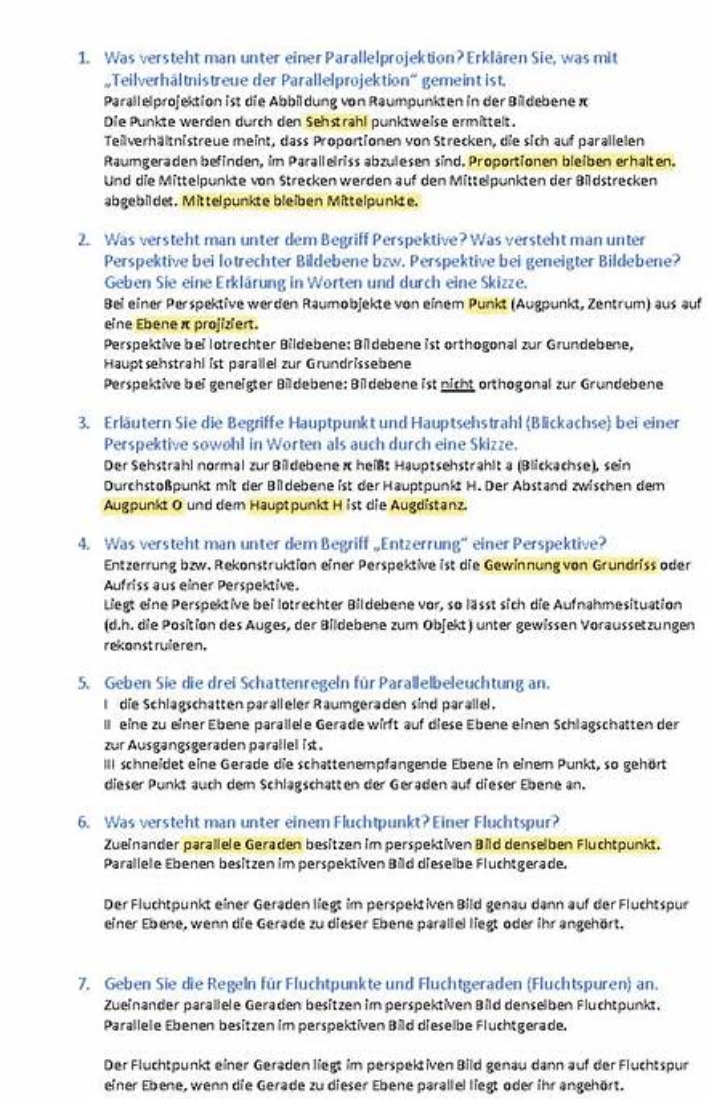
112-57 Deutsche Prüfungsfragen, 112-57 Testengine



1. Was versteht man unter einer Parallelprojektion? Erklären Sie, was mit „Teilverhältnistreue der Parallelprojektion" gemeint ist.
Parallelprojektion ist die Abbildung von Raumpunkten in der Bildebene π
Die Punkte werden durch den Sehstrahl punktweise ermittelt.
Teilverhältnistreue meint, dass Proportionen von Strecken, die sich auf parallelen Raumgeraden befinden, im Parallelriss abzulesen sind. Proportionen bleiben erhalten.
Und die Mittelpunkte von Strecken werden auf den Mittelpunkten der Bildstrecken abgebildet. Mittelpunkte bleiben Mittelpunkte.

2. Was versteht man unter dem Begriff Perspektive? Was versteht man unter Perspektive bei lotrechter Bildebene bzw. Perspektive bei geneigter Bildebene? Geben Sie eine Erklärung in Worten und durch eine Skizze.
Bei einer Perspektive werden Raumobjekte von einem Punkt (Augpunkt, Zentrum) aus auf eine Ebene π projiziert.
Perspektive bei lotrechter Bildebene: Bildebene ist orthogonal zur Grundebene, Hauptsehstrahl ist parallel zur Grundrissebene
Perspektive bei geneigter Bildebene: Bildebene ist nicht orthogonal zur Grundebene

3. Erläutern Sie die Begriffe Hauptpunkt und Hauptsehstrahl (Blickachse) bei einer Perspektive sowohl in Worten als auch durch eine Skizze.
Der Sehstrahl normal zur Bildebene π heißt Hauptsehstrahl a (Blickachse), sein Durchstoßpunkt mit der Bildebene ist der Hauptpunkt H. Der Abstand zwischen dem Augpunkt O und dem Hauptpunkt H ist die Augdistanz.

4. Was versteht man unter dem Begriff „Entzerrung" einer Perspektive?
Entzerrung bzw. Rekonstruktion einer Perspektive ist die Gewinnung von Grundriss oder Aufriss aus einer Perspektive.
Liegt eine Perspektive bei lotrechter Bildebene vor, so lässt sich die Aufnahmesituation (d.h. die Position des Auges, der Bildebene zum Objekt) unter gewissen Voraussetzungen rekonstruieren.

