Pass Guaranteed Quiz 312-38 - High Pass-Rate EC-Council Certified Network Defender CND Exams Dumps

DOWNLOAD the newest BraindumpQuiz 312-38 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1i_TwNCWiigGM3L7mrUDfoOzaMqayK06S

These practice tools are developed by professionals who work in fields impacting EC-COUNCIL certification, giving them a foundation of knowledge and actual competence. Our EC-COUNCIL 312-38 Exam Questions are created and curated by industry specialists. BraindumpQuiz Is Here To Provide Top-Notch EC-COUNCIL 312-38 Exam Questions

EC-COUNCIL 312-38 certification exam is designed to test the knowledge and skills of individuals who are interested in network defense and security. EC-Council Certified Network Defender CND certification is also known as the EC-Council Certified Network Defender (CND) certification. 312-38 Exam is designed to ensure that candidates have the necessary skills to protect networks against cyberattacks and other security threats.

>> 312-38 Exams Dumps <<

EC-COUNCIL 312-38 Practice Test In Desktop Format

With our 312-38 test prep, you don't have to worry about the complexity and tediousness of the operation. Our 312-38 exam torrent is available in different versions. Whether you like to study on a computer or enjoy reading paper materials, our test prep can meet your needs. Our PDF version of the 312-38 quiz guide is available for customers to print. You can print it out, so you can practice it repeatedly conveniently. And our 312-38 Exam Torrent make it easy for you to take notes on it so that your free time can be well utilized and you can often consolidate your knowledge. Everything you do will help you successfully pass the exam and get the card.

EC-COUNCIL EC-Council Certified Network Defender CND Sample Questions (Q376-Q381):

NEW QUESTION # 376
Which among the following filter is used to detect a SYN/FIN attack?

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

Answer: C

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.
References: The use of the filter tcp.flags==0x003 for detecting SYN/FIN attacks is discussed in various cybersecurity resources and aligns with the knowledge required for the Certified Network Defender (CND) certification. This specific filter is mentioned in discussions about network security and intrusion detection techniques1.

NEW QUESTION # 377
What is the correct order of activities that a IDS is supposed to attempt in order to detect an intrusion?

- A. Prevention, Intrusion Monitoring, Intrusion Detection, Response
- B. Intrusion Monitoring, Intrusion Detection, Response, Prevention
- C. Intrusion Detection, Response, Prevention, Intrusion Monitoring
- D. Prevention, Intrusion Detection, Response, Intrusion Monitoring

Answer: B

Explanation:
An Intrusion Detection System (IDS) is designed to monitor network or system activities for malicious actions or policy violations. The correct order of activities that an IDS follows to detect an intrusion starts with Intrusion Monitoring, where it observes the network traffic or system events. Following this, Intrusion Detection takes place, where the IDS analyzes the monitored data to identify potential security breaches. Once a potential intrusion is detected, the Response mechanism is activated to address the intrusion, which may include alerts or automatic countermeasures. Finally, Prevention is applied to improve the system's defenses against future intrusions based on the detected patterns and responses.

NEW QUESTION # 378
Which of the following layers of the OSI model provides physical addressing?

- A. Data link layer
- B. Network layer
- C. Application layer
- D. Physical layer

Answer: A

NEW QUESTION # 379
John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization's network. Which of the following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt?

- A. Tcp.flags==0x2b
- B. Tcp.options.wscale_val==20
- C. Tcp.flags=0x00
- D. Tcp.options.mss_val<1460

Answer: A,C,D

NEW QUESTION # 380
Which encryption algorithm h used by WPA5 encryption?

- A. AES-GCMP 256
- B. RC4
- C. RC4.TKIP
- D. AES-CCMP

Answer: D

NEW QUESTION # 381
.....

As what have been demonstrated in the records concerning the pass rate of our 312-38 free demo, our pass rate has kept the historical record of 98% to 99% from the very beginning of their foundation. Although at this moment, the pass rate of our 312-38 test torrent can be said to be the best compared with that of other exam tests, our experts all are never satisfied with the current results because they know the truth that only through steady progress can our 312-38 Preparation materials win a place in the field of 312-38 exam question making forever.

312-38 Best Study Material: https://www.braindumpquiz.com/312-38-exam-material.html

- Free PDF Quiz 312-38 - EC-Council Certified Network Defender CND –Efficient Exams Dumps □ Download （ 312-38 ） for free by simply searching on ▹ www.practicevce.com ◃ □New 312-38 Exam Pattern
- Valid Test 312-38 Fee □ Reliable 312-38 Study Plan □ New 312-38 Exam Pattern □ Open ➥ www.pdfvce.com □ enter 「 312-38 」 and obtain a free download □312-38 Guaranteed Questions Answers
- www.prepawaypdf.com is A Perfect and Reliable Option for 312-38 Exam Questions □ Copy URL { www.prepawaypdf.com } open and search for （ 312-38 ） to download for free □Sample 312-38 Questions
- Reliable 312-38 Exam Tips □ Reliable 312-38 Exam Tips □ New 312-38 Exam Pattern □ { www.pdfvce.com } is best website to obtain □ 312-38 □ for free download □VCE 312-38 Dumps
- Valid 312-38 Test Labs □ 312-38 Exam Topics Pdf □ Reliable 312-38 Test Review □ Search for □ 312-38 □ and download exam materials for free through ▸ www.torrentvce.com ◂ □Reliable 312-38 Test Review
- Sample 312-38 Questions □ 312-38 Guaranteed Questions Answers □ Reliable 312-38 Exam Tips □ Copy URL ➤ www.pdfvce.com □ open and search for ▹ 312-38 ◃ to download for free □Accurate 312-38 Test
- 312-38 Guaranteed Questions Answers □ 312-38 Guaranteed Questions Answers □ Accurate 312-38 Test □ “ www.practicevce.com ” is best website to obtain ➠ 312-38 □ for free download □VCE 312-38 Dumps
- 312-38 Excellect Pass Rate □ Interactive 312-38 Course □ Valid Test 312-38 Fee □ Search for ⇛ 312-38 ⇚ and download it for free on ✔ www.pdfvce.com □✔□ website □Reliable 312-38 Study Plan
- Reliable 312-38 Study Plan □ 312-38 Excellect Pass Rate □ New 312-38 Exam Pattern □ Copy URL 【 www.prepawaypdf.com 】 open and search for ➽ 312-38 □ to download for free □312-38 Guaranteed Questions Answers
- Free PDF Quiz The Best EC-COUNCIL - 312-38 Exams Dumps □ Search for { 312-38 } and download it for free on 「 www.pdfvce.com 」 website □Interactive 312-38 Course
- Reliable 312-38 Exam Labs □ Accurate 312-38 Test □ Reliable 312-38 Study Plan □ Search for ▹ 312-38 ◃ on ➠ www.dumpsmaterials.com □ immediately to obtain a free download □312-38 Guaranteed Questions Answers
- bbs.t-firefly.com, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 EC-COUNCIL 312-38 dumps are available on Google Drive shared by BraindumpQuiz: https://drive.google.com/open?id=1i_TwNCWiigGM3L7mrUDfoOzaMqayK06S