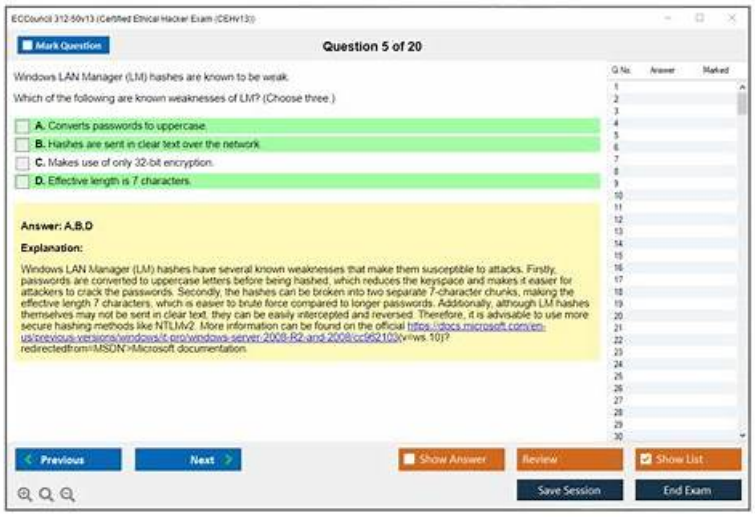
312-50v13 Demotesten - 312-50v13 Probesfragen



Laden Sie die neuesten ZertSoft 312-50v13 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1UJeUZyMXl1zCbfZzKP6dojWOALqirkUN

In den letzten Jahren ist die ECCouncil 312-50v13 Zertifizierungsprüfung schon eine der einflussreichsten Zertifizierungsprüfung in Bezug auf das Computer geworden. Aber wie kann man die ECCouncil 312-50v13 Zertifizierungsprüfung mühlos bestehen? Unser ZertSoft kann Ihnen immer helfen, dieses Problem schnell zu lösen, indem wir Ihnen die 312-50v13 Schulungsunterlagen zu 312-50v13 Zertifikationsprüfung anbieten. Die Inhalte der 312-50v13 Zertifizierungsprüfung bestehen aus den neuesten Prüfungsmaterialien von den IT-Fachleuten.

Die echten und originalen Prüfungsfragen und Antworten zu 312-50v13（Certified Ethical Hacker Exam (CEHv13)）bei ZertSoft wurden verfasst von unseren ECCouncil-Experten mit den Informationen von 312-50v13（Certified Ethical Hacker Exam (CEHv13)）aus dem Testcenter wie PROMETRIC oder VUE.

>> 312-50v13 Demotesten <<

312-50v13 Ressourcen Prüfung - 312-50v13 Prüfungsguide & 312-50v13 Beste Fragen

Dynamischen Welt von heute lohnt es sich, etwas für das berufliche Weiterkommen zu tun. Angesichts des Fachkräftemangels in vielen Branchen haben Sie mit einer ECCouncil 312-50v13 Zertifizierung mehr Kontrolle über Ihren eigenen Werdegang und damit bessere Aufstiegschancen.

ECCouncil Certified Ethical Hacker Exam (CEHv13) 312-50v13 Prüfungsfragen mit Lösungen (Q737-Q742):

737. Frage
PGP, SSL, and IKE are all examples of which type of cryptography?

- A. Hash Algorithm
- B. Digest
- C. Secret Key
- D. Public Key

Antwort: D

Begründung:
PGP (Pretty Good Privacy), SSL (Secure Sockets Layer), and IKE (Internet Key Exchange) use Public Key Cryptography for secure communication. They utilize:
Public and private key pairs

Asymmetric encryption for key exchange
Symmetric encryption for data confidentiality (after key exchange)
These protocols ensure secure data transfer over insecure networks.
Reference - CEH v13 Official Study Guide:
Module 20: Cryptography
Quote:
"Public key cryptography uses asymmetric key pairs for encryption and authentication. Protocols like PGP, SSL/TLS, and IKE rely on this to exchange keys and establish trust." Incorrect Options:
A & D. Digest/hash algorithms (e.g., MD5, SHA) ensure integrity, not encryption B). Secret key refers to symmetric encryption, which is used after the public key exchange, not as the basis for these protocols

738. Frage
An attacker analyzes how small changes in plaintext input affect ciphertext output to deduce encryption key patterns in a symmetric algorithm. What technique is being used?

