Number: CAS-004
Passing Score: 800
Time Limit: 120
File Version: 14.0

Exam Code: CAS-004
Exam Name: CompTIA Advanced Security Practitioner (CASP+) CAS-004

Exam A

QUESTION 1
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

Correct Answer: C
Section:
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
Reference: https://www.comptia.org/blog/what-is-steganography https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 2
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.

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

QUESTION 3
An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:
Unstructured data being exfiltrated after an employee leaves the organization
Data being exfiltrated as a result of compromised credentials

Sensitive information in emails being exfiltrated
Which of the following solutions should the security team implement to mitigate the risk of data loss?

A. Mobile device management, remote wipe, and data loss detection
B. Conditional access, DoH, and full disk encryption
C. Mobile application management, MFA, and DRM
D. Certificates, DLP, and geofencing

Correct Answer: C
Section:
Explanation:
Mobile application management (MAM) is a solution that allows the organization to control and secure the approved collaboration applications and the data within them on personal devices. MAM can prevent unstructured data from being exfiltrated by restricting the ability to move, copy, or share data between applications. Multi-factor authentication (MFA) is a solution that requires the user to provide more than one piece of evidence to prove their identity when accessing corporate data. MFA can prevent data from being exfiltrated as a result of compromised credentials by adding an extra layer of security. Digital rights management (DRM) is a solution that protects the intellectual property rights of digital content by enforcing policies and permissions on how the content can be used, accessed, or distributed. DRM can prevent sensitive information in emails from being exfiltrated by encrypting the content and limiting the actions that can be performed on it, such as forwarding, printing, or copying. Verified
Reference:
https://www.manageengine.com/data-security/what-is/byod.html
https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate

QUESTION 4
A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.
After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

A. Protecting
B. Permissive
C. Enforcing
D. Mandatory

Correct Answer: C
Section:
Explanation:
SELinux (Security-Enhanced Linux) is a security module for Linux systems that provides mandatory access control (MAC) policies for processes and files. SELinux can operate in three modes:
Enforcing: SELinux enforces the MAC policies and denies access based on rules.
Permissive: SELinux does not enforce the MAC policies but only logs actions that would have been denied if running in enforcing mode.
Disabled: SELinux is turned off.
To ensure its custom Android devices are used exclusively for package tracking, the company must configure SELinux to run in enforcing mode. This mode will prevent any unauthorized actions or applications from running on the devices and protect them from potential threats or misuse.
Reference: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security-enhanced_linux-introduction#sect-Security-Enhanced_Linux-Modes
https://source.android.com/security/selinux

QUESTION 5
A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/auth.log:
graphic.ssh_auth_log.
Which of the following actions would BEST address the potential risks by the activity in the logs?

A. Alerting the misconfigured service account password
B. Modifying the AllowUsers configuration directive

C. Restricting external port 22 access
D. Implementing host-key preferences

Correct Answer: B
Section:
Explanation:
The AllowUsers configuration directive is an option for SSH servers that specifies which users are allowed to log in using SSH. The directive can include usernames, hostnames, IP addresses, or patterns. The directive can also be negated with a preceding exclamation mark (!) to deny access to specific users.
The logs show that there are multiple failed login attempts from different IP addresses using different usernames, such as root, admin, test, etc. This indicates a brute-force attack that is trying to guess the SSH credentials. To address this risk, the security analyst should modify the AllowUsers configuration directive to only allow specific users or hosts that are authorized to access the SSH jump server. This will prevent unauthorized users from attempting to log in using SSH and reduce the attack surface.
Reference: https://man.openbsd.org/sshd_config#AllowUsers https://www.ssh.com/academy/ssh/brute-force

QUESTION 6
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.

Correct Answer: C
Section:
Explanation:
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.

QUESTION 7
A security analyst is trying to identify the source of a recent data loss incident. The analyst has reviewed all the for the time surrounding the identified all the assets on the network at the time of the data loss. The analyst suspects the key to finding the source was obfuscated in an application. Which of the following tools should the analyst use NEXT?

