

GIAC

GCED
GIAC Certified Enterprise Defender

- **Up to Date products, reliable and verified.**
- **Questions and Answers in PDF Format.**

Full Version Features:

- **90 Days Free Updates**
- **30 Days Money Back Guarantee**
- **Instant Download Once Purchased**
- **24 Hours Live Chat Support**

For More Information:

<https://www.testsexpert.com/>

- **Product Version**

Latest Version: 6.0

Question: 1

What does manual malware code reversal involve?

Response:

- A. Executing malware in a sandbox environment
- B. Running malware in a virtual machine
- C. Analyzing malware behavior in real-time
- D. Decompiling malware code to its original source code

Answer: D

Question: 2

During interactive malware analysis, what is the purpose of a sandbox environment?

Response:

- A. To remove the malware from the system
- B. To execute the malware and observe its behavior in a controlled environment
- C. To disassemble the malware code
- D. To patch vulnerabilities in the malware

Answer: B

Question: 3

Which of the following is a key advantage of disassembling malware code?

Response:

- A. It helps to remove the malware from the system
- B. It provides insights into the malware's behavior and functionality
- C. It prevents the malware from executing
- D. It encrypts the malware code

Answer: B

Question: 4

_____ logs provide information about system and application errors, which can be valuable for diagnosing issues or identifying security incidents.

Response:

- A. System
- B. Traffic
- C. Billing
- D. Access

Answer: A

Question: 5

In cloud-based infrastructure, what is the main responsibility of a Cloud Access Security Broker (CASB)?

Response:

- A. Managing network traffic
- B. Monitoring user activity
- C. Securing cloud applications and data
- D. Providing network connectivity

Answer: C

Question: 6

In penetration testing, what is the primary purpose of "pivoting"?

Response:

- A. To infiltrate the target organization's management team
- B. To move from one compromised system to others within the network
- C. To report findings to the client
- D. To perform vulnerability scanning

Answer: B

Question: 7

Why might an administrator not be able to delete a file using the Windows del command without specifying additional command line switches?

Response:

- A. Because it has the read-only attribute set
- B. Because it is encrypted
- C. Because it has the nodel attribute set
- D. Because it is an executable file

Answer: A

Question: 8

At the start of an investigation on a Windows system, the lead handler executes the following commands after inserting a USB drive. What is the purpose of this command?

C:\>dir /s /a dhsra d:\> a:\IRCD.txt

Response:

- A. To create a file on the USB drive that contains a listing of the C: drive
- B. To show hidden and archived files on the C: drive and copy them to the USB drive
- C. To copy a forensic image of the local C: drive onto the USB drive
- D. To compare a list of known good hashes on the USB drive to files on the local C: drive

Answer: C

Question: 9

When analyzing network flows, a sudden and unexplained increase in the number of outgoing _____ connections might indicate a security breach.

Response:

- A. Outbound
- B. Intranet
- C. Wireless
- D. Peripheral

Answer: A

Question: 10

What is the primary goal of "containment" in incident response?

Response:

- A. Eradicate the attacker from the network
- B. Monitor the attacker's activities for future intelligence
- C. Inform the public about the incident

D. Isolate the affected systems to prevent further damage

Answer: D

For More Information – Visit link below:
<https://www.testsexpert.com/>

16\$ Discount Coupon: **9M2GK4NW**

Features:

■ Money Back Guarantee.....



■ 100% Course Coverage.....



■ 90 Days Free Updates.....



■ Instant Email Delivery after Order.....