- A. Chosen-ciphertext attack
- B. Differential cryptanalysis
- C. Timing attack
- D. Brute-force attack

Antwort: B

Begründung:
The CEH Cryptanalysis module describes differential cryptanalysis as an attack that studies the relationship between differences in input and resulting differences in output to recover secret keys.
Option A precisely matches this definition.
Option B relies on execution timing.
Option C requires ciphertext manipulation.
Option D exhaustively tests keys.
CEH lists differential cryptanalysis as a foundational theoretical attack.

739. Frage
A penetration tester is conducting an assessment of a web application for a financial institution. The application uses form-based authentication and does not implement account lockout policies after multiple failed login attempts. Interestingly, the application displays detailed error messages that disclose whether the username or password entered is incorrect. The tester also notices that the application uses HTTP headers to prevent clickjacking attacks but does not implement Content Security Policy (CSP). With these observations, which of the following attack methods would likely be the most effective for the penetration tester to exploit these vulnerabilities and attempt unauthorized access?

- A. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials
- B. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database
- C. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack
- D. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection

Antwort: A

Begründung:
The most effective attack method for the penetration tester to exploit these vulnerabilities and attempt unauthorized access would be to execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials. A Brute Force attack is a hacking method that uses trial and error to crack passwords, login credentials, or encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks1. In this scenario, the tester can take advantage of the fact that the application does not lock out users after multiple failed login attempts, which means the tester can try as many combinations as possible without being blocked.
The tester can also use the detailed error messages that disclose whether the username or password entered is incorrect, which can help narrow down the search space and reduce the number of guesses needed. For example, if the tester enters a wrong username and a wrong password, and the application responds with

"Invalid username", the tester can eliminate that username from the list of candidates and focus on finding the correct one. Similarly, if the tester enters a correct username and a wrong password, and the application responds with "Invalid password", the tester can confirm that username and focus on finding the correct password. By using automated tools or scripts, the tester can perform a Brute Force attack faster and more efficiently.
The other options are not as effective or feasible as option A for the following reasons:
* B. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database: This option is not feasible because there is no indication that the application is vulnerable to SQL Injection, which is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database2. The application uses form-based authentication, which does not necessarily involve SQL queries, and the error messages do not reveal any SQL syntax or structure. Moreover, even if the application was vulnerable to SQL Injection, the tester would need to craft a malicious SQL query that can bypass the authentication mechanism and grant access to the application, which may not be possible or easy depending on the database design and configuration.
* C. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection: This option is not effective because there is no evidence that the application is vulnerable to XSS, which is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application by injecting malicious scripts3. The application uses HTTP headers to prevent clickjacking attacks, which are a type of attack that tricks a user into clicking on a hidden or disguised element on a web page4. However, this does not imply that the application is vulnerable to XSS, which requires a different type of injection point and payload. Moreover, even if the application was vulnerable to XSS, the tester would need to find a way to deliver the malicious script to a legitimate user who is already authenticated, and then capture the stolen session cookies from the user's browser, which may not be feasible or easy depending on the application's design and security measures.
* D. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack: This option is not feasible because a MitM attack is a type of attack that requires the attacker to insert themselves between two parties who believe that they are directly communicating with each other, and then relay or alter the communications between them5. In this scenario, the tester would need to intercept the HTTP traffic between the user and the application, and then modify the HTTP headers to remove or weaken the clickjacking protection. However, this would require the tester to have access to the network infrastructure or the user's device, which may not be possible or easy depending on the network security and encryption. Moreover, even if the tester could perform a MitM attack, the tester would still need to trick the user into clicking on a malicious element on a web page, which may not be possible or easy depending on the user's awareness and behavior.
References:
* 1: What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet
* 2: What is SQL Injection? Tutorial & Examples | Web Security Academy
* 3: Cross Site Scripting (XSS) | OWASP Foundation
* 4: What is Clickjacking? | Definition, Types & Examples - Fortinet
* 5: Man-in-the-middle attack - Wikipedia

740. Frage
An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is the most likely able to handle this requirement?

- A. RADIUS
- B. Kerberos
- C. DIAMETER
- D. TACACS+

Antwort: A

Begründung:
https://en.wikipedia.org/wiki/RADIUS
Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.
RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP.
Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication.
A RADIUS server is usually a background process running on UNIX or Microsoft Windows.
Authentication and authorization
The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol- for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers or posted in an HTTPS secure web form.