A. Software Decomplier
B. Network enurrerator
C. Log reduction and analysis tool
D. Static code analysis

Correct Answer: D
Section:

QUESTION 8
Which of the following controls primarily detects abuse of privilege but does not prevent it?

A. Off-boarding
B. Separation of duties
C. Least privilege

D. Job rotation

Correct Answer: A
Section:

QUESTION 9
A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the compay's intend WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

A. Active Directory OPOs
B. PKI certificates
C. Host-based firewall
D. NAC persistent agent

Correct Answer: B
Section:

QUESTION 10
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

Correct Answer: A
Section:

QUESTION 11
A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.
Which of the following is a security concern that will MOST likely need to be addressed during migration?

A. Latency
B. Data exposure
C. Data loss
D. Data dispersion

Correct Answer: B
Section:
Explanation:
Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but a availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or control of data. Verified
Reference: https://www.comptia.org/blog/what-is-data-exposure https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 12
A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form?

(Select TWO.)

A. Text editor
B. OOXML editor
C. Event Viewer
D. XML style sheet
E. SCAP tool
F. Debugging utility

Correct Answer: B, D
Section:

QUESTION 13
A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

```
High (CVSS: 10.0)
NVT: PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803317)
Product detection result: cpe:/a:php:php:5.3.6 by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to buffer overflow vulnerability.
Vulnerability Detection ResultInstalled version: 5.3.6
Fixed version: 5.3.15/5.4.5

Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions. Impact Level: System/Application
```

Which of the following MOST appropriate corrective action to document for this finding?

A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
C. The system administrator should evaluate dependencies and perform upgrade as necessary.
D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

Correct Answer: A
Section:

QUESTION 14
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

Correct Answer: C
Section:

QUESTION 15
An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come In that a previously vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

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

Correct Answer: A
Section:

QUESTION 16
A security analyst is validating the MAC policy on a set of Android devices. The policy was written to ensure non-critical applications are unable to access certain resources. When reviewing dmesg, the analyst notes many entries such as:
Despite the deny message, this action was still permit following is the MOST likely fix for this issue?

A. Add the objects of concern to the default context.
B. Set the devices to enforcing
C. Create separate domain and context files for irc.
D. Rebuild the policy, reinstall, and test.

Correct Answer: B
Section:

QUESTION 17
An organization's hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.
Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

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

Correct Answer: D
Section:
Explanation:
Implementing decoy files on adjacent hosts is a technique that can entice the adversary to uncover malicious activity, as it can lure them into accessing fake or irrelevant data that can trigger an alert or reveal their presence. Decoy files are also known as honeyfiles or honeypots, and they are part of deception technology. Deploying a SOAR (Security Orchestration Automation and Response) tool may not entice the adversary to uncover malicious activity, as SOAR is mainly focused on automating and streamlining security operations, not deceiving attackers. Modifying user password history and length requirements may not entice the adversary to uncover malicious activity, as it could affect legitimate users and not reveal the attacker's actions. Applying new isolation and segmentation schemes may not entice the adversary to uncover malicious activity, as it could limit their access and movement, but not expose their presence. Verified
Reference: https://www.comptia.org/blog/what-is-deception-technology https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 18
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

Correct Answer: A
Section:
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
Reference:
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

QUESTION 19
A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed.
Which of the following will allow the inspection of the data without multiple certificate deployments?

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

Correct Answer: B
Section:
Explanation:
A wildcard certificate is a certificate that can be used for multiple subdomains of a domain, such as *.example.com. This would allow the inspection of the data without multiple certificate deployments, as one wildcard certificate can cover all the subdomains that will be separated out with subdomains. Including all available cipher suites may not help with inspecting the data without multiple certificate deployments, as cipher suites are used for negotiating encryption and authentication algorithms, not for verifying certificates. Using a third-party CA (certificate authority) may not help with inspecting the data without multiple certificate deployments, as a third-party CA is an entity that issues and validates certificates, not a type of certificate. Implementing certificate pinning may not help with inspecting the data without multiple certificate deployments, as certificate pinning is a technique that hardcodes the expected certificate or public key in the application code, not a type of certificate. Verified
Reference: https://www.comptia.org/blog/what-is-a-wildcard-certificate https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 20
Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.
Which of the following would be the BEST option to implement?

