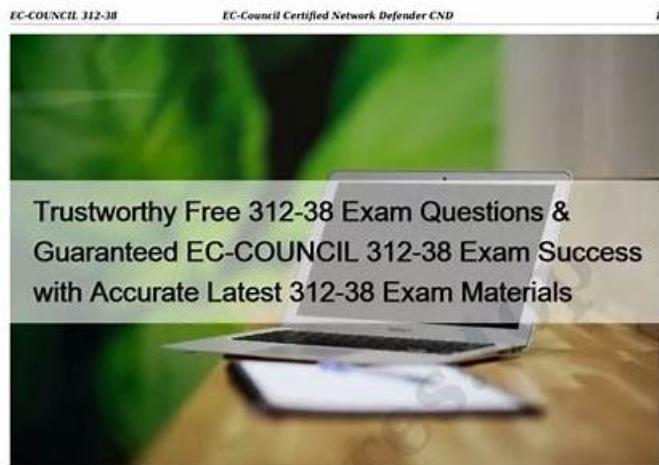


Latest 312-38 Exam Torrent Must Be a Great Beginning to Prepare for Your Exam - Itcerttest



Pass4sure provides updated and valid EC-COUNCIL 312-38 Exam Questions because we are aware of the absolute importance of updates, keeping in mind the EC-COUNCIL 312-38 Exam Syllabus. We provide you update checks for 365 days after purchase for absolutely no cost. And the EC-Council Certified Network Defender CND 312-38 price is affordable.

To keep with such an era, when new knowledge is emerging, you need to pursue latest news and grasp the direction of entire development tendency, our 312-38 training questions have been constantly improving our performance and updating the exam bank to meet the conditional changes. Our working staff regards checking update of our 312-38 Preparation exam as a daily routine. So without doubt, our 312-38 exam questions are always the latest and valid.

>> Free 312-38 Exam Questions <<

Latest 312-38 Exam Materials - Certification 312-38 Exam Dumps

EC-COUNCIL 312-38 certification exam is one of the most valuable certification exams. IT industry is under rapid development in the new century, the demands for IT talents are increased year by year. Therefore, a lots of people want to become the darling of the workplace by IT certification. How to get you through the EC-COUNCIL 312-38 certification? The questions and the answers Pass4sure EC-COUNCIL provides are your best choice. It is difficult to pass the test and the proper shortcut is necessary. EC-COUNCIL Business Solutions Pass4sure 312-38 Dumps rewritten by high rated top IT experts to the ultimate level of technical accuracy. The version is the most latest and it has a high quality products.

Trustworthy Free 312-38 Exam Questions & Guaranteed EC-COUNCIL 312-38 Exam Success with Accurate Latest 312-38 Exam Materials

P.S. Free 2026 EC-COUNCIL 312-38 dumps are available on Google Drive shared by Itcerttest: https://drive.google.com/open?id=1xEUrbu3J3w2vnLCo_Lcc6VPoDwF1hLq

Our 312-38 practice quiz will provide three different versions, the PDF version, the software version and the online version. The trait of the software version of our 312-38 exam dump is very practical. Although this version can only be run on the windows operating system, the software version our 312-38 Guide materials is not limited to the number of computers installed, you can install the software version in several computers. So you will like the software version, of course, you can also choose other versions of our 312-38 study torrent if you need.

The EC-Council Certified Network Defender (CND) exam is designed to test a candidate's knowledge and skills in network security and defense. It is a vendor-neutral certification that is recognized globally and is highly sought after by organizations looking to hire professionals who can protect their networks from cyber threats. 312-38 Exam covers topics such as network security protocols, perimeter defense, intrusion detection and prevention, and incident response and recovery.

>> 312-38 Reliable Exam Tutorial <<

Study 312-38 Plan & 312-38 New Study Questions

With the development of information and communications technology, we are now living in a globalized world. 312-38 information

technology learning is correspondingly popular all over the world. Modern technology has changed the way how we live and work. When it comes to the study materials selling in the market, qualities are patchy. But our 312-38 test material has been recognized by multitude of customers, which possess of the top-class quality, can help you pass exam successfully. On the other hand, our 312-38 Latest Dumps are designed by the most experienced experts, thus it can not only teach you knowledge, but also show you the method of learning in the most brief and efficient ways.

The EC-Council Certified Network Defender CND certification exam is intended for IT professionals who are involved in network defense and are responsible for securing the infrastructure of an organization against a range of cyber threats. EC-Council Certified Network Defender CND certification is globally recognized as a benchmark for network defense expertise and is considered by many organizations to be a prerequisite for roles such as Network Administrator, Security Officer, and Information Security Analyst.

EC-COUNCIL EC-Council Certified Network Defender CND Sample Questions (Q674-Q679):

NEW QUESTION # 674

Which among the following filter is used to detect a SYN/FIN attack?

