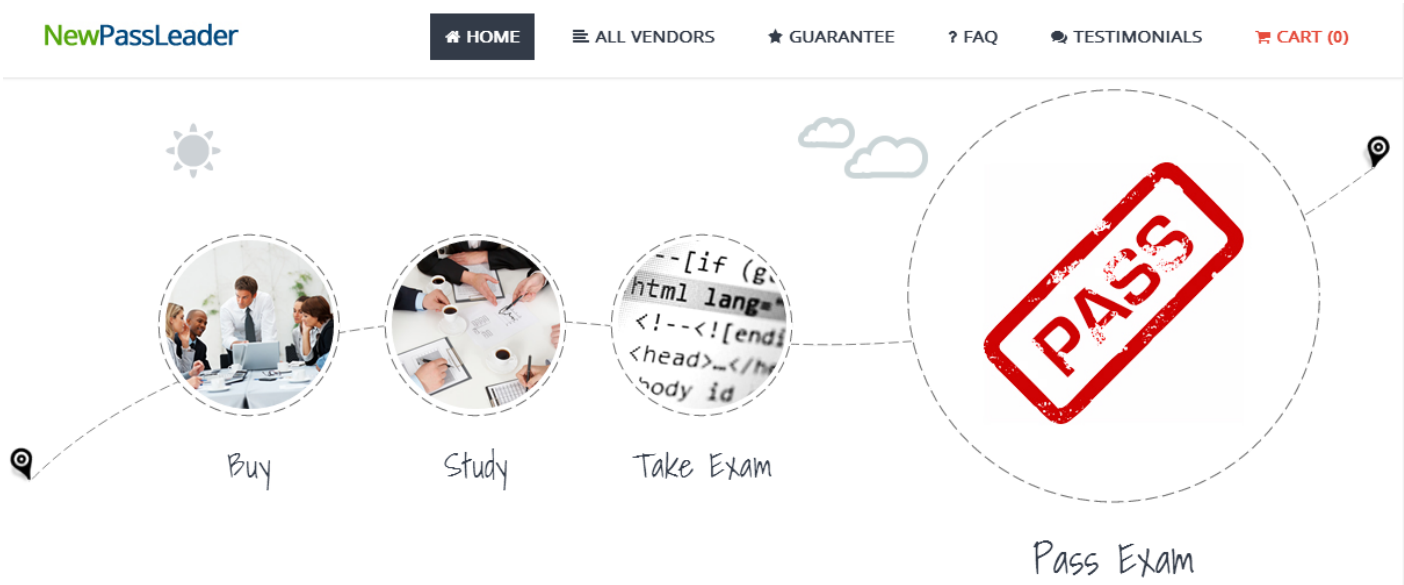
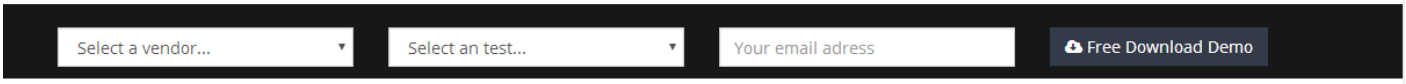
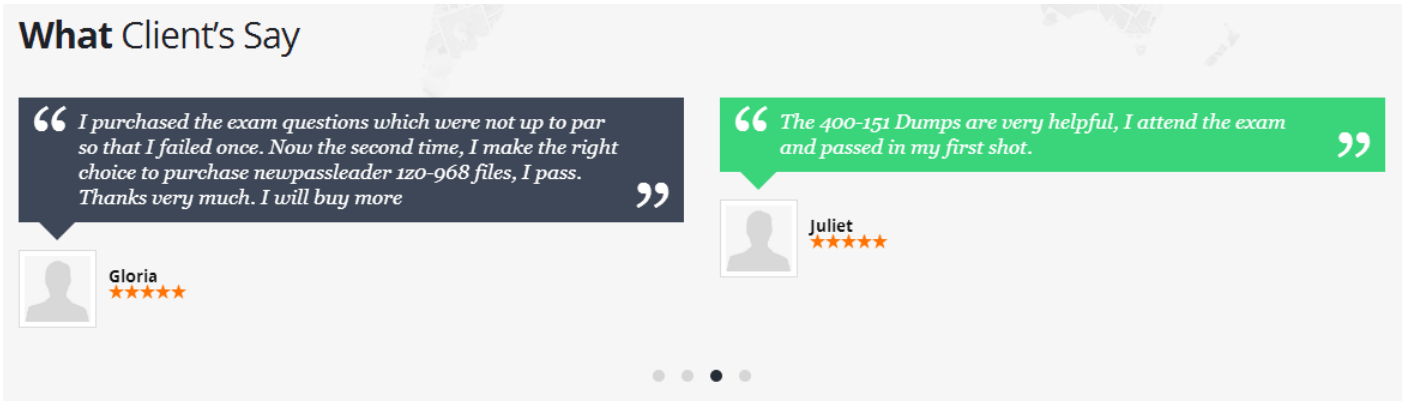
NewPassleader





