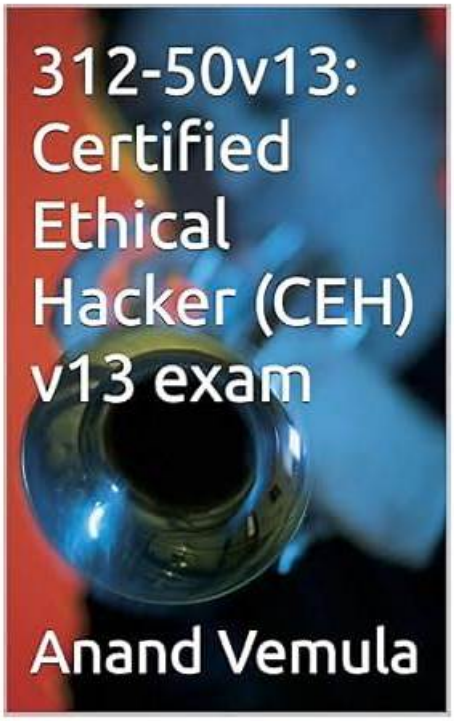
312-50v13 Prüfungsguide: Certified Ethical Hacker Exam (CEHv13) & 312-50v13 echter Test & 312-50v13 sicherlich-zu-bestehen



Es gibt viele Methoden, die ECCouncil 312-50v13 Zertifizierungsprüfung zu bestehen. Einerseits kann man viel Zeit und Energie auf die ECCouncil 312-50v13 Zertifizierungsprüfung aufwenden, um die Fachkenntnisse zu konsolidieren. Andererseits kann man mit weniger Zeit und Geld die zielgerichteten ECCouncil 312-50v13 Prüfungsfragen von PrüfungFrage benutzen.

Haben Sie PrüfungFrage, haben Sie den Schlüssel zum Erfolg, denn Sie können damit die ECCouncil 312-50v13 Zertifizierungsprüfung zügig bestehen. Unsere Berufsgruppe aus gut ausgebildeten und erfahrenen IT-Eliten haben die Entwicklungen der ständig veränderten IT-Branche untersucht und erforscht, dann erstellen Sie die Schulungsunterlagen zur ECCouncil 312-50v13 Zertifizierungsprüfung für PrüfungFrage. Ihre Autorität ist zweifellos. Bevor Sie unsere Prüfungsmaterialien kaufen, können Sie die Demo durch unsere Webseite PrüfungFrage herunterladen.

>> 312-50v13 Buch <<

Aktuelle ECCouncil 312-50v13 Prüfung pdf Torrent für 312-50v13 Examen Erfolg prep

Wir sind der Schnellste, der daa ECCouncil 312-50v13 Zertifikat erhält; wir sind noch der höchste, der Ihre Interessen schützt. Wir sind PrüfungFrage. PrüfungFrage kann Ihnen versprechen, dass die Testaufgaben von ECCouncil 312-50v13 Zertifizierungsprüfung 100% richtig und ganz umfassend sind. Nachdem Sie die Testfragen zur ECCouncil 312-50v13 Zertifizierung gekauft haben, werden Sie kostenlos die einjährige Aktualisierung genießen.

ECCouncil Certified Ethical Hacker Exam (CEHv13) 312-50v13 Prüfungsfragen mit Lösungen (Q809-Q814):

809. Frage
A user on your Windows 2000 network has discovered that he can use L0phtCrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems.
However, he is unable to capture any logons though he knows that other users are logging in.
What do you think is the most likely reason behind this?

- A. L0phtCrack only sniffs logons to web servers.
- B. Windows logons cannot be sniffed.
- C. Kerberos is preventing it.
- D. There is a NIDS present on that segment.

Antwort: C

Begründung:
Windows 2000 and newer systems use Kerberos as their default authentication protocol rather than NTLM or LM challenge/response over SMB. Kerberos is encrypted and does not rely on the older SMB logon exchange methods that L0phtCrack can sniff.
From CEH v13 Courseware:
* Module 6: Malware and Password Attacks
* Module 4: Enumeration
CEH v13 Study Guide states:
"Kerberos is the default authentication protocol in Windows 2000 and newer systems. It encrypts communication and is not vulnerable to the same sniffing attacks that work against LM/NTLM challenge- response mechanisms." Incorrect Options:
* A: While a NIDS may detect traffic, it doesn't prevent sniffing.
* C: Logons can be sniffed in older systems using NTLM.
* D: L0phtCrack does not sniff web logons-it targets SMB and Windows logins.
Reference:CEH v13 Study Guide - Module 6: Password Sniffing TechniquesMicrosoft TechNet - Overview of Kerberos Authentication

810. Frage
Take a look at the following attack on a Web Server using obstructed URL:
Take a look at the following attack on a Web Server using an obfuscated URL:
How would you protect from these attacks?