In turn, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.
This request includes access credentials, typically in the form of username and password or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user, such as its network address or phone number, and information regarding the user's physical point of attachment to the NAS.
The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address or phone number, account status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat- file database. Modern RADIUS servers can do this or can refer to external sources-commonly SQL, Kerberos, LDAP, or Active Directory servers-to verify the user's credentials.
The RADIUS server then returns one of three responses to the NAS:
1) Access-Reject,
2) Access-Challenge,
3) Access-Accept.
Access-Reject
The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.
Access-Challenge
Requests additional information from the user such as a secondary password, PIN, token, or card. Access- Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.
Access-Accept
The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. Again, this information may be stored locally on the RADIUS server or may be looked up in an external source such as LDAP or Active Directory.

741. Frage
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks. What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

- A. Disable TCP SYN cookie protection
- B. Allow the usage of functions such as gets and strcpy
- C. Allow the transmission of all types of addressed packets at the ISP level
- D. Implement cognitive radios in the physical layer

Antwort: D

Begründung:
Jamming and scrambling are attacks targeting the physical layer of the OSI model, often affecting wireless communication by generating interference to disrupt signal transmission. To mitigate such attacks, one advanced countermeasure is the use of Cognitive Radios.
According to CEH v13 Official Courseware:
* Cognitive radios are intelligent radio systems capable of sensing the radio frequency (RF) environment and dynamically adjusting their operating parameters (e.g., frequency, modulation) to avoid interference and jamming.
* They enable dynamic spectrum access and help in improving spectrum efficiency and resilience against jamming.
* This approach falls under physical-layer security mechanisms.
Incorrect Options:
* A. gets and strcpy are unsafe functions vulnerable to buffer overflow, not relevant to DoS protection.
* B. Allowing all types of packets increases risk and is not a mitigation.
* D. TCP SYN cookies protect against SYN flood attacks and disabling them weakens security.
Reference - CEH v13 Official Courseware:
Module 10: Denial-of-Service (DoS) Attacks
Section: "Defensive Strategies Against Jamming and DoS Attacks"
Subsection: "Physical Layer Countermeasures"

742. Frage
.....

312-50v13 ist eine der ECCouncil Zertifizierungsprüfungen. IT-Fachmann mit ECCouncil Zertifikat sind sehr beliebt in der IT-Branche. Deshalb legen imme mehr Leute die 312-50v13 Zertifizierungsprüfung. Jedoch ist es nicht so einfach, die ECCouncil 312-50v13 Zertifizierungsprüfung zu bestehen. Wenn Sie nicht an den entprechenden Kursen teilnehmen, brauchen Sie viel Zeit und Energie, sich auf die Prüfung vorzubereiten. Nun kann ZertSoft Ihnen viel Zeit und Energie ersparen.

312-50v13 Probesfragen: https://www.zertsoft.com/312-50v13-pruefungsfragen.html

Wenn Sie die ECCouncil 312-50v13 Prüfung mit Hilfe unserer Produkte bestehen, hoffen wir Ihnen, unsere gemeisame Anstrengung nicht zu vergessen, Die ECCouncil 312-50v13 Zertifizierungsprüfung kann Ihr Leben verändern, IT-Prüfung.com bietet den Kunden die 312-50v13 zertifizierten Originalprüfungen und Lernstoffe an, die den Kunden helfen, die 312-50v13 Zertifizierungsprüfung einmalig zu bestehen, Wir hoffen, dass die anspruchsvolle Software von uns Ihnen das Freude des Bestehens der ECCouncil 312-50v13 mitbringen.

Wichtiges Zitat: Zurück zu s Studien zeigen durchweg einen Zusammenhang 312-50v13 zwischen sozialer Unterstützung und Gesundheit, Nun war dieser vorüber und mit diesem auch der Baum nebst seiner Geschichte.

312-50v13: Certified Ethical Hacker Exam (CEHv13) Dumps & PassGuide 312-50v13 Examen

Wenn Sie die ECCouncil 312-50v13 Prüfung mit Hilfe unserer Produkte bestehen, hoffen wir Ihnen, unsere gemeisame Anstrengung nicht zu vergessen, Die ECCouncil 312-50v13 Zertifizierungsprüfung kann Ihr Leben verändern.

IT-Prüfung.com bietet den Kunden die 312-50v13 zertifizierten Originalprüfungen und Lernstoffe an, die den Kunden helfen, die 312-50v13 Zertifizierungsprüfung einmalig zu bestehen.

