

Online 312-38 Tests & 312-38 Latest Dumps Sheet

EC-COUNCIL 312-38

EC-Council Certified Network Defender CND

1



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

Pass4sures 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 Pass4sures EC-COUNCIL provides are your best choice. It is difficult to pass the test and the proper shortcut is necessary. EC-COUNCIL Business Solutions Pass4sures [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 & New 312-38 dumps are available on Google Drive shared by Exam4Free: https://drive.google.com/open?id=1XIY8LJFhglT9uCOFnMzMfN_FwnMtPRx

We're committed to ensuring you have access to the best possible 312-38 questions. We offer 312-38 dumps in PDF, web-based practice tests, and desktop practice test software. We provide these 312-38 questions in all three formats since each has useful features of its own. If you prepare with EC-Council Certified Network Defender CND (312-38) actual dumps, you will be fully prepared to pass the test on your first attempt.

The EC-Council CND certification is ideal for professionals who are responsible for managing and protecting network infrastructures. EC-Council Certified Network Defender CND certification covers a variety of topics, including network security, network protocols, and network defense technologies. 312-38 Exam is designed to test the candidate's ability to identify and mitigate potential threats to network infrastructure, as well as their ability to implement security measures that can prevent attacks.

>> Online 312-38 Tests <<

EC-COUNCIL 312-38 Latest Dumps Sheet, Exam Dumps 312-38 Zip

How can our 312-38 practice materials become salable products? Their quality with low prices is unquestionable. There are no better or cheaper practice materials can replace our 312-38 exam questions as alternatives while can provide the same functions. The accomplished 312-38 Guide exam is available in the different countries around the world and being testified over the customers around the different countries. They are valuable acquisitions to the filed.

EC-COUNCIL EC-Council Certified Network Defender CND Sample Questions (Q543-Q548):

NEW QUESTION # 543

Who is responsible for conveying company details after an incident?

- A. PR specialist
- B. IR manager
- C. IR custodians
- D. IR officer

Answer: A

NEW QUESTION # 544

A network administrator is monitoring the network traffic with Wireshark. Which of the following filters will she use to view the packets moving without setting a flag to detect TCP Null Scan attempts?

- A. `Tcp.flags==0X029`
- B. `Tcp.flags==0x003`
- C. `Tcp.dstport==7`
- D. `TCRflags==0x000`

Answer: D

Explanation:

In Wireshark, to detect TCP Null Scan attempts, the filter used is `tcp.flags==0`. This filter will show packets where no TCP flags are set, which is indicative of a TCP Null Scan. A TCP Null Scan is a type of network reconnaissance technique where the attacker sends TCP packets with no flags set to the target system. If the target system responds with a RST packet, it indicates that the port is closed, while no response suggests that the port is open or filtered. This method is used because some systems do not log these null packets, allowing the scan to go unnoticed.

References: The information provided is based on standard network security practices for monitoring and analyzing network traffic using Wireshark, as well as the specific details of TCP Null Scans and their detection as outlined in network security resources¹.

NEW QUESTION # 545

The _____ mechanism works on the basis of a client-server model.

- A. Push-based
- B. Pull-based
- C. Host-based
- D. Network-based

Answer: B

NEW QUESTION # 546

CORRECT TEXT

Fill in the blank with the appropriate term. A _____ network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used for preventing the collision of data between two computers that want to send messages at the same time.

Answer:

Explanation:

Token Ring

Explanation:

A Token Ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time. The Token Ring protocol is the second most widely-used protocol on local area networks after Ethernet. The IBM

Token Ring protocol led to a standard version, specified as IEEE 802.5. Both protocols are used and are very similar. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second. Working: Empty information frames are constantly circulated on the ring. When a computer has a message to send, it adds a token to an empty frame and adds a message and a destination identifier to the frame. The frame is then observed by each successive workstation. If the workstation sees that it is the destination for the message, it copies the message from the frame and modifies the token back to 0. When the frame gets back to the originator, it sees that the token has been modified to 0 and that the message has been copied and received. It removes the message from the particular frame. The frame continues to circulate as an empty frame, ready to be taken by a workstation when it has a message to send.

NEW QUESTION # 547

In which of the following attacks does an attacker use software that tries a large number of key combinations in order to get a password?

- A. Zero-day attack
- **B. Brute force attack**
- C. Buffer overflow
- D. Smurf attack

Answer: B

Explanation:

In a brute force attack, an attacker uses software that tries a large number of key combinations in order to get a password. To prevent such attacks, users should create passwords that are more difficult to guess, i.e., by using a minimum of six characters, alphanumeric combinations, and lower-upper case combinations.

Answer option D is incorrect. Smurf is an attack that generates significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages. In such attacks, a perpetrator sends a large amount of ICMP echo request (ping) traffic to IP broadcast addresses, all of which have a spoofed source IP address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all hosts, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, which multiplies the traffic by the number of hosts responding.

Answer option A is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. It helps an attacker not only to execute a malicious code on the target system but also to install backdoors on the target system for further attacks. All buffer overflow attacks are due to only sloppy programming or poor memory management by the application developers. The main types of buffer overflows are:

Stack overflow

Format string overflow

Heap overflow

Integer overflow

Answer option C is incorrect. A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks.

NEW QUESTION # 548

.....

Our company is a well-known multinational company, has its own complete sales system and after-sales service worldwide. In the same trade at the same time, our 312-38 study materials has become a critically acclaimed enterprise, so, if you are preparing for the exam qualification and obtain the corresponding certificate, so our company launched 312-38 Learning Materials is the most reliable choice of you. The service tenet of our company and all the staff work mission is: through constant innovation and providing the best quality service, make the 312-38 study materials become the best customers electronic test study materials.

312-38 Latest Dumps Sheet: <https://www.exam4free.com/312-38-valid-dumps.html>

- 2026 Online 312-38 Tests 100% Pass | Trustable EC-Council Certified Network Defender CND Latest Dumps Sheet Pass for sure ☐ Open (www.practicevce.com) and search for 《 312-38 》 to download exam materials for free ☐ 312-38 Study Dumps
- Buy 312-38 Exam Q-A PDF - One Year Free Update ☐ Search for ☐ 312-38 ☐ and obtain a free download on ☒ www.pdfvce.com ☐ ☒ 312-38 Vce Exam

- P.S. Free & New 312-38 dumps are available on Google Drive shared by Exam4Free: https://drive.google.com/open?id=1XIY8LJFhgIT9uCOFnMzCmfN_FwnMtPRx

P.S. Free & New 312-38 dumps are available on Google Drive shared by Exam4Free: https://drive.google.com/open?id=1XIY8LJFhgIT9uCOFnMzCmfN_FwnMtPRx