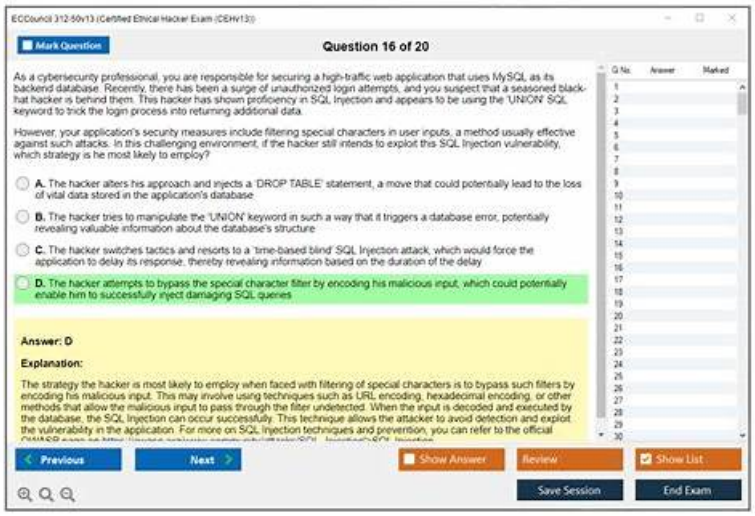
Hot Review 312-50v13 Guide Pass Certify | High-quality Pdf 312-50v13 Exam Dump: Certified Ethical Hacker Exam (CEHv13)



P.S. Free & New 312-50v13 dumps are available on Google Drive shared by TestkingPDF: https://drive.google.com/open?id=14l0mcUBVMMVaZyfoTXuNseQ6y75hdLvA

You can try the free demo version of any ECCouncil 312-50v13 exam dumps format before buying. For your satisfaction, TestkingPDF gives you a free demo download facility. You can test the features and then place an order. So, these real and updated ECCouncil dumps are essential to pass the 312-50v13 Exam on the first try.

Our excellent ECCouncil 312-50v13 practice materials beckon exam candidates around the world with their attractive characters. Our experts made significant contribution to their excellence. So we can say bluntly that our 312-50v13 Actual Exam is the best. Our effort in building the content of our 312-50v13 study dumps lead to the development of 312-50v13 learning guide and strengthen their perfection.

>> Review 312-50v13 Guide <<

Reliable ECCouncil Review 312-50v13 Guide & The Best TestkingPDF - Leading Provider in Qualification Exams

If you're looking to advance your career, passing the ECCouncil 312-50v13 Certification Exam is crucial. As with any certification exam, success requires time and effort. While there are many online study materials available, not all of them are accurate or reliable. Many professionals struggle with managing their time and studying effectively, making it difficult to pass the Certified Ethical Hacker Exam (CEHv13) (312-50v13) Exam.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q337-Q342):

NEW QUESTION # 337
If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, what do you know about the firewall you are scanning?

- A. There is no firewall in place.
- B. This event does not tell you anything about the firewall.
- C. It is a non-stateful firewall.
- D. It is a stateful firewall

Answer: D

Explanation:
In CEH v13 Module 03: Scanning Networks, the behavior of firewalls in response to ACK scans is described in detail, especially regarding stateful vs. stateless firewalls.
An ACK scan (nmap -sA) is primarily used for firewall rule analysis. Here's how it works:
When you send a TCP ACK segment:
If the port is closed and no firewall is present, the target should respond with a TCP RST packet.
If a stateless (non-stateful) firewall is used, it typically allows or blocks packets based only on rules about IP addresses, ports, and protocol type, without tracking session state.
If a stateful firewall is used, it keeps track of connection states. Therefore:
An unsolicited ACK packet (not part of any established session) will be silently dropped, because it doesn't correspond to any active connection.
No RST is sent back because the firewall suppresses it, recognizing it as potentially malicious or out of context.
Therefore:
No RST response = packet was silently dropped.
Silent dropping of unsolicited ACK packets = Stateful Firewall Behavior.
Option Analysis:
A). There is no firewall in place
Incorrect. If there were no firewall, an RST would be sent from the closed port.
B). This event does not tell you anything about the firewall
Incorrect. The lack of a response is actually meaningful and implies stateful filtering behavior.
C). It is a stateful firewall
Correct. A stateful firewall inspects the packet, sees no valid session, and drops it silently.
D). It is a non-stateful firewall
Incorrect. A non-stateful firewall would typically not inspect session state, and you'd still expect to see a response (likely an RST).
Reference from CEH v13 Study Guide and Courseware:
Module 03 - Scanning Networks, Section: Nmap Scanning Techniques # TCP ACK Scan CEH Engage Labs - Network Scanning Phase: Firewall Rule Detection using ACK Scans