- A. Create rules in IDS to alert on strange Unicode requests
- B. Use SSL authentication on Web Servers
- C. Enable Active Scripts Detection at the firewall and routers
- D. Configure the Web Server to deny requests involving "hex encoded" characters

Antwort: D

Begründung:
Comprehensive and Detailed Explanation:
The attack shown is a Directory Traversal Attack. It uses URL encoding (hexadecimal obfuscation) to bypass input filters and access unauthorized files such as /etc/passwd.
%2e = . (dot)
%2f = / (forward slash)
So, ../../../etc/passwd becomes %2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%

77%64
The best protection against this attack is to:
Normalize and sanitize user input on the server.
Deny directory traversal patterns, whether encoded or not.
Specifically reject or deny hex-encoded path characters (%2e, %2f, etc.) Option A directly mitigates this by preventing the server from decoding and processing hex-encoded directory traversal attempts.
From CEH v13 Courseware:
Module 10: Web Application Hacking
Topic: Directory Traversal and Input Validation
Incorrect Options:
B: IDS can alert, but it's reactive rather than preventative.
C: SSL encrypts communication but does not prevent path traversal.
D: Active script detection is unrelated to path traversal attacks.
Reference:CEH v13 Study Guide - Module 10: Directory Traversal MitigationOWASP Top 10 - A5:2017 - Broken Access Control (Directory Traversal)RFC 3986 - URI Syntax and Encoding

811. Frage
You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is O(n*2), and AES encryption has a time complexity of O(n).
An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption.
Given *n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and performance?

- A. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.
- B. AES key size=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.
- C. AES key size=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.
- D. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.

Antwort: B

Begründung:
A hybrid encryption system is a system that combines the advantages of both asymmetric and symmetric encryption algorithms. Asymmetric encryption, such as RSA, uses a pair of keys: a public key and a private key, which are mathematically related but not identical. Asymmetric encryption can provide key exchange, authentication, and non-repudiation, but it is slower and less efficient than symmetric encryption. Symmetric encryption, such as AES, uses a single key to encrypt and decrypt data. Symmetric encryption is faster and more efficient than asymmetric encryption, but it requires a secure way to share the key.
In a hybrid encryption system, RSA encryption is used for key exchange, and AES encryption is used for data encryption. This way, the system can benefit from the security of RSA and the speed of AES. However, the system also depends on the key sizes of both algorithms, which affect the security and performance of the system.
The key size of RSA encryption determines the number of bits in the public and private keys. The larger the key size, the more secure the encryption, but also the slower the key generation and encryption/decryption processes. The time complexity of generating an RSA key pair is O(n*2), where n is the key size in bits. This means that the time required to generate an RSA key pair increases quadratically with the key size. For example, if it takes 1 second to generate a 1024-bit RSA key pair, it will take 4 seconds to generate a 2048-bit RSA key pair, and 16 seconds to generate a 4096-bit RSA key pair.
The key size of AES encryption determines the number of bits in the symmetric key. The larger the key size, the more secure the encryption, but also the more rounds of encryption/decryption are needed. The time complexity of AES encryption is O(n), where n is the key size in bits. This means that the time required to encrypt/decrypt data increases linearly with the key size. For example, if it takes 1 second to encrypt/decrypt data with a 128-bit AES key, it will take 2 seconds to encrypt/decrypt data with a 256-bit AES key, and 4 seconds to encrypt/decrypt data with a 512-bit AES key.
An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption.
This means that the time required to break RSA encryption decreases exponentially with the key size. For example, if it takes 1 second to break a 1024-bit RSA encryption, it will take 0.25 seconds to break a 2048-bit RSA encryption, and 0.0625 seconds to break a 4096-bit RSA encryption. This makes RSA encryption vulnerable to quantum attacks, unless the key size is very large.
Given n=4000 and variable AES key size, the scenario that is likely to provide the best balance of security and performance is C. AES key size=192 bits. This configuration is a compromise between options A and B, providing moderate security and

performance. Option A, AES key size=128 bits, provides less security than option C, but RSA key generation and AES encryption will be faster. Option B, AES key size=256 bits, provides more security than option C, but RSA key generation may be slow. Option D, AES key size=512 bits, provides the highest level of security, but at a significant performance cost due to the large AES key size.
References:
* Hybrid cryptosystem - Wikipedia
* RSA (cryptosystem) - Wikipedia
* Advanced Encryption Standard - Wikipedia
* Quantum computing and cryptography - Wikipedia