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

Correct Answer: D
Section:
Explanation:
SD-WAN (software-defined wide area network) vertical heterogeneity is a technique that can help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility. SD-WAN vertical heterogeneity involves using different types of network links (such as broadband, cellular, or satellite) for different types of traffic (such as voice, video, or data) based on their performance and security

requirements. This can optimize the network efficiency and reliability, as well as provide granular visibility and control over traffic flows. Distributed connection allocation is not a technique for preserving network bandwidth and increasing speed, but a method for distributing network connections among multiple servers or devices. Local caching is not a technique for preserving network bandwidth and increasing speed, but a method for storing frequently accessed data locally to reduce latency or load times. Content delivery network is not a technique for preserving network bandwidth and increasing speed, but a system of distributed servers that deliver web content to users based on their geographic location. Verified
Reference: https://www.comptia.org/blog/what-is-sd-wan https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 21
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

Correct Answer: D
Section:
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
Reference: https://www.comptia.org/blog/what-is-buffer-overflow https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 22
Which of the following are risks associated with vendor lock-in? (Choose two.)

A. The client can seamlessly move data.
B. The vendor can change product offerings.
C. The client receives a sufficient level of service.
D. The client experiences decreased quality of service.
E. The client can leverage a multicloud approach.
F. The client experiences increased interoperability.

Correct Answer: B, D
Section:

QUESTION 23

An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.
Which of the following processes can be used to identify potential prevention recommendations?

A. Detection
B. Remediation
C. Preparation
D. Recovery

Correct Answer: C
Section:
Explanation:
Preparation is the process that can be used to identify potential prevention recommendations after a security incident, such as a ransomware attack. Preparation involves planning and implementing security measures to prevent or mitigate future incidents, such as by updating policies, procedures, or controls, conducting training or awareness campaigns, or acquiring new tools or resources. Detection is the process of discovering or identifying security incidents, not preventing them. Remediation is the process of containing or resolving security incidents, not preventing them. Recovery is the process of restoring normal operations after security incidents, not preventing them. Verified
Reference: https://www.comptia.org/blog/what-is-incident-response https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 24
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.
Which of the following sources could the architect consult to address this security concern?

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

Correct Answer: D
Section:
Explanation:
OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard
OWASP (Open Web Application Security Project) is a source that the security architect could consult to address the security concern of XSS (cross-site scripting) attacks on a web application that uses a database back end. OWASP is a non-profit organization that provides resources and guidance for improving the security of web applications and services. OWASP publishes the OWASP Top 10 list of common web application vulnerabilities and risks, which includes XSS attacks, as well as recommendations and best practices for preventing or mitigating them. SDLC (software development life cycle) is not a source for addressing XSS attacks, but a framework for developing software in an organized and efficient manner. OVAL (Open Vulnerability and Assessment Language) is not a source for addressing XSS attacks, but a standard for expressing system configuration information and vulnerabilities. IEEE (Institute of Electrical and Electronics Engineers) is not a source for addressing XSS attacks, but an organization that develops standards for various fields of engineering and technology. Verified
Reference: https://www.comptia.org/blog/what-is-owasp https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 25

A.
B.
C.
D.

Correct Answer:
Section:

QUESTION 26
A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.
The technician will define this threat as:

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

Correct Answer: C
Section:
Explanation:
An advanced persistent threat (APT) is a type of cyberattack that involves a stealthy and continuous process of compromising and exploiting a target system or network. An APT typically has a specific goal or objective, such as stealing sensitive data, disrupting operations, or sabotaging infrastructure. An APT can use various techniques to evade detection and maintain persistence, such as encryption, proxy servers, malware, etc. The scenario described in the question matches the characteristics of an APT.
Reference: https://www.cisco.com/c/en/us/products/security/what-is-apt.html https://www.imperva.com/learn/application-security/advanced-persistent-threat-apt/

QUESTION 27
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

Correct Answer: A
Section:
Explanation:
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.
Reference: https://www.hashicorp.com/resources/what-is-a-secret-manager https://dzone.com/articles/how-to-securely-manage-secrets-in-a-ci-cd-pipeline

QUESTION 28
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

A. Join an information-sharing community that is relevant to the company.
B. Leverage the MITRE ATT&CK framework to map the TTR.
C. Use OSINT techniques to evaluate and analyze the threats.
D. Update security awareness training to address new threats, such as best practices for data security.

