

Vendor: CompTIA

Exam Code: CAS-002

Exam Name: CompTIA Advanced Security Practitioner (CASP)

Version: Demo

QUESTION 1

An attacker attempts to create a DoS event against the VoIP system of a company. The attacker uses a tool to flood the network with a large number of SIP INVITE traffic. Which of the following would be LEAST likely to thwart such an attack?

- A. Install IDS/IPS systems on the network
- B. Force all SIP communication to be encrypted
- C. Create separate VLANs for voice and data traffic
- D. Implement QoS parameters on the switches

Correct Answer: D

Explanation

QUESTION 2

Joe, the Chief Executive Officer (CEO), was an Information security professor and a Subject Matter Expert for over 20 years. He has designed a network defense method which he says is significantly better than prominent international standards. He has recommended that the company use his cryptographic method. Which of the following methodologies should be adopted?

- A. The company should develop an in-house solution and keep the algorithm a secret.
- B. The company should use the CEO's encryption scheme.
- C. The company should use a mixture of both systems to meet minimum standards.
- D. The company should use the method recommended by other respected information security organizations.

Correct Answer: D

Explanation

QUESTION 3

A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks. Which of the following should the CSO conduct FIRST?

- A. Survey threat feeds from services inside the same industry.
- B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic.
- C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
- D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

Correct Answer: A

Explanation

QUESTION 4

An administrator wants to enable policy based flexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST accomplish this?

- A. Access control lists
- B. SELinux
- C. IPtables firewall
- D. HIPS

Correct Answer: B

Explanation

QUESTION 5

Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company's purchased application? (Select TWO).

- A. Code review
- B. Sandbox
- C. Local proxy
- D. Fuzzer
- E. Port scanner

Correct Answer: CD

Explanation

QUESTION 6

A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

- A. Client side input validation
- B. Stored procedure
- C. Encrypting credit card details
- D. Regular expression matching

Correct Answer: D

Explanation

QUESTION 7

A Chief Financial Officer (CFO) 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 funded 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 CFO 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 CFO.
- D. Security controls are generally never 100% effective and gaps should be explained to stakeholders and managed accordingly.

Correct Answer: D

Explanation

QUESTION 8

A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

- A. Determining how to install HIPS across all server platforms to prevent future incidents

- B. Preventing the ransomware from re-infecting the server upon restore
- C. Validating the integrity of the deduplicated data
- D. Restoring the data will be difficult without the application configuration

Correct Answer: D

Explanation

QUESTION 9

The security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?

- A. PING
- B. NESSUS
- C. NSLOOKUP
- D. NMAP

Correct Answer: D

Explanation

QUESTION 10

A large enterprise acquires another company which uses antivirus from a different vendor. The CISO has requested that data feeds from the two different antivirus platforms be combined in a way that allows management to assess and rate the overall effectiveness of antivirus across the entire organization. Which of the following tools can BEST meet the CISO's requirement?

- A. GRC
- B. IPS
- C. CMDB
- D. Syslog-ng
- E. IDS

Correct Answer: A

Explanation

QUESTION 11

Due to a new regulatory requirement, ABC Company must now encrypt all WAN transmissions. When speaking with the network administrator, the security administrator learns that the existing routers have the minimum processing power to do the required level of encryption. Which of the following solutions minimizes the performance impact on the router?

- A. Deploy inline network encryption devices
- B. Install an SSL acceleration appliance
- C. Require all core business applications to use encryption
- D. Add an encryption module to the router and configure IPsec

Correct Answer: A

Explanation

QUESTION 12

The source workstation image for new accounting PCs has begun blue-screening. A technician notices that the date/time stamp of the image source appears to have changed. The desktop support director has asked the Information Security department to determine if any changes were made to the source image. Which of the following methods would BEST help with this process? (Select TWO).

- A. Retrieve source system image from backup and run file comparison analysis on the two images.
- B. Parse all images to determine if extra data is hidden using steganography.
- C. Calculate a new hash and compare it with the previously captured image hash.
- D. Ask desktop support if any changes to the images were made.
- E. Check key system files to see if date/time stamp is in the past six months.

