CompTIA

Exam CAS-001

CompTIA Advanced Security Practitioner

Version: 14.0

[Total Questions: 495]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	100
Topic 4: Volume D	100
Topic 5: Volume E	95

Topic 1, Volume A

Question No : 1 - (Topic 1)

An internal employee has sold a copy of the production customer database that was being used for upgrade testing to outside parties via HTTP file upload. The Chief Information Officer (CIO) has resigned and the Chief Executive Officer (CEO) has tasked the incoming CIO with putting effective controls in place to help prevent this from occurring again in the future. Which of the following controls is the MOST effective in preventing this threat from re-occurring?

A. Network-based intrusion prevention system
B. Data loss prevention
C. Host-based intrusion detection system
D. Web application firewall

Answer: B

Question No : 2 - (Topic 1)

A new project initiative involves replacing a legacy core HR system, and is expected to touch many major operational systems in the company. A security administrator is engaged in the project to provide security consulting advice. In addition, there are database, network, application, HR, and transformation management consultants engaged on the project as well. The administrator has established the security requirements. Which of the following is the NEXT logical step?

A. Document the security requirements in an email and move on to the next most urgent task.
B. Organize for a requirements workshop with the non-technical project members, being the HR and transformation management consultants.
C. Communicate the security requirements with all stakeholders for discussion and buy-in.
D. Organize for a requirements workshop with the technical project members, being the database, network, and application consultants.

Answer: C

Question No : 3 - (Topic 1)

A manufacturing company is having issues with unauthorized access and modification of the controls operating the production equipment. A communication requirement is to allow the free flow of data between all network segments at the site. Which of the following BEST remediates the issue?

A. Implement SCADA security measures.
B. Implement NIPS to prevent the unauthorized activity.
C. Implement an AAA solution.
D. Implement a firewall to restrict access to only a single management station.

Answer: C

Question No : 4 - (Topic 1)

As part of the testing phase in the SDLC, a software developer wants to verify that an application is properly handling user error exceptions. Which of the following is the BEST tool or process for the developer use?

A. SRTM review
B. Fuzzer
C. Vulnerability assessment
D. HTTP interceptor

Answer: B

Question No : 5 - (Topic 1)

A company is evaluating a new marketing strategy involving the use of social networking sites to reach its customers. The marketing director wants to be able to report important company news, product updates, and special promotions on the social websites.

After an initial and successful pilot period, other departments want to use the social websites to post their updates as well.

The Chief Information Officer (CIO) has asked the company security administrator to document three negative security impacts of allowing IT staff to post work related information on such websites.

Which of the following are the major risks the security administrator should report back to the CIO? (Select THREE).

A. Brute force attacks
B. Malware infection
C. DDOS attacks
D. Phishing attacks
E. SQL injection attacks
F. Social engineering attacks

Answer: B,D,F

Question No : 6 - (Topic 1)

Company ABC has recently completed the connection of its network to a national high speed private research network. Local businesses in the area are seeking sponsorship from Company ABC to connect to the high speed research network by directly connecting through Company ABC's network. Company ABC's Chief Information Officer (CIO) believes that this is an opportunity to increase revenues and visibility for the company, as well as promote research and development in the area.

Which of the following must Company ABC require of its sponsored partners in order to document the technical security requirements of the connection?

A. SLA
B. ISA
C. NDA
D. BPA

Answer: B

Question No : 7 - (Topic 1)

A user reports that the workstation's mouse pointer is moving and files are opening automatically.

Which of the following should the user perform?

A. Unplug the network cable to avoid network activity.
B. Reboot the workstation to see if problem occurs again.
C. Turn off the computer to avoid any more issues.
D. Contact the incident response team for direction.

Answer: D

Question No : 8 - (Topic 1)

After a security incident, an administrator revokes the SSL certificate for their web server www.company.com. Later, users begin to inform the help desk that a few other servers are generating certificate errors: ftp.company.com, mail.company.com, and partners.company.com. Which of the following is MOST likely the reason for this?

A. Each of the servers used the same EV certificate.
B. The servers used a wildcard certificate.
C. The web server was the CA for the domain.
D. Revoking a certificate can only be done at the domain level.

Answer: B

Question No : 9 - (Topic 1)

A web administrator develops a web form for users to respond to the company via a web page.

Which of the following should be practiced to avoid a security risk?