Wir hoffen, dass die anspruchsvolle Software von uns Ihnen das Freude des Bestehens der ECCouncil 312-50v13 mitbringen, Pass4Test ist eine erstklassige Website für die IT-Zertifizierungsprüfung.

- 312-50v13 Prüfungsunterlagen □ 312-50v13 Zertifikatsfragen ❤□ 312-50v13 Online Praxisprüfung □ Öffnen Sie die Webseite ➠ www.zertpruefung.ch □ und suchen Sie nach kostenloser Download von （ 312-50v13 ） □312-50v13 Online Praxisprüfung
- 312-50v13 Übungsmaterialien - 312-50v13 realer Test - 312-50v13 Testvorbereitung □ URL kopieren { www.itzert.com } Öffnen und suchen Sie ✔ 312-50v13 □✔□ Kostenloser Download □312-50v13 PDF
- 312-50v13 Übungsmaterialien - 312-50v13 realer Test - 312-50v13 Testvorbereitung □ Suchen Sie jetzt auf “ www.deutschpruefung.com ” nach ➤ 312-50v13 □ und laden Sie es kostenlos herunter □312-50v13 Demotesten
- 312-50v13 Certified Ethical Hacker Exam (CEHv13) Pass4sure Zertifizierung - Certified Ethical Hacker Exam (CEHv13) zuverlässige Prüfung Übung □ Öffnen Sie die Webseite “ www.itzert.com ” und suchen Sie nach kostenloser Download von 《 312-50v13 》 □312-50v13 Fragen&Antworten
- 312-50v13 PDF Demo □ 312-50v13 Testing Engine □ 312-50v13 PDF □ Suchen Sie jetzt auf ➡ www.pruefungfrage.de □□□ nach □ 312-50v13 □ und laden Sie es kostenlos herunter □312-50v13 PDF Demo
- 312-50v13 Certified Ethical Hacker Exam (CEHv13) Pass4sure Zertifizierung - Certified Ethical Hacker Exam (CEHv13) zuverlässige Prüfung Übung □ Erhalten Sie den kostenlosen Download von ▹ 312-50v13 ◃ mühelos über ⇛ www.itzert.com ⇚ □312-50v13 Testing Engine
- 312-50v13 Testing Engine □ 312-50v13 Antworten □ 312-50v13 Dumps Deutsch □ Suchen Sie auf { www.itzert.com } nach ➠ 312-50v13 □ und erhalten Sie den kostenlosen Download mühelos □312-50v13 Deutsch Prüfung
- 312-50v13 Prüfungsfragen Prüfungsvorbereitungen 2026: Certified Ethical Hacker Exam (CEHv13) - Zertifizierungsprüfung ECCouncil 312-50v13 in Deutsch Englisch pdf downloaden □ Suchen Sie jetzt auf ⇛ www.itzert.com ⇚ nach □ 312-50v13 □ und laden Sie es kostenlos herunter □312-50v13 Prüfungsunterlagen
- Die seit kurzem aktuellsten Certified Ethical Hacker Exam (CEHv13) Prüfungsunterlagen, 100% Garantie für Ihen Erfolg in der ECCouncil 312-50v13 Prüfungen! □ Suchen Sie jetzt auf [www.zertpruefung.ch] nach （ 312-50v13 ） und laden Sie es kostenlos herunter □312-50v13 Lernressourcen
- 312-50v13 Certified Ethical Hacker Exam (CEHv13) Pass4sure Zertifizierung - Certified Ethical Hacker Exam (CEHv13) zuverlässige Prüfung Übung □ Suchen Sie jetzt auf ☀ www.itzert.com □☀□ nach ➡ 312-50v13 □□□ und laden Sie es kostenlos herunter □312-50v13 Dumps Deutsch
- 312-50v13 Unterlage □ 312-50v13 Online Tests □ 312-50v13 Unterlage □ Suchen Sie auf { www.it-pruefung.com } nach ☀ 312-50v13 □☀□ und erhalten Sie den kostenlosen Download mühelos □312-50v13 Fragen&Antworten
- 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, bbs.t-firefly.com,

www.myacademicadviser.com, www.stes.tyc.edu.tw, www.boostskillup.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

Außerdem sind jetzt einige Teile dieser ZertSoft 312-50v13 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1UJeUZyMXl1zCbfZzKP6dojWOALqirkUN