- **Vendor: CompTIA**
- **Exam Code: CAS-003**
- **Exam Name: CompTIA Advanced Security Practitioner (CASP)**
- **New Updated Questions from Braindump2go (Updated in Dec./2020)**

QUESTION 618
The Chief Information Security Officer (CISO) of a company that has highly sensitive corporate locations wants its security engineers to find a solution to growing concerns regarding mobile devices.
The CISO mandates the following requirements:
- The devices must be owned by the company for legal purposes.
- The device must be as fully functional as possible when off site.
- Corporate email must be maintained separately from personal email
- Employees must be able to install their own applications.
Which of the following will BEST meet the CISO's mandate? (Select TWO).

A. Disable the device's camera
B. Allow only corporate resources in a container.
C. Use an MDM to wipe the devices remotely
D. Block all sideloading of applications on devices
E. Use geofencmg on certain applications
F. Deploy phones in a BYOD model

Answer: BE

QUESTION 619
After analyzing code, two developers al a company bring these samples to the security operations manager.

```
Example Language: Java
# Java Web App ResourceBundle properties file
...
webapp.ldap.username=secretUsername
webapp.ldap.password=secretPassword
...
The following example shows a portion of a configuration file for an ASP.Net application.
Example Language: ASP.NET
...
<connectionStrings>
<add name="ud_DEV" connectionString="connectDB=uDB; uid=dbladmin; pwd=password; dbalias=uDB;" providerName="System.Data.Odbc" />
</connectionStrings>
...
```

Which of the following would BEST solve these coding problems?

A. Use a privileged access management system
B. Prompt the administrator for the password .
C. Use salted hashes with PBKDF2.
D. Increase the complexity and length of the password

Answer: B

QUESTION 620
A security administrator receives reports that several workstations are unable to access resources within one network segment.
A packet capture shows the segment is flooded with ICMPv6 traffic from the source fe80::21ae;4571:42ab:1fdd and for

the destination ff02::1.
Which of the following should the security administrator integrate into the network to help prevent this from occurring?

A. Raise the dead peer detection interval to prevent the additional network chatter
B. Deploy honeypots on the network segment to identify the sending machine.
C. Ensure routers will use route advertisement guards.
D. Deploy ARP spoofing prevention on routers and switches.

Answer: D

QUESTION 621
Joe an application security engineer is performing an audit of an environmental control application.
He has implemented a robust SDLC process and is reviewing API calls available to the application.
During the review, Joe finds the following in a log file.

```
POST /API/Data/Username=Jim&Password=Rustle&PowerKW&Efficiency
POST /API/Data/Username=John&Password=Doe&Uptime&Temperature
POST /API/Data/Username=OTManager&Password=1gudPW&Sector5ESensor2=Off&Sector5ESensor2Status
```

Which of the following would BEST mitigate the issue Joe has found?

A. Ensure the API uses SNMPv1.
B. Perform authentication via a secure channel
C. Verify the API uses HTTP GET instead of POST
D. Deploy a WAF in front of the API and implement rate limiting

Answer: B

QUESTION 622
An organization implemented a secure boot on its most critical application servers which produce content and capability for other consuming servers A recent incident, however led the organization to implement a centralized attestation service for these critical servers.
Which of the following MOST likely explains the nature of the incident that caused the organization to implement this remediation?

A. An attacker masqueraded as an internal DNS server
B. An attacker leveraged a heap overflow vulnerability in the OS
C. An attacker was able to overwrite an OS integrity measurement register
D. An attacker circumvented IEEE 802.1X network-level authentication requirements.

Answer: C

QUESTION 623
A company's Internet connection is commonly saturated during business hours, affecting Internet availability.
The company requires all Internet traffic to be business related.
After analyzing the traffic over a period of a few hours, the security administrator observes the following:

Protocol	Usage	%
TCP/SSL	324Gb	85%
TCP/HTTP	37Gb	10%
UDP/DNS	10Gb	3%
Other	8GB	2%

The majority of the IP addresses associated with the TCP/SSL traffic resolve to CDNs.
Which of the following should the administrator recommend for the CDN traffic to meet the corporate security requirements?