Correct Answer: AC

Explanation

QUESTION 13

The risk manager is reviewing a report which identifies a requirement to keep a business critical legacy system operational for the next two years. The legacy system is out of support because the vendor and security patches are no longer released. Additionally, this is a proprietary embedded system and little is documented and known about it. Which of the following should the Information Technology department implement to reduce the security risk from a compromise of this system?

- A. Virtualize the system and migrate it to a cloud provider.
- B. Segment the device on its own secure network.
- C. Install an antivirus and HIDS on the system.
- D. Hire developers to reduce vulnerabilities in the code.

Correct Answer: B

Explanation

QUESTION 14

An organization has decided to reduce labor costs by outsourcing back office processing of credit applications to a provider located in another country. Data sovereignty and privacy concerns raised by the security team resulted in the third-party provider only accessing and processing the data via remote desktop sessions. To facilitate communications and improve productivity, staff at the third party has been provided with corporate email accounts that are only accessible via the remote desktop sessions. Email forwarding is blocked and staff at the third party can only communicate with staff within the organization. Which of the following additional controls should be implemented to prevent data loss? (Select THREE).

- A. Implement hashing of data in transit
- B. Session recording and capture
- C. Disable cross session cut and paste
- D. Monitor approved credit accounts
- E. User access audit reviews
- F. Source IP whitelisting

Correct Answer: CEF

Explanation

QUESTION 15

The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management's directives?

- A. Develop an information classification scheme that will properly secure data on corporate systems.
- B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
- C. Publish a policy that addresses the security requirements for working remotely with company equipment.

D. Work with mid-level managers to identify and document the proper procedures for telecommuting.

Correct Answer: C

Explanation

QUESTION 16

A security engineer is responsible for monitoring company applications for known vulnerabilities. Which of the following is a way to stay current on exploits and information security news?

- A. Update company policies and procedures
- B. Subscribe to security mailing lists
- C. Implement security awareness training
- D. Ensure that the organization vulnerability management plan is up-to-date

Correct Answer: B

Explanation

QUESTION 17

A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?

- A. Memorandum of Agreement
- B. Interconnection Security Agreement
- C. Non-Disclosure Agreement
- D. Operating Level Agreement

Correct Answer: B

Explanation

QUESTION 18

A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).

- A. Demonstration of IPS system
- B. Review vendor selection process
- C. Calculate the ALE for the event
- D. Discussion of event timeline
- E. Assigning of follow up items

Correct Answer: DE

Explanation

QUESTION 19

The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction. Which of the following designs BEST supports the given requirements?

- A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.
- B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.
- C. A SaaS based firewall which logs to the company's local storage via SSL, and is managed by the change control team.

- D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

Correct Answer: A
Explanation

QUESTION 20

Which of the following provides the BEST risk calculation methodology?

- A. Annual Loss Expectancy (ALE) x Value of Asset
- B. Potential Loss x Event Probability x Control Failure Probability
- C. Impact x Threat x Vulnerability
- D. Risk Likelihood x Annual Loss Expectancy (ALE)

Correct Answer: B
Explanation

QUESTION 21

Ann, a systems engineer, is working to identify an unknown node on the corporate network. To begin her investigative work, she runs the following nmap command string:

```
user@hostname:~$ sudo nmap -O 192.168.1.54
```

Based on the output, nmap is unable to identify the OS running on the node, but the following ports are open on the device:

TCP/22

TCP/111

TCP/512-514

TCP/2049

TCP/32778

Based on this information, which of the following operating systems is MOST likely running on the unknown node?

