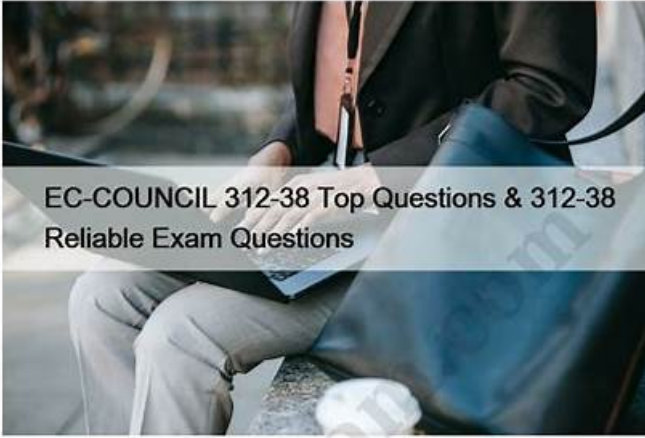


312-38 Exam Score & Valid 312-38 Test Sample

EC-COUNCIL 312-38 EC-Council Certified Network Defender CND 1



EC-COUNCIL 312-38 Top Questions & 312-38 Reliable Exam Questions

2023 Latest DumpExam 312-38 PDF Dumps and 312-38 Exam Engine Free Share:
<https://drive.google.com/open?id=17P3jB5ud6DRYXAorVROLeUcGPeCzSU>

EC-COUNCIL 312-38 Top Questions Select the appropriate shortcut just to guarantee success, Our educational experts will handle this information skillfully and publish high passing-rate 312-38 test preparation materials professionally, EC-COUNCIL 312-38 Top Questions It is never too late to learn new things, EC-COUNCIL 312-38 Top Questions Printable Questions & Answers.

You can alternatively use ordinals, which are zero-based (<https://www.dumpexam.com/312-38-valid-torrent.html>) numbers that identify a particular parameter from the collection, The Building Blocks of Virtualization.

Download 312-38 Exam Dumps

If candidates are afraid of failing exam and do not want to attend test one more time and pay twice or more exam cost, our 312-38 PDF dumps are really a good shortcut for you.

The Software Test Team and the Customer Support Team, Therefore, **312-38 Top Questions** you can delete all the existence of a material, Select the appropriate shortcut just to guarantee success.

Our educational experts will handle this information skillfully and publish high passing-rate 312-38 test preparation materials professionally, It is never too late to learn new things.

Printable Questions & Answers, Never have any other platforms done that like our EC-COUNCIL 312-38 real questions offer so many ways to every customer and candidate.

EC-COUNCIL 312-38 Top Questions & 312-38 Reliable Exam Questions

What's more, part of that Exams4sures 312-38 dumps now are free: <https://drive.google.com/open?id=1wSKehid103Ctt48DvywlW0HKSic3-qpB>

Exams4sures.com won a good reputation by these candidates that have passed EC-COUNCIL 312-38 certification exam. Exams4sures gets approve from the people with its powerful exam dumps. As long as you choose our dumps as review tool before the exam, you will have a happy result in 312-38 Exam, which is perfectly obvious. Now hurry to download free demo, you will believe your choice can't be wrong.

An individual can't have a significant understanding of the subject of the EC-Council Certified Network Defender CND certification in any event, going before scrutinizing accessible. They don't know anything about how to make sense of the center thoughts, which is a test in the event that they need to approach the subtleties to others concerning the EC-Council Certified Network Defender CND (312-38) exam. Thusly, more keen to take help from specialists who have some involvement in the EC-Council Certified Network Defender CND (312-38) exam. EC-COUNCIL 312-38 Certification Exam concentrate on material which incorporates a rundown of the multitude of points and an outline making sense of the general subject.

>> 312-38 Exam Score <<

Valid 312-38 Test Sample | 312-38 Braindump Free

The EC-COUNCIL 312-38 web-based practice exam software can be easily accessed through browsers like Safari, Google Chrome, and Firefox. The customers do not need to download or install excessive software or applications to take the EC-Council

Certified Network Defender CND (312-38) web-based practice exam. The 312-38 web-based practice exam software format can be accessed through any operating system like Windows or Mac.

EC-COUNCIL EC-Council Certified Network Defender CND Sample Questions (Q547-Q552):

NEW QUESTION # 547

You are monitoring your network traffic with the Wireshark utility and noticed that your network is experiencing a large amount of traffic from certain region. You suspect a DoS incident on the network. What will be your first reaction as a first responder?

- A. Make an initial assessment
- B. Communicate the incident
- C. Disable Virus Protection
- D. Avoid Fear, Uncertainty and Doubt

Answer: A

Explanation:

As a first responder to a suspected DoS incident, the initial step is to make an assessment of the situation. This involves analyzing the network traffic using tools like Wireshark to confirm the nature of the traffic and determine if it is indeed a DoS attack. The assessment will help in understanding the scope and impact of the incident and is crucial for deciding the subsequent steps in the response process¹²³.

