TestkingPDF

Try before you buy

Download a free sample of any of our exam questions and answers

Download Demo

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

Quality and Value

TestkingPDF Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our TestkingPDF testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

TestkingPDF offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.testkingpdf.com

Valid test online & stable pass king & latest PDF dumps

Exam : **GDAT**

Title : GIAC Defending Advanced Threats

Vendor : GIAC

Version : DEMO

NO.1 What is a common payload execution technique used by malware after initial infection?
Response:
A. Disk defragmentation
B. Execution through macros in documents
C. Automatic system updates
D. Network traffic encryption
Answer: B

NO.2 What is a recommended approach for removing malware persistence mechanisms?
Response:
A. Isolating the infected systems from the network
B. Performing a system format on all workstations
C. Updating all third-party applications
D. Reinstalling the operating system
Answer: A

NO.3 Which of the following methods is commonly used for delivering malicious payloads in phishing attacks?
Response:
A. Social engineering through phone calls
B. Embedded links in emails
C. SQL injection
D. DDoS attacks
Answer: B

NO.4 What are key indicators of lateral movement within a network?
(Choose Three)
Response:
A. Unusual outbound traffic patterns
B. Anomalies in account logins
C. Frequent changes in file permissions
D. Spike in database read operations
Answer: A,B,C

NO.5 Which phase of the Software Development Lifecycle (SDLC) is most critical for applying security patches?
Response:
A. Design
B. Implementation
C. Testing
D. Maintenance
Answer: D

NO.6 Which of the following is a key technical control that should be considered when conducting adversary emulation?
Response:
A. Data encryption at rest and in transit
B. Regular software updates and patch management
C. Continuous integration and continuous deployment practices
D. All of the above
Answer: D

NO.7 Which of the following best describes threat modeling in the context of application security?
Response:
A. A process for identifying, quantifying, and addressing security risks
B. A method for encrypting sensitive data within an application
C. A testing approach used to discover user interface flaws
D. A strategy for optimizing the performance of software applications
Answer: A

NO.8 Which of the following describes how application control policies contribute to payload execution prevention?
Response:
A. They monitor and filter browsing behavior in real-time.
B. They prevent the execution of unauthorized applications.
C. They detect changes in network configurations.
D. They enforce two-factor authentication.
Answer: B

NO.9 How does a deception grid contribute to threat handling?
Response:
A. By encrypting all network traffic
B. By attracting attackers to decoy systems to analyze their tactics
C. By reducing the workload of IT staff
D. By automatically patching software vulnerabilities
Answer: B

NO.10 What is a common tool used by attackers to perform lateral movement within a network?
Response:
A. Netcat
B. Wireshark
C. OpenSSL
D. Kerberos
Answer: A

NO.11 Your security operations center has detected a surge in login attempts from a service account

that should only be used by the IT department. The login attempts are originating from multiple machines within the network, some of which belong to departments with no IT access requirements. Further investigation reveals that the service account was compromised.
What immediate action should you take to contain the lateral movement?
Response:
A. Disable the compromised account and enforce MFA for all privileged accounts
B. Disconnect the entire network from the internet until the issue is resolved
C. Monitor the service account for further activity without taking action
D. Initiate a company-wide password reset for all users
Answer: A

NO.12 The use of _____ tools, which include both software and methodologies, can help an organization identify vulnerabilities that could be exploited by an adversary.
Response:
A. documentation
B. encryption
C. red teaming
D. accounting
Answer: C

NO.13 Which of the following file types is most likely to be used in delivering a malicious payload via email attachments?
Response:
A. .txt
B. .exe
C. .pdf
D. .docx
Answer: B

NO.14 Which exploit mitigation technique involves analyzing software to detect and resolve vulnerabilities before deployment?
Response:
A. Threat modeling
B. Fuzz testing
C. Code obfuscation
D. Signature-based detection
Answer: B

NO.15 In what scenario might an attacker use social engineering as part of their exfiltration strategy?
Response:
A. To gain initial access through phishing
B. To learn schedules that reduce detection risk
C. To physically access restricted areas

D. To understand the organization's data classification policy
Answer: A