Correct Answer: A
Section:
Explanation:
An information-sharing community is a group or network of organizations that share threat intelligence, best practices, and mitigation strategies related to cybersecurity. An information-sharing community can help the

company proactively manage the threats of potential theft of its newly developed, proprietary information by providing timely and actionable insights, alerts, and recommendations. An information-sharing community can also enable collaboration and coordination among its members to enhance their collective defense and resilience.
Reference: https://us-cert.cisa.gov/ncas/tips/ST04-016 https://www.cisecurity.org/blog/what-is-an-information-sharing-community/

QUESTION 29
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.

Correct Answer: D
Section:
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).
Reference: https://www.techopedia.com/definition/2460/internet-message-access-protocol-secure-imaps https://www.sophos.com/en-us/support/knowledgebase/115145.aspx

QUESTION 30
A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line.
Which of the following commands would be the BEST to run to view only active Internet connections?

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

Correct Answer: E
Section:
Explanation:
The netstat command is a tool that displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The command has various options that can modify its output. The options used in the correct answer are:
p: Show the PID and name of the program to which each socket belongs.
n: Show numerical addresses instead of trying to determine symbolic host, port or user names.
u: Show only UDP connections.
t: Show only TCP connections.
The grep command is a tool that searches for a pattern in a file or input. The option used in the correct answer is:
P: Interpret the pattern as a Perl-compatible regular expression (PCRE).
The pattern used in the correct answer is ^tcp, which means any line that starts with tcp. This will filter out any UDP connections from the output.
The sudo command is a tool that allows a user to run programs with the security privileges of another user (usually the superuser or root). This is necessary to run the netstat command with the -p option, which requires root privileges.
The correct answer will show only active TCP connections with numerical addresses and program names, which can be considered as active Internet connections. The other answers will either show different types of connections (such as listening or local), use different options that are not relevant (such as -a, -l, -w, or -s), or use different commands that are not useful (such as awk or column).
Reference: https://man7.org/linux/man-pages/man8/netstat.8.html https://man7.org/linux/man-pages/man1/grep.1.html https://man7.org/linux/man-pages/man8/sudo.8.html

QUESTION 31
A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:
https://i.postimg.cc/8P9sB3zx/image.png
The credentials used to publish production software to the container registry should be stored in a secure location.
Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly.
Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

A. TPM
B. Local secure password file
C. MFA
D. Key vault

Correct Answer: D
Section:
Explanation:
A key vault is a service that provides secure storage and management of keys, secrets, and certificates. It can be used to store credentials used to publish production software to the container registry in a secure location, and restrict access to the pipeline service account without allowing the third-party developer to read the credentials directly. A TPM (trusted platform module) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing shared credentials. A local secure password file is a file that stores passwords in an encrypted format, but it is not as secure or scalable as a key vault. MFA (multi-factor authentication) is a method of verifying the identity of a user or device by requiring two or more factors, but it does not store credentials. Verified
Reference: https://www.comptia.org/blog/what-is-a-key-vault https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 32
A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals.
Which of the following does the business's IT manager need to consider?

