

2026 100% Free 312-50v13–High-quality 100% Free Test Topics Pdf | Pdf Demo 312-50v13 Download

► When was AUE2601 Assignment 01 submitted? Answer: 16 March 2020.

► What is the consequence of allowing another student to copy your work? Answer: It violates the declaration and could lead to disciplinary action.

► What is the purpose of the Unisa Disciplinary Code for Students? Answer: To outline the rules and consequences regarding academic integrity and conduct.

► What should students do if they are found in violation of the assignment declaration? Answer: They will receive 0% for the assignment.

► What is the correct sequence for answering sub-sections in AUE2601? Answer: Answer in numerical sequence.

► What is the nature of audit evidence according to the assignment? Answer: Audit evidence is persuasive rather than conclusive.

► What is one responsibility of shareholders regarding financial statements? Answer: They are responsible for reporting the results of their stewardship in the annual financial statements.

2026 Latest Actual Tests Quiz 312-50v13 PDF Dumps and 312-50v13 Exam Engine Free Share: <https://drive.google.com/open?id=18Vpr4ek0qQE-daUe9YKlbfEiUgg64k3>

We invited a large group of professional experts who dedicated in this 312-50v13 training guide for more than ten years. To improve the accuracy of the 312-50v13 guide preparations, they keep up with the trend closely. Every page is carefully arranged by them with high efficiency and high quality. Up to now, there are three versions of 312-50v13 Exam Materials for your choice. So high-quality contents and flexible choices of 312-50v13 learning mode will bring about the excellent learning experience for you.

We offer you to take back your money, if you do not succeed in 312-50v13 exam. Such a guarantee in itself is concrete evidence on the unmatched quality of our 312-50v13 dumps. For the reason, they are approved not only by a large number of professionals who are busy in developing their careers but also by the industry experts. Get the right reward for your potential, believing in the easiest and to the point 312-50v13 Exam Questions that are meant to bring you a brilliant success in 312-50v13 exams.

>> 312-50v13 Test Topics Pdf <<

Unparalleled ECCouncil 312-50v13 Test Topics Pdf: Certified Ethical Hacker Exam (CEHv13) Pass Guaranteed

Our Certified Ethical Hacker Exam (CEHv13) (312-50v13) practice exam simulator mirrors the Certified Ethical Hacker Exam (CEHv13) (312-50v13) exam experience, so you know what to anticipate on Certified Ethical Hacker Exam (CEHv13) (312-50v13) certification exam day. Our ECCouncil 312-50v13 Practice Test software features various question styles and levels, so you can customize your ECCouncil 312-50v13 exam questions preparation to meet your needs.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q354-Q359):

NEW QUESTION # 354

A large enterprise has been experiencing sporadic system crashes and instability, resulting in limited access to its web services. The security team suspects it could be a result of a Denial of Service (DoS) attack. A significant increase in traffic was noticed in the network logs, with patterns suggesting packet sizes exceeding the prescribed size limit. Which among the following DoS attack techniques best describes this scenario?

- A. Smurf attack
- **B. Ping of Death attack**
- C. Pulse wave attack
- D. UDP flood attack

Answer: B

Explanation:

A Ping of Death attack is a type of DoS attack that exploits a vulnerability in the IP protocol that allows packets to be fragmented and reassembled at the destination. The attacker sends a malformed packet that exceeds the maximum size of 65,535 bytes, which causes the target system to crash or become unstable when it tries to reassemble the packet. This attack can affect various operating systems and devices, such as routers, switches, and firewalls. A Ping of Death attack can be detected by monitoring the network traffic for unusually large packets or ICMP messages. References:

* Ping of Death (PoD) Attack

* Denial-of-Service Attacks: History, Techniques & Prevention

* What is a denial-of-service (DoS) attack?

NEW QUESTION # 355

What does a firewall check to prevent particular ports and applications from getting packets into an organization?

- A. Application layer port numbers and the transport layer headers
- **B. Transport layer port numbers and application layer headers**
- C. Presentation layer headers and the session layer port numbers
- D. Network layer headers and the session layer port numbers

Answer: B

NEW QUESTION # 356

Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints.

What is the technique followed by Peter to send files securely through a remote connection?

- A. Switch network
- B. DMZ
- C. SMB signing
- **D. VPN**

Answer: D

Explanation:

In CEH v13 Module 14: Cryptography, VPN (Virtual Private Network) technology is described as the method that allows users to securely transmit data over an insecure (public) network by establishing a secure, encrypted tunnel.

VPN Features:

Encrypts all traffic between the user's device and the target network.

Prevents session hijacking, eavesdropping, and man-in-the-middle (MITM) attacks.

Common protocols: IPSec, L2TP, SSL VPN, and OpenVPN.

Option Clarification:

- A). DMZ: A network segmentation strategy, not an encryption method.
- B). SMB signing: Ensures integrity for SMB protocol, but not for remote tunneling.
- C). VPN: Correct. Used to securely tunnel over public networks.
- D). Switch network: Refers to network segmentation using switches, unrelated to tunneling.

Reference:

Module 14 - VPNs and Secure Communication Protocols

CEH iLabs: Configuring and Testing a VPN Tunnel

NEW QUESTION # 357

Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?

- A. Compound SQLi
- **B. Blind SQLi**
- C. DMS-specific SQLi
- D. Classic SQLi

Answer: B

Explanation:

https://en.wikipedia.org/wiki/SQL_injection#Blind_SQL_injection

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered, and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

NEW QUESTION # 358

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?

- A. The security breach was a false positive.
- B. The attacker altered or erased events from the logs.
- **C. The network devices are not all synchronized.**
- D. Proper chain of custody was not observed while collecting the logs.

Answer: C

Explanation:

Many network and system administrators don't pay enough attention to system clock accuracy and time synchronization. Computer clocks can run faster or slower over time, batteries and power sources die, or daylight-saving time changes are forgotten. Sure, there are many more pressing security issues to deal with, but not ensuring that the time on network devices is synchronized can cause problems. And these problems often only come to light after a security incident.

If you suspect a hacker is accessing your network, for example, you will want to analyze your log files to look for any suspicious activity. If your network's security devices do not have synchronized times, the timestamps' inaccuracy makes it impossible to correlate log files from different sources. Not only will you have difficulty in tracking events, but you will also find it difficult to use such evidence in court; you won't be able to illustrate a smooth progression of events as they occurred throughout your network.

NEW QUESTION # 359

.....

No doubt the Certified Ethical Hacker Exam (CEHv13) (312-50v13) certification exam is a challenging exam that always gives a tough time to their candidates. However, with the help of ActualTestsQuiz ECCouncil Exam Questions, you can prepare yourself quickly to pass the Certified Ethical Hacker Exam (CEHv13) exam. The ActualTestsQuiz ECCouncil 312-50v13 Exam Dumps are real, valid, and updated ECCouncil 312-50v13 practice questions that are ideal study material for quick Certified Ethical Hacker

Pdf Demo 312-50v13 Download: <https://www.actualtestsquiz.com/312-50v13-test-torrent.html>

Any individual with a valid card could gain access to the building. This gives them the ability to pick up and move whenever they want. Please try 312-50v13 Free Practice pdf demo we offer you.

So you can do your decision whether to choose 312-50v13 exam dumps or not, And at the same time, there are many incomprehensible knowledge points and boring descriptions 312-50v13 in the book, so that many people feel a headache and sleepy when reading books.

[illegible]

BTW, DOWNLOAD part of ActualTestsQuiz 312-50v13 dumps from Cloud Storage: <https://drive.google.com/open?id=18Vpr4ek0qOE-daUe9YiKlbFEiUgg64k3>