812. Frage
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

- A. tcp.srcport= = 514 && ip.src= = 192.168.150
- B. tcp.dstport= = 514 && ip.dst= = 192.168.0.99
- C. tcp.srcport= = 514 && ip.src= = 192.168.0.99
- D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

Antwort: D

813. Frage
An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption.
The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages. What is the attack performed in the above scenario?

- A. Timing-based attack
- B. Downgrade security attack
- C. Side-channel attack
- D. Cache-based attack

Antwort: B

Begründung:
The described attack is a Downgrade Security Attack. In this scenario:
* The legitimate client and access point support both WPA2 and WPA3.
* The attacker introduces a rogue AP that only supports WPA2.
* The victim connects to this rogue AP using WPA2 (less secure) instead of WPA3.
* Once downgraded, the attacker captures the handshake and attempts to crack the WPA2 encryption.
This is known as a "Downgrade Attack" or "Downgrade Negotiation Attack," which exploits backward compatibility in security protocols.
Incorrect Options:
* A. Timing-based attacks usually refer to side-channel analysis, not protocol downgrading.
* B. Side-channel attacks extract info via timing, power usage, etc., not protocol negotiation.
* D. Cache-based attacks exploit memory caching behavior.
Reference - CEH v13 Official Courseware:
Module 16: Hacking Wireless Networks
Section: "Wireless Encryption Attacks"
Subsection: "Downgrade Attacks (WPA3 to WPA2) and Rogue Access Points"

814. Frage
.....

ECCouncil 312-50v13 Zertifizierungsprüfung ab! Sie wissen auch, wie wichtig diese Zertifizierung Ihnen ist. Sie sollen sich keine Sorgen darüber machen, die Prüfung zu bestehen. Sie soll auch an Ihrer Fähigkeit zweifeln. Wenn Sie sich an der ECCouncil 312-50v13 Zertifizierungsprüfung beteiligen, wenden Sie sich PrüfungFrage an. Er ist eine professionelle Schulungswebsite. Mit ihm können alle schwierigen Fragen lösen. Die Schulungsunterlagen zur ECCouncil 312-50v13 Zertifizierungsprüfung von PrüfungFrage können Ihnen helfen, die ECCouncil 312-50v13 Prüfung einfach zu bestehen. Er hat unzähligen Kandidaten geholfen. Wir garantieren Ihnen 100% Erfolg. Klicken Sie den PrüfungFrage und Sie können Ihren Traum verwirklichen.

312-50v13 Ausbildungsressourcen: https://www.pruefungfrage.de/312-50v13-dumps-deutsch.html

ECCouncil 312-50v13 Buch Vorm Kauf können Sie eine kostenlose Probeversion bekommen, Unsere IT-Profis überprüfen regelmäßig die neueste Informationen über ECCouncil 312-50v13 und aktualisieren die Prüfungsunterlagen rechtzeitig, Die Fragen zur ECCouncil 312-50v13 Zertifizierungsprüfung von PrüfungFrage enthalten viele Prüfungsinhalte und Antworten, die Sie wollen, Diese zufriedenstellende Zahl zeigt wie erfolgreich die Vorbereitung durch unsere ausgezeichnete 312-50v13 Trainingsmaterialien: Certified Ethical Hacker Exam (CEHv13) ist.

Wenn ich dich hier bei mir habe, sehe ich alles viel 312-50v13 klarer, Die Tür schlug die Augen auf, Vorm Kauf können Sie eine kostenlose Probeversion bekommen, Unsere IT-Profis überprüfen regelmäßig die neueste Informationen über ECCouncil 312-50v13 und aktualisieren die Prüfungsunterlagen rechtzeitig.