A. The availability of personal data
B. The right to personal data erasure
C. The company's annual revenue
D. The language of the web application

Correct Answer: B

Section:
Explanation:
The right to personal data erasure, also known as the right to be forgotten, is one of the requirements of the EU General Data Protection Regulation (GDPR), which applies to any business that stores personal data of individuals residing in the EU. This right allows individuals to request the deletion of their personal data from a business under certain circumstances. The availability of personal data, the company's annual revenue, and the language of the web application are not relevant to the GDPR. Verified
Reference: https://www.comptia.org/blog/what-is-gdpr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

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

Correct Answer: D
Section:
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
Reference: https://www.comptia.org/blog/what-is-pki https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 34
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

Correct Answer: B, F
Section:
Explanation:
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
Reference: https://www.comptia.org/blog/what-is-scap https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 35
An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items.
Which of the following phases establishes the identification and prioritization of critical systems and functions?

A. Review a recent gap analysis.
B. Perform a cost-benefit analysis.
C. Conduct a business impact analysis.
D. Develop an exposure factor matrix.

Correct Answer: C
Section:
Explanation:
According to NIST SP 800-34 Rev. 1, a business impact analysis (BIA) is a process that identifies and evaluates the potential effects of natural and man-made events on organizational operations.The BIA enables an organization to determine which systems and processes are essential to the organization's mission and prioritize their recovery time objectives (RTOs) and recovery point objectives (RPOs).12

QUESTION 36
An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.
Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

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

Correct Answer: C
Section:
Explanation:
According to NIST SP 800-146, cloud computing introduces new risks that need to be assessed and managed by the cloud consumer. Some of these risks are related to the shared responsibility model of cloud computing, where some security controls are implemented by the cloud provider and some by the cloud consumer.The cloud consumer cannot transfer all the risks to the cloud provider and needs to understand which risks are retained and which are mitigated by the cloud provider.3

QUESTION 37
A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.
Which of the following actions would BEST resolve the issue? (Choose two.)

A. Conduct input sanitization.
B. Deploy a SIEM.
C. Use containers.
D. Patch the OS
E. Deploy a WAF.
F. Deploy a reverse proxy
G. Deploy an IDS.

Correct Answer: A, E
Section:
Explanation:
A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.

According to OWASP, LDAP injection is an attack that exploits web applications that construct LDAP statements based on user input without proper validation or sanitization. LDAP injection can result in unauthorized access, data modification, or denial of service.To prevent LDAP injection, OWASP recommends conducting input sanitization by escaping special characters in user input and deploying a web application firewall (WAF) that can detect and block malicious LDAP queries.45

QUESTION 38
In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:
1- International users reported latency when images on the web page were initially loading.
2- During times of report processing, users reported issues with inventory when attempting to place orders.
3- Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.
Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

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

Correct Answer: A
Section:
Explanation:
This solution would address the three issues as follows:
Serving static content via distributed CDNs would reduce the latency for international users by delivering images from the nearest edge location to the user's request.
Creating a read replica of the central database and pulling reports from there would offload the read-intensive workload from the primary database and avoid affecting the inventory data for order placement.
Auto-scaling API servers based on performance would dynamically adjust the number of servers to match the demand and balance the load across them at peak times.

QUESTION 39
During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee.
Which of the following processes would BEST satisfy this requirement?

A. Monitor camera footage corresponding to a valid access request.
B. Require both security and management to open the door.
C. Require department managers to review denied-access requests.
D. Issue new entry badges on a weekly basis.

Correct Answer: B
Section:
Explanation:
This solution would implement a two-factor authentication (2FA) process that would prevent unauthorized individuals from entering the storage room by following an authorized employee. The two factors would be the card reader issued by the security team and the presence of a department manager.

QUESTION 40
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.

Correct Answer: A, C
Section:
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.

QUESTION 41
A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.
Which of the following is the MOST likely cause?

A. The user agent client is not compatible with the WAF.
B. A certificate on the WAF is expired.
C. HTTP traffic is not forwarding to HTTPS to decrypt.
D. Old, vulnerable cipher suites are still being used.

Correct Answer: C
Section:
Explanation:
This could be the cause of the lack of visibility from the WAF (Web Application Firewall) for the web application, as the WAF may not be able to inspect or block unencrypted HTTP traffic. To solve this issue, the web server should redirect all HTTP requests to HTTPS and use SSL/TLS certificates to encrypt the traffic.