NEW QUESTION # 338
You are Sameer Das, an ethical hacker hired by a national utilities provider to assess the resilience of its power grid infrastructure. During your red team operation, you conduct a phishing campaign targeting field engineers and successfully gain access to the internal OT network. From there, you identify unsecured access to the substation's programmable controllers and replace one of the system's firmware components with a custom payload. This payload silently processes your commands while maintaining access across reboots.
Based on this action, which type of IoT OT threat are you simulating?

- A. Exploit kits
- B. Firmware update attack
- C. Forged malicious device
- D. Remote access using backdoor

Answer: B

Explanation:
The described activity most directly matches a firmware update attack. In CEH coverage of IoT and OT threats, firmware represents the low-level code that runs on embedded devices and industrial controllers, and compromising it is one of the most impactful persistence methods because it survives reboots and often persists through normal configuration resets. The scenario states that Sameer "replaces one of the system's firmware components with a custom payload" and that the payload "maintains access across reboots." Those are signature characteristics of a firmware-level compromise, typically achieved through insecure firmware update mechanisms, weak signing or verification controls, exposed update interfaces, or inadequate access controls on management ports.
A firmware update attack can occur when devices accept unsigned firmware, use weak integrity checks, allow downgrade to vulnerable versions, or expose update services without strong authentication. Once malicious firmware is installed, it can covertly execute commands, manipulate device behavior, hide its presence from higher-level monitoring, and create a durable foothold in OT environments where patching and reimaging are difficult. CEH emphasizes that OT devices such as programmable controllers and substation automation equipment are especially sensitive because firmware tampering can affect availability and safety, not just confidentiality.
Remote access using a backdoor is a broader concept and could be the payload's function, but the primary technique here is achieving persistence by modifying firmware. Forged malicious device refers to introducing rogue hardware, and exploit kits are typically used for automated exploitation on endpoints, not controller firmware replacement.

NEW QUESTION # 339
Emma, an ethical hacker at a Chicago-based healthcare provider, is performing a penetration test on the organization's patient record system following a recent data breach. During her investigation, she discovers that attackers gained access to a large volume of encrypted patient records but had no knowledge of the original data or encryption keys. Emma observes that the system uses a block cipher and suspects the attackers may have applied a cryptanalytic method that examines encrypted outputs in bulk to detect structural or statistical patterns in the encrypted data.
Which cryptanalysis technique should Emma investigate to assess the system's vulnerability in this scenario?

- A. Ciphertext-only attack
- B. Chosen-ciphertext attack
- C. Known-plaintext attack
- D. Chosen-plaintext attack

