



CERTSWARRIOR

GIAC GCPN

GIAC Cloud Penetration Tester (GCPN)

Questions&AnswersPDF

ForMoreInformation:

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

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Visit us at: <https://www.certswarrior.com/exam/gcpn>

Latest Version: 6.0

Question: 1

Which tool is commonly used to enumerate Azure Functions for security assessments?

Response:

- A. Azucar
- B. Nikto
- C. SQLmap
- D. Metasploit

Answer: A

Question: 2

What security measures should be implemented to prevent unauthorized discovery of cloud resources?
(Choose two)

Response:

- A. Enforce least privilege access policies
- B. Enable logging and monitoring for API calls
- C. Disable firewall protections to reduce latency
- D. Allow unrestricted access to cloud storage

Answer: A,B

Question: 3

During a security audit, you find that a Windows Container is running with excessive privileges and can access the host system. What is the best mitigation strategy?

Response:

- A. Apply the principle of least privilege to the container permissions
- B. Increase the memory allocation to improve container performance
- C. Restart the container every hour to reduce attack risk
- D. Remove logging configurations to prevent unauthorized access

Answer: A

Question: 4

A security team detects unauthorized API calls originating from an unknown IP address via Azure CLI.

What is the best remediation action?

Response:

- A. Rotate API keys and revoke all active CLI sessions
- B. Increase the timeout limit for API requests
- C. Delete all virtual machines running in Azure
- D. Allow list the unknown IP address for investigation

Answer: A

Question: 5

Which stealth techniques can Red Teams use to evade detection in cloud penetration testing?

(Choose two)

Response:

- A. Rotating API keys frequently
- B. Using cloud-based VPNs for lateral movement
- C. Disabling cloud security monitoring tools
- D. Implementing role assumption techniques in AWS

Answer: B,D

Question: 6

Which of the following techniques can be used to secure Windows Containers in Azure?

(Choose two)

Response:

- A. Enforcing least privilege container permissions
- B. Running all containers as root users
- C. Enabling Microsoft Defender for Containers
- D. Allowing unrestricted outbound network access

Answer: A,C

Question: 7

You are performing a penetration test on an AWS environment and discover an IAM policy that grants "s3:*" permissions to "Principal": "*" on an S3 bucket. What is the most significant security risk associated with this configuration?

Response:

- A. The S3 bucket may be deleted accidentally
- B. Unauthorized users can read, write, and delete objects in the S3 bucket
- C. AWS Lambda functions will fail to execute
- D. The S3 bucket performance will degrade

Answer: B

Question: 8

How can attackers harvest usernames in Azure Active Directory environments?

Response:

- A. By using OpenID Connect (OIDC) enumeration
- B. By disabling logging in Azure Monitor
- C. By modifying cloud storage permissions
- D. By using SQL injection on cloud databases

Answer: A

Question: 9

What is the primary security risk of exposing API keys in web applications?

Response:

- A. Unauthorized access to cloud services
- B. Increased application latency
- C. Inability to execute server-side code
- D. Reduced CPU performance in virtual machines

Answer: A

Question: 10

What methods can be used to discover exposed cloud databases?

(Choose two)

Response:

- A. Shodan searches for cloud-based databases
- B. Cloud SQL enumeration tools
- C. Restricting database connections
- D. Removing all database logs

Answer: A,B



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