Echte 212-82 Fragen und Antworten der 212-82 Zertifizierungsprüfung

2025 Die neuesten Zertpruefung 212-82 PDF-Versionen Prüfungsfragen und 212-82 Fragen und Antworten sind kostenlos verfügbar: https://drive.google.com/open?id=1gyXtSyWZmIB5v67hGTmmB60cBgljwcMe

Zertpruefung haben ein riesiges Senior IT-Experten-Team. Sie nutzen ihre professionellen IT-Kenntnisse und reiche Erfahrung aus, um unterschiedliche Prüfungsfragen und Antworten zu bearbeiten, die Ihnen helfen, die ECCouncil 212-82 Zertifizierungsprüfung erfolgreich zu bestehen. In Zertpruefung können Sie immer die geeigneten Ausbildungsmethoden herausfinden, die Ihnen helfen, die ECCouncil 212-82 Prüfung zu bestehen. Egal, welche Ausbildungsart Sie wählen, bietet Zertpruefung einen einjährigen kostenlosen Update-Service. Die Informationsressourcen von Zertpruefung sind sehr umfangreich und auch sehr genau. Bei der Auswahl Zertpruefung können Sie ganz einfach die ECCouncil 212-82 Zertifizierungsprüfung bestehen.

Die ECCouncil 212-82 Prüfung umfasst eine Reihe von Themen im Zusammenhang mit Cyber-Sicherheit, einschließlich Netzwerksicherheitskonzepten, Kryptographie, Malware und Angriffen, Sicherheitsoperationen und -verwaltung sowie Vorfallreaktion und -wiederherstellung. Die Prüfung besteht aus 100 Multiple-Choice-Fragen und die Kandidaten haben zwei Stunden Zeit, um sie zu absolvieren. Die Prüfung ist computerbasiert und kann in jedem Pearson VUE-Testzentrum weltweit abgelegt werden. Nach Bestehen der Prüfung erhalten die Kandidaten die Zertifizierung als zertifizierter Cyber-Sicherheitstechniker, die drei Jahre gültig ist. Die Zertifizierung wird weltweit anerkannt und von Arbeitgebern in der Cyber-Sicherheitsbranche hoch geschätzt.

>> 212-82 German <<

212-82 Übungsmaterialien - 212-82 Prüfungsmaterialien

Ea ist Traum der Angestellten, sich in der IT-Branche engagieren zu können, die ECCouncil 212-82 Zertifizierungsprüfung zu bestehen. Wenn Sie Ihren Traum verwirklichen wollen, brauchen Sie nur fachliche Ausbildung zu wählen. Zertpruefung ist eine fachliche Website, die Schulungsunterlagen zur ECCouncil 212-82 Zertifizierung bietet. Wählen Sie Zertpruefung. Und wir versprechen, dass Sie den Erfolg erlangen und Ihren Traum verwirklichen , egal welches hohes Ziel Sie anstreben, können.

Die ECCouncil 212-82 (Certified Cybersecurity Technician) Prüfung ist eine Zertifizierung für Personen, die eine Karriere im Bereich Cybersecurity anstreben. Diese Zertifizierung ist in der Industrie weit verbreitet und ein Zeugnis für das Wissen und die Fähigkeiten einer Person im Bereich Cybersecurity. Die Prüfung umfasst eine Reihe von Themen, einschließlich Netzwerksicherheit, Kryptographie, ethisches Hacking und Incident Response.

ECCouncil Certified Cybersecurity Technician 212-82 Prüfungsfragen mit Lösungen (Q164-Q169):

164. Frage
Gideon, a forensic officer, was examining a victim's Linux system suspected to be involved in online criminal activities. Gideon navigated to a directory containing a log file that recorded information related to user login/logout. This information helped Gideon to determine the current login state of cyber criminals in the victim system, identify the Linux log file accessed by Gideon in this scenario.

- A. /va r/l og /wt m p
- B. /va r/l og /mysq Id. log
- C. /ar/log/boot.iog
- D. /var/log/httpd/

Antwort: A

Begründung:
/var/log/wtmp is the Linux log file accessed by Gideon in this scenario. /var/log/wtmp is a log file that records information related to user login/logout, such as username, terminal, IP address, and login time. /var/log/wtmp can be used to determine the current login state of users in a Linux system. /var/log/wtmp can be viewed using commands such as last, lastb, or utmpdump1.