5. Geben Sie die drei Schattenregeln für Parallelbeleuchtung an.
I die Schlagschatten paralleler Raumgeraden sind parallel.
II eine zu einer Ebene parallele Gerade wirft auf diese Ebene einen Schlagschatten der zur Ausgangsgeraden parallel ist.
III schneidet eine Gerade die schattenempfangende Ebene in einem Punkt, so gehört dieser Punkt auch dem Schlagschatten der Geraden auf dieser Ebene an.

6. Was versteht man unter einem Fluchtpunkt? Einer Fluchtspur?
Zueinander parallele Geraden besitzen im perspektiven Bild denselben Fluchtpunkt.
Parallele Ebenen besitzen im perspektiven Bild dieselbe Fluchtgerade.

Der Fluchtpunkt einer Geraden liegt im perspektiven Bild genau dann auf der Fluchtspur einer Ebene, wenn die Gerade zu dieser Ebene parallel liegt oder ihr angehört.

7. Geben Sie die Regeln für Fluchtpunkte und Fluchtgeraden (Fluchtspuren) an.
Zueinander parallele Geraden besitzen im perspektiven Bild denselben Fluchtpunkt.
Parallele Ebenen besitzen im perspektiven Bild dieselbe Fluchtgerade.

Der Fluchtpunkt einer Geraden liegt im perspektiven Bild genau dann auf der Fluchtspur einer Ebene, wenn die Gerade zu dieser Ebene parallel liegt oder ihr angehört.

Ea ist Traum der Angestellten, sich in der IT-Branche engagieren zu können, die EC-COUNCIL 112-57 Zertifizierungsprüfung zu bestehen. Wenn Sie Ihren Traum verwirklichen wollen, brauchen Sie nur fachliche Ausbildung zu wählen. ZertFragen ist eine fachliche Website, die Schulungsunterlagen zur EC-COUNCIL 112-57 Zertifizierung bietet. Wählen Sie ZertFragen. Und wir versprechen, dass Sie den Erfolg erlangen und Ihren Traum verwirklichen , egal welches hohes Ziel Sie anstreben, können.

EC-COUNCIL 112-57 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Computer Forensics Investigation Process: This module explains the phases of the forensic investigation process, including pre-investigation, investigation, and post-investigation. It also covers evidence integrity methods such as hashing and disk imaging.
Thema 2	• Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications.

Thema 3	• Dark Web Forensics: This module explains the investigation of dark web activities, including analyzing artifacts related to the Tor browser and identifying dark web usage on systems.
Thema 4	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.
Thema 5	• Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence.
Thema 6	• Computer Forensics Fundamentals: This module introduces the core concepts of computer forensics, including digital evidence, forensic readiness, and the role of investigators. It also explains legal and compliance requirements involved in forensic investigations.
Thema 7	• Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic.
Thema 8	• 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.

Die anspruchsvolle 112-57 echte Prüfungsfragen von uns garantiert Ihre bessere Berufsaussichten!

Die Testaufgaben von EC-COUNCIL 112-57 Zertifizierungsprüfung aus ZertFragen sind durch die Praxis getestet, daher sind sie zur Zeit das gründlichste, das genauste und das neueste Produkt auf dem Markt. Unser ZertFragen bietet Ihnen präzise Lehrbücher und Erfahrungen, die auf umfangreichern Erfahungen und der realen Welt basieren, was Ihnen verspricht, dass Sie in kürzester Zeit die Zertifizierungsprüfung von EC-COUNCIL 112-57 bestehen können. Nach dem Kauf unserer Produkte werden Sie einjährige Aktualisierung genießen.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) 112-57 Prüfungsfragen mit Lösungen (Q49-Q54):

49. Frage
Below are the elements included in the order of volatility for a typical computing system as per the RFC 3227 guidelines for evidence collection and archiving.
Archival media
Remote logging and monitoring data related to the target system
Routing table, process table, kernel statistics, and memory
Registers and processor cache
Physical configuration and network topology
Disk or other storage media
Temporary system files
Identify the correct sequence of order of volatility from the most to least volatile for a typical system.

