation:
Yesware is a tool primarily known for its email tracking capabilities, which can be useful for sales, marketing, and customer relationship management. However, in the context of investigating email attacks and analyzing incidents to extract details such as sender identity, mail server, sender's IP address, and location, a more appropriate tool would be one that specializes in analyzing and extracting detailed header information from emails, providing insights into the path an email took across the internet. While Yesware can provide data related to email interactions, it might not offer the depth of forensic analysis required for incident investigation.
Tools like email header analyzers, which are designed specifically for dissecting and interpreting email headers, would be more fitting. In the absence of a direct match from the given options, the description might imply a broader interpretation oftools like Yesware in context but traditionally, tools specifically designed for email forensics would be sought after for this task.
References:Understanding email headers and using tools to analyze them is an important part of email incident response, as discussed in cybersecurity training programs like ECIH v3 by EC-Council, which covers the methodologies for analyzing various types of cybersecurity incidents, including email-based threats.

NEW QUESTION # 79
The free, open source, TCP/IP protocol analyzer, sniffer and packet capturing utility standard across many industries and educational institutions is known as:

- A. nmap
- B. Cain & Able
- C. Wireshark
- D. Snort

Answer: C

NEW QUESTION # 80
Jason is setting up a computer forensics lab and must perform the following steps:
1. physical location and structural design considerations;
2. planning and budgeting;
3. work area considerations;
4. physical security recommendations;
5. forensic lab licensing;
6. human resource considerations.
Arrange these steps in the order of execution.

- A. 2->1->3->6->4->5
- B. 3->2->1->4->6->5
- C. 5->2->1->3->4->6
- D. 2->3->1->4->6->5

Answer: A

NEW QUESTION # 81

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. Damage to corporate reputation
- B. Psychological damage
- C. Lost productivity damage
- D. Loss of goodwill

Answer: C

NEW QUESTION # 82
Which of the following is defined as the identification of the boundaries of an IT system along with the resources and information that constitute the system?

- A. Control analysis
- B. Threat identification
- C. Vulnerability identification
- D. System characterization

Answer: D

NEW QUESTION # 83
.....

About the materials that relate to EC-COUNCIL 212-89 exam, many websites can offer the exam materials. But these websites can't guarantee the quality of the exam dumps, meanwhile when you fail the exam, they can't also give you FULL REFUND guarantee. Compared with common reference materials, PassTestking EC-COUNCIL 212-89 certification training materials is the tool that worth your use. With the help of PassTestking EC-COUNCIL 212-89 Real Questions and answers, you can absolutely well prepare for the exam and pass the exam with ease. If you want to great development in IT industry, you need to take IT certification exam. If you want to pass your IT certification test successfully, it is necessary for you to use PassTestking exam dumps.

www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, test.paisaaloan.com, Disposable vapes

P.S. Free & New 212-89 dumps are available on Google Drive shared by PassTestking: https://drive.google.com/open?id=152Y-dX5FpMTYRRSc9S9CDVMCRjcglR8w