Vendor: CompTIA

Exam Code: CAS-004

Exam Name: CompTIA Advanced Security Practitioner (CASP+)

Version: DEMO

QUESTION 1
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks. Which of the following sources could the architect consult to address this security concern?

A. SDLC
B. OVAL
C. IEEE
D. OWASP

Answer: D
Explanation:
OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard.

QUESTION 2
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels. Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

A. Spawn a shell using sudo and an escape string such as sudo vim -c `!sh'.
B. Perform ASIC password cracking on the host.
C. Read the /etc/passwd file to extract the usernames.
D. Initiate unquoted service path exploits.
E. Use the UNION operator to extract the database schema.

Answer: A
Explanation:
/etc/passwd is a plain text-based database that contains information for all user accounts on the system. It is owned by root and has 644 permissions. The file can only be modified by root or users with sudo privileges and readable by all system users.
Reference: https://linuxize.com/post/etc-passwd-file/

QUESTION 3
A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.
Which of the following would provide the BEST boot loader protection?

A. TPM
B. HSM
C. PKI
D. UEFI/BIOS

Answer: D
Explanation:

This task describes how to use the vSphere Client to enable and disable secure boot for a virtual machine. You can also write scripts to manage virtual machine settings. For example, you can automate changing the firmware from BIOS to EFI for virtual machines with the following PowerCLI code:

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

Reference:
https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-898217D4-689D-4EB5-866C-888353FE241C.html

QUESTION 4
A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.
Which of the following would be the BEST solution against this type of attack?

A. Cookies
B. Wildcard certificates
C. HSTS
D. Certificate pinning

Answer: C
Explanation:

ALTS has a secure handshake protocol similar to mutual TLS. Two services wishing to communicate using ALTS employ this handshake protocol to authenticate and negotiate communication parameters before sending any sensitive information. The protocol is a two-step process:

- **Step 1:Handshake** The client initiates an elliptic curve-Diffie Hellman (ECDH) handshake with the server using Curve25519. The client and server each have certified ECDH public parameters as part of their certificate, which is used during a Diffie Hellman key exchange. The handshake results in a common traffic key that is available on the client and the server. The peer identities from the certificates are surfaced to the application layer to use in authorization decisions.
- **Step 2: Record encryption** Using the common traffic key from Step 1, data is transmitted from the client to the server securely. Encryption in ALTS is implemented using BoringSSL and other encryption libraries. Encryption is most commonly AES-128-GCM while integrity is provided by AES-GCM's GMAC.

Reference: https://cloud.google.com/security/encryption-in-transit

QUESTION 5
A threat hunting team receives a report about possible APT activity in the network. Which of the following threat management frameworks should the team implement?

A. NIST SP 800-53
B. MITRE ATT&CK
C. The Cyber Kill Chain
D. The Diamond Model of Intrusion Analysis

Answer: B
Explanation:
MITRE ATT&CK is the right answer, Cyber kill chain doesn't hand persistent as specific case since in chain event persistence is part of it. Review the link below for side by side comparison and also talks about how MITRE handles persistence attacks (search for the word).
https://verveindustrial.com/resources/blog/what-is-mitre-attack-framework/

QUESTION 6
Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.
Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement rate limiting on the API.
B. Implement geoblocking on the WAF.
C. Implement OAuth 2.0 on the API.
D. Implement input validation on the API.

Answer: C
Explanation:
Keyword here is that the API does not require authentication. OAUTH 2.0 solves that and will improve performance by only processing authenticated calls.

QUESTION 7
Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility. Which of the following would be the BEST option to implement?

A. Distributed connection allocation
B. Local caching
C. Content delivery network
D. SD-WAN vertical heterogeneity

Answer: B
Explanation:
Local Caching, ts260 has a point but also in the question said internal and external sources caching handles both internal and external. CDN will only handle internal sources.

QUESTION 8
A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources. Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

A. Union filesystem overlay
B. Cgroups
C. Linux namespaces
D. Device mapper

Answer: B
Explanation:
Namespaces provide isolation of system resources, and cgroups allow for fine-grained control and enforcement of limits for those resources.

