- **Vendor: CompTIA**
- **Exam Code: CAS-003**
- **Exam Name: CompTIA Advanced Security Practitioner (CASP)**
- **New Updated Questions from Braindump2go (Updated in October/2021)**

QUESTION 801
Over the last 90 days, many storage services has been exposed in the cloud services environments, and the security team does not have the ability to see is creating these instance. Shadow IT is creating data services and instances faster than the small security team can keep up with them. The Chief information security Officer (CIASO) has asked the security officer (CISO) has asked the security lead architect to architect to recommend solutions to this problem. Which of the following BEST addresses the problem best address the problem with the least amount of administrative effort?

A. Compile a list of firewall requests and compare than against interesting cloud services.
B. Implement a CASB solution and track cloud service use cases for greater visibility.
C. Implement a user-behavior system to associate user events and cloud service creation events.
D. Capture all log and feed then to a SIEM and then for cloud service events

Answer: C

QUESTION 802
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:
- Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
- SSL Medium Strength Cipher Suites Supported
- Vulnerability in DNS Resolution Could Allow Remote Code Execution
- SMB Host SIDs allows Local User Enumeration

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

A. Password cracker
B. Port scanner
C. Account enumerator
D. Exploitation framework

Answer: A

QUESTION 803
The Chief information Officer (CIO) wants to establish a non-banding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership.
Which of the follow would MOST likely be used?

A. MOU
B. OLA
C. NDA
D. SLA

Answer: A

QUESTION 804
A security analyst is trying to identify the source of a recent data loss incident. The analyst has reviewed all the for the time surrounding the identified all the assets on the network at the time of the data loss.
The analyst suspects the key to finding the source was obfuscated in an application. Which of the following tools should the analyst use NEXT?

A. Software Decomplier
B. Network enurrerator
C. Log reduction and analysis tool
D. Static code analysis

Answer: D

QUESTION 805
Which of the following controls primarily detects abuse of privilege but does not prevent it?

A. Off-boarding
B. Separation of duties
C. Least privilege
D. Job rotation

Answer: A

QUESTION 806
A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the compay's intend WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration.
Which of the following must be installed on authorized hosts for this new configuration to work properly?

A. Active Directory OPOs
B. PKI certificates
C. Host-based firewall
D. NAC persistent agent

Answer: B

QUESTION 807
The goal of a Chief information Security Officer (CISO) providing up-to-date metrics to a bank's risk committee is to ensure:

A. Budgeting for cybersecurity increases year over year.
B. The committee knows how much work is being done.
C. Business units are responsible for their own mitigation.
D. The bank is aware of the status of cybersecurity risks

Answer: A

QUESTION 808
A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output.
Which of the following would enable the engineer to interpret the results in a human readable form? (Select TWO.)

A. Text editor
B. OOXML editor

C. Event Viewer
D. XML style sheet
E. SCAP tool
F. Debugging utility

Answer: AE

QUESTION 809
A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

Which of the following MOST appropriate corrective action to document for this finding?

A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
C. The system administrator should evaluate dependencies and perform upgrade as necessary.
D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

Answer: A

QUESTION 810
The Chief information Security Officer (CISO) of a small locate bank has a compliance requirement that a third-party penetration test of the core banking application must be conducted annually. Which of the following services would fulfill the compliance requirement with the LOWEST resource usage?

A. Black-box testing
B. Gray-box testing
C. Red-team hunting
D. White-box testing
E. Blue-learn exercises

Answer: C