CAS-003Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A large industrial system\\'s smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs, the company\\'s security manager notices the generator\\'s IP is sending packets to an internal file server\\'s IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation

B. Firewall whitelisting

C. Containment

D. Isolation

Correct Answer: A

QUESTION 2

A web developer has implemented HTML5 optimizations into a legacy web application. One of the modifications the web developer made was the following client side optimization:

localStorage.setItem("session-cookie", document.cookie);

Which of the following should the security engineer recommend?

A. SessionStorage should be used so authorized cookies expire after the session ends

B. Cookies should be marked as "secure" and "HttpOnly"

C. Cookies should be scoped to a relevant domain/path

D. Client-side cookies should be replaced by server-side mechanisms

Correct Answer: C

QUESTION 3

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.

Correct Answer: D

QUESTION 4

A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (IO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

A. Multi-tenancy SaaS

B. Hybrid IaaS

C. Single-tenancy PaaS

D. Community IaaS

Correct Answer: C

QUESTION 5

An organization is implementing a virtualized thin-client solution for normal user computing and access. During a review of the architecture, concerns were raised that an attacker could gain access to multiple user environments by simply gaining a foothold on a single one with malware. Which of the following reasons BEST explains this?

A. Malware on one virtual environment could enable pivoting to others by leveraging vulnerabilities in the hypervisor.

B. A worm on one virtual environment could spread to others by taking advantage of guest OS networking services vulnerabilities.

C. One virtual environment may have one or more application-layer vulnerabilities, which could allow an attacker to escape that environment.

D. Malware on one virtual user environment could be copied to all others by the attached network storage controller.

Correct Answer: A

QUESTION 6

Wireless users are reporting issues with the company\\'s video conferencing and VoIP systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).

A. Install a HIPS on the SIP servers

B. Configure 802.1X on the network

C. Update the corporate firewall to block attacking addresses

D. Configure 802.11e on the network

E. Configure 802.1q on the network

Correct Answer: AD

Host-based intrusion prevention system (HIPS) is an installed software package that will monitor a single host for suspicious activity by analyzing events taking place within that host. IEEE 802.11e is deemed to be of significant consequence for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia.

QUESTION 7

The email administrator must reduce the number of phishing emails by utilizing more appropriate security controls The following configurations already are in place

1.

Keyword Mocking based on word lists

2.

URL rewriting and protection

3.

Stopping executable files from messages

Which of the following is the BEST configuration change for the administrator to make?

A. Configure more robust word lists for blocking suspicious emails

B. Configure appropriate regular expression rules per suspicious email received

C. Configure Bayesian filtering to block suspicious inbound email

D. Configure the mail gateway to strip any attachments

Correct Answer: B

QUESTION 8

The risk manager at a small bank wants to use quantitative analysis to determine the ALE of running a business system at a location which is subject to fires during the year. A risk analyst reports to the risk manager that the asset value of the business system is $120,000 and, based on industry data, the exposure factor to fires is only 20% due to the fire suppression system installed at the site. Fires occur in the area on average every four years. Which of the following is the ALE?

A. $6,000

B. $24,000

C. $30,000

D. $96,000

Correct Answer: A

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF)

SLE = AV x EF = $120 000 x 20% = $ 24,000 (this is over 4 years)

Thus ALE = $ 24,000 / 4 = $ 6,000

References:

http://www.financeformulas.net/Return_on_Investment.html

https://en.wikipedia.org/wiki/Risk_assessment Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition, Project Management Institute, Inc., Newtown Square, 2013, p. 198

McMillan, Troy and Robin Abernathy, CompTIA Advanced Security Practitioner (CASP) CAS-002 Cert Guide, Pearson Education, Indianapolis, 2015, p. 305

QUESTION 9

A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an except of output from the troubleshooting session:

```
openssl s_client -host ldaps.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=danville/CN=chicago
```

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

A. The clients may not trust idapt by default.

B. The secure LDAP service is not started, so no connections can be made.

C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.

D. Secure LDAP should be running on UDP rather than TCP.

E. The company is using the wrong port. It should be using port 389 for secure LDAP.

F. Secure LDAP does not support wildcard certificates.

G. The clients may not trust Chicago by default.

Correct Answer: BE

QUESTION 10

During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

A. Code repositories

B. Security requirements traceability matrix

C. Software development lifecycle

D. Data design diagram

E. Roles matrix

F. Implementation guide

Correct Answer: B

QUESTION 11

A server was compromised recently, and two unauthorized daemons were set up to listen for incoming connections. In addition, CPU cycles were being used by an additional unauthorized cron job. Which of the following would have prevented the breach if it was properly configured?

A. Set up log forwarding and utilize a SIEM for centralized management and alerting.

B. Use a patch management system to close the vulnerabilities in a shorter time frame.

C. Implement a NIDS/NIPS.

D. Deploy SELinux using the system baseline as the starting point.

E. Configure the host firewall to block unauthorized inbound connections.

Correct Answer: C

QUESTION 12

An administrator is working with management to develop policies related to the use of the cloud-based resources that contain corporate data. Management plans to require some control over organizational data stored on personal devices, such as tablets. Which of the following controls would BEST support management\\'s policy?

A. MDM

B. Sandboxing

C. Mobile tokenization

D. FDE

E. MFA

Correct Answer: A

QUESTION 13

The Chief Financial Officer (CFO) of an organization wants the IT department to add the CFO\\'s account to the domain administrator group The IT department thinks this is nsky and wants support from the security manager before proceeding. Which of the following BEST supports the argument against providing the CFO with domain administrator access?

A. Discretionary access control

B. Separation of duties

C. Data classification

D. Mandatory access control

Correct Answer: B

QUESTION 14

Which of the following is MOST likely to be included in a security services SLA with a third-party vendor?

A. The standard of quality for anti-malware engines

B. Parameters for applying critical patches

C. The validity of program productions

D. Minimum bit strength for encryption-in-transit.

Correct Answer: A

QUESTION 15

A network printer needs Internet access to function. Corporate policy states all devices allowed on the network must be authenticated. Which of the following is the MOST secure method to allow the printer on the network without violating policy?

A. Request an exception to the corporate policy from the risk management committee

B. Require anyone trying to use the printer to enter their username and password

C. Have a help desk employee sign in to the printer every morning

D. Issue a certificate to the printer and use certificate-based authentication

Correct Answer: D