Answer: A

Explanation:
The correct answer is D, ciphertext-only attack, because the attackers possess only encrypted data and have neither the encryption key nor any confirmed samples of the original plaintext. In CEH-aligned cryptography concepts, cryptanalytic attacks are categorized by what information and capabilities the attacker has. A ciphertext-only attack is the most constrained model: the attacker attempts to infer the plaintext or key by analyzing ciphertext alone, often leveraging statistical properties, repetitions, formatting assumptions, and structural patterns that may leak information when encryption is misused.
The scenario highlights that the attacker "examines encrypted outputs in bulk" to detect "structural or statistical patterns." That wording maps directly to ciphertext-only analysis: looking for patterns caused by weak modes of operation, poor IV/nonce handling, deterministic encryption, repeated blocks (common in ECB mode), predictable headers, or consistent record templates. With block ciphers, large datasets increase the chance that repeated plaintext blocks produce repeated ciphertext blocks if the system uses an unsafe mode or reuses IVs, allowing an attacker to correlate records, identify fields, or sometimes recover content when combined with protocol or file-format knowledge.
The other options require more attacker capability than the prompt provides. Known-plaintext attacks require some plaintext-ciphertext pairs. Chosen-plaintext attacks require the ability to encrypt attacker-chosen inputs.
Chosen-ciphertext attacks require a decryption oracle or the ability to submit ciphertext for decryption. Since none of those are present here, Emma should evaluate ciphertext-only exposure and specifically validate the cipher mode, IV/nonce uniqueness, padding behavior, and whether encryption is semantically secure for stored patient records.
yes do please

NEW QUESTION # 340
During a physical penetration test at Sterling Electronics in Cleveland, ethical hacker Priya waits near the employee entrance during a shift change. When a group of staff enters the building using their access cards, Priya closely follows behind without swiping her own badge. None of the employees confront her, assuming she belongs there. Once inside, Priya proceeds to the break area where she documents the success of the exercise.
Which social engineering technique is Priya demonstrating?

- A. Piggybacking
- B. Shoulder Surfing
- C. Dumpster Diving
- D. Tailgating

Answer: D

Explanation:
This scenario demonstrates tailgating, which is gaining unauthorized physical access to a secure area by following an authorized person through an access-controlled entry point. Priya does not present credentials, swipe a badge, or otherwise authenticate; instead, she leverages normal human behavior and social assumptions during a busy shift change. Because employees assume she belongs there and do not challenge her, she successfully bypasses the physical access control.
Tailgating is common in workplaces with high traffic, open-plan culture, or weak enforcement of "no badge, no entry" rules. Attackers may exploit politeness, distraction, or the desire to hold doors open. It is especially effective during shift changes, deliveries, or when people are carrying items and appreciate someone holding the door. The security weakness being tested here is not the badge technology itself but the human factor: lack of challenge culture and inconsistent adherence to access policies.
Tailgating versus piggybacking: in many security references, piggybacking implies the authorized person knowingly allows the other to enter (e.g., holds the door intentionally after being asked). Tailgating typically implies the intruder enters without explicit

permission, often by slipping in behind a group. In this scenario, no one confronts her and they "assume she belongs there," indicating she is following them in without asking or being granted explicit permission-tailgating.
The other options are unrelated: shoulder surfing is visual observation of sensitive input; dumpster diving is retrieving information from trash. Therefore, the correct answer is C. Tailgating.

NEW QUESTION # 341
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

- A. PPP
- B. NTP
- C. OSPP
- D. Time Keeper

Answer: B

NEW QUESTION # 342
.....

By practicing our 312-50v13 exam braindumps, you will get the most coveted certificate smoothly. Before getting ready for your exam, having the ability to choose the best 312-50v13 practice materials is the manifestation of wisdom. Our 312-50v13 training engine can help you effectively pass the exam within a week. That is also proved that we are worldwide bestseller. Come and buy our 312-50v13 study dumps, you will get unexpected surprise.

Pdf 312-50v13 Exam Dump: https://www.testkingpdf.com/312-50v13-testking-pdf-torrent.html

TestkingPDF facilitates its customers with all the Q&A of the 312-50v13 ECCouncil Information Management real test, We highly recommend going through the 312-50v13 answers multiple times so you can assess your preparation for the Certified Ethical Hacker Exam (CEHv13), The ECCouncil 312-50v13 certification is a valuable credential and comes with certain benefits, Our 312-50v13 questions pdf is up to date, and we provide user-friendly 312-50v13 practice test software for the Certified Ethical Hacker Exam (CEHv13) exam.

