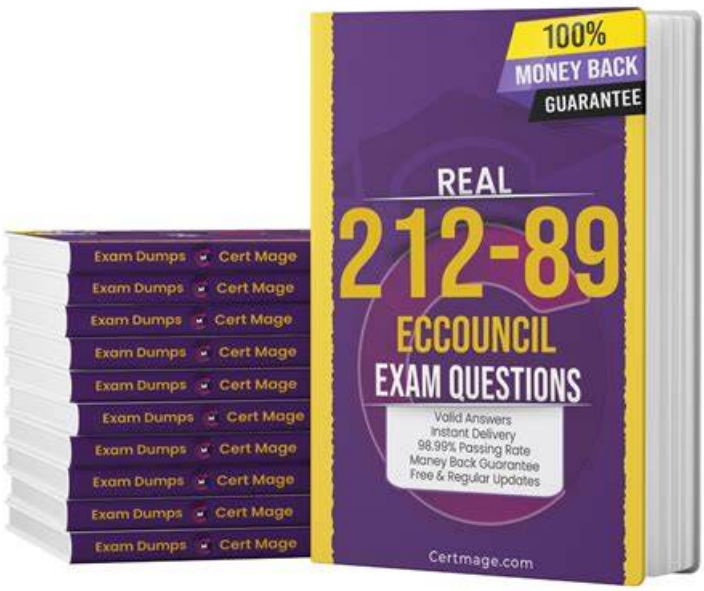
Exam 212-89 Tests, Latest 212-89 Dumps



P.S. Free & New 212-89 dumps are available on Google Drive shared by PassLeaderVCE: https://drive.google.com/open?id=1ynggBuMUumRAYR19vKRNqxyo18xJ-OAN

PassLeaderVCE are supposed to help you pass the exam smoothly. Do not worry about channels to the best EC Council Certified Incident Handler (ECIH v3) 212-89 study materials because we are the exactly best vendor in this field for more than ten years. And so many exam candidates admire our generosity of the EC-COUNCIL 212-89 Practice Questions offering help for them. Up to now, no one has ever challenged our leading position of this area.

EC-COUNCIL 212-89 Exam Syllabus Topics:

Section	Weight	Objectives
Handling and Responding to Malware Incidents	18%	- Malware incident response procedures • 1. Isolating infected systems • 2. Removing malware and recovering - Types of malware and attack vectors • 1. Viruses, worms, trojans, ransomware • 2. Social engineering and phishing - Malware analysis techniques • 1. Identifying malware behavior • 2. Static and dynamic analysis

Post-Incident Activities and Reporting	7%	- Incident documentation and reporting • 1. Creating incident reports • 2. Communicating with stakeholders - Lessons learned and improvement • 1. Conducting post-incident reviews • 2. Updating policies and procedures
Handling and Responding to Endpoint Security Incidents	13%	- Endpoint incident response • 1. Investigating compromised endpoints • 2. Remediation and hardening - Endpoint threats and vulnerabilities • 1. Unpatched systems, misconfigurations • 2. Endpoint attack vectors
Handling and Responding to Network Security Incidents	15%	- Network attacks and threats • 1. Network intrusion techniques • 2. DDoS, man-in-the-middle, SQL injection - Response and mitigation strategies • 1. Blocking malicious traffic • 2. Securing network infrastructure - Network incident detection and analysis • 1. Using IDS/IPS tools • 2. Monitoring network traffic
Handling and Responding to Cloud Security Incidents	10%	- Cloud computing concepts and risks • 1. Cloud service models and deployment models • 2. Cloud-specific threats - Cloud incident response process • 1. Responding in multi-tenant environments • 2. Detecting and analyzing cloud incidents - Legal and ethical aspects • 1. Privacy and data protection • 2. Compliance requirements
Introduction to Incident Handling and Response	12%	- Fundamentals of incident handling and response • 1. Incident response lifecycle • 2. Key concepts and terminology

Incident Handling Process	15%	- Preparation phase • 1. Developing incident response policies • 2. Building incident response teams - Containment, eradication, and recovery • 1. Strategies for containment • 2. Eradicating threats and vulnerabilities • 3. Restoring systems and services - Detection and analysis phase • 1. Classifying and prioritizing incidents • 2. Identifying security incidents

New Release EC-COUNCIL 212-89 Dumps [2026]

We often ask, what is the purpose of learning? Why should we study? Why did you study for 212-89exam so long? As many people think that, even if one day we forget the formula for the area of a triangle, we can still live very well, but if it were not for the knowledge of learning 212-89 Exam and try to obtain certification, how can we have the opportunity to good to future life? So, the examination is necessary, only to get the test 212-89 certification, get a certificate, to prove better us, to pave the way for our future life.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q313-Q318):

NEW QUESTION # 313
Adam is an attacker who along with his team launched multiple attacks on target organization for financial benefits. Worried about getting caught, he decided to forge his identity. To do so, he created a new identity by obtaining information from different victims. Identify the type of identity theft Adam has performed.