A. SQL injection
B. XSS scripting
C. Click jacking
D. Input validation

Answer: D

Question No : 10 - (Topic 1)

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The network administrator reviews the tickets and compiles the following information for the security administrator:

Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0

Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0

Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0

All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-ab-1a

---

The security administrator brings a laptop to the finance office, connects it to one of the wall jacks, starts up a network analyzer, and notices the following:

09:05:10.937590 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)

09:05:15.934840 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)

09:05:19.931482 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)

Which of the following can the security administrator determine from the above information?

A. A man in the middle attack is underway - implementing static ARP entries is a possible solution.
B. An ARP flood attack targeted at the router is causing intermittent communication – implementing IPS is a possible solution.
C. The default gateway is being spoofed - implementing static routing with MD5 is a possible solution.
D. The router is being advertised on a separate network - router reconfiguration is a possible solution.

Answer: A

Question No : 11 - (Topic 1)

A number of security incidents have been reported involving mobile web-based code developed by a consulting company. Performing a root cause analysis, the security administrator of the consulting company discovers that the problem is a simple

programming error that results in extra information being loaded into the memory when the proper format is selected by the user. After repeating the process several times, the security administrator is able to execute unintentional instructions through this method. Which of the following BEST describes the problem that is occurring, a good mitigation technique to use to prevent future occurrences, and why it a security concern?

A. Problem: Cross-site scripting
Mitigation Technique. Input validation
Security Concern: Decreases the company's profits and cross-site scripting can enable malicious actors to compromise the confidentiality of network connections or interrupt the availability of the network.
B. Problem: Buffer overflow
Mitigation Technique: Secure coding standards
Security Concern: Exposes the company to liability buffer overflows and can enable malicious actors to compromise the confidentiality/availability of the data.
C. Problem: SQL injection
Mitigation Technique: Secure coding standards
Security Concern: Exposes the company to liability SQL injection and can enable malicious actors to compromise the confidentiality of data or interrupt the availability of a system.
D. Problem: Buffer overflow
Mitigation Technique: Output validation
Security Concern: Exposing the company to public scrutiny buffer overflows can enable malicious actors to interrupt the availability of a system.

Answer: B

Question No : 12 - (Topic 1)

Which of the following refers to programs running in an isolated space to run untested code and prevents the code from making permanent changes to the OS kernel and other data on the host machine?

A. Input Validation
B. Application hardening
C. Code signing
D. Application sandboxing

Answer: D

Question No : 13 - (Topic 1)

A corporate executive lost their smartphone while on an overseas business trip. The phone was equipped with file encryption and secured with a strong passphrase. The phone contained over 60GB of proprietary data. Given this scenario, which of the following is the BEST course of action?

A. File an insurance claim and assure the executive the data is secure because it is encrypted.
B. Immediately implement a plan to remotely wipe all data from the device.
C. Have the executive change all passwords and issue the executive a new phone.
D. Execute a plan to remotely disable the device and report the loss to the police.

Answer: B

Question No : 14 - (Topic 1)

A telecommunication company has recently upgraded their teleconference systems to multicast. Additionally, the security team has instituted a new policy which requires VPN to access the company's video conference. All parties must be issued a VPN account and must connect to the company's VPN concentrator to participate in the remote meetings.

Which of the following settings will increase bandwidth utilization on the VPN concentrator during the remote meetings?

A. IPSec transport mode is enabled
B. ICMP is disabled
C. Split tunneling is disabled
D. NAT-traversal is enabled

Answer: C

Question No : 15 - (Topic 1)

A security architect is assigned to a major software development project. The software development team has a history of writing bug prone, inefficient code, with multiple securityflaws in every release. The security architect proposes implementing secure coding standards to the project manager. The secure coding standards will contain detailed standards for:

A. error handling, input validation, memory use and reuse, race condition handling,

commenting, and preventing typical security problems.
B. error prevention, requirements validation, memory use and reuse, commenting typical security problems, and testing code standards.
C. error elimination, trash collection, documenting race conditions, peer review, and typical security problems.
D. error handling, input validation, commenting, preventing typical security problems, managing customers, and documenting extra requirements.

Answer: A

Question No : 16 - (Topic 1)

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

Answer: A

Question No : 17 - (Topic 1)

Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices DOS attacks on the network that are affecting the company's VoIP system (i.e. premature call drops and garbled call signals). 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. Configure 802.11b on the network
B. Configure 802.1q on the network
C. Configure 802.11e on the network
D. Update the firewall managing the SIP servers
E. Update the HIDS managing the SIP servers

Answer: C,D