CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

NEW QUESTION 1
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: A

Explanation:
Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

NEW QUESTION 2
In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:
* 1. International users reported latency when images on the web page were initially loading.
* 2. During times of report processing, users reported issues with inventory when attempting to place orders.
* 3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.
Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.
B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.
C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.
D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

Answer: A

NEW QUESTION 3
A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.
Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

A. The company will have access to the latest version to continue development.
B. The company will be able to force the third-party developer to continue support.
C. The company will be able to manage the third-party developer's development process.
D. The company will be paid by the third-party developer to hire a new development team.

Answer: B

NEW QUESTION 4
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: C

NEW QUESTION 5
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

NEW QUESTION 6
A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLSprotected HTTP sessions from systems that do not send traffic to those sites.
The technician will define this threat as:

A. a decrypting RSA using obsolete and weakened encryption attack.
B. a zero-day attack.
C. an advanced persistent threat.
D. an on-path attack.

Answer: A

Explanation:
Reference: https://www.internetsociety.org/deploy360/tls/basics/

NEW QUESTION 7
A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:
Unauthorized insertions into application development environments
Authorized insiders making unauthorized changes to environment configurations Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

A. Perform static code analysis of committed code and generate summary reports.
B. Implement an XML gateway and monitor for policy violations.
C. Monitor dependency management tools and report on susceptible third-party libraries.
D. Install an IDS on the development subnet and passively monitor for vulnerable services.
E. Model user behavior and monitor for deviations from normal.
F. Continuously monitor code commits to repositories and generate summary logs.

Answer: CD

NEW QUESTION 8
Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours.
Based on RPO requirements, which of the following recommendations should the management team make?

A. Leave the current backup schedule intact and pay the ransom to decrypt the data.
B. Leave the current backup schedule intact and make the human resources fileshare read-only.
C. Increase the frequency of backups and create SIEM alerts for IOCs.
D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Answer: C

NEW QUESTION 9
A security engineer thinks the development team has been hard-coding sensitive environment variables in its code. Which of the following would BEST secure the company's CI/CD pipeline?

A. Utilizing a trusted secrets manager
B. Performing DAST on a weekly basis
C. Introducing the use of container orchestration
D. Deploying instance tagging

Answer: A

Explanation:
Reference: https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/

When creating a CI/CD variable in the settings, GitLab gives the user more configuration options for the variable. Use these extra configuration options for stricter control over more sensitive variables:

1. **Environment scope**: If a variable only ever needs to be used in one specific environment, set it to only ever be available in that environment. For example, you can set a deploy token to only be available in the `production` environment.
2. **Protected variables**: Similar to the environment scope, you can set a variable to be available only when the pipeline runs on a protected branch, like your default branch.
3. **Masked**: Variables that contain secrets should always be masked. This lets you use the variable in job scripts without the risk of exposing the value of the variable. If someone tries to output it in a job log with a command like `echo $VARIABLE`, the job log will only show `echo [masked]`. There are limits to the types of values that can be masked.

NEW QUESTION 10
A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.
Which of the following would be BEST suited to meet these requirements?

A. ARF
B. ISACs
C. Node.js
D. OVAL

Answer: D

NEW QUESTION 10
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

A. Key sharing
B. Key distribution
C. Key recovery
D. Key escrow

Answer: B

Explanation:
Reference: https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48322§ion=1.3

NEW QUESTION 15
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.
Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

A. Execute never
B. No-execute
C. Total memory encryption
D. Virtual memory encryption

Answer: A

Explanation:
Reference: https://developer.arm.com/documentation/102433/0100/Stack-smashing-and-execution-permissions

NEW QUESTION 18
A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed.
Which of the following will allow the inspection of the data without multiple certificate deployments?

A. Include all available cipher suites.
B. Create a wildcard certificate.
C. Use a third-party CA.
D. Implement certificate pinning.

Answer: D

NEW QUESTION 23
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:
Reference: https://cloud.google.com/security/encryption-in-transit

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

NEW QUESTION 26
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: B

Explanation:
Reference: https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy-answers-forwhich-to-choose-when

NEW QUESTION 31
A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year.
Which of the following will MOST likely secure the data on the lost device?

A. Require a VPN to be active to access company data.
B. Set up different profiles based on the person's risk.
C. Remotely wipe the device.
D. Require MFA to access company applications.

Answer: D

NEW QUESTION 34
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:
Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe

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" >]>
```

NEW QUESTION 38
A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

Which of the following ciphers should the security analyst remove to support the business requirements?

A. TLS_AES_128_CCM_8_SHA256
B. TLS_DHE_DSS_WITH_RC4_128_SHA
C. TLS_CHACHA20_POLY1305_SHA256
D. TLS_AES_128_GCM_SHA256

Answer: C

NEW QUESTION 40
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:
Reference: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-898217D4-689D-4EB5-866C-888353FE241C.html

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)
```

NEW QUESTION 42
An organization’s hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.
Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

A. Deploy a SOAR tool.
B. Modify user password history and length requirements.
C. Apply new isolation and segmentation schemes.
D. Implement decoy files on adjacent hosts.

Answer: C

Explanation:
Reference: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/

NEW QUESTION 45
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: B

NEW QUESTION 47

A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line. Which of the following commands would be the BEST to run to view only active Internet connections?

A. sudo netstat -antu | grep “LISTEN” | awk ‘{print$5}’
B. sudo netstat -nlt -p | grep “ESTABLISHED”
C. sudo netstat -plntu | grep -v “Foreign Address”
D. sudo netstat -pnut -w | column -t -s $’\w’
E. sudo netstat -pnut | grep -P ^tcp

Answer: B

Explanation:
Reference: https://www.codegrepper.com/code-examples/shell/netstat+find+port

NEW QUESTION 50
A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

Which of the following would BEST mitigate this type of attack?

A. Installing a network firewall
B. Placing a WAF inline
C. Implementing an IDS
D. Deploying a honeypot

Answer: A

NEW QUESTION 52
Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

A. Importing the availability of messages
B. Ensuring non-repudiation of messages
C. Enforcing protocol conformance for messages
D. Assuring the integrity of messages

Answer: D

NEW QUESTION 56
While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware.
Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

A. Pay the ransom within 48 hours.
B. Isolate the servers to prevent the spread.
C. Notify law enforcement.
D. Request that the affected servers be restored immediately.

Answer: C

NEW QUESTION 60
An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.
Which of the following historian server locations will allow the business to get the required reports in an ?? and IT environment?

A. In the ?? environment, use a VPN from the IT environment into the ?? environment.
B. In the ?? environment, allow IT traffic into the ?? environment.
C. In the IT environment, allow PLCs to send data from the ?? environment to the IT environment.
D. Use a screened subnet between the ?? and IT environments.

Answer: A

NEW QUESTION 62
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: C

Explanation:
Reference: https://searchsecurity.techtarget.com/definition/cryptanalysis

NEW QUESTION 66
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation: graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?

A. NX bit
B. ASLR
C. DEP
D. HSM

Answer: B

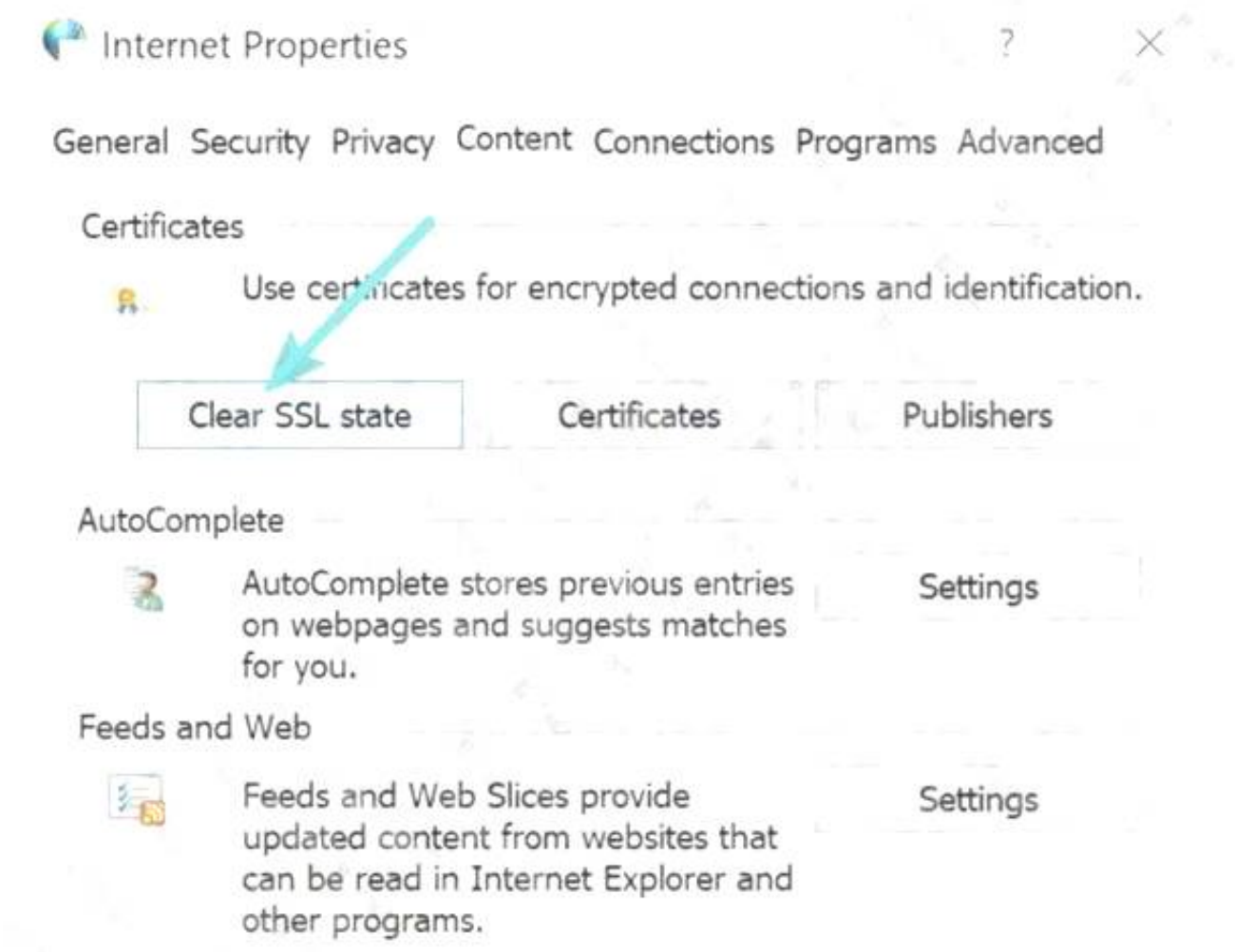
Explanation:
Reference: http://webpages.eng.wayne.edu/~fy8421/19sp-csc5290/labs/lab2-instruction.pdf (3)

NEW QUESTION 70
An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

A. The client application is testing PFS.
B. The client application is configured to use ECDHE.
C. The client application is configured to use RC4.
D. The client application is configured to use AES-256 in GCM.

Answer: C

Explanation:
Reference: https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/



NEW QUESTION 73
A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources.
The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.
Which of the following should the security team recommend FIRST?

A. Investigating a potential threat identified in logs related to the identity management system

B. Updating the identity management system to use discretionary access control
C. Beginning research on two-factor authentication to later introduce into the identity management system
D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Answer: A

NEW QUESTION 77
An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.
Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

A. Migrating operations assumes the acceptance of all risk.
B. Cloud providers are unable to avoid risk.
C. Specific risks cannot be transferred to the cloud provider.
D. Risks to data in the cloud cannot be mitigated.

Answer: C

Explanation:
Reference: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

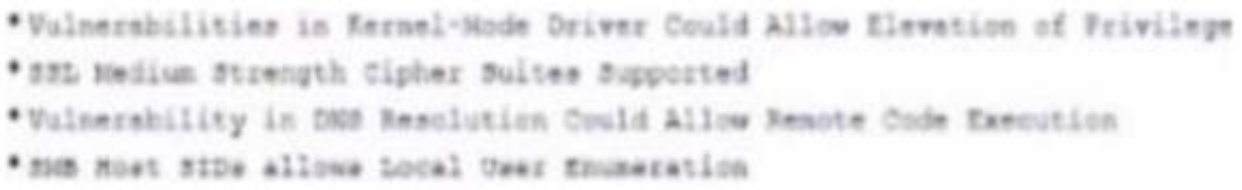
NEW QUESTION 79
A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells. Which of the following techniques will MOST likely meet the business's needs?

A. Performing deep-packet inspection of all digital audio files
B. Adding identifying filesystem metadata to the digital audio files
C. Implementing steganography
D. Purchasing and installing a DRM suite

Answer: C

Explanation:
Reference: https://portswigger.net/daily-swig/what-is-steganography-a-complete-guide-to-the-ancient-art-of-concealingmessages

NEW QUESTION 80
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:



Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

A. Password cracker
B. Port scanner
C. Account enumerator
D. Exploitation framework

Answer: A

NEW QUESTION 83
An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come In that a previously vulnerability has returned .
Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

A. Peer review
B. Regression testing
C. User acceptance
D. Dynamic analysis

Answer: A

NEW QUESTION 85
The Chief information Officer (CIO) wants to establish a non-banding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership .
Which of the follow would MOST likely be used?

A. MOU
B. OLA
C. NDA
D. SLA

Answer: A

NEW QUESTION 89
A developer implement the following code snippet.

```
catch (Exception e)
{
   if(log.isDebugEnabled())
   {
      log.debug("Caught InvalidSSHException Exception --"
      + e.toString());
   }
}
```

Which of the following vulnerabilities does the code snippet resolve?

A. SQL inject
B. Buffer overflow
C. Missing session limit
D. Information leakage

Answer: D

NEW QUESTION 90
Company A is establishing a contractual with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights .
Which of the following documents will MOST likely contain these elements?

A. Company A-B SLA v2.docx
B. Company A OLA v1b.docx
C. Company A MSA v3.docx
D. Company A MOU v1.docx
E. Company A-B NDA v03.docx

Answer: A

NEW QUESTION 94
Ann, a CIRT member, is conducting incident response activities on a network that consists of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belong to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management. However, she still needs to collect evidence of the intrusion that caused the incident .
Which of the following should Ann use to gather the required information?

A. Traffic interceptor log analysis
B. Log reduction and visualization tools
C. Proof of work analysis
D. Ledger analysis software

Answer: B

NEW QUESTION 98
A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option .
Which of the following is the BEST solution for this company?

A. Community cloud service model
B. Multinency SaaS
C. Single-tenancy SaaS
D. On-premises cloud service model

Answer: A

NEW QUESTION 99
A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that approved to be claim form, but it installed malicious software on the employee's laptop when was opened.

A. Impalement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.
B. Required all laptops to connect to the VPN before accessing email.

C. Implement cloud-based content filtering with sandboxing capabilities.
D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

Answer: C

NEW QUESTION 100
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CAS-004 Practice Exam Features:

* CAS-004 Questions and Answers Updated Frequently

* CAS-004 Practice Questions Verified by Expert Senior Certified Staff

* CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year