- A. Medical identity theft
- B. Social identity theft
- C. Tax identity theft
- D. Synthetic identity theft

Answer: D

Explanation:
Synthetic identity theft is a type of fraud where the perpetrator combines real (often stolen) and fake information to create a new identity. This can include combining a real social security number with a fictitious name, or other variations that result in an identity that is not entirely real but has elements that can pass through verification processes. In the scenario described, Adam is creating a new identity using information from different victims,which is characteristic of synthetic identity theft. This type of fraud is particularly challenging to detect and counter because it does not directly impersonate a single real individual but creates a plausible new identity that can be used to open accounts, obtain credit, and conduct transactions that can be financially beneficial to the attacker.
References:The concept and techniques of synthetic identity theft are covered in detail in the Incident Handler (ECIH v3) curriculum, where the focus is on identifying, understanding, and mitigating various forms of identity theft, including synthetic identity theft, as part of incident response activities.

NEW QUESTION # 314
An IoT device deployed in a smart city infrastructure project begins transmitting data at an unusually high rate, signaling a potential security compromise. This device is part of a critical system that monitors traffic flow and controls street lighting, making unauthorized access or manipulation a significant concern for public safety and urban efficiency. What should be the first action taken by the smart city's incident response team to handle this IoT-based security incident effectively?

- A. Immediately isolate the compromised IoT device from the network to prevent further unauthorized activity.
- B. Launch a city-wide campaign to raise awareness about the security risks associated with IoT devices.
- C. Collaborate with the device manufacturer to investigate the cause of the unusual data transmission.
- D. Update the firmware of all IoT devices within the smart city infrastructure as a precautionary measure.

Answer: A

Explanation:
In IoT and OT environments, the ECIH curriculum emphasizes that containment is the highest first-response priority, especially when public safety and critical services are involved. The abnormal data transmission strongly suggests compromise, and allowing the device to remain connected risks lateral movement, data exfiltration, and operational disruption.
Option C is correct because immediate isolation of the affected IoT device prevents further unauthorized communication while preserving the system's current state for forensic analysis.
Isolation limits the blast radius without unnecessarily disrupting the entire infrastructure.
Option A introduces risk by changing system states during an active incident. Option B is preventive and not an incident response action. Option D is appropriate after containment but not before.
Thus, isolating the compromised device aligns with ECIH endpoint and IoT incident handling principles.

NEW QUESTION # 315
Which of the following port scanning techniques involves resetting the TCP connection between client and server abruptly before completion of the three-way handshake signals, making the connection half-open?

- A. Full connect scan
- B. Stealth scan
- C. Null scan
- D. Xmas scan

Answer: B

Explanation:
The port scanning technique that involves resetting the TCP connection between the client and server abruptly before the completion of the three-way handshake, thereby leaving the connection half-open, is known as a Stealth scan (also referred to as a SYN scan). This technique allows the scanner to inquire about the status of a port without establishing a full TCP connection, making the scan less detectible to intrusion detection systems and lesslikely to be logged by the target. It's a method used to discreetly discover open ports on a target machine without establishing a full connection that would be visible in logs.References:ECIH v3 certification materials often cover different types of network scanning techniques, including Stealth scans, explaining their methodologies, purposes, and how they can be detected or mitigated.

NEW QUESTION # 316
After a web application attack, HealthFirst traced the breach to an insecure Direct Object Reference (IDOR) vulnerability. They want to patch it and fortify the app. What should be their primary action?

- A. Conduct regular penetration testing on the application.
- B. Introduce a WAF with default rules.
- C. Implement role-based access controls (RBAC) for data access.
- D. Encrypt all data at rest and in transit.

Answer: C

Explanation:
Explanation (fixing IDOR correctly):
IDOR is fundamentally an authorization flaw: the application exposes object identifiers (IDs) and fails to enforce that the requesting user is allowed to access that object. The primary remediation is to implement robust authorization checks-commonly RBAC (C) plus object-level access control-so every request verifies user identity and privileges against the requested resource.
(A) WAFs can help with certain injection patterns, but default WAF rules rarely fix logical authorization flaws like IDOR. A WAF also risks false positives and doesn't replace secure design. (B) pen testing is important for assurance, but it's not the primary patch; it helps validate the fix later. (D) encryption protects confidentiality in transit/at rest, but it does not prevent an authenticated user from accessing another user's records if authorization checks are missing.
Therefore (C) is the correct first-line fix: enforce authorization server-side, avoid predictable identifiers, and ensure access control is

consistently applied across all endpoints (including APIs).

NEW QUESTION # 317
Matt is an incident handler working for one of the largest social network companies, which was affected by malware. According to the company's reporting timeframe guidelines, a malware incident should be reported within 1 h of discovery/detection after its spread across the company.
Which category does this incident belong to?

- A. CAT 4
- B. CAT 2
- C. CAT 3
- D. CAT 1

Answer: C

NEW QUESTION # 318
.....

There are more opportunities for possessing with a certification, and our 212-89 study tool is the greatest resource to get a leg up on your competition. When it comes to our time-tested 212-89 latest practice materials, for one thing, we have a professional team contains a lot of experts who have devoted themselves to development of our 212-89 Exam Guide, thus we feel confident enough under the intensely competitive market. For another thing, conforming to the real exam our 212-89 study tool has the ability to catch the core knowledge. So our customers can pass the exam with ease.