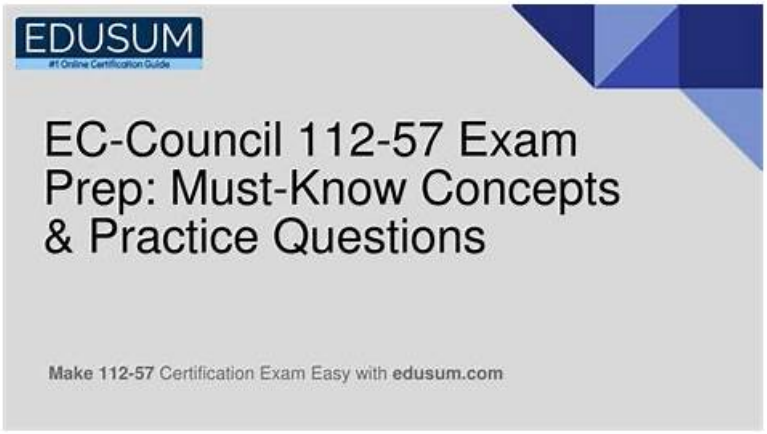
Enhance Your Preparation with EC-COUNCIL 112-57 Practice Test Engine



BTW, DOWNLOAD part of itPass4sure 112-57 dumps from Cloud Storage: https://drive.google.com/open?id=1y_KZGa17wgV-0RmnuTvRljB2Df0REauh

In fact, a number of qualifying exams and qualifications will improve your confidence and sense of accomplishment to some extent, so our 112-57 test practice question can be your new target. When we get into the job, our 112-57 training materials may bring you a bright career prospect. Companies need employees who can create more value for the company, but your ability to work directly proves your value. Our 112-57 Certification guide can help you improve your ability to work in the shortest amount of time, thereby surpassing other colleagues in your company, for more promotion opportunities and space for development. Believe it or not that up to you, our 112-57 training materials are powerful and useful, it can solve all your stress and difficulties in reviewing the 112-57 exams.

EC-COUNCIL 112-57 Exam Syllabus Topics:

Topic	Details
Topic 1	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.
Topic 2	• Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications.
Topic 3	• Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic.
Topic 4	• Understanding Hard Disks and File Systems: This module covers disk structures, types of storage drives, and operating system boot processes. It also explains how investigators analyze file systems and recover deleted data.
Topic 5	• Linux and Mac Forensics: This module explains forensic analysis techniques for Linux and Mac systems. It focuses on analyzing system data, file systems, and memory to recover digital evidence.
Topic 6	• Defeating Anti-forensics Techniques: This module discusses anti-forensic methods used to hide or destroy evidence. It also explains techniques investigators use to detect hidden data and recover deleted or protected information.

>> Exam 112-57 Guide Materials <<

112-57 Simulated Study Material & 112-57 Vce Training File & 112-57 Valid

Test Questions

itPass4sure EC-COUNCIL 112-57 practice test software is the answer if you want to score higher in the EC-COUNCIL 112-57 exam and achieve your academic goals. Don't let the EC-Council Digital Forensics Essentials (DFE) (112-57) certification exam stress you out! Prepare with our EC-Council Digital Forensics Essentials (DFE) (112-57) exam dumps and boost your confidence in the EC-Council Digital Forensics Essentials (DFE) (112-57) exam. We guarantee your road toward success by helping you prepare for the EC-Council Digital Forensics Essentials (DFE) (112-57) certification exam. Use the best itPass4sure EC-COUNCIL 112-57 practice questions to pass your EC-Council Digital Forensics Essentials (DFE) (112-57) exam with flying colors!

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q74-Q79):

NEW QUESTION # 74
Bob, a forensic specialist at a newly established NGO, discovered a security loophole in the NGO's web application, which unintentionally reveals early enrolled NGO members' biodata to attackers. Bob immediately employed a content filtering mechanism to protect all the NGO's data sources and prevent further damage.
Identify the web application threat identified by Bob in the above scenario.

- A. Cookie poisoning
- B. Authentication hijacking
- C. Buffer overflow
- D. Information leakage

Answer: D

Explanation:
The scenario describes a web application thatunintentionally reveals sensitive member biodatato attackers.
This is a classic case ofinformation leakage, where confidential or private data becomes exposed due to poor access control, improper output handling, verbose error messages, misconfigured endpoints, insecure direct object references, or unintended exposure through pages, APIs, backups, or logs. In forensic and web security documentation, information leakage is defined by theunauthorized disclosure of data, even if the attacker does not alter the system. The key indicator here is that the application is "revealing" biodata-meaning confidentiality is breached.
Bob's response-using acontent filtering mechanism-also aligns with mitigating data exposure. Content filtering can prevent sensitive fields from being returned, mask personally identifiable information, restrict responses based on user role, and sanitize outputs before they leave the server.
The other options do not match the described impact.Buffer overflowis a low-level memory corruption vulnerability, typically associated with native code execution rather than accidental biodata exposure.
Authentication hijackinginvolves taking over sessions/credentials, andcookie poisoninginvolves manipulating cookie values to gain privileges or alter behavior-neither is explicitly indicated. Therefore, the identified threat isInformation leakage (B).

