GIAC
GDAT
GIAC Defending Advanced Threats

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

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

Latest Version: 6.1

Question: 1

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

Question: 2

Which tool is commonly used by attackers for lateral movement within a network?
Response:

A. Nmap
B. PowerShell
C. Snort
D. OpenSSL

Answer: B

Question: 3

What are the primary indicators of a Golden Ticket attack in an Active Directory environment? (Choose two)
Response:

A. Unusual Kerberos ticket lifetimes
B. Account logins from multiple locations
C. Integrity issues in the Active Directory database
D. Antivirus flagging unusual behavior in the network

Answer: A,B

Question: 4

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

Question: 5

Which method is commonly used by attackers to exfiltrate data using the DNS tunneling technique?
Response:

A. Transferring data via encrypted HTTP requests
B. Embedding data within DNS queries
C. Using FTP servers to upload stolen data
D. Exploiting open SMB shares for file transfer

Answer: B

Question: 6

Which operating system features can be exploited by attackers to execute malicious payloads? (Choose two)
Response:

A. AutoRun and AutoPlay features
B. Secure Boot
C. Command-line interfaces
D. Secure Shell (SSH) protocols

Answer: A,C

Question: 7

What is the primary goal of integrating threat modeling into the software development lifecycle?
Response:

A. To identify potential security vulnerabilities early in the development process
B. To improve the efficiency of the development team
C. To enhance the user interface design
D. To reduce the cost of software development

Answer: A

Question: 8

Which of the following are common techniques used by attackers for lateral movement?
(Choose two)
Response:

A. Pass-the-Hash
B. Cross-site scripting (XSS)
C. Remote Desktop Protocol (RDP)
D. Phishing

Answer: A,C

Question: 9

Which of the following are techniques used by malware for maintaining persistence?
(Choose Two)
Response:

A. Writing scripts in the startup folder
B. Encrypting all files on the hard drive
C. Installing new services
D. Frequent system reboots

Answer: A,C

Question: 10

Which exploit mitigation techniques are used to prevent application exploitation?
(Choose two)
Response:

A. Fuzz testing
B. Role-based access control
C. Web Application Firewalls (WAF)
D. File hashing for integrity verification

Answer: A,C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/