

GDAT Reliable Exam Dumps - Exam GDAT Question



After using our GDAT learning materials, you will find that things that have been difficult before have become simple. Of course, that's because you are better. Opportunities are for those who are prepared. And our GDAT exam questions are the right tool to help you get prepared. With the most up-to-date knowledge and information of the GDAT Practice Braindumps, you can be capable to deal with all of the conditions in your job. Believe it, good people will be better!

After you pay for our GDAT exam material online, you will get the link to download it in only 5 to 10 minutes. You don't need to worry about safety in buying our GDAT exam materials. Our products are free from computer virus and we will protect your private information. You won't get any telephone harassment or receiving junk E-mails after purchasing our GDAT Study Guide. If we have a new version of your study material, we will send an E-mail to you. Whenever you have questions about our GDAT study material, you are welcome to contact us via E-mail.

>> **GDAT Reliable Exam Dumps** <<

Updated GIAC GDAT Practice Questions In Three Formats

Thanks to our diligent experts, wonderful study tools are invented for you to pass the GDAT exam. You can try the demos of our GDAT exam questions first and find that you just can't stop studying. There are three kinds of the free demos according to the three versions of the GDAT learning guide. Using our GDAT study materials, you will just want to challenge yourself and get to know more.

GIAC Defending Advanced Threats Sample Questions (Q126-Q131):

NEW QUESTION # 126

Your security team has identified unusual outbound traffic from your organization's network to external IP addresses. Upon further analysis, the traffic consists of a high volume of encrypted HTTP POST requests, with some payloads resembling legitimate DNS queries.

What is the most likely method of data exfiltration being used, and how should you proceed?

Response:

- A. Phishing attack; notify users to change their passwords and monitor account activity
- B. Ransomware attack; isolate the affected systems and begin recovery operations

- C. DNS tunneling; block external DNS requests and investigate the internal DNS servers
- D. SQL injection; patch the vulnerable web applications and monitor the database for anomalies

Answer: C

NEW QUESTION # 127

What strategy is used to deliver payloads in a watering hole attack?

Response:

- A. Sending personalized emails to targeted users
- B. Attacking directly through network vulnerabilities
- C. Compromising commonly visited websites to load malicious scripts
- D. Physically tampering with network hardware

Answer: C

NEW QUESTION # 128

Identify the techniques used to detect domain fronting within an enterprise network.

Response:

- A. Monitoring for inconsistencies between DNS requests and TLS handshake SNI fields
- B. Regular scanning for unauthorized VPN connections
- C. Deep packet inspection of HTTP/S traffic
- D. Analyzing patterns of failed authentication attempts

Answer: A,C

NEW QUESTION # 129

What is a common method by which malware ensures its persistence on a host system after reboot?

Response:

- A. Adding entries to the Windows Registry
- B. Modifying user profiles
- C. Registering a new user account
- D. Deleting system logs

Answer: A

NEW QUESTION # 130

Which of the following are signs of a successful payload delivery?

(Choose Two)

Response:

- A. Increased network traffic to unknown IPs
- B. Unexpected pop-up windows
- C. Unusual system behavior and crashes
- D. Faster system boot-up times

Answer: A,C

NEW QUESTION # 131

.....

There is a succession of anecdotes, and there are specialized courses. Experts call them experts, and they must have their advantages. They are professionals in every particular field. The GDAT test material, in order to enhance the scientific nature of the

- [illegible]