- A. Linux
- B. Windows
- C. Solaris
- D. OSX

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 22

A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

- A. Insecure direct object references, CSRF, Smurf
- B. Privilege escalation, Application DoS, Buffer overflow
- C. SQL injection, Resource exhaustion, Privilege escalation

D. CSRF, Fault injection, Memory leaks

Correct Answer: A

Explanation

QUESTION 23

A company sales manager received a memo from the company's financial department which stated that the company would not be putting its software products through the same security testing as previous years to reduce the research and development cost by 20 percent for the upcoming year. The memo also stated that the marketing material and service level agreement for each product would remain unchanged. The sales manager has reviewed the sales goals for the upcoming year and identified an increased target across the software products that will be affected by the financial department's change. All software products will continue to go through new development in the coming year. Which of the following should the sales manager do to ensure the company stays out of trouble?

- A. Discuss the issue with the software product's user groups
- B. Consult the company's legal department on practices and law
- C. Contact senior finance management and provide background information
- D. Seek industry outreach for software practices and law

Correct Answer: B

Explanation

QUESTION 24

The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges.

Web server logs show the following:

```
90.76.165.40 -- [08/Mar/2014:10:54:04] "GET calendar.php?create%20table%20hidden HTTP/1.1" 200 5724
```

```
90.76.165.40 -- [08/Mar/2014:10:54:05] "GET ../../../../root/.bash_history HTTP/1.1" 200 90.76.165.40 ?- [08/Mar/2014:10:54:04] "GET index.php?user<;scrip>;Creat<:/scrip>; HTTP/1.1" 200 5724
```

The security administrator also inspects the following file system locations on the database server using the command `ls -al /root`

```
drwxrwxrwx 11 root root 4096 Sep 28 22:45 .
drwxr-xr-x 25 root root 4096 Mar 8 09:30 ..
-rws----- 25 root root 4096 Mar 8 09:30 .bash_history
-rw----- 25 root root 4096 Mar 8 09:30 .bash_history
-rw----- 25 root root 4096 Mar 8 09:30 .profile
-rw----- 25 root root 4096 Mar 8 09:30 .ssh
```

Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).

- A. Privilege escalation
- B. Brute force attack
- C. SQL injection
- D. Cross-site scripting
- E. Using input validation, ensure the following characters are sanitized: <>
- F. Update crontab with: `find /\(-perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh`

- G. Implement the following PHP directive: `$clean_user_input = addslashes($user_input)`
- H. Set an account lockout policy

Correct Answer: AF

Explanation

Explanation/Reference:

QUESTION 25

A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

- A. Purchase new hardware to keep the malware isolated.
- B. Develop a policy to outline what will be required in the secure lab.
- C. Construct a series of VMs to host the malware environment.
- D. Create a proposal and present it to management for approval.

Correct Answer: D

Explanation

QUESTION 26

Company XYZ provides cable television service to several regional areas. They are currently installing fiber-to-the-home in many areas with hopes of also providing telephone and Internet services. The telephone and Internet services portions of the company will each be separate subsidiaries of the parent company. The board of directors wishes to keep the subsidiaries separate from the parent company. However all three companies must share customer data for the purposes of accounting, billing, and customer authentication. The solution must use open standards, and be simple and seamless for customers, while only sharing minimal data between the companies. Which of the following solutions is BEST suited for this scenario?

- A. The companies should federate, with the parent becoming the SP, and the subsidiaries becoming an IdP.
- B. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SSP.
- C. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SP.
- D. The companies should federate, with the parent becoming the ASP, and the subsidiaries becoming an IdP.

Correct Answer: C

Explanation

QUESTION 27

The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?

- A. Avoid
- B. Accept
- C. Mitigate
- D. Transfer

Correct Answer: C

Explanation

QUESTION 28

A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of-concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?

- A. Assess the reliability of the information source, likelihood of exploitability, and impact to hosted data. Attempt to exploit via the proof-of-concept code. Consider remediation options.
- B. Hire an independent security consulting agency to perform a penetration test of the web servers. Advise management of any 'high' or 'critical' penetration test findings and put forward recommendations for mitigation.
- C. Review vulnerability write-ups posted on the Internet. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software.
- D. Notify all customers about the threat to their hosted data. Bring the web servers down into "maintenance mode" until the vulnerability can be reliably mitigated through a vendor patch.

