



CERTSWARRIOR

G/AC

GDAT
GIAC Defending Advanced Threats

Questions & Answers PDF

For More Information:
<https://www.certswarrior.com/>

Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

Latest Version: 6.0

Question: 1

What are key indicators of an effective exploit mitigation strategy?

Response:

- A. Quick identification of new vulnerabilities
- B. Immediate deployment of software patches
- C. No reported security incidents
- D. Regular security training for developers

Answer: A,B,D

Question: 2

Regarding Kerberos authentication, which of the following steps are involved in the process of obtaining a service ticket?

Response:

- A. The client requests an authentication ticket (TGT) from the Key Distribution Center (KDC).
- B. The client presents the TGT to the Ticket Granting Server (TGS) to request a service ticket.
- C. The client uses the service ticket to authenticate directly to the Active Directory database.
- D. The Ticket Granting Server (TGS) issues a service ticket after validating the TGT.

Answer: B,D

Question: 3

In the context of lateral movement, what is the function of using pass-the-ticket (PtT) techniques?

Response:

- A. To escalate privileges on the target system
- B. To maintain persistence in the network
- C. To impersonate legitimate users
- D. To encrypt data being exfiltrated

Answer: C

Question: 4

Which strategies are effective in preventing privilege escalation attacks?

Response:

- A. Conducting regular privilege audits
- B. Implementing strong password policies
- C. Using non-administrative accounts for daily operations
- D. Encrypting sensitive data at rest

Answer: A,C

Question: 5

Which phase of the software development lifecycle is most critical for implementing security patches?

Response:

- A. Requirements gathering
- B. Design
- C. Implementation
- D. Maintenance

Answer: D

Question: 6

Why is regular vulnerability scanning crucial for application security?

Response:

- A. It aligns IT strategies with business objectives
- B. It identifies weaknesses that could be exploited by attackers
- C. It ensures compliance with international standards
- D. It facilitates faster software release cycles

Answer: B

Question: 7

What role does sandboxing play in defending against payload delivery?

Response:

- A. It isolates potentially malicious programs in a separate environment from the host system.
- B. It filters incoming network traffic to prevent unauthorized access.
- C. It encrypts sensitive information stored on the device.
- D. It logs user activities for audit purposes.

Answer: A

Question: 8

What is the primary benefit of employing encryption in data exfiltration techniques?

Response:

- A. It reduces the amount of data needing exfiltration
- B. It ensures faster transfer of data
- C. It masks the content from network monitoring tools
- D. It complies with international data protection laws

Answer: C

Question: 9

An effective adversary emulation plan should include detailed _____ to ensure that all actions are reversible and non-disruptive to daily operations.

Response:

- A. escalation procedures
- B. rollback procedures
- C. deployment strategies
- D. communication plans

Answer: B

Question: 10

How does application whitelisting help prevent the execution of malicious payloads?

Response:

- A. By only allowing pre-approved applications to run
- B. By detecting zero-day exploits
- C. By encrypting data transmitted over the network
- D. By monitoring outbound traffic for anomalies

Answer: A



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