- A. `tcp.flags==0x003`
- B. `tcp.flags==0x004`
- C. `tcp.flags==0x001`
- D. `tcp.flags==0x002`

Answer: A

Explanation:

The filter `tcp.flags==0x003` is used to detect SYN/FIN attacks. This filter is designed to identify packets where both the SYN and FIN flags are set, which is an unusual combination and indicative of a potential SYN/FIN attack. In a typical TCP communication, a SYN flag is used to initiate a connection, and a FIN flag is used to gracefully close a connection. Therefore, seeing both flags set in a single packet suggests a malformed or malicious packet, which is characteristic of a SYN/FIN attack.

NEW QUESTION # 675

Which of the following examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations?

- A. Wireless Intrusion Prevention System
- B. **Network Behavior Analysis**
- C. Host-based Intrusion Prevention
- D. Network-based Intrusion Prevention

Answer: B

Explanation:

Explanation

Explanation:

Network Behavior Analysis examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.

Answer option B is incorrect. Network-based Intrusion Prevention (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

Answer option C is incorrect. Wireless Intrusion Prevention System (WIPS) monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

Answer option D is incorrect. Host-based Intrusion Prevention (HIPS) is an installed software package that monitors a single host for suspicious activity by analyzing events occurring within that host.

NEW QUESTION # 676

A local bank wants to protect their card holder data. The bank should comply with the _____ standard to ensure the security of card holder data.

- A. SOAX
- B. HIPAA

- C. ISEC
- D. PCI DSS

Answer: D

NEW QUESTION # 677

The risk assessment team in Southern California has estimated that the probability of an incident that has potential to impact almost 80% of the bank's business is very high. How should this risk be categorized in the risk matrix?

- A. Low
- B. Extreme
- C. High
- D. Medium

Answer: B

Explanation:

In the context of risk assessment, an incident that has a very high probability of occurring and the potential to impact almost 80% of a business is considered an extreme risk. This categorization is based on the severity of the impact and the likelihood of the event. The risk matrix, a tool used in risk assessment, helps in the classification of risks by considering both the impact and the probability of potential incidents. An event that affects such a significant portion of the business would typically necessitate immediate attention and the implementation of mitigation strategies to prevent substantial loss or damage.

References: The Certified Network Defender (CND) curriculum includes principles of risk assessment and the use of risk matrices to categorize and prioritize risks. It outlines that risks with high impact and high probability should be classified as extreme, requiring urgent action12.

NEW QUESTION # 678

Which of the following statements best describes the consequences of a disaster recovery test?

- A. If no deficiencies were found during the test, the test was probably erroneous.
- B. The test results should be kept secret.
- C. If no deficiencies were found during the test, so the plan is probably perfect.
- D. None
- E. The plan should not change any of the test results would be.

Answer: A

NEW QUESTION # 679

.....

Study 312-38 Plan: https://www.itcerttest.com/312-38_braindumps.html

- Latest 312-38 Study Materials □ 312-38 Valid Study Guide □ 312-38 New Dumps Files □ Search on  www.easy4engine.com  for (312-38) to obtain exam materials for free download □ 312-38 New Dumps Files
- 312-38 Latest Exam Practice □ Detailed 312-38 Answers □ Exams 312-38 Torrent □ Open ➔ www.pdfvce.com □  enter 「 312-38 」 and obtain a free download □ Pass 312-38 Rate
- 312-38 Exam Study Guide - 312-38 PDF prep material - 312-38 Exam Training Test □ Search for ✓ 312-38 □ ✓ □ and download it for free immediately on “ www.pass4test.com ” □ Latest 312-38 Exam Online
- 312-38 New Dumps Files □ New 312-38 Test Materials □ Pass 312-38 Rate □ Download 《 312-38 》 for free by simply searching on ➔ www.pdfvce.com  312-38 Latest Practice Materials
- 100% Pass 2026 High Pass-Rate 312-38: EC-Council Certified Network Defender CND Reliable Exam Tutorial □ Search on □ www.examcollectionpass.com □ for □ 312-38 □ to obtain exam materials for free download □ 312-38 Latest Practice Materials
- 100% Pass 2026 High Pass-Rate 312-38: EC-Council Certified Network Defender CND Reliable Exam Tutorial □ Search for ➤ 312-38 □ on □ www.pdfvce.com □ immediately to obtain a free download □ New 312-38 Test Materials
- 312-38 Review Guide □ 312-38 Latest Material □ New 312-38 Test Materials □ Search on ➔ www.troyecdumps.com  for 《 312-38 》 to obtain exam materials for free download □ 312-38 New Dumps Files

P.S. Free 2026 EC-COUNCIL 312-38 dumps are available on Google Drive shared by Itcerttest: https://drive.google.com/open?id=1xEUrxbu3J3w2vnLCo_Lcc6VPoDwF1hLq