Exporting a Presentation, The specific formula is, TestkingPDF facilitates its customers with all the Q&A of the 312-50v13 ECCouncil Information Management real test.

We highly recommend going through the 312-50v13 answers multiple times so you can assess your preparation for the Certified Ethical Hacker Exam (CEHv13), The ECCouncil 312-50v13 certification is a valuable credential and comes with certain benefits.

100% Pass Latest ECCouncil - Review 312-50v13 Guide

Our 312-50v13 questions pdf is up to date, and we provide user-friendly 312-50v13 practice test software for the Certified Ethical Hacker Exam (CEHv13) exam, Our ECCouncil 312-50v13 study materials will be your best dependable and reliable backup with guaranteed content.

- 100% Pass High Pass-Rate 312-50v13 - Review Certified Ethical Hacker Exam (CEHv13) Guide □ Simply search for [312-50v13] for free download on □ www.validtorrent.com □ □Certification 312-50v13 Test Questions
- Reliable 312-50v13 Test Question □ New 312-50v13 Exam Cram □ 312-50v13 Study Center □ Copy URL （ www.pdfvce.com ） open and search for { 312-50v13 } to download for free □Reliable 312-50v13 Test Question
- Error-Free ECCouncil 312-50v13 Exam Questions PDF Format □ 「 www.pdfdumps.com 」 is best website to obtain ➡ 312-50v13 □□□ for free download ♣New 312-50v13 Test Cram
- 312-50v13 Reliable Exam Voucher □ Latest 312-50v13 Test Testking ❊ Accurate 312-50v13 Test □ Search on □ www.pdfvce.com □ for ✔ 312-50v13 □✔□ to obtain exam materials for free download □312-50v13 Reliable Exam Pdf
- New 312-50v13 Exam Cram □ Authorized 312-50v13 Certification □ Exam 312-50v13 Guide Materials □ Search for ➡ 312-50v13 □□□ and easily obtain a free download on □ www.practicevce.com □ □Accurate 312-50v13 Test
- 100% Pass High Pass-Rate 312-50v13 - Review Certified Ethical Hacker Exam (CEHv13) Guide □ Open □ www.pdfvce.com □ and search for 《 312-50v13 》 to download exam materials for free □312-50v13 Reliable Exam

Pdf

- Certification 312-50v13 Test Questions □ 312-50v13 Study Center □ 312-50v13 Reliable Exam Pdf □ The page for free download of ➤ 312-50v13 □ on ➠ www.dumpsmaterials.com □ will open immediately □312-50v13 Latest Learning Materials
- Accurate 312-50v13 Test □ 312-50v13 Latest Learning Materials □ Latest 312-50v13 Test Testking □ Easily obtain " 312-50v13 " for free download through □ www.pdfvce.com □ □312-50v13 Reliable Exam Voucher
- Certification 312-50v13 Test Questions □ Complete 312-50v13 Exam Dumps □ 312-50v13 Valid Test Guide □ Simply search for □ 312-50v13 □ for free download on 「 www.easy4engine.com 」 ⌨Reliable 312-50v13 Test Question
- 312-50v13 Valid Test Guide □ 312-50v13 Reliable Exam Pdf □ 312-50v13 Study Center □ Copy URL ➽ www.pdfvce.com □ open and search for ➠ 312-50v13 □ to download for free □312-50v13 Study Center
- Latest 312-50v13 Study Materials □ Exam 312-50v13 Cram □ 312-50v13 Pass Rate □ Go to website ➤ www.troytecdumps.com □ open and search for 【 312-50v13 】 to download for free □Official 312-50v13 Study Guide
- 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, k12.instructure.com, 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, 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, Disposable vapes

BTW, DOWNLOAD part of TestkingPDF 312-50v13 dumps from Cloud Storage: https://drive.google.com/open?id=14l0mcUBVMMVaZyfoTXuNseQ6y75hdLvA