



CERTSWARRIOR

GIAC GMOB

GIAC Mobile Device Security Analyst

Questions&AnswersPDF

ForMoreInformation:

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

Features:

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

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

Latest Version: 6.1

Question: 1

Which tool is commonly used for reverse engineering Android applications?

Response:

- A. Burp Suite
- B. APKTool
- C. Nessus
- D. Wireshark

Answer: B

Question: 2

Which of these features should be enabled to help track and potentially recover a lost or stolen device that might contain sensitive data?

Response:

- A. Developer options
- B. Mobile device encryption
- C. Remote wipe
- D. USB debugging

Answer: C

Question: 3

In the context of SSL/TLS exploitation, what tools can be used to perform a successful Man-in-the-Middle attack?

(Choose Two)

Response:

- A. Metasploit
- B. Burp Suite
- C. OpenSSL
- D. Wireshark

Answer: A,B

Question: 4

What is the first step in a mobile app security assessment?

Response:

- A. Reverse engineering the app
- B. Reviewing the app's permissions
- C. Auditing the backend server
- D. Testing user input validation

Answer: B

Question: 5

What should be a primary consideration when setting up a mobile device for business use to prevent data loss in case of theft?

Response:

- A. High screen brightness settings
- B. Automatic locking mechanisms
- C. Frequent location-based reminders
- D. Integration of entertainment apps

Answer: B

Question: 6

What are two common techniques to mitigate against mobile malware infections?

(Choose two)

Response:

- A. Installing apps only from trusted sources
- B. Disabling automatic updates for apps
- C. Regularly scanning devices with anti-malware software
- D. Sideloaded apps from third-party stores

Answer: A,C

Question: 7

Which security model does iOS primarily rely on to protect sensitive user data?

Response:

- A. Sandboxing
- B. Application Verification
- C. Trusted Execution Environment (TEE)
- D. Root of Trust

Answer: A

Question: 8

What aspect does MASVS L2 add to the basic security requirements of L1?

(Choose Three)

Response:

- A. Protection against reverse engineering
- B. Enforcement of stronger encryption algorithms
- C. Usage of more secure data storage and communication mechanisms
- D. Compliance with specific industry regulations

Answer: A,B,C

Question: 9

What does the OWASP MASVS framework focus on?

Response:

- A. Data encryption methods
- B. Secure software development lifecycle
- C. Security controls in mobile applications
- D. Penetration testing practices

Answer: C

Question: 10

In mobile application testing, what type of tool would be used to inject malicious input into an application to observe its behavior?

Response:

- A. Database management system

- B. Fuzzer
- C. Code compiler
- D. File explorer

Answer: 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