Try **PDF Demo** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.
PDF format: Easy to read and print learning materials, our products are available in PDF file format.
Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.



http://www.newpassleader.com/

Attentive Service Exam Torrent and Valid Dumps - NewPassLeader

Exam : **CAS-003**

Title : CompTIA Advanced Security Practitioner (CASP)

Vendor : CompTIA

Version : DEMO

NO.1 The Chief Executive Officer (CEO) of a small company decides to use cloud computing to host critical corporate data for protection from natural disasters. The recommended solution is to adopt the public cloud for its cost savings If the CEO insists on adopting the public cloud model, which of the following would be the BEST advice?

A. Ensure the cloud provider supports a secure virtual desktop infrastructure

B. Ensure the ISP is using a standard help-desk ticketing system to respond to any system outages

C. Ensure the on-premises datacenter employs fault tolerance and load balancing capabilities.

D. Ensure the colocation facility implements a robust DRP to help with business continuity planning.

Answer: D

NO.2 A systems administrator recently joined an organization and has been asked to perform a security assessment of controls on the organization's file servers, which contain client data from a number of sensitive systems. The administrator needs to compare documented access requirements to the access implemented within the file system.

Which of the following is MOST likely to be reviewed during the assessment? (Select two.)

A. Data design document

B. Security requirements traceability matrix

C. Data owner matrix

D. Access control list

E. Data access policies

F. Roles matrix

Answer: E,F

NO.3 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=db2admin; pwd=password; dbalias=uDB;" providerName="System.Data.Odbc" />
</connectionStrings>
...
```

Which of the following would BEST solve these coding problems?

A. Increase the complexity and length of the password

B. Use a privileged access management system

C. Prompt the administrator for the password .

D. Use salted hashes with PBKDF2.

Answer: B

NO.4 A company has gone through a round of phishing attacks. More than 200 users have had their workstation infected because they clicked on a link in an email. An incident analysis has determined an executable ran and compromised the administrator account on each workstation. Management is demanding the information security team prevent this from happening again. Which of the following would BEST prevent this from happening again?

A. Log monitoring
B. Awareness training
C. Antivirus
D. Application whitelisting
E. Patch management
Answer: C

NO.5 An internal staff member logs into an ERP platform and clicks on a record. The browser URL changes to:
URL: http://192.168.0.100/ERP/accountId=5&action=SELECT
Which of the following is the MOST likely vulnerability in this ERP platform?
A. SQL injection of ERP back end
B. Brute forcing of account credentials
C. Plan-text credentials transmitted over the Internet
D. Insecure direct object reference
Answer: D

NO.6 An e-commerce company that provides payment gateways is concerned about the growing expense and time associated with PCI audits of its payment gateways and external audits by customers for their own compliance reasons The Chief Information Officer (CIO) asks the security team to provide a list of options that will:
1. Reduce the overall cost of these audits
2. Leverage existing infrastructure where possible
3. Keep infrastructure costs to a minimum
4. Provide some level of attestation of compliance
Which of the following will BEST address the CIO"s concerns? (Select TWO)
A. Install EDR agents on all corporate endpoints
B. Invest in new UBA to detect report, and remediate attacks faster
C. Undertake ISO certification for all core infrastructure including datacenters.
D. Implement a GRC system to track and monitor controls
E. Implement DLP controls on HTTP'HTTPS and email
F. Segment the network to reduce and limit the audit scope
Answer: C,E

NO.7 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. OLA
B. NDA
C. MOU
D. SLA
Answer: C

NO.8 An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions.
Which of the following types of information could be drawn from such participation?
A. Threat modeling
B. Exploit frameworks
C. Risk metrics
D. Risk assessment
E. Vulnerability data
F. Threat intelligence
Answer: B

NO.9 Users of a newly deployed VoIP solution report multiple instances of dropped or garbled calls. Thirty users connect to the primary site via a site-to-site VPN, and the primary site supplies a dial tone to all satellite locations. The network engineer who installed the equipment copied the configuration from a site that has two users on a low bandwidth DSL connection. Which of the following is MOST likely to restore telephone availability at the 30-user site?
A. Enable point-to-point tunneling for all VoIP traffic at the new site
B. Configure QoS settings to support the larger bandwidth available
C. Provision new firewalls at all sites to enable QoS management of VoIP traffic
D. Disable Layer 2 encryption on the site-to-site VPNs throughout the company
E. Prioritize ICMP and TCP traffic over UDP traffic using QoS
Answer: B

NO.10 A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patching routine. Which of the following steps should also be taken to harden the smart switch?
A. Place the switch in a Faraday cage.
B. Install a cable lock on the switch.
C. Change the default password for the switch.
D. Set up an air gap for the switch.
Answer: C

NO.11 A new employee is plugged into the network on a BYOD machine but cannot access the network Which of the following must be configured so the employee can connect to the network?
A. VPN
B. Remote access
C. Port security
D. Firewall
Answer: C

NO.12 A developer is reviewing the following transaction logs from a web application:
Username: John Doe
Street name: Main St.
Street number: <script>alert('test')</alert>
Which of the following code snippets should the developer implement given the above transaction logs?
A. $input=strip_tags(trim($_POST['var1']));
B. <html><form name="myform" action="www.server.com/php/submit.php action=GET"
C. if ($input != strcmp($var1, "<>")) {die();}
D. <form name ="form1" action="/submit.php" onsubmit="return validate()" action=POST>
Answer: C

NO.13 An organization is improving its web services to enable better customer engagement and self-service. The organization has a native mobile application and a rewards portal provided by a third party. The business wants to provide customers with the ability to log in once and have SSO between each of the applications. The integrity of the identity is important so it can be propagated through to back-end systems to maintain a consistent audit trail. Which of the following authentication and authorization types BEST meet the requirements? (Choose two.)
A. Social login
B. XACML
C. SPML
D. SAML
E. OAuth
F. OpenID connect
Answer: A,F

NO.14 An application developer has been informed of a web application that is susceptible to a clickjacking vulnerability Which of the following code snippets would be MOST applicable to resolve this vulnerability?
A)