QUESTION 9
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

A. Instance-based
B. Storage-based
C. Proxy-based
D. Array controller-based

Answer: A
Explanation:
The instance-based is the most secure method that can be used to implement volume-storage encryption in IaaS environment. https://cloudgal42.com/cloud-data-encryption-architecture-and-options/

QUESTION 10
A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident. Which of the following would be BEST to proceed with the transformation?

A. An on-premises solution as a backup
B. A load balancer with a round-robin configuration
C. A multicloud provider solution
D. An active-active solution within the same tenant

Answer: C
Explanation:
An active-active cluster does nothing if the cloud provider goes down. One of the main features of multi-cloud is redundancy.
https://www.cloudflare.com/learning/cloud/what-is-multicloud/

QUESTION 11
A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption. The edge network is protected by a web proxy. Which of the following solutions should the security architect recommend?

A. Replace the current antivirus with an EDR solution.
B. Remove the web proxy and install a UTM appliance.
C. Implement a deny list feature on the endpoints.
D. Add a firewall module on the current antivirus solution.

Answer: A
Explanation:
(EDR) is a proactive endpoint security approach designed to supplement existing defenses. This advanced endpoint approach shifts security from a reactive threat approach to one that can detect and prevent threats before they reach the organization.
https://www.malwarebytes.com/cybersecurity/business/what-is-edr

QUESTION 12
All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:

```
- Leaked to the media via printing of the documents
- Sent to a personal email address
- Accessed and viewed by systems administrators
- Uploaded to a file storage site
```

Which of the following would mitigate the department's concerns?

A. Data loss detection, reverse proxy, EDR, and PGP
B. VDI, proxy, CASB, and DRM
C. Watermarking, forward proxy, DLP, and MFA
D. Proxy, secure VPN, endpoint encryption, and AV

Answer: C
Explanation:
Watermarking would help against leaking to 3rd-parties, and DLP would help with sending to unauthorized email addresses. Forward proxy would deal with uploading to file storage site.

QUESTION 13
Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

A. Lattice-based cryptography
B. Quantum computing
C. Asymmetric cryptography
D. Homomorphic encryption

Answer: D
Explanation:
Homomorphic encryption is a form of encryption that is unique in that it allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

QUESTION 14
A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services. Which of the following should be modified to prevent the issue from reoccurring?

A. Recovery point objective
B. Recovery time objective
C. Mission-essential functions
D. Recovery service level

Answer: D
Explanation:
Explanation:
Parallel Test - Uses recovery systems that are built and tested to see if they can perform actual business transactions to support key processes.
Recovery Service Level (RSL) - A metric that is displayed as a percentage of how much computing power will be needed during a disaster.

The essential element of traditional disaster recovery is a secondary data center, which can store all redundant copies of critical data, and to which you can fail over production workloads. A traditional on-premises DR site generally includes the following:

- A dedicated facility for housing the IT infrastructure, including maintenance employees and computing equipment.
- Sufficient server capacity to ensure a high level of operational performance and allow the data center to scale up or scale out depending on your business needs.
- Internet connectivity with sufficient bandwidth to enable remote access to the secondary data center.
- Network infrastructure, including firewalls, routers, and switches, to ensure a reliable connection between the primary and secondary data centers, as well as provide data availability.

QUESTION 15
A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA.
Which of the following is the BEST solution?

A. Deploy an RA on each branch office.
B. Use Delta CRLs at the branches.
C. Configure clients to use OCSP.
D. Send the new CRLs by using GPO.

Answer: C
Explanation:
OCSP stapling: OCSP stapling enables the server, rather than the client, to make the request to the OCSP responder. The server staples the OCSP response to the certificate and returns it to the client during the TLS handshake. This approach enables the presenter of the certificate, rather than the issuing CA, to bear the resource cost of providing OCSP responses. It also enables the server to cache the OCSP responses and supply them to all clients. This significantly reduces the load on the OCSP responder because the response can be cached and periodically refreshed by the server rather than by each client.
Reference: https://www.sciencedirect.com/topics/computer-science/revoke-certificate

QUESTION 16
After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used. Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

A. Disable BGP and implement a single static route for each internal network.
B. Implement a BGP route reflector.
C. Implement an inbound BGP prefix list.
D. Disable BGP and implement OSPF.

Answer: C
Explanation:
Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

QUESTION 17
A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times. Which of the following should the engineer report as the ARO for successful breaches?

A. 0.5
B. 8
C. 50
D. 36,500

Answer: A
Explanation:

There are two types of risk analysis — quantitative and qualitative:

- **Quantitative risk analysis** is an objective approach that uses hard numbers to assess the likelihood and impact of risks. The process involves calculating metrics, such as annual loss expectancy, to help you determine whether a given risk mitigation effort is worth the investment. The assessment requires well-developed project models and high-quality data.
- **Qualitative risk analysis** is a quicker way to gauge the likelihood of potential risks and their impact so you can prioritize them for further assessment. While quantitative risk analysis is objective, qualitative risk analysis is a subjective approach that ranks risks in broader terms, such as a scale of 1–5 or simply low, medium and

Both forms of risk analysis are valuable tools in risk management. In this article, we will focus on quantitative risk analysis and explain how to calculate annual loss expectancy (ALE).

Reference: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/

QUESTION 18
A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation. Which of the following is the BEST solution to meet these objectives?

A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.

B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: B
Explanation:
To improve accounts lifecycle and management, it is recommended you manage privilege access management within PAM, by importing the local administrators into PAM, reducing the number of local administrators and prevent them to see those accounts passwords.

QUESTION 19
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<!ENTITY xxe SYSTEM "file:///etc/password" >]>
<doc>&xxe;</doc>
```

Which of the following would BEST mitigate this vulnerability?

A. CAPTCHA
B. Input validation
C. Data encoding
D. Network intrusion prevention

Answer: B
Explanation:
Example #1: The attacker attempts to extract data from the server

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]> <foo>&xxe;</foo>
```

Example #2: An attacker probes the server's private network by changing the above ENTITY line to

```
<!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>
```

Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe

QUESTION 20
A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the

issue right away.
Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

A. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
B. Change privileged usernames, review the OS logs, and deploy hardware tokens.
C. Implement MFA, review the application logs, and deploy a WAF.
D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

Answer: C
Explanation:
Specifying a repository serves no purpose. You already know the library has a vulnerability. You need something which mitigates the unauthorized access, which MFA does, and a properly configured WAF would also provide protection.

QUESTION 21
A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Signature hash algorithm:
sha256
Public key:
RSA (2048 Bits)
.htaccess config:
<VirtualHost> *:80>
ServerName www.test.com
Redirect / https://www.test.com
</VirtualHost>
<VirtualHost _default_:443>
ServerName www.test.com
DocumnetRoot /usr/local/apache2/htdocs
SSLEngine On
...
</VirtualHost>
```

Which of the following is the MOST likely cause of the customer's inability to connect?

A. Weak ciphers are being used.
B. The public key should be using ECDSA.
C. The default should be on port 80.
D. The server name should be test.com.

Answer: A
Explanation:
New vulnerabilities like Zombie POODLE, GOLDENDOODLE, 0-Length OpenSSL and Sleeping POODLE were published for websites that use CBC (Cipher Block Chaining) block cipher modes. These vulnerabilities are applicable only if the server uses TLS 1.2 or TLS 1.1 or TLS 1.0 with CBC cipher modes.
Reference:
https://community.progress.com/s/article/unable-to-connect-to-site-externally-weak-cipher-or-http2-error

QUESTION 22
An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access. Which of the following describes the administrator's discovery?

A. A vulnerability
B. A threat
C. A breach
D. A risk

Answer: A
Explanation:
A vulnerability refers to a weakness in your system while the risk is related to the potential for lost, damaged, or destroyed assets.
Reference: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

QUESTION 23
After investigating virus outbreaks that have cost the company $1,000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:

	Solution Cost	Year 1 Support	Year 2 Support	Estimated Yearly Incidents
Product A	$10,000	$3,000	$1,000	1
Product B	$14,250	$1,000	$1,000	0
Product C	$9,500	$2,000	$2,000	1
Product D	$7,000	$1,000	$2,000	2
Product E	$7,000	$4,000	$4,000	0

Using the table above, which of the following would be the BEST business-driven choice among five possible solutions?

A. Product A
B. Product B
C. Product C
D. Product D
E. Product E

Answer: D
Explanation:
Product E total for Solution cost and 2 years of Support Cost is $15,000 (and will have NO costs for incidents)
Product D total for Solution cost and 2 years of Support Cost is $10,000, plus 2 Annual Incident costs total = $12,000

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**