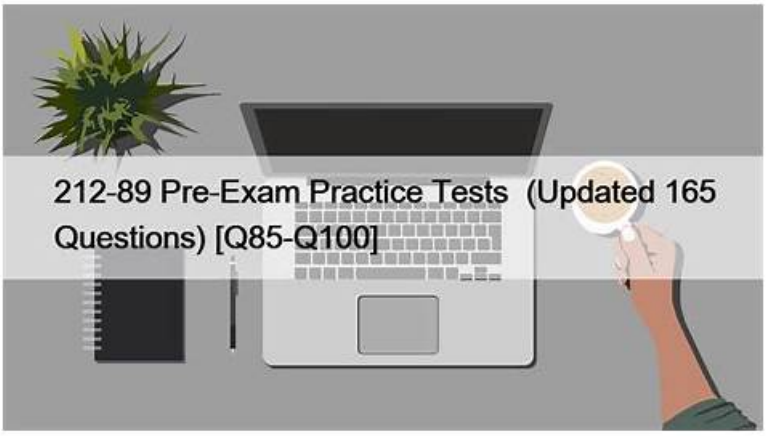
Pass-Sure Testing 212-89 Center - Updated Source of 212-89 Exam



What's more, part of that DumpsActual 212-89 dumps now are free: https://drive.google.com/open?id=1RnlpRSpBfV6TEVO-wqyTY8D9pvwr8uJ5

We provide you free demo with you to help you have a deeper understanding about 212-89 study materials. Free demo can be found in our website, and we recommend you to have a try before buying. Furthermore, 212-89 exam materials of us have the questions and answers, and you can have a convenient check of your answers after you finish practicing. We are pass guarantee and money back guarantee for your failure after purchasing 212-89 Study Materials. You just need to give your failure scanned and we will give you full refund. Choose us, and we can help you to pass the exam successfully.

The ECIH certification exam is a multiple-choice exam and consists of 100 questions. 212-89 Exam is two hours long, and candidates must score at least 70% to pass. 212-89 exam is available at Pearson VUE testing centers worldwide. Candidates can prepare for the exam by taking EC-Council's official training course, which covers all the topics tested in the certification exam.

>> Testing 212-89 Center <<

EC-COUNCIL 212-89 Exam Topics Pdf & Latest 212-89 Braindumps Pdf

The EC-COUNCIL 212-89 certification is one of the top-rated career advancement certifications in the market. This EC Council Certified Incident Handler (ECIH v3) (212-89) certification exam has been inspiring candidates since its beginning. Over this long time period, thousands of 212-89 exam candidates have passed their EC Council Certified Incident Handler (ECIH v3) (212-89) certification exam and now they are doing jobs in the world's top brands. The DumpsActual 212-89 Dumps will provide you with everything that you need to learn, prepare and pass the challenging Network Security Specialist 212-89 exam with flying colors. You must try DumpsActual 212-89 exam questions today.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q40-Q45):

NEW QUESTION # 40
Bran is an incident handler who is assessing the network of the organization. He wants to detect ping sweep attempts on the network using Wire shark.
Which of the following W re shark filters would Bran use to accomplish this task?

- A. icmp.redir_gw
- B. icmp.type== 8
- C. icmp.ident
- D. icmp.seq

Answer: B

NEW QUESTION # 41
Computer Forensics is the branch of forensic science in which legal evidence is found in any computer or any digital media device. Of the following, who is responsible for examining the evidence acquired and separating the useful evidence?

- A. Evidence Manager
- B. Evidence Supervisor
- C. Evidence Documenter
- D. Evidence Examiner/ Investigator

Answer: D

NEW QUESTION # 42
In which of the following phases of the incident handling and response (IH&R) process is the identified security incidents analyzed, validated, categorized, and prioritized?

- A. Incident triage
- B. Incident recording and assignment
- C. Containment
- D. Notification

Answer: A

Explanation:
Incident triage is the phase in the Incident Handling and Response (IH&R) process where identified security incidents are analyzed, validated, categorized, and prioritized. This step is crucial for determining the severity of incidents and deciding on the order in which they should be addressed. During triage, incident handlers assess the impact, urgency, and potential harm of an incident to prioritize their response efforts effectively.
This ensuresthat resources are allocated efficiently, and the most critical incidents are handled first. Incident recording and assignment involve logging incidents and assigning them to handlers, containment focuses on limiting the extent of damage, and notification involves informing stakeholders about the incident.References:The Incident Handler (ECIH v3) courses and study guides detail the IH&R process, emphasizing the importance of triage in managing and responding to security incidents effectively.

NEW QUESTION # 43
Employee monitoring tools are mostly used by employers to find which of the following?

- A. Malicious insider threats
- B. Stolen credentials
- C. Conspiracies
- D. Lost registry keys

Answer: A

Explanation:
Employee monitoring tools are primarily used by employers to detect and prevent malicious insider threats.
These tools can track activities such as data access, data exfiltration attempts, unauthorized actions, and other behaviors that could indicate malicious intent or pose a risk to the organization's security. While such tools may also incidentally uncover issues like lost registry keys, conspiracies, or stolen credentials, their main purpose is to safeguard against insiders who might misuse their access to harm the organization, steal data, sabotage systems, or engage in espionage.References:ECIH v3 study materials cover various security measures and tools that organizations can use to protect against insider threats, emphasizing the role ofmonitoring in detecting and responding to malicious activities by insiders.

NEW QUESTION # 44
Rachel, a first responder, finds a smartphone in an executive's office that is powered ON and actively displaying a messaging app with potentially incriminating information. She avoids locking the screen or turning off the device, photographs the current display, and collects its charging cable. She then safely packages the device and ensures it is kept charged during transport. What principle is Rachel applying in her evidence handling approach?

- A. Forcing a factory reset to preserve evidence.
- B. Extracting deleted messages from the cache.
- C. Preserving screen-based digital evidence.
- D. Allowing device shutdown to save battery.

Answer: C

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
Rachel is applying the forensic principle of preserving volatile and screen-based digital evidence, which is a core concept in the ECIH First Response and Digital Forensics modules. When a mobile device is powered on and unlocked, the data visible on the screen-such as messages, timestamps, sender details, and session states-constitutes volatile evidence that may be lost permanently if the device locks, reboots, or powers off.
ECIH guidance instructs first responders to document the live state of a device before any interaction that could alter its condition. Photographing the screen captures evidence that may not be recoverable later due to encryption or session expiration. Maintaining power ensures the device does not enter a locked or encrypted state during transport.
Option A refers to forensic analysis, not first response. Option C would destroy evidence and violates forensic principles. Option D risks loss of volatile data.
Preserving screen-based evidence ensures integrity, admissibility, and continuity of evidence, making Option B correct.

NEW QUESTION # 45
......

id=1RnlpRSpBfV6TEVO-wqyTY8D9pvwr8uJ5