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

Antwort: C

Begründung:
RFC 3227's "order of volatility" principle guides responders to collect themost perishableevidence first because some data can disappear immediately when power is lost, processes terminate, or the system state changes during response actions. The most volatile items areCPU registers and processor cache (4)because they change continuously at instruction speed and are lost instantly

on shutdown or context switching. Next arerouting table, process table, kernel statistics, and memory (3)because live RAM contents and active system tables can change within seconds and are lost if the machine is powered off or rebooted.
After volatile memory,temporary system files (7)are collected because they are frequently overwritten or cleaned by the OS, users, or malware. Then comesdisk or other storage media (6)which is more persistent but still subject to modification, log rotation, and overwriting through normal activity; hence imaging should occur before extensive interaction.
Less volatile still areremote logging and monitoring data (2)since they may persist off-host, but can be rotated or altered by retention policies.Physical configuration and network topology (5)generally changes less frequently and can often be re-documented later.
Finally,archival media (1)is the least volatile because it is typically write-once or preserved storage. Thus the correct sequence is4#3#7#6#2#5#1 (Option B).

50. Frage
Bob, a network specialist in an organization, is attempting to identify malicious activities in the network. In this process, Bob analyzed specific data that provided him a summary of a conversation between two network devices, including a source IP and source port, a destination IP and destination port, the duration of the conversation, and the information shared during the conversation.
Which of the following types of network-based evidence was collected by Bob in the above scenario?

- A. Session data
- B. Statistical data
- C. Alert data
- D. Full content data

Antwort: A

Begründung:
The description matchessession data, often calledflow records(for example, NetFlow/IPFIX-style evidence).
In network forensics, session/flow evidence summarizes a communication "conversation" between two endpoints using the5-tuple(source IP, source port, destination IP, destination port, and protocol) and typically addsstart/end time or duration,bytes/packets sent, and sometimes directionality. This allows an investigator to reconstructwho talked to whom, when, and for how long, even when packet payloads are unavailable (because of encryption, storage limits, or privacy constraints).
"Full content data" refers to complete packet captures (PCAP) containing payload bytes; that is far more detailed and would include the actual transmitted content, not just a summary. "Statistical data" is broader aggregate metrics (overall bandwidth trends, interface counters) and generally lacks per-conversation attribution. "Alert data" comes from IDS/IPS/SIEM detections and represents triggered events or signatures, not a neutral conversation summary.
Because Bob's evidence contains per-connection identifiers (IPs/ports) and conversation duration-typical of flow/session summaries-the correct evidence type isSession data (C).

51. Frage
Benoy, a security professional at an organization, extracted Apache access log entries to view critical information about all the operations performed on a web server. The Apache access log extracted by Benoy is given below:
"10.10.10.10 - Jason [17/Aug/2019:00:12:34 +0300] "GET /images/content/bg_body_1.jpg HTTP/1.0" 500 1458"
Identify the HTTP status code in the Apache access log entry above that indicates the response was successful.

- A. 0
- B. 1.0
- C. +0300
- D. 1

Antwort: A

Begründung:
In the Apache Combined/Custom access log format, the value immediately after the quoted request (here," GET ... HTTP/1.0") is theHTTP status codereturned by the server. In the provided entry, that field is500.
From a forensic analysis standpoint, recognizing field positions matters because investigators correlate client IPs, timestamps, requested resources, and server outcomes to reconstruct attack timelines and identify failed exploitation attempts or misconfigurations.
It is important to note thatsuccessful HTTP responses are typically in the 2xx range, most commonly200 (OK), while3xxindicates redirects,4xxindicates client-side errors (such as 404 Not Found), and5xxindicates server-side failures. Specifically,500represents

anInternal Server Error, meaning the server encountered an unexpected condition and could not fulfill the request successfully.
The other options are not HTTP status codes in this entry:+0300is the timezone offset in the timestamp,1.0is the HTTP protocol version, and2019is part of the date. Therefore, the only HTTP status code present-and the correct choice among the options-is500 (B), even though it reflects an error rather than success.

52. Frage
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. 2-->4-->3-->1
- B. 1-->3-->2-->4
- C. 1-->3-->4-->2
- D. 2-->1-->4-->3

Antwort: D

Begründung:
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).

53. Frage
An investigator wants to extract information about the status of the network interface cards (NICs) in an organization's Windows-based systems. Identify the command-line utility that can help the investigator detect the network status.

- A. ipconfig
- B. PsList
- C. ifconfig
- D. PsLoggedOn

Antwort: A

Begründung:
On Windows systems,ipconfigis the standard command-line utility used to display and troubleshootTCP/IP configurationand the operational status of network interfaces. From a forensic and incident-response perspective, it helps investigators quickly identify whether a NIC is enabled and configured, and it reveals key network parameters tied to "network status," such as theassigned IPv4/IPv6 addresses,subnet mask,default gateway, andDNS servers. Using variants likeipconfig /all, responders can also capture adapter-specific metadata includingMAC address (physical address), DHCP enablement, DHCP server, lease timestamps, and interface descriptions-useful for correlating an endpoint to switch-port logs, DHCP logs, and network monitoring data. This is often part of live triage because it documents the system's current connectivity and routing context at the time of seizure or investigation.
The other options are not appropriate for NIC status:PsLoggedOnreports logged-on users, andPsListenumerates running processes-both are Sysinternals tools focused on user/process state rather than network interface configuration.ifconfigis a UNIX/Linux command (and not the primary Windows utility), so it would not be the correct choice for Windows-based systems.
Therefore,ipconfig (A)is correct.

