100% Garantie 212-89 Prüfungserfolg

Laden Sie die neuesten PrüfungFrage 212-89 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1-4cVJE4NMMS9i6vtXuH-I3fzam7zGGsI

Die Materialien zur EC-COUNCIL 212-89 Zertifizierungsprüfung von PrüfungFrage werden speziell von dem IT-Expertenteam entworfen. Sie sind zielgerichtet. Durch die Zertifizierung können Sie Ihren internationalen Wert in der IT-Branche verwirklichen. Viele Anbieter für Antwortenspeicherung und die Schulungsunterlagen versprechen, dass Sie die EC-COUNCIL 212-89 Zertifizierungsprüfung mit ihren Produkten bestehen können. PrüfungFrage sagen mit den Beweisen. Der Moment, wenn das Wunder vorkommt, kann jedes Wort von uns beweisen.

Wenn Sie die Produkte von PrüfungFrage kaufen, werden wir mit äußerster Kraft Ihnen helfen, die EC-COUNCIL 212-89 Zertifizierungsprüfung zu bstehen. Außerdem bieten wir Ihnen einen einjährigen kostenlosen Update-Service. Wenn der Prüfungsplan von staatlicher Seite geändert werden, benachrichtigen wir die Kunden sofort. Wenn unsere Software neue Version hat, liefern wir den Kunden sofort. PrüfungFrage verspricht, dass Sie nur einmal die EC-COUNCIL 212-89 Zertifizierungsprüfung bestehen können.

>> 212-89 Deutsche <<

212-89 Übungstest: EC Council Certified Incident Handler (ECIH v3) & 212-89 Braindumps Prüfung

Die EC-COUNCIL 212-89 Zertifizierungsprüfung sit eine Prüfung, die IT-Technik testet. PrüfungFrage ist eiune Website, die Ihnen zum Bestehen der EC-COUNCIL 212-89 Zertifizierungsprüfung verhilft. Viele Menschen verwenden viel Zeit und Energie auf die EC-COUNCIL 212-89 Zertifizierungsprüfung oder sie geben viel Geld für die Kurse aus, um die EC-COUNCIL 212-89 Zertifizierungsprüfung zu bestehen. Mit PrüfungFrage brauchen Sie nicht so viel Geld, Zeit und Energie. Die zielgerichteten Übungen von PrüfungFrage dauern nur 20 Stunden. Sie können dann die EC-COUNCIL 212-89 Zertifizierungsprüfung leicht bestehen.

Die EC-COUNCIL 212-89 Zertifizierungsprüfung umfasst eine Reihe von Themen rund um das Incident Handling, einschließlich Incident Response Prozess und Verfahren, digitale Forensik, Netzwerksicherheitsgrundlagen und Schwachstellenmanagement. Die Prüfung besteht aus 100 Multiple-Choice-Fragen und den Kandidaten werden zwei Stunden gegeben, um sie zu absolvieren. Die Prüfung ist computerbasiert und kann in einem der autorisierten Testzentren von EC-COUNCIL abgelegt werden.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) 212-89 Prüfungsfragen mit Lösungen (Q113-Q118):

113. Frage
They type of attack that prevents the authorized users to access networks, systems, or applications by exhausting the network resources and sending illegal requests to an application is known as:

- A. Session Hijacking attack
- B. Man in the Middle attack
- C. Denial of Service attack
- D. SQL injection attack

Antwort: C

114. Frage
Your manager hands you several items of digital evidence and asks you to investigate them in the order of volatility. Which of the following is the MOST volatile?

- A. Cache
- B. Temp files
- C. Emails
- D. Disk

Antwort: A

Begründung:
In the context of digital evidence investigation, volatility refers to how quickly data can change or be lost when power is removed or systems are altered. Among the options provided, cache is the most volatile because it is temporary storage that is designed to speed up access to data and is frequently overwritten.
Cache data resides in RAM and includes things like memory buffers, system and network information, and process execution data, which are lost upon reboot or power loss. This contrasts with disks, emails, and temp files, which are considered less volatile because they are stored on permanent or semi-permanent media and are less likely to be immediately lost or overwritten.
References:The Incident Handler (ECIH v3) curriculum includes principles of digital evidence handling, which emphasizes the importance of collecting evidence in descending order of volatility to ensure that the most ephemeral data is preserved before it's lost.