Correct Answer: A

Explanation

QUESTION 29

A software project manager has been provided with a requirement from the customer to place limits on the types of transactions a given user can initiate without external interaction from another user with elevated privileges. This requirement is BEST described as an implementation of:

- A. an administrative control
- B. dual control
- C. separation of duties
- D. least privilege
- E. collusion

Correct Answer: C

Explanation

QUESTION 30

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?

- A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates.
- B. Implementation of an offsite data center hosting all company data, as well as deployment of VDI for all client computing needs.
- C. Host based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs.
- D. Behavior based IPS with a communication link to a cloud based vulnerability and threat feed.

Correct Answer: D

Explanation

QUESTION 31

An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

- A. Replicate NAS changes to the tape backups at the other datacenter.
- B. Ensure each server has two HBAs connected through two routes to the NAS.
- C. Establish deduplication across diverse storage paths.
- D. Establish a SAN that replicates between datacenters.

Correct Answer: D

Explanation

QUESTION 32

A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls **MUST** be implemented to minimize the risk of data leakage? (Select TWO).

- A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.
- B. A DLP gateway should be installed at the company border.
- C. Strong authentication should be implemented via external biometric devices.
- D. Full-tunnel VPN should be required for all network communication.
- E. Full-drive file hashing should be implemented with hashes stored on separate storage.
- F. Split-tunnel VPN should be enforced when transferring sensitive data.

Correct Answer: BD

Explanation

QUESTION 33

An organization would like to allow employees to use their network username and password to access a third-party service. The company is using Active Directory Federated Services for their directory service. Which of the following should the company ensure is supported by the third-party? (Select TWO).

- A. LDAP/S
- B. SAML
- C. NTLM
- D. OAUTH
- E. Kerberos

Correct Answer: BE

Explanation

QUESTION 34

A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization's configuration management process using?

- A. Agile
- B. SDL
- C. Waterfall
- D. Joint application development

Correct Answer: A

Explanation

QUESTION 35

Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

- A. Integer overflow
- B. Click-jacking
- C. Race condition
- D. SQL injection
- E. Use after free
- F. Input validation

Correct Answer: E
Explanation

QUESTION 36

A forensic analyst works for an e-discovery firm where several gigabytes of data are processed daily. While the business is lucrative, they do not have the resources or the scalability to adequately serve their clients. Since it is an e-discovery firm where chain of custody is important, which of the following scenarios should they consider?

- A. Offload some data processing to a public cloud
- B. Aligning their client intake with the resources available
- C. Using a community cloud with adequate controls
- D. Outsourcing the service to a third party cloud provider

Correct Answer: C
Explanation

QUESTION 37

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
Explanation

QUESTION 38

A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

- A. RAS

- B. Vulnerability scanner
- C. HTTP intercept
- D. HIDS
- E. Port scanner
- F. Protocol analyzer

Correct Answer: DF

Explanation

QUESTION 39

A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?

- A. Agile
- B. Waterfall
- C. Scrum
- D. Spiral

Correct Answer: B

Explanation

QUESTION 40

Which of the following BEST constitutes the basis for protecting VMs from attacks from other VMs hosted on the same physical platform?

- A. Aggressive patch management on the host and guest OSs.
- B. Host based IDS sensors on all guest OSs.
- C. Different antivirus solutions between the host and guest OSs.
- D. Unique Network Interface Card (NIC) assignment per guest OS.

Correct Answer: A

Explanation

QUESTION 41

The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer's (CSO) request to harden the corporate network's perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

- A. The corporate network is the only network that is audited by regulators and customers.
- B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.
- C. Home networks are unknown to attackers and less likely to be targeted directly.
- D. Employees are more likely to be using personal computers for general web browsing when they are at home.

Correct Answer: B

Explanation

QUESTION 42

An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

- A. Ensure the SaaS provider supports dual factor authentication.
- B. Ensure the SaaS provider supports encrypted password transmission and storage.
- C. Ensure the SaaS provider supports secure hash file exchange.
- D. Ensure the SaaS provider supports role-based access control.
- E. Ensure the SaaS provider supports directory services federation.

Correct Answer: E

Explanation