```
Content-Security-Policy frame-ancestors: 'none'
```

B)

```
$escaped_command = escapeshellcmd($args);
exec($escaped_command, $output, $return_var);

  sqlQuery='SELECT * FROM custTable WHERE User=? AND Pass=?'
  parameters.add("User", username)
```

D)

```
  require 'digest/sha2'
  sha256 = Digest::SHA2.new(256)
```

A. Option D

B. Option A
C. Option C
D. Option B
Answer: D

NO.15 A technician is configuring security options on the mobile device manager for users who often utilize public Internet connections while travelling. After ensuring that full disk encryption is enabled, which of the following security measures should the technician take? (Choose two.)
A. Issue a remote wipe of corporate and personal partitions
B. Ensure all mobile devices back up using USB OTG
C. Require all mobile device backups to be encrypted
D. Restrict devices from making long-distance calls during business hours
E. Implement an always-on VPN
Answer: A,E

NO.16 A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.
Which of the following exercise types should the analyst perform?
A. Research industry best practices and latest RFCs.
B. Conduct a threat modeling exercise.
C. Summarize the most recently disclosed vulnerabilities.
D. Undertake an external vulnerability scan and penetration test.
Answer: B

NO.17 A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely ? (Select TWO.)
A. Chief use of UDP protocols
B. VPN on the mobile device
C. Disabled GPS on mobile devices
D. Privilege escalation attack
E. Unrestricted email administrator accounts
F. Outdated escalation attack
Answer: B,C

NO.18 A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix.
Which of the following MOST likely need to be configured to ensure the system are mitigated

accordingly? (Select two.)
A. HIPS
B. Patch management
C. Firmware updates
D. Application whitelisting
E. Antivirus
F. Group policy implementation
Answer: B,C

NO.19 A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:
Configuration file 1:
Operator ALL=/sbin/reboot
Configuration file 2:
Command="/sbin/shutdown now", no-x11-forwarding, no-pty, ssh-dss
Configuration file 3:
Operator:x:1000:1000::/home/operator:/bin/bash
Which of the following explains why an intended operator cannot perform the intended action?
A. The sudoers file is locked down to an incorrect command
B. The passwd file is misconfigured
C. The SSH command is not allowing a pty session
D. SSH command shell restrictions are misconfigured
Answer: C

NO.20 Following a security assessment, the Chief Information Security Officer (CISO) is reviewing the results of the assessment and evaluating potential risk treatment strategies. As part of the CISO's evaluation, a judgment of potential impact based on the identified risk is performed. To prioritize response actions, the CISO uses past experience to take into account the exposure factor as well as the external accessibility of the weakness identified.
Which of the following is the CISO performing?
A. Business impact scoring
B. Documentation of lessons learned
C. Qualitative assessment of risk
D. Quantitative risk assessment
E. Threat modeling
Answer: C

NO.21 A security engineer is attempting to inventory all network devices Most unknown devices are not responsive to SNMP queries. Which of the following would be the MOST secure configuration?
A. Enable SSH for all switches and routers
B. Set SFTP to enabled on all network devices
C. Switch to SNMPv1 device inventory credentials
D. Configure SNMPv3 server settings to match client settings

Answer: D

NO.22 A security engineer wants to introduce key stretching techniques to the account database to make password guessing attacks more difficult Which of the following should be considered to achieve this? (Select TWO)

A. Record-level encryption

B. SHA-256

C. bcrypt

D. P-384

E. Digital signature

F. PBKDF2

G. Perfect forward secrecy

Answer: C,F

NO.23 An external red team member conducts a penetration test, attempting to gain physical access to a large organization's server room in a branch office. During reconnaissance, the red team member sees a clearly marked door to the server room, located next to the lobby, with a tumbler lock.
Which of the following is BEST for the red team member to bring on site to open the locked door as quickly as possible without causing significant damage?

A. Rake picking

B. RFID duplicator

C. Bump key

D. Screwdriver set

Answer: C

NO.24 A company is trying to resolve the following issues related to its web servers and Internet presence:

* The company's security rating declined on multiple occasions when it failed to renew a TLS certificate on one or more infrequently used web servers
* The company is running out of public IPs assigned by its ISP
* The company is implementing a WAF. and the WAF vendor charges by back-end hosts to which the WAF routes Which of the following solutions will help the company mitigate these issues'? (Select TWO).

A. Implement reverse proxy servers

B. Deploy IPv6 for external-facing servers

C. Use a DMZ architecture

D. Implement self-signed certificates and disable trust verification.

E. Work with the company's ISP to configure BGP

F. Use an automated CA service API for certificate renewal

Answer: B,C

NO.25 Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure

which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an exploit.
Which of the following would provide greater insight on the potential impact of this attempted attack?

A. Analyze network logs for unusual traffic.

B. Run an antivirus scan on the finance PC.

C. Run a baseline analyzer against the user's computer.

D. Perform reverse engineering on the document.

E. Use a protocol analyzer on the air-gapped PC.

Answer: E

NO.26 A security is testing a server finds the following in the output of a vulnerability scan:

```
PORT STATE SERVICE
139/tcp open netbios-ssn
Host script results:
| samba-vuln-cve-2018-1264:
| SAMBA remote heap overflow
| State: VULNERABLE
| Risk factor: HIGH CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
| Description:
| Samba versions 4.1.3 and all versions previous to this are affected by
| a vulnerability that allows remote code execution as the "root" user
| from an anonymous connection.
|
|_Disclosure date: 2018-03-15
```

Which of the following will the security analyst most likely use NEXT to explore this further?

A. Visualization tool

B. Reverse engineering tools

C. Vulnerability scanner

D. Exploitation framework

Answer: D

NO.27 A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:
The tool needs to be responsive so service teams can query it, and then perform an automated response action.
The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.
Which of the following need specific attention to meet the requirements listed above? (Choose three.)

A. Latency

B. Usability
C. Scalability
D. Maintainability
E. Recoverability
F. Availability
Answer: A,E,F

NO.28 While standing a proof-of-concept solution with a vendor, the following direction was given of connections to the default environments.

Test	10.10.24.38:443	www.vendordomain.com/testlogin
QA	10.10.24.38:443	www.vendordomain.com/qalogin
Production	10.10.24.38:443	www.vendordomain.com/prodlogin

Which of the following is using used to secure the three environments from overlap if all of them reside on separate serves in the same DM2?
A. Logical access controls
B. Segmentation of VlLNs
C. Subnetting of cloud environments
D. Separation of environments policy
Answer: D

NO.29 An organization has hardened its end points m the following ways
* USB ports are disabled except for approved input device IDs (e.g, mouse, keyboard)
* A desktop firewall is Mocking all outbound network connections, except to approved internal systems
* A VPN client is the only way to connect to the corporate network remotely and split tunneling is disabled
* Bluetooth is disabled
* Web browsing from end points is permitted but the traffic is directed through the VPN to the corporate gateway
* The email client is permitted to connect to the internal server over the VPN and DLP rules prohibit sending sensitive information to external recipients The organization recently suffered a security breach which a file containing PII somehow made it from a remote user's laptop to an unauthorized host Which of the following is the MOST likely for how (his happened?
A. The end user attached a USB flash drive that has the same device ID as an approved mouse and copied the file to it.
B. The end user transferred the file to a mobile phone through a wireless connection
C. The end user attached the file to an email message and sent it to a personal email account
D. The end user uploaded the file to an unauthorized website
E. The end user connected the computer to a home network and copied the file to an unauthorized host
Answer: A

NO.30 A security analyst is inspecting pseudocode of the following multithreaded application:

1. perform daily ETL of data
1.1 validate that yesterday's data model file exists
1.2 validate that today's data model file does not exist
1.2 extract yesterday's data model
1.3 transform the format
1.4 load the transformed data into today's data model file
1.5 exit
Which of the following security concerns is evident in the above pseudocode?

A. Resource exhaustion

B. Privilege escalation

C. Improper storage of sensitive data

D. Time of check/time of use

Answer: D