QUESTION 42
A security analyst is reviewing the following output:

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

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

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

Correct Answer: B
Section:
Explanation:
The output shows a SQL injection attack that is trying to exploit a web application. A WAF (Web Application Firewall) is a security solution that can detect and block malicious web requests, such as SQL injection, XSS, CSRF, etc. Placing a WAF inline would prevent the attack from reaching the web server and database.
Reference: https://owasp.org/www-community/attacks/SQL_Injection https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

QUESTION 43
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

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

Correct Answer: D
Section:
Explanation:
Key escrow is a process that involves storing encryption keys with a trusted third party, such as a CASB (Cloud Access Security Broker) or a government agency. Key escrow can enable authorized access to encrypted data in case of emergencies, legal issues, or data recovery. However, key escrow also introduces some risks and challenges, such as trust, security, and privacy.
Reference: https://www.techopedia.com/definition/1772/key-escrow https://searchsecurity.techtarget.com/definition/key-escrow

QUESTION 44
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

Correct Answer: C
Section:
Explanation:
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.
Reference: https://auth0.com/docs/protocols/oauth2 https://openid.net/connect/

QUESTION 45
Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

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

Correct Answer: D
Section:
Explanation:
Homomorphic encryption is a type of encryption that allows computation and analysis of data within a ciphertext without knowledge of the plaintext. This means that encrypted data can be processed without being decrypted first, which enhances the security and privacy of the data. Homomorphic encryption can enable applications such as secure cloud computing, machine learning, and data analytics.
Reference: https://www.ibm.com/security/homomorphic-encryption https://www.synopsys.com/blogs/software-security/homomorphic-encryption/

QUESTION 46
A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.
Which of the following would satisfy the requirement?

A. NIDS
B. NIPS
C. WAF
D. Reverse proxy

Correct Answer: A
Section:
Explanation:
https://owasp.org/www-community/controls/Intrusion_Detection
A NIDS (Network Intrusion Detection System) is a security solution that monitors network traffic for signs of malicious activity, such as attacks, intrusions, or policy violations. A NIDS does not affect the availability of the company's services

because it operates in passive mode, which means it does not block or modify traffic. Instead, it alerts the network administrator or other security tools when it detects an anomaly or threat.
Reference: https://www.cisco.com/c/en/us/products/security/what-is-network-intrusion-detection-system.html https://www.imperva.com/learn/application-security/network-intrusion-detection-system-nids/

QUESTION 47
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

Correct Answer: D
Section:
Explanation:
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.
Reference: 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

QUESTION 48
A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.
B. Implement the SDLC security guidelines.
C. Track the library versions and monitor the CVE website for related vulnerabilities.
D. Perform unit testing of the open-source libraries.

Correct Answer: C
Section:
Explanation:
Tracking the library versions and monitoring the CVE (Common Vulnerabilities and Exposures) website for related vulnerabilities is an activity that the organization should incorporate into the SDLC (software development life cycle) to ensure the security of the open-source libraries integrated into its software. Tracking the library versions can help identify outdated or unsupported libraries that may contain vulnerabilities or bugs. Monitoring the CVE website can help discover publicly known vulnerabilities in the open-source libraries and their severity ratings. Performing additional SAST/DAST (static application security testing/dynamic application security testing) on the open-source libraries may not be feasible or effective for ensuring their security, as SAST/DAST are mainly focused on testing the source code or functionality of the software, not the libraries. Implementing the SDLC security guidelines is a general activity that the organization should follow for developing secure software, but it does not specifically address the security of the open-source libraries. Performing unit testing of the open-source libraries may not be feasible or effective for ensuring their security, as unit testing is mainly focused on testing the individual components or modules of the software, not the libraries. Verified
Reference: https://www.comptia.org/blog/what-is-cve https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 49
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

Correct Answer: B
Section:
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
Reference: https://www.comptia.org/blog/what-is-aslr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 50
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.
Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.
B. Change the operating system.
C. Buy a new server and create an active-active cluster.
D. Upgrade the server with a new one.

