2026 112-57–100% Free Reliable Test Bootcamp | Professional EC-Council Digital Forensics Essentials (DFE) Study Material

DOWNLOAD the newest CertkingdomPDF 112-57 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1SzflB0Zn3vN13hgVRDVdqT8hjiDjY5AO

We have free demo of our 112-57 exam questions offering the latest catalogue and brief contents for your information on the website, if you do not have thorough understanding of our 112-57 study materials. Many exam candidates build long-term relation with our company on the basis of our high quality 112-57 Guide engine. And our 112-57 training braindumps have became their best assistant on the way to pass the exam.

Since it is obvious that different people have different preferences, we have prepared three kinds of different versions of our 112-57 practice test, namely, PDF version, Online App version and software version. Last but not least, our customers can accumulate exam experience as well as improving their exam skills in the mock exam. Tthere is no limitation on our software version of 112-57 practice materials about how many computers our customers used to download it, but it can only be operated under the Windows operation system. I strongly believe that you can find the version you want in multiple choices of our 112-57 practice test.

>> 112-57 Reliable Test Bootcamp <<

112-57 Study Material - 112-57 Upgrade Dumps

Through CertkingdomPDF you can get the latest EC-COUNCIL certification 112-57 exam practice questions and answers. Please purchase it earlier, it can help you pass your first time to participate in the EC-COUNCIL Certification 112-57 Exam. Currently, CertkingdomPDF uniquely has the latest EC-COUNCIL certification 112-57 exam exam practice questions and answers.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q43-Q48):

NEW QUESTION # 43
Given below are different steps involved in event correlation.
Event masking
Event aggregation
Root cause analysis
Event filtering
Identify the correct sequence of steps involved in event correlation.

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

Answer: C

Explanation:
In event correlation (as applied in SOC/SIEM-driven investigations), the workflow typically starts byreducing complexityandnormalizing what "one incident" looks likebefore attempting conclusions about causality.Event aggregation (2)is performed early to combine multiple low-level, related events (for example repeated authentication failures, repeated firewall denies, or multiple IDS hits for the same signature) into higher-level
"grouped" records. This prevents analysts from treating every raw log line as a separate incident and makes correlation computationally and operationally feasible.
Next,event masking (1)suppresses events that are already known to be irrelevant or repetitive in a way that does not add investigative value (for example, routine scheduled scans, approved admin tools, or duplicate alerts already represented in the aggregated set). After masking,event filtering (4)further removes remaining noise using rules, thresholds, whitelists, time windows, or relevance criteria (scope, asset criticality, and known-benign sources), leaving a cleaner dataset that represents probable security-relevant activity.
Only after the dataset is consolidated and noise-reduced doesroot cause analysis (3)become reliable, because RCA depends on a clear chain of correlated events to identify the initiating action and propagation path.
Hence the correct sequence is2 # 1 # 4 # 3 (Option B).

NEW QUESTION # 44
Below is the syntax of a command-line utility that displays active TCP connections and ports on which the computer is listening.
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
Identify the netstat parameter that displays active TCP connections and includes the process ID (PID) for each connection.

- A. [-s]
- B. [-n]
- C. [-a]
- D. [-o]

Answer: D

Explanation:
In Windows forensics and incident response, investigators often need to linknetwork activity(remote IPs, ports, connection states) to theresponsible processto determine whether traffic is legitimate or associated with malware, unauthorized tools, or data exfiltration.
The Windowsnetstatutility can enumerate current TCP connections and listening ports, but the key flag that enables attribution to a running program is-o. The-o parameter instructs netstat to include theOwning Process ID (PID)with each connection or listening socket.
Once the PID is known, examiners can correlate it with process listings (e.g., Task Manager,tasklist, memory forensics output) to identify the executable name, path, user context, and parent process-critical steps in reconstructing attacker behavior and persistence.
The other options do not provide PID mapping:-nshows addresses and ports in numeric form (useful for speed and to avoid DNS lookups),-adisplays all connections and listening ports but without PID attribution by itself, and-sshows protocol statistics rather than per-connection ownership. Therefore, the parameter that shows active connectionsandincludes the PID for each is[-o](Option C).

NEW QUESTION # 45
Below are the various steps involved in forensic readiness planning.
Keep an incident response team ready to review the incident and preserve the evidence.
Create a process for documenting the procedure.
Identify the potential evidence required for an incident.
Determine the sources of evidence.
Establish a legal advisory board to guide the investigation process.
Identify if the incident requires full or formal investigation.
Establish a policy for securely handling and storing the collected evidence.
Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption.
Identify the correct sequence of steps involved in forensic readiness planning.

- A. 3-->4-->8-->7-->6-->2-->5-->1
- B. 1-->2-->3-->4-->5-->6-->7-->8
- C. 3-->1-->4-->5-->8-->2-->6-->7
- D. 2-->3-->1-->4-->6-->5-->7-->8

Answer: A

Explanation:
Forensic readiness planning focuses on ensuring an organization canlegally, efficiently, and reliablycollect usable digital evidence before an incident occurs. The planning sequence typically begins by definingwhat evidence would be neededto support likely incidents (3) and then mappingwhere that evidence residesacross systems, services, logs, endpoints, and network components (4). Once evidence needs and sources are known, readiness requires alegally compliant extraction pathwaythat minimizes business disruption and prevents evidence contamination (8). After defining extraction, an organization must formalizesecure handling and storage policies(chain of custody, access control, retention, integrity protection) so collected evidence remains admissible and trustworthy (7).
With those foundations in place, the organization can define decision criteria forwhen an event becomes a formal investigationand triggers deeper forensic procedures (6). A structureddocumentation processis then set so actions taken during acquisition and analysis are repeatable and defensible (2). Governance is reinforced by establishinglegal oversight/advisory supportto ensure compliance with jurisdictional requirements and internal policy (5). Finally, the plan is operationalized by ensuring anincident response team is preparedto preserve evidence promptly when incidents occur (1). Hence,3#4#8#7#6#2#5#1is the correct sequence.

NEW QUESTION # 46
Given below is a regex signature used by security professionals for detecting an XSS attack:
/((%3C)|<)[