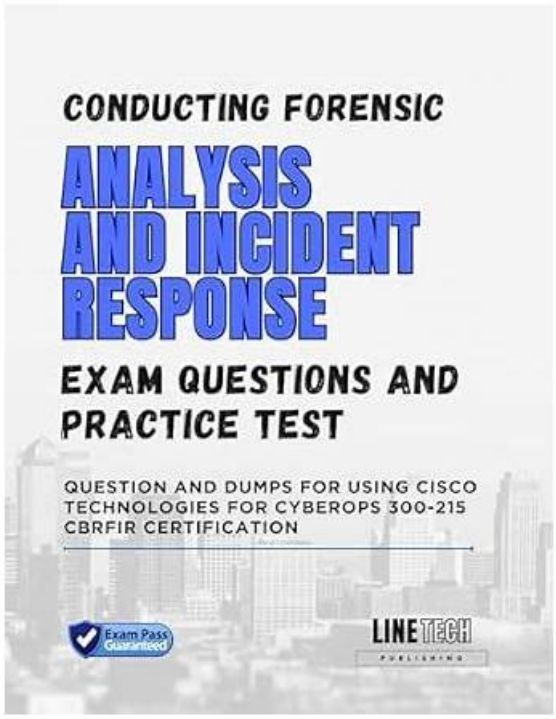
300-215 Prüfungsfragen, 300-215 Fragen und Antworten, Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps



2026 Die neuesten Zertpruefung 300-215 PDF-Versionen Prüfungsfragen und 300-215 Fragen und Antworten sind kostenlos verfügbar: https://drive.google.com/open?id=16VnbcAJwrSzBlLj16AAt3sq6ZZMLo_QK

Zertpruefung hat schon einen guten Ruf im vielen Zertifizierungsbranchen erhalten, weil wir die Testfagen, die Lernhilfe und Dumps zur 300-215 Zertifizierungsprüfung haben. Zur Zeit als der professionellster Anbieter im Internet bieten wir perfekten Kundenservice und einen einjährigen kostenlosen Update-Service. Wenn der Fragenkataloge zur Cisco 300-215 Zertifizierungsprüfung geändert werden, bieten wir den Kunden Schutz. Die Fragen zur 300-215 Zertifizierungsprüfung werden von den IT-Experten sorgfältig bearbeitet. Mit den Prüfungsmaterialien zur 300-215 Zertifizierungsprüfung von Zertpruefung wird Ihre Zukunft sicher glänzend sein.

Die Cisco 300-215 Zertifizierung wird in der IT-Branche hoch geschätzt und von vielen Arbeitgebern als wertvolle Referenz für Sicherheitsfachleute anerkannt. Die Zertifizierung demonstriert, dass der Inhaber über das Wissen und die Fähigkeiten verfügt, um Sicherheitsvorfälle mithilfe von Cisco-Technologien für CyberOps zu erkennen, zu untersuchen und darauf zu reagieren. Sie kann auch dazu beitragen, dass Fachleute ihre Karriere vorantreiben, indem sie neue Jobmöglichkeiten eröffnen und ihr Verdienstpotenzial erhöhen.

>> 300-215 Prüfungsaufgaben <<

Echte und neueste 300-215 Fragen und Antworten der Cisco 300-215 Zertifizierungsprüfung

Unser Zertpruefung ist eine fachliche Website, die Prüfungsmaterialien für zahlreiche Cisco 300-215 Zertifizierungsprüfung bieten. Unser Zertpruefung wird vielen IT-Fachleuten zum Berufsaufstieg verhelfen. Die Kraft unserer Eliteteams ist unglaublich. Sie können die Cisco 300-215 Examensübungen-und antworten teilweise als Probe umsonst herunterladen, so dass Sie die Glaubwürdigkeit vom Zertpruefung testen können.

Cisco Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps 300-215 Prüfungsfragen mit Lösungen (Q48-Q53):

48. Frage
Refer to the exhibit.
Which type of code is being used?

- A. VBScript
- B. BASH
- C. Python
- D. Shell

Antwort: C

Begründung:
The code in the exhibit is written in Python. Here's how we can confirm:
* The function definition uses Python syntax: def function_name(args):
* It uses the b64encode and decode functions - typical of Python's base64 module.
* Data structures such as dictionaries are used with curly braces (e.g., form_data = {entry1: enc1, ...}).
* The conditional syntax uses "if r.status_code == 200:" which is Pythonic.
* The request object "r = post(...)" and use of headers show standard use of the Python requests library.
This type of script is typical in exfiltration scenarios where encoded information is sent via a web form (in this case Google Forms), bypassing detection systems.
Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on "Working with Malware and Exploit Scripts," which includes analysis of obfuscated and encoded scripts written in Python used for data exfiltration or C2 communication.

49. Frage
Refer to the exhibit.
What should be determined from this Apache log?

- A. The private key does not match with the SSL certificate.
- B. A module named mod_ssl is needed to make SSL connections.
- C. The SSL traffic setup is improper
- D. The certificate file has been maliciously modified

Antwort: A

Begründung:
The error logs indicate multiplePKCS12andASN.1 decodingerrors, such as:
* PKCS12 routines:PKCS12_parse:mac verify failure
* rsa routines:old_rsa_priv_decode:RSA lib
* PKCS12 routines:PKCS12_key_gen_uni:malloc
These specific errors most commonly occur when:
* Theprivate key does not correspondto the certificate being used.
* There is amismatchbetween the public and private key pair required for SSL handshakes.
This is a well-documented condition in Apache SSL configuration issues and explicitly covered under TLS /SSL troubleshooting sections in cybersecurity operations contexts. The Cisco CyberOps guide also notes that SSL errors with key verification usually result from "improper key/certificate pairing" rather than file corruption or missing modules.
Thus, the correct answer is:
B). The private key does not match with the SSL certificate.

50. Frage
A security team received an alert of suspicious activity on a user's Internet browser. The user's anti-virus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address. Which two actions should be taken by the security analyst with the executable file for further analysis? (Choose two.)

- A. Analyze the Magic File type in Cisco Umbrella.
- B. Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).
- C. Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).
- D. Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).
- E. Evaluate the process activity in Cisco Umbrella.

Antwort: C,D

Begründung:
Explanation/Reference:

51. Frage
Refer to the exhibit.
Which element in this email is an indicator of attack?

- A. IP Address: 202.142.155.218
- B. subject: "Service Credit Card"
- C. attachment: "Card-Refund"
- D. content-Type: multipart/mixed

Antwort: C

Begründung:
According to the Cisco Certified CyberOps Associate guide (Chapter 5 - Identifying Attack Methods), attachments in emails-especially with file extensions like.xlsm-are high-risk indicators when analyzing suspicious or phishing emails. Malicious actors often use macro-enabled Excel files (.xlsm) as a payload delivery mechanism for malware or other exploits. These attachments are typically disguised as legitimate content such as refunds or invoices to trick the recipient into opening them.
The presence of"Card_Refund_18_6913.xlsm"is a strongIndicator of Compromise (IoC), as.xlsmfiles can contain VBA macros capable of executing malicious code. This matches exactly with examples provided in the study material discussing how macro-based payloads are delivered and recognized.
Hence,option Cis the most direct indicator of attack in this email.

52. Frage
An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing capability, which complicates the analysis process. Which two actions should the engineer take? (Choose two.)

- A. Replace the faulty CPU.
- B. Disconnect from the network.
- C. Take an image of the workstation.
- D. Format the workstation drives.
- E. Restore to a system recovery point.

Antwort: B,C

Begründung:
When suspicious activity is detected on a workstation, immediate steps need to be taken to preserve evidence and prevent further compromise:
* Disconnecting the system from the network (C)is crucial to stop potential exfiltration of data or ongoing communications with a command-and-control server. This isolation prevents further spread or damage while preserving the state of the compromised system for further investigation.
* Taking an image of the workstation (E)is part of the forensics acquisition process. It involves creating a bit-by-bit copy of the system's disk, which preserves all evidence in its current state. This allows for thorough forensic analysis without affecting the original

evidence.
These steps align with the best practices outlined in the incident response and forensics processes (as described in theCyberOps Technologies (CBRFIR) 300-215 study guide). Specifically, in theIdentification and Containmentphases of the incident response cycle, it's emphasized that isolating the system and preserving evidence through imaging are critical to ensuring both containment of the threat and successful forensic investigation.
Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Understanding the Security Incident Response Process, Identification and Containment Phases, page 102-104.

53. Frage
.....

Die Produkte von Zertpruefung werden den Kandidaten nicht nur helfen, die Cisco 300-215 Zertifizierrungsprüfung zu bestehen, sondern Ihnen auch einen einjährigen kostenlosen Update-Service bieten. Sie wird den Kunden die neuesten Cisco 300-215 Prüfungsmaterialien so schnell wie möglich liefern, so dass sich die Kunden über die Prüfungsinformationen zur Cisco 300-215 Zertifizierung informieren können. Deshalb ist Zertpruefung eine erstklassige Website. Außerdem ist der Service hier auch ausgezeichnet.