A. Block outbound SSL traffic to prevent data exfiltration.
B. Confirm the use of the CDN by monitoring NetFlow data
C. Further investigate the traffic using a sanctioned MITM proxy.
D. Implement an IPS to drop packets associated with the CDN.

Answer: A

QUESTION 624
An attacker has been compromising banking institution targets across a regional area.
The Chief Information Security Officer (CISO) at a local bank wants to detect and prevent an attack before the bank becomes a victim.
Which of the following actions should the CISO take?

A. Utilize cloud-based threat analytics to identify anomalous behavior in the company's B2B and vendor traffic
B. Purchase a CASB solution to identify and control access to cloud-based applications and services and integrate them with on-premises legacy security monitoring
C. Instruct a security engineer to configure the IDS to consume threat intelligence feeds from an information-sharing association in the banking sector
D. Attend and present at the regional banking association lobbying group meetings each month and facilitate a discussion on the topic.

Answer: C

QUESTION 625
Users have reported that an internally developed web application is acting erratically, and the response output is inconsistent.
The issue began after a web application dependency patch was applied to improve security.
Which of the following would be the MOST appropriate tool to help identify the issue?

A. Fuzzer
B. SCAP scanner
C. Vulnerability scanner
D. HTTP interceptor

Answer: A

QUESTION 626
A company makes consumer health devices and needs to maintain strict confidentiality of unreleased product designs.
Recently unauthorized photos of products still in development have been for sale on the dark web.
The Chief Information Security Officer (CISO) suspects an insider threat, but the team that uses the secret outdoor testing area has been vetted many times and nothing suspicious has been found.
Which of the following is the MOST likely cause of the unauthorized photos?

A. The location of the testing facility was discovered by analyzing fitness device information the test engineers posted on a website
B. One of the test engineers is working for a competitor and covertly installed a RAT on the marketing department's servers
C. The company failed to implement least privilege on network devices, and a hacktivist published stolen public relations photos
D. Pre-release marketing materials for a single device were accidentally left in a public location

Answer: D

QUESTION 627

A manufacturing company's security engineer is concerned a remote actor may be able to access the ICS that is used to monitor the factory lines.
The security engineer recently proposed some techniques to reduce the attack surface of the ICS to the Chief Information Security Officer (CISO).
Which of the following would BEST track the reductions to show the CISO the engineer's plan is successful during each phase?

A. Conducting tabletop exercises to evaluate system risk
B. Contracting a third-party auditor after the project is finished
C. Performing pre- and post-implementation penetration tests
D. Running frequent vulnerability scans during the project

Answer: D

QUESTION 628
A new corporate policy requires that all employees have access to corporate resources on personal mobile devices.
The information assurance manager is concerned about the potential for inadvertent and malicious data disclosure if a device is lost, while users are concerned about corporate overreach.
Which of the following controls would address these concerns and should be reflected in the company's mobile device policy?

A. Place corporate applications in a container
B. Enable geolocation on all devices
C. install remote wiping capabilities
D. Ensure all company communications use a VPN

Answer: A

QUESTION 629
A security consultant is conducting a penetration test against a customer enterprise local comprises local hosts and cloud-based servers.
The hosting service employs a multitenancy model with elastic provisioning to meet customer demand.
The customer runs multiple virtualized servers on each provisioned cloud host.
The security consultant is able to obtain multiple sets of administrator credentials without penetrating the customer network.
Which of the following is the MOST likely risk the tester exploited?

A. Data-at-rest encryption misconfiguration and repeated key usage
B. Offline attacks against the cloud security broker service
C. The ability to scrape data remnants in a multitenancy environment
D. VM escape attacks against the customer network hypervisors

Answer: C