165. Frage
A large-scale financial Institution was targeted by a sophisticated cyber-attack that resulted In substantial data leakage and financial loss. The attack was unique in its execution, involving multiple stages and techniques that evaded traditional security measures. The institution's cybersecurity team, in their post-incident analysis, discovered that the attackers followed a complex methodology aligning with a well-known hacking framework. Identifying the framework used by the attackers is crucial for the institution to revise its defense strategies. Which of the following hacking frameworks/methodologles most likely corresponds to the attack pattern observed?

- A. OWASP Top Ten. focusing on web application security risks
- B. ISO/IEC 27001. focusing on information security management systems
- C. MITRE ATT&CK, encompassing a wide range of tactics and techniques used in real-world attacks
- D. NIST Cybersecurity Framework, primarily used for managing cybersecurity risks

Antwort: C

Begründung:
Comprehensive Detailed Step by Step Explanation with All References from CyberSecurity:
* MITRE ATT&CK Framework:
* MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

166. Frage
Anderson, a security engineer, was Instructed to monitor all incoming and outgoing traffic on the organization's network to identify any suspicious traffic. For this purpose, he employed an analysis technique using which he analyzed packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit.

Identify the type of attack signature analysis performed by Anderson in the above scenario.

- A. Content-based signature analysis
- B. Composite-signature-based analysis
- C. Atomic-signature-based analysis
- D. Context-based signature analysis

Antwort: A

Begründung:
Content-based signature analysis is the type of attack signature analysis performed by Anderson in the above scenario. Content-based signature analysis is a technique that analyzes packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit. Content-based signature analysis can help detect attacks that manipulate packet headers to evade detection or exploit vulnerabilities . Context-based signature analysis is a technique that analyzes packet payloads such as application data or commands to check whether they match any known attack patterns or signatures. Atomic-signature-based analysis is a technique that analyzes individual packets to check whether they match any known attack patterns or signatures. Composite-signature-based analysis is a technique that analyzes multiple packets or sessions to check whether they match any known attack patterns or signatures.

167. Frage
Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN. To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer. Identify the type of wireless encryption employed by Charlie in the above scenario.

- A. CCMP
- B. AES
- C. TKIP
- D. WEP

Antwort: D

Begründung:
WEP is the type of wireless encryption employed by Charlie in the above scenario. Wireless encryption is a technique that involves encoding or scrambling the data transmitted over a wireless network to prevent unauthorized access or interception. Wireless encryption can use various algorithms or protocols to encrypt and decrypt the data, such as WEP, WPA, WPA2, etc. WEP (Wired Equivalent Privacy) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer . WEP can be used to provide basic security and privacy for wireless networks, but it can also be easily cracked or compromised by various attacks . In the scenario, Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN (Wireless Local Area Network). To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer.
This means that he employed WEP for this purpose. TKIP (Temporal Key Integrity Protocol) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer with dynamic keys . TKIP can be used to provide enhanced security and compatibility for wireless networks, but it can also be vulnerable to certain attacks . AES (Advanced Encryption Standard) is a type of wireless encryption that uses the Rijndael algorithm to encrypt information in the data link layer with fixed keys . AES can be used to provide strong security and performance for wireless networks, but it can also require more processing power and resources . CCMP (Counter Mode with Cipher Block Chaining Message Authentication CodeProtocol) is a type of wireless encryption that uses the AES algorithm to encrypt information in the data link layer with dynamic keys . CCMP can be used to provide robust security and reliability for wireless networks, but it can also require more processing power and resources

168. Frage
Dany, a member of a forensic team, was actively involved in an online crime investigation process. Dany's main responsibilities included providing legal advice on conducting the investigation and addressing legal issues involved in the forensic investigation process. Identify the role played by Dany in the above scenario.

- A. Incident responder
- B. Incident analyzer
- C. Attorney
- D. Expert witness

Antwort: C

Begründung:
Attorney is the role played by Dany in the above scenario. Attorney is a member of a forensic team who provides legal advice on conducting the investigation and addresses legal issues involved in the forensic investigation process. Attorney can help with obtaining search warrants, preserving evidence, complying with laws and regulations, and presenting cases in court.

169. Frage
.....