54. Frage

.....

Das Expertenteam von ZertFragen nutzt ihre Erfahrungen und Kenntnisse aus, um die Schulungsunterlagen zur EC-COUNCIL 112-57 Zertifizierungsprüfung zu bearbeiten. Unsere Schulungsunterlagen zur EC-COUNCIL 112-57 Zertifizierungsprüfung sind bei den Kunden sehr beliebt. Das sind die Ergebnisse der fleißigen Experten-Teams. Diese Simulationsfragen und Antworten sind von guter Qualität. Und die Ähnlichkeit beträgt über 95%. Sie sind eher zuverlässig. Wenn Sie die Trainingsinstrumente von ZertFragen benutzen, können Sie 100% die EC-COUNCIL 112-57 (EC-Council Digital Forensics Essentials (DFE)) Zertifizierungsprüfung bestehen.

112-57 Testengine: https://www.zertfragen.com/112-57_prufung.html

- 112-57 Mit Hilfe von uns können Sie bedeutendes Zertifikat der 112-57 einfach erhalten! □ Geben Sie ➥ www.zertfragen.com □ ein und suchen Sie nach kostenloser Download von ▹ 112-57 ◃ □112-57 Quizfragen Und Antworten
- 112-57 Schulungsangebot, 112-57 Testing Engine, EC-Council Digital Forensics Essentials (DFE) Trainingsunterlagen □ Sie müssen nur zu { www.itzert.com } gehen um nach kostenloser Download von { 112-57 } zu suchen □112-57 Zertifizierungsprüfung
- Hohe Qualität von 112-57 Prüfung und Antworten □ Erhalten Sie den kostenlosen Download von ✔ 112-57 □✔□ mühelos über { www.pass4test.de } □112-57 Pruefungssimulationen
- Kostenlos 112-57 dumps torrent - EC-COUNCIL 112-57 Prüfung prep - 112-57 examcollection braindumps □ Suchen Sie auf ➠ www.itzert.com □ nach kostenlosem Download von □ 112-57 □ □112-57 Antworten
- 112-57 Dumps und Test Überprüfungen sind die beste Wahl für Ihre EC-COUNCIL 112-57 Testvorbereitung □ Suchen Sie auf 《 www.echtefrage.top 》 nach { 112-57 } und erhalten Sie den kostenlosen Download mühelos □112-57 Pruefungssimulationen
- 112-57 PDF □ 112-57 Prüfungsunterlagen □ 112-57 Deutsch □ Erhalten Sie den kostenlosen Download von 「 112-57 」 mühelos über ▹ www.itzert.com ◃ □112-57 Examengine
- 112-57 Fragen Antworten □ 112-57 Zertifizierungsprüfung □ 112-57 Fragenpool □ Sie müssen nur zu ▸ www.zertfragen.com ◂ gehen um nach kostenloser Download von ▸ 112-57 ◂ zu suchen □112-57 Testking
- 112-57 PDF □ 112-57 Prüfungsmaterialien □ 112-57 Fragenpool □ Erhalten Sie den kostenlosen Download von □ 112-57 □ mühelos über 【 www.itzert.com 】 □112-57 Testking
- 112-57 Schulungsangebot, 112-57 Testing Engine, EC-Council Digital Forensics Essentials (DFE) Trainingsunterlagen □ Suchen Sie auf ▸ www.echtefrage.top ◂ nach ➥ 112-57 □ und erhalten Sie den kostenlosen Download mühelos □112-57 Quizfragen Und Antworten
- 112-57 Fragen Antworten □ 112-57 Zertifizierungsprüfung □ 112-57 Fragen Und Antworten □ Suchen Sie jetzt auf ▹ www.itzert.com ◃ nach ▸ 112-57 ◂ um den kostenlosen Download zu erhalten □112-57 Fragenpool
- Kostenlos 112-57 dumps torrent - EC-COUNCIL 112-57 Prüfung prep - 112-57 examcollection braindumps □ Suchen Sie einfach auf [www.zertsoft.com] nach kostenloser Download von ➡ 112-57 □□□ □112-57 Exam
- www.stes.tyc.edu.tw, hamzahudwp425372.blogginaway.com, a.zhhxq.cn, jayaxpvc647508.blogofchange.com, 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, phoenixavyt952035.answerblogs.com, 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, 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, darrenljhb275828.mywikiparty.com, tiannadblo478850.yourkwikimage.com, Disposable vapes