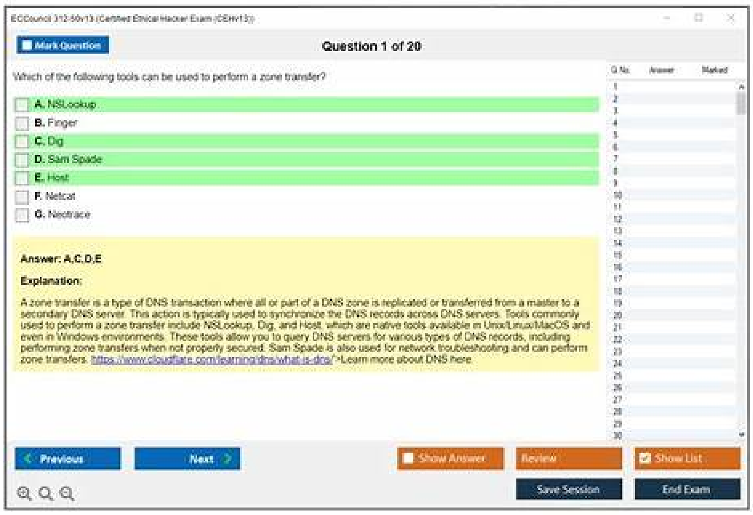
Will ECCouncil 312-50v13 Practice Questions help You to Pass the certification exam?



Which of the following tools can be used to perform a zone transfer?

- □ A. NSLookup
- □ B. Finger
- □ C. Dig
- □ D. Sam Spade
- □ E. Host
- □ F. Netcat
- □ G. Neotrace

Answer: A,C,D,E

Explanation:

A zone transfer is a type of DNS transaction where all or part of a DNS zone is replicated or transferred from a master to a secondary DNS server. This action is typically used to synchronize the DNS records across DNS servers. Tools commonly used to perform a zone transfer include NSLookup, Dig, and Host, which are native tools available in Unix/Linux/MacOS and even in Windows environments. These tools allow you to query DNS servers for various types of DNS records, including performing zone transfers when not properly secured. Sam Spade is also used for network troubleshooting and can perform zone transfers. https://www.cloudflare.com/learning/dns/what-is-dns/">Learn more about DNS here

BTW, DOWNLOAD part of Pass4suresVCE 312-50v13 dumps from Cloud Storage: https://drive.google.com/open?id=1JxZui3B87W5w-mdGq7dXrsGVtdzZI9pS

Pass4suresVCE is a website which always provide you the latest and most accurate information about ECCouncil certification 312-50v13 exam. In order to allow you to safely choose us, you can free download part of the exam practice questions and answers on Pass4suresVCE website as a free try. Pass4suresVCE can ensure you 100% pass ECCouncil Certification 312-50v13 Exam.

The majority of people encounter the issue of finding extraordinary Certified Ethical Hacker Exam (CEHv13) (312-50v13) exam dumps that can help them prepare for the actual ECCouncil 312-50v13 exam. They strive to locate authentic and up-to-date ECCouncil 312-50v13 Practice Questions for the Financials in Certified Ethical Hacker Exam (CEHv13) (312-50v13) exam, which is a tough ask.

>> 312-50v13 Exam Simulator Free <<

312-50v13 100% Accuracy | 312-50v13 Flexible Learning Mode

However, Pass4suresVCE saves your money by offering 312-50v13 real questions at an affordable price. In addition, we offer up to 12 months of free 312-50v13 exam questions. This way you can save money even if 312-50v13 introduces fresh Certified Ethical Hacker Exam (CEHv13) 312-50v13 exam updates. Purchase the ECCouncil 312-50v13 preparation material to get certified on the first attempt.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q258-Q263):

NEW QUESTION # 258
A city's power management system relies on SCADA infrastructure. Recent anomalies include inconsistent sensor readings and intermittent outages. Security analysts suspect a side-channel attack designed to extract sensitive information covertly from SCADA devices. Which investigative technique would best confirm this type of attack?

- A. Assessing SCADA user interfaces for unauthorized access or misuse.
- B. Measuring unusual physical or electrical fluctuations during device operation at the hardware level.
- C. Identifying weak cryptographic configurations in device communications.

Answer: B

Explanation:
According to the Certified Ethical Hacker (CEH) IoT, OT, and SCADA Security module, side-channel attacks exploit indirect

information leaks such as power consumption, electromagnetic emissions, timing variations, or thermal output rather than software vulnerabilities.
Option A is correct because monitoring hardware-level anomalies is the primary method for detecting side- channel exploitation.
CEH materials emphasize that these attacks bypass traditional security controls.
Option B relates to cryptographic weaknesses, not side-channel analysis.
Option C addresses interface misuse, not covert data leakage.
CEH highlights that SCADA systems are especially vulnerable due to legacy hardware and limited monitoring capabilities.

NEW QUESTION # 259
Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port
445 is active and listening. Eve uses the ENUM tool to enumerate Alice's machine. From the command prompt, she types the following command:
What is Eve trying to do?

- A. Eve is trying to connect as a user with Administrator privileges
- B. Eve is trying to enumerate all users with Administrative privileges
- C. Eve is trying to escalate privilege of the null user to that of Administrator
- D. Eve is trying to carry out a password crack for user Administrator

Answer: D

Explanation:
The command shown is a Windows batch loop that attempts to mount a hidden administrative share (c$) on a remote machine (\10.1.2.3) using the username "Administrator" and a list of passwords from the file hackfile.
txt.
* for /f "tokens=1 %%a in (hackfile.txt) # Reads one password per line from the file
* do net use * \10.1.2.3\c$ /user:"Administrator" %%a # Tries to authenticate to the share using the Administrator account and each password This is a classic brute-force password attack attempting to crack the Administrator account using a wordlist.
From CEH v13 Official Courseware:
* Module 4: Enumeration
* Module 6: Malware and Password Cracking Techniques
CEH v13 Study Guide states:
"Tools and scripts that automate login attempts using SMB shares and administrative credentials can be used to brute force user accounts. An attacker attempts access using a list of passwords (dictionary attack)." Incorrect Options:
* A: The connection attempt is made, but the success is dependent on password cracking.
* B: This command does not enumerate users.
* D: No null session involved; this is a brute-force attempt, not privilege escalation.
Reference:CEH v13 Study Guide - Module 4: Enumeration # Brute-force TechniquesMicrosoft TechNet: net use command documentation

NEW QUESTION # 260
Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

- A. SSH communications are encrypted; it's impossible to know who is the client or the server.
- B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.
- C. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.
- D. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.

Answer: C

Explanation:
Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip Let's just disassemble this entry.
Mar 1, 2016, 7:33:28 AM - time of the request
10.240.250.23 - 54373 - client's IP and port
10.249.253.15 - server IP
- 22 - SSH port

NEW QUESTION # 261

Multiple internal workstations and IoT devices are compromised and transmitting large volumes of traffic to numerous external targets under botnet control. Which type of denial-of-service attack best describes this situation?

- A. An internal amplification attack using spoofed DNS responses
- B. A direct botnet flood without spoofing intermediary services
- C. An attack where compromised internal devices participate in a botnet and flood external targets
- D. An attack relying on spoofed IP addresses to trick external servers

Answer: C

Explanation:
This scenario represents a Botnet-Based Distributed Denial-of-Service (DDoS) attack, as described in CEH v13 Network Attacks. Compromised internal devices become part of a botnet and are used to launch attacks against external targets.
CEH v13 notes that botnets frequently include IoT devices and employee workstations, making insider- originated DDoS activity a serious concern.

NEW QUESTION # 262

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

Answer: D

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