115. Frage
Rose is an incident-handling person and she is responsible for detecting and eliminating any kind of scanning attempts over the network by any malicious threat actors. Rose uses Wireshark tool to sniff the network and detect any malicious activities going on. Which of the following Wireshark filters can be used by her to detect TCP Xmas scan attempt by the attacker?

- A. tcp.flags==0X000
- B. tcp.flags==0X029
- C. tcp.dstport==7
- D. tcp.flags.reset==1

Antwort: B

Begründung:
A TCP Xmas scan is a type of network scanning technique used by attackers to identify open ports on a target machine. The name "Xmas" comes from the set of flags that are turned on within the packet, making it 'lit up like a Christmas tree'. Specifically, the FIN, PSH, and URG flags are set, which corresponds to the hexadecimal value 0X029 in the TCP header's flags field. Wireshark, a popular network protocol analyzer, allows users to create custom filters to detect specific types of network traffic, including malicious scanning attempts. By using the filtertcp.flags==0X029, Rose can detect packets that have these specific flags set, indicating a potential TCP Xmas scan attempt.
References:The technique of using Wireshark to detect specific types of scans, including the TCP Xmas scan, is covered in cybersecurity training materials and documentation related to network analysis and incident handling, such as those associated with the ECIH certification.

116. Frage
Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues. Which of the following documents helps in protecting evidence from physical or logical damage:

- A. Forensic analysis report
- B. Network and host log records
- C. Chain-of-Precedence
- D. Chain-of-Custody

Antwort: D

117. Frage
Rica works as an incident handler for an international company. As part of her role, she must review the present security policy implemented. Upon inspection, Rica finds that the policy is wide open, and only known dangerous services/attacks or behaviors are blocked. Which of the following is the current policy that Rica identified?

- A. Promiscuous policy
- B. Prudent policy
- C. Permissive policy
- D. Paranoic policy

Antwort: C

118. Frage
.....

nach " 212-89 " und erhalten Sie den kostenlosen Download mühelos □212-89 Probesfragen

- 212-89 Lerntipps □ 212-89 Fragenpool □ 212-89 Prüfungs-Guide □ Öffnen Sie die Webseite ▸ www.deutschpruefung.com ◂ und suchen Sie nach kostenloser Download von " 212-89 " □212-89 Trainingsunterlagen
- 212-89 Prüfungsfragen, 212-89 Fragen und Antworten, EC Council Certified Incident Handler (ECIH v3) □ Erhalten Sie den kostenlosen Download von 「 212-89 」 mühelos über ▸ www.itzert.com ◂ □212-89 Lernhilfe
- 212-89 Prüfungsressourcen: EC Council Certified Incident Handler (ECIH v3) - 212-89 Reale Fragen □ Öffnen Sie 【 www.zertfragen.com 】 geben Sie [212-89] ein und erhalten Sie den kostenlosen Download □212-89 Trainingsunterlagen
- 212-89 neuester Studienführer - 212-89 Training Torrent prep □ URL kopieren 【 www.itzert.com 】 Öffnen und suchen Sie □ 212-89 □ Kostenloser Download □212-89 Prüfungsmaterialien
- Die seit kurzem aktuellsten EC Council Certified Incident Handler (ECIH v3) Prüfungsunterlagen, 100% Garantie für Ihen Erfolg in der EC-COUNCIL 212-89 Prüfungen! □ Suchen Sie auf ⇛ www.itzert.com ⇚ nach □ 212-89 □ und erhalten Sie den kostenlosen Download mühelos □212-89 Deutsche Prüfungsfragen
- www.speaksmart.site, eskillhive.com, www.stes.tyc.edu.tw, www.lilly-angel.co.uk, www.stes.tyc.edu.tw, m.871v.com, www.stes.tyc.edu.tw, academy.caps.co.id, 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, doxaglobalnetwork.org, Disposable vapes

P.S. Kostenlose 2025 EC-COUNCIL 212-89 Prüfungsfragen sind auf Google Drive freigegeben von PrüfungFrage verfügbar: https://drive.google.com/open?id=1-4cVJE4NMMS9i6vtXuH-I3fzam7zGGsI