NEW QUESTION # 75
James, a forensic specialist, was appointed to investigate an incident in an organization. As part of the investigation, James is attempting to identify whether any external storage devices are connected to the internal systems. For this purpose, he employed a utility to capture the list of all devices connected to the local machine and removed suspicious devices.
Identify the tool employed by James in the above scenario.

- A. ProcDump
- B. ESEDatabaseView
- C. DriveLetterView
- D. PromiscDetect

Answer: C

NEW QUESTION # 76
Which of the following layers of the TCP/IP model serves as the backbone for data flow between two devices in a network and enables peer entities on the source and destination devices to communicate with each other?

- A. Transport layer
- B. Network access layer
- C. Internet layer
- D. Application layer

Answer: A

Explanation:
In the TCP/IP model, theTransport layeris responsible forend-to-end communication between peer entitieson the source and destination systems. "Peer entities" here refers to the corresponding transport components (and the applications that use them) on two different hosts communicating across a network. This layer forms the practical "backbone" of host-to-host data flow because it provides the mechanisms that allow data to be deliveredfrom one endpoint process to another endpoint processreliably or efficiently, depending on the protocol used.
The Transport layer includes protocols such asTCPandUDP. TCP supports connection-oriented communication with sequencing, acknowledgments, retransmissions, and flow control-features that are fundamental when reconstructing sessions during network forensic investigations (e.g., rebuilding a file transfer or a web session). UDP provides connectionless delivery used by many services where speed is preferred over guaranteed delivery, which is also significant in investigations of DNS, streaming, or certain malware communications.
By contrast, theInternet layerfocuses on logical addressing and routing (IP), theNetwork access layerhandles local delivery on the physical/link network, and theApplication layerprovides user-facing protocols.
Therefore, the layer enabling peer communication between endpoints is theTransport layer (C).

NEW QUESTION # 77
An organization decided to strengthen the security of its network by studying and analyzing the behavior of attackers. For this purpose, Steven, a security analyst, was instructed to deploy a device to bait attackers.
Steven selected a solution that appears to contain very useful information to lure attackers and find their locations and techniques.
Identify the type of device deployed by Steven in the above scenario.

- A. Honeypot
- B. Router
- C. Intrusion detection system
- D. Firewall

Answer: A

Explanation:
Ahoneypotis a deliberately deployed decoy system or service designed toattract attackersby appearing valuable or vulnerable, thereby enabling defenders to observe malicious behavior in a controlled manner.
Digital forensics and incident response references describe honeypots as tools forthreat intelligence and evidence collection, because they can record interaction details such as connection sources, exploited services, commands executed, malware dropped, and attempted privilege escalation. This directly matches the scenario: Steven deployed something that "appears to contain very useful information" tolure attackersand help identify theirlocations and techniques. Honeypots are typically instrumented with extensive logging and monitoring, making them especially useful for building timelines, extracting indicators of compromise, and understanding adversary tactics, techniques, and procedures.
The other options do not align with the "bait attackers" goal. AnIDSprimarily detects and alerts on suspicious activity but is not intended to impersonate a valuable target. Afirewallenforces access control rules to block /allow traffic, not entice attackers. Arouterforwards packets and provides network connectivity; it is not a deception platform.
Therefore, the device type described is aHoneypot (C).

NEW QUESTION # 78
A government organization decided to establish a computer forensics lab to perform transparent investigation processes on highly sensitive cases. The organization also decided to establish strong physical security around the premises of the forensics lab.
Which of the following security measures helps the organization in providing strong physical security to the forensics lab?

- A. Shield workstations from transmitting electromagnetic signals
- B. Never keep the lab under surveillance
- C. Never place fire extinguishers in and outside the lab
- D. Do not maintain a log register at the entrance of the lab

Answer: A

Explanation:
Forensics labs handling highly sensitive investigations must protect evidence confidentiality and prevent unauthorized disclosure. Strong physical security includes not only access control and surveillance, but also protections againstelectromagnetic (EM) emanationrisks. Computers and displays can unintentionally emit electromagnetic signals that, under certain conditions, may be intercepted and reconstructed to reveal sensitive information (for example, case notes, recovered evidence content, or credentials). Digital forensics lab design guidance recognizes this as a real threat in high-sensitivity environments and recommendsEM shielding / TEMPEST-style controlswhere appropriate. Shielding workstations reduces the chance of data leakage through side-channel interception and helps ensure that confidential investigative activities cannot be monitored from outside controlled areas.
The other options directly weaken physical security and safety. Fire extinguishers are required for facility safety and risk management, so "never place" them is unsafe and contrary to secure lab standards. Not maintaining an entrance log register undermines chain-of-custody support and accountability by removing a basic access auditing mechanism. "Never keep the lab under surveillance" removes a core deterrent and detection control for unauthorized entry, evidence tampering, and theft. Therefore, shielding workstations from transmitting electromagnetic signals is the only option thatstrengthensphysical security for a sensitive forensics lab.

NEW QUESTION # 79
.....

P.S. Free & New 112-57 dumps are available on Google Drive shared by itPass4sure: https://drive.google.com/open?id=1y_KZGa17wgV-0RmnuTvRljB2Df0REauh