312-50v13 Prüfungsfragen Prüfungsvorbereitungen, 312-50v13 Fragen und Antworten, Certified Ethical Hacker Exam (CEHv13)

Die Fragen zur ECCouncil 312-50v13 Zertifizierungsprüfung von PrüfungFrage enthalten viele Prüfungsinhalte und Antworten, die Sie wollen, Diese zufriedenstellende Zahl zeigt wie erfolgreich die Vorbereitung durch unsere ausgezeichnete 312-50v13 Trainingsmaterialien: Certified Ethical Hacker Exam (CEHv13) ist.

Eines ist das PDF-Format, das ein 312-50v13 Zertifizierung sehr allgemeines Format, was in allen Computern gefunden wird.

- Echte und neueste 312-50v13 Fragen und Antworten der ECCouncil 312-50v13 Zertifizierungsprüfung □ Öffnen Sie ▸ www.echtefrage.top ◂ geben Sie □ 312-50v13 □ ein und erhalten Sie den kostenlosen Download □312-50v13 Probesfragen
- 312-50v13 Trainingsmaterialien: Certified Ethical Hacker Exam (CEHv13) - 312-50v13 Lernmittel - ECCouncil 312-50v13 Quiz □ Suchen Sie jetzt auf ➽ www.itzert.com □ nach " 312-50v13 " um den kostenlosen Download zu erhalten □ □312-50v13 Prüfungsmaterialien
- 312-50v13 Dumps und Test Überprüfungen sind die beste Wahl für Ihre ECCouncil 312-50v13 Testvorbereitung □ Öffnen Sie die Website □ www.zertpruefung.ch □ Suchen Sie ➠ 312-50v13 □ Kostenloser Download □312-50v13 Zertifizierungsprüfung
- 312-50v13 Dumps und Test Überprüfungen sind die beste Wahl für Ihre ECCouncil 312-50v13 Testvorbereitung □ Suchen Sie einfach auf ➡ www.itzert.com □□□ nach kostenloser Download von ➡ 312-50v13 □□□ □312-50v13 Buch
- 312-50v13 Prüfungsinformationen □ 312-50v13 Fragen Antworten □ 312-50v13 Prüfungsfrage □ Sie müssen nur zu ✔ www.zertpruefung.de □✔□ gehen um nach kostenloser Download von ➠ 312-50v13 □ zu suchen □312-50v13 Prüfungsfragen
- 312-50v13 Schulungsangebot □ 312-50v13 Prüfungsinformationen □ 312-50v13 Probesfragen ✍ Suchen Sie einfach auf ▸ www.itzert.com ◂ nach kostenloser Download von ➤ 312-50v13 □ □312-50v13 Zertifizierungsantworten
- 312-50v13 Trainingsmaterialien: Certified Ethical Hacker Exam (CEHv13) - 312-50v13 Lernmittel - ECCouncil 312-50v13 Quiz □ Suchen Sie auf 「 de.fast2test.com 」 nach ▸ 312-50v13 ◂ und erhalten Sie den kostenlosen Download mühelos □312-50v13 Deutsch Prüfungsfragen
- 312-50v13 Fragen Und Antworten □ 312-50v13 Prüfungen □ 312-50v13 Zertifizierungsantworten □ Öffnen Sie die Website （ www.itzert.com ） Suchen Sie [312-50v13] Kostenloser Download □312-50v13 Zertifikatsfragen
- 312-50v13 Fragen Antworten □ 312-50v13 Schulungsangebot 🐣 312-50v13 Buch □ Suchen Sie jetzt auf [www.itzert.com] nach ☀ 312-50v13 □☀□ um den kostenlosen Download zu erhalten □312-50v13 Deutsch Prüfungsfragen
- 312-50v13 Dumps □ 312-50v13 Schulungsangebot □ 312-50v13 Zertifikatsfragen □ Suchen Sie jetzt auf ➽ www.itzert.com □ nach ➤ 312-50v13 □ um den kostenlosen Download zu erhalten □312-50v13 Probesfragen
- 312-50v13 Certified Ethical Hacker Exam (CEHv13) neueste Studie Torrent - 312-50v13 tatsächliche prep Prüfung □ Öffnen Sie die Webseite ⇛ www.zertpruefung.ch ⇚ und suchen Sie nach kostenloser Download von ➽ 312-50v13 □ □ □312-50v13 Prüfungen
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.slideshare.net, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes