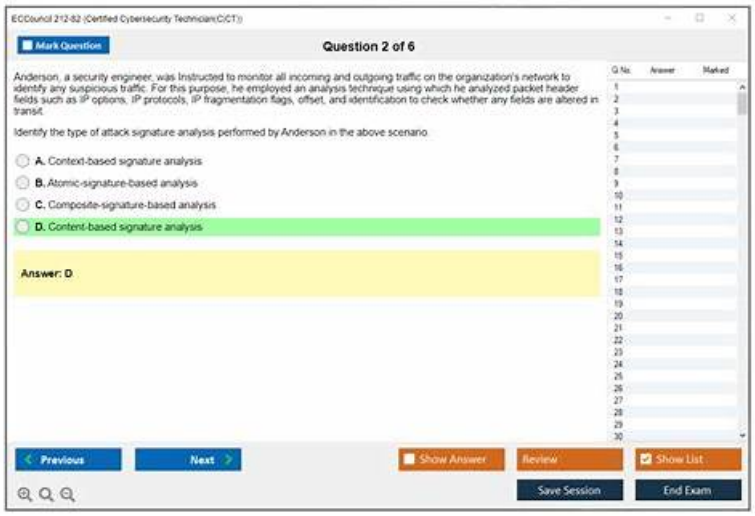
212-82 Prüfungsguide: Certified Cybersecurity Technician & 212-82 echter Test & 212-82 sicherlich-zu-bestehen



P.S. Kostenlose 2025 ECCouncil 212-82 Prüfungsfragen sind auf Google Drive freigegeben von It-Pruefung verfügbar: https://drive.google.com/open?id=1YNpAXlvM8Pv9sZeKZKQJTTDkOFi2PH7Z

Die ECCouncil 212-82 Zertifizierungsprüfung gehört zu den beliebtesten IT-Zertifizierungen. Viele ambitionierte IT-Fachleute wollen auch ECCouncil 212-82 Prüfung bestehen. Viele Kandidaten sollen genügende Vorbereitungen treffen, um eine hohe Note zu bekommen und sich den Bedürfnissen des Marktes anzupassen.

Die Zertifizierungsprüfung für Cybersecurity-Techniker von ECCOUNCIL 212-82 zertifizierte Cybersicherheitstechniker ist eine begehrte Zertifizierung auf dem Gebiet der Cybersicherheit. Diese Zertifizierung bietet Einzelpersonen die notwendigen Fähigkeiten und Kenntnisse, um die Cybersicherheit zu beeinträchtigen und für jede Organisation ein wichtiges Kapital zu werden. Die Zertifizierungsprüfung umfasst Themen wie Netzwerksicherheit, ethisches Hacking, Cybersicherheitstools und Vorfälle.

>> 212-82 Dumps Deutsch <<

ECCouncil 212-82 Fragen&Antworten, 212-82 Exam Fragen

Es ist uns allen bekannt, dass IT-Branche eine neue Branche und auch eine Kette ist, die die wirtschaftliche Entwicklung fördert. So ist ihre Position nicht zu ignorieren. Die ECCouncil 212-82 IT-Zertifizierung ist eine Methode für den Wettbewerb. Durch die ECCouncil 212-82 Zertifizierung werden Sie sich in allen Aspekten verbessern. Aber es ist nicht so einfach, die Prüfung zu bestehen. So empfehle ich Ihnen unsere originale Fragen. Wenn Sie die Schulungsressourcen wählen, ist It-Pruefung die erste Wahl. Seine Erfolgsquote beträgt 100%. Und Sie können die ECCouncil 212-82 Prüfung sicher bestehen.

Nach erfolgreicher Fertigstellung der Zertifizierung von ECCOUNCIL 212-82 (zertifizierter Cybersicherheitstechniker) können die Kandidaten Cybersicherheitslösungen zur Verhinderung, Erkennung und Reaktion verschiedener Cyber-Bedrohungen beherrschen. Außerdem werden zertifizierte Personen ihre Karriere in der Cybersecurity -Branche vorantreiben, indem sie weitere Beschäftigungsmöglichkeiten wie Cybersicherheitsanalyst, Techniker oder Ingenieur in verschiedenen Organisationen eröffnen.

ECCouncil Certified Cybersecurity Technician 212-82 Prüfungsfragen mit Lösungen (Q53-Q58):

53. Frage
An international bank recently discovered a security breach in its transaction processing system. The breach involved a sophisticated malware that not only bypassed the standard antivirus software but also remained undetected by the intrusion detection systems for months. The malware was programmed to intermittently alter transaction values and transfer small amounts to a foreign account, making detection challenging due to the subtlety of its actions. After a thorough investigation, cybersecurity experts identified the

nature of this malware. Which of the following best describes the type of malware used in this breach?

- A. Spyware, gathering sensitive information about the bank's transactions and customers Rootki'
- B. Ransomware, encrypting transaction data to extort money from the bank
- C. embedding itself deeply in the system to manipulate transaction processes
- D. presenting itself as legitimate software while performing malicious transactions

Antwort: C

Begründung:
* Definition of Rootkit:
* A rootkit is a type of malicious software designed to provide continued privileged access to a computer while actively hiding its presence. Rootkits can be installed at the hardware, firmware, or software level of a system.

54. Frage
Perform vulnerability assessment of an Android device located at IP address 172.30.20.110.
Identify the severity score for the device. You can use the OpenVAS vulnerability scanner, available with Parrot Security, with credentials admln/password for this challenge. (Practical Question)

- A. 2.8
- B. 02.6
- C. 2.2
- D. 2.4

Antwort: A

55. Frage
The IH&R team in an organization was handling a recent malware attack on one of the hosts connected to the organization's network. Edwin, a member of the IH&R team, was involved in reinstating lost data from the backup media. Before performing this step, Edwin ensured that the backup does not have any traces of malware.
Identify the IH&R step performed by Edwin in the above scenario.

- A. Eradication
- B. Recovery
- C. Incident containment
- D. Notification

Antwort: B

Begründung:
Recovery is the IH&R step performed by Edwin in the above scenario. IH&R (Incident Handling and Response) is a process that involves identifying, analyzing, containing, eradicating, recovering from, and reporting on security incidents that affect an organization's network or system. Recovery is the IH&R step that involves restoring the normal operation of the system or network after eradicating the incident. Recovery can include reinstating lost data from the backup media, applying patches or updates, reconfiguring settings, testing functionality, etc. Recovery also involves ensuring that the backup does not have any traces of malware or compromise.Eradication is the IH&R step that involves removing all traces of the incident from the system or network, such as malware, backdoors, compromised files, etc. Incident containment is the IH&R step that involves implementing appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization. Notification is the IH&R step that involves informing relevant stakeholders, authorities, or customers about the incident and its impact.

56. Frage
A text file containing sensitive information about the organization has been leaked and modified to bring down the reputation of the organization. As a safety measure, the organization did contain the MD5 hash of the original file. The file which has been leaked is retained for examining the integrity. A file named "Sensitiveinfo.txt" along with OriginalFileHash.txt has been stored in a folder named Hash in Documents of Attacker Machine-1. Compare the hash value of the original file with the leaked file and state whether the file has been modified or not by selecting yes or no.

- A. No
- B. Yes

Antwort: B

57. Frage
Miguel, a professional hacker, targeted an organization to gain illegitimate access to its critical information. He identified a flaw in the end-point communication that can disclose the target application's data.
Which of the following secure application design principles was not met by the application in the above scenario?

- A. Secure the weakest link
- B. Do not trust user input
- C. Exception handling
- D. Fault tolerance

Antwort: C

Begründung:
Exception handling is a secure application design principle that states that the application should handle errors and exceptions gracefully and securely, without exposing sensitive information or compromising the system's functionality. Exception handling can help prevent attackers from exploiting errors or exceptions to gain access to data or resources or cause denial-of-service attacks. In the scenario, Miguel identified a flaw in the end-point communication that can disclose the target application's data, which means that the application did not meet the exception handling principle.

58. Frage
.....