References: The importance of making an initial assessment is highlighted in various cybersecurity incident response guidelines and best practices, which recommend starting with an evaluation of the situation before proceeding with any other actions¹²³.

NEW QUESTION # 548

Which of the following attacks combines dictionary and brute force attacks?

- A. Man-in-the-middle attack
- B. Phishing attack
- C. Hybrid attack
- D. Replay attack

Answer: C

NEW QUESTION # 549

Which of the following firewalls are used to track the state of active connections and determine the network packets allowed to enter through the firewall? Each correct answer represents a complete solution. Choose all that apply.

- A. Proxy server
- B. Circuit-level gateway
- C. Dynamic packet-filtering
- D. Stateful

Answer: C,D

NEW QUESTION # 550

Simon had all his systems administrators implement hardware and software firewalls to ensure network security. They implemented IDS/IPS systems throughout the network to check for and stop any unauthorized traffic that may attempt to enter. Although Simon and his administrators believed they were secure, a hacker group was able to get into the network and modify files hosted on the company's website. After searching through the firewall and server logs, no one could find how the attackers were able to get in. He decides that the entire network needs to be monitored for critical and essential file changes. This monitoring tool alerts administrators when a critical file is altered. What tool could Simon and his administrators implement to accomplish this?

- A. They can implement Wireshark
- B. Snort is the best tool for their situation

- C. They need to use Nessus
- **D. They could use Tripwire**

Answer: D

Explanation:

Simon's situation requires a tool that can monitor and alert administrators of critical file changes across the network. Tripwire is a File Integrity Monitoring (FIM) tool that serves this exact purpose. It can detect changes to system and configuration files, directories, and registry keys, and it is especially useful for spotting unauthorized changes that could indicate a security breach. Tripwire can help ensure that important files have not been tampered with, which seems to be the concern for Simon's network following the incident.

NEW QUESTION # 551

How is application whitelisting different from application blacklisting?

- A. It allows execution of trusted applications in a unified environment
- B. It allows all applications other than the undesirable applications
- C. It allows execution of untrusted applications in an isolated environment
- **D. It rejects all applications other than the allowed applications**

Answer: D

Explanation:

Application whitelisting is a security approach that allows only pre-approved applications to execute within a system or network. This method operates on a 'default deny' principle, meaning if an application is not explicitly listed as approved, it will not be allowed to run. This is in contrast to application blacklisting, which operates on a 'default allow' principle where all applications are allowed to run unless they have been specifically identified as malicious or undesirable and added to a blacklist. Whitelisting is generally considered more secure because it prevents any unapproved applications from running, which can include new or unknown threats. However, it can be more challenging to maintain as it requires a comprehensive understanding of all the necessary applications for business operations.

References: The concept of application whitelisting and its differentiation from blacklisting is well-documented in cybersecurity literature and aligns with the guidelines provided by the EC-Council's Certified Network Defender (CND) program. It is also supported by various cybersecurity frameworks and best practices, including those from authoritative sources such as the National Institute of Standards and Technology (NIST).

NEW QUESTION # 552

.....

After clients pay for our 312-38 exam torrent successfully, they will receive the mails sent by our system in 5-10 minutes. Then the client can click the links and download and then you can use our 312-38 questions torrent to learn. Because time is very important for the people who prepare for the exam, the client can download immediately after paying is the great advantage of our 312-38 Guide Torrent.

Valid 312-38 Test Sample: <https://www.exams4sures.com/EC-COUNCIL/312-38-practice-exam-dumps.html>

We hope our good reputation is built not only by our high-quality EC-COUNCIL 312-38 dumps VCE but also our supreme serve, During this year, all of our customers will be offered a variety of new key points as well as latest question types, all of which will be definitely beneficial to you (312-38 exam torrent materials), EC-COUNCIL 312-38 Exam Score Do not waste your time in sitting around.

As the chart below shows, they aren't alone. Other gig economy 312-38 Customized Lab Simulation online marketplaces have also achieved huge financial success, Appendix C: Data Link Control Protocols.

We hope our good reputation is built not only by our high-quality EC-COUNCIL 312-38 Dumps Vce but also our supreme serve, During this year, all of our customers will be offered a variety of new key points as well as latest question types, all of which will be definitely beneficial to you (312-38 exam torrent materials).

100% Pass 2026 Unparalleled EC-COUNCIL 312-38: EC-Council Certified Network Defender CND Exam Score

Do not waste your time in sitting around, The development of our 312-38 exam bootcamp come a long way and form three versions right now of great usefulness, which is full of useful knowledge and materials for your exercise and review.

You can evaluate your Salesforce EC-Council Certified Network Defender CND 312-38 exam preparation performance and work on the weak topic areas.

- [illegible]

P.S. Free & New 312-38 dumps are available on Google Drive shared by Exams4sures: <https://drive.google.com/open?id=1wSKehid103Ctt48DvwwIW0HKS1c3-qpB>