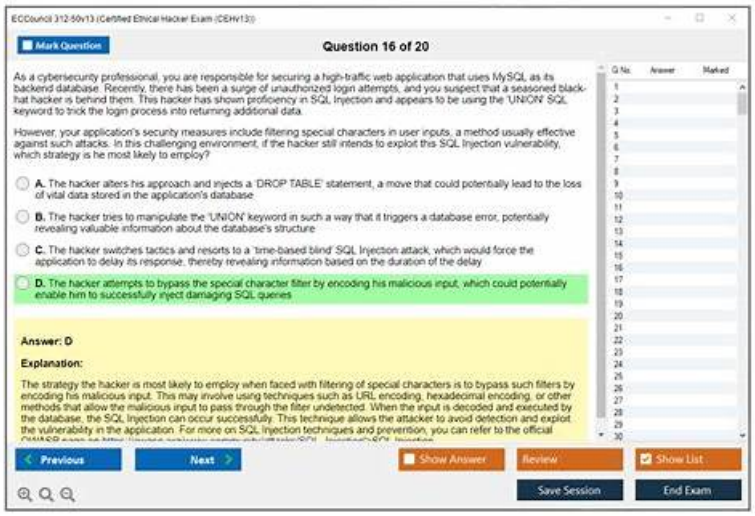
Regualer ECCouncil 312-50v13 Update, 312-50v13 Reliable Test Bootcamp



DOWNLOAD the newest RealVCE 312-50v13 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1ALFSesVMmY1JaOzdP-TSM0sHysd2GNto

If you are anxious about whether you can pass your exam and get the certificate, we think you need to buy our 312-50v13 study materials as your study tool, our product will lend you a good helping hand. If you are willing to take our 312-50v13 study materials into more consideration, it must be very easy for you to pass your exam in a short time. 99% people who have used our 312-50v13 Study Materials passed their exam and got their certificate successfully, it is no doubt that it means our 312-50v13 study materials have a 99% pass rate. So our product will be a very good choice for you.

This is the 312-50v13 PDF format which contains real 312-50v13 exam questions. You can print it and make a hard copy of this PDF file as well which helps you to prepare on the go. It comes in handy format and helps you prepare well with updated Certified Ethical Hacker Exam (CEHv13) exam questions. Moreover, this PDF has questions that are according to the present content of the test. This PDF format helps you to enhance your understanding of each topic which you need to self-evaluate to boost your ECCouncil 312-50v13 Exam Score.

>> Regualer ECCouncil 312-50v13 Update <<

312-50v13 Reliable Test Bootcamp | 312-50v13 Standard Answers

As we all know, if the content of your exam materials is complex and confusing, then if you want to pass the exam, you will be quite worried. Our 312-50v13 study guide helps the candidates to easily follow the needed contents with simplified languages and skillfully explanations according the perfect designs of the professional experts. Preparing with the help of our 312-50v13 Exam Questions frees you from getting help from other study sources, and you can pass the exam with 100% success guarantee.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q81-Q86):

NEW QUESTION # 81
During a red team engagement, an ethical hacker is tasked with testing the security measures of an organization's wireless network. The hacker needs to select an appropriate tool to carry out a session hijacking attack. Which of the following tools should the hacker use to effectively perform session hijacking and subsequent security analysis, given that the target wireless network has the Wi-Fi Protected Access-preshared key (WPA-PSK) security protocol in place?

- A. FaceNiff
- B. Hetty
- C. bettercap
- D. Droidsheep

Answer: C

Explanation:
bettercap is a tool that can perform session hijacking attacks on wireless networks, among other network security and penetration testing tasks. bettercap can capture and manipulate network traffic, perform man-in- the-middle attacks, spoof and sniff protocols, inject custom payloads, and more1.
bettercap can perform session hijacking attacks on wireless networks that use the WPA-PSK security protocol by exploiting the four-way handshake process that occurs when a client connects to a wireless access point.
The four-way handshake is used to establish a shared encryption key between the client and the access point, based on the pre-shared key (PSK) that is configured on both devices. However, the four-way handshake also exposes some information that can be used to crack the PSK offline, such as the nonce values, the MAC addresses, and the message integrity code (MIC) of the packets2.
bettercap can capture the four-way handshake packets using its Wi-Fi module and save them in a file. The file can then be fed to a tool like Hashcat or Aircrack-ng to crack the PSK using brute force or dictionary attacks. Once the PSK is obtained, bettercap can use it to decrypt the wireless traffic and perform session hijacking attacks on the clients connected to the access point3.
Therefore, bettercap is an appropriate tool to carry out a session hijacking attack on a wireless network that uses the WPA-PSK security protocol.
References:
bettercap: the Swiss Army knife for 802.11, BLE and Ethernet networks reconnaissance and MITM attacks How the WPA2 Enterprise Wireless Security Protocol Works Cracking WPA/WPA2 Passwords with Bettercap and Hashcat

NEW QUESTION # 82
Joe, a cybersecurity analyst at XYZ-FinTech, has been assigned to perform a quarterly vulnerability assessment across the organization ' s Windows-based servers and employee workstations. His objective is to detect issues such as software configuration errors, incorrect registry or file permissions, native configuration table problems, and other system-level misconfigurations. He is instructed to log into each system using valid credentials to ensure comprehensive data collection. Based on this assignment, which type of vulnerability scanning should Joe perform?

- A. Application Scanning
- B. External Scanning
- C. Network-based Scanning
- D. Host-based Scanning

Answer: D

Explanation:
The correct answer is Host-based Scanning. CEH vulnerability assessment material explains that host-based scanning focuses on individual systems such as servers, desktops, and workstations, and is intended to discover local security weaknesses including file permissions, registry permissions, patch issues, configuration errors, installed software problems, and operating-system-level exposures. The question explicitly mentions Windows servers and workstations, valid logins to each device, and inspection targets such as registry settings and local file permissions. Those are classic indicators of host-based scanning.
Network-based scanning would focus more on exposed network services, listening ports, protocol behavior, and remotely visible vulnerabilities. External scanning is concerned with internet-facing exposure from outside the organization. Application scanning is too narrow because the scenario is not limited to a specific software application but instead covers broad system-level posture. CEH guidance often notes that host-based vulnerability scans may be credentialed so the scanner can inspect the internal configuration of each machine in detail. Because the assessment is centered on system-specific misconfigurations and local security settings across endpoints and servers, host-based scanning is the best classification.

NEW QUESTION # 83
What kind of detection technique is used in antivirus software that collects data from multiple protected systems and performs analysis in a cloud-based environment?

- A. Heuristics based
- B. Honeypot based
- C. VCloud based
- D. Behavior based

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
VCloud-based (also known as Cloud-based or Cloud-assisted) antivirus leverages cloud computing to:
Offload detection and analysis to powerful remote servers
Provide real-time updates and threat intelligence
Aggregate data from multiple endpoints to improve detection
This method is efficient, especially for zero-day threats and large-scale protection.
From CEH v13 Courseware:
Module 6: Malware Threats # Modern Antivirus Technologies
Reference:CEH v13 Study Guide - Cloud-Based Antivirus Detection
═══

NEW QUESTION # 84
Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However, you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?

- A. Switching all data transmission to the HTTPS protocol.
- B. Implementing SSL certificates on your company's web servers.
- C. Applying the Diffie-Hellman protocol to exchange the symmetric key.
- D. Utilizing SSH for secure remote logins to the servers.

Answer: C

Explanation:
The protocol that you would recommend to the team to achieve the secure exchange of the symmetric key is the Diffie-Hellman protocol. The Diffie-Hellman protocol is a key agreement protocol that allows two or more parties to establish a shared secret key over an unsecured communication channel, without having to exchange the key itself. The Diffie-Hellman protocol works as follows12:
* The parties agree on a large prime number p and a generator g, which are public parameters that can be known by anyone.
* Each party chooses a random private number a or b, which are kept secret from anyone else.
* Each party computes a public value A or B, by raising g to the power of a or b modulo p, i.e., A = g