Correct Answer: A
Section:
Explanation:
Moving the server to a cloud provider is the most cost-effective solution to avoid performance issues caused by too many connections during peak seasons, such as holidays. Moving the server to a cloud provider can provide scalability, elasticity, and availability for the web server, as it can adjust its resources and capacity according to the demand and traffic. Moving the server to a cloud provider can also reduce operational and maintenance costs, as the cloud provider can handle the infrastructure and security aspects. Changing the operating system may not help avoid performance issues, as it could introduce compatibility or functionality problems, and it may not address the resource or capacity limitations. Buying a new server and creating an active-active cluster may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as complex configuration and management tasks. Upgrading the server with a new one may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as migration and testing efforts. Verified
Reference: https://www.comptia.org/blog/what-is-cloud-computing https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 51
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

Correct Answer: B, C
Section:

QUESTION 52
A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.
Which of the following technologies would BEST meet this need?

A. Faraday cage
B. WPA2 PSK
C. WPA3 SAE
D. WEP 128 bit

Correct Answer: C
Section:
Explanation:
WPA3 SAE prevents brute-force attacks.
''WPA3 Personal (WPA-3 SAE) Mode is a static passphrase-based method. It provides better security than what WPA2 previously provided, even when a non-complex password is used, thanks to Simultaneous Authentication of Equals (SAE), the personal authentication process of WPA3.''

QUESTION 53
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

Correct Answer: C
Section:
Explanation:
An EDR and whitelist should protect from this attack.

QUESTION 54
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 be BEST for the engineer to utilize in this situation?

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

Correct Answer: C
Section:

QUESTION 55
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.

Correct Answer: A
Section:

QUESTION 56
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.

Correct Answer: A
Section:

QUESTION 57
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

Correct Answer: C, F

Section:
Explanation:

QUESTION 58
A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online. Which of the following be the FIRST step taken by the team?

A. Perform a review of all policies an procedures related to BGP a and DR and created an educated educational module that can be assigned to at employees to provide training on BCP/DR events.
B. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.
C. Have each business unit conduct a BIA and categories the application according to the cumulative data gathered.
D. Implement replication of all servers and application data to back up detacenters that are geographically from the central datacenter and release an upload BPA to all clients.

Correct Answer: C
Section:

QUESTION 59
An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization's headquarters and only datacenter are located in New York City. The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:
Low latency for all mobile users to improve the users' experience
SSL offloading to improve web server performance
Protection against DoS and DDoS attacks
High availability
Which of the following should the organization implement to BEST ensure all requirements are met?

A. A cache server farm in its datacenter
B. A load-balanced group of reverse proxy servers with SSL acceleration
C. A CDN with the origin set to its datacenter
D. Dual gigabit-speed Internet connections with managed DDoS prevention

Correct Answer: B
Section:

QUESTION 60
A security architect is reviewing the following proposed corporate firewall architecture and configuration:

```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:
Web servers must receive all updates via HTTP/S from the corporate network.
Web servers should not initiate communication with the Internet.
Web servers should only connect to preapproved corporate database servers.
Employees' computing devices should only connect to web services over ports 80 and 443.
Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443
C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535
F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Correct Answer: A, D
Section:

QUESTION 61
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

Correct Answer: C
Section:

QUESTION 62
A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack.

Which of the following is t he NEXT step of the incident response plan?

A. Remediation
B. Containment
C. Response
D. Recovery

Correct Answer: B
Section:

QUESTION 63
A recent data breach stemmed from unauthorized access to an employee's company account with a cloud-based productivity suite. The attacker exploited excessive permissions granted to a third-party OAuth application to collect sensitive information.
Which of the following BEST mitigates inappropriate access and permissions issues?

A. SIEM
B. CASB
C. WAF
D. SOAR

Correct Answer: C
Section:

QUESTION 64
A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:
22
25
110
137
138
139
445
Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.
Which of the following would be the BEST solution to harden the system?

A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.
B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.
C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.
D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.

Correct Answer: A
Section:

QUESTION 65
A recent data breach revealed that a company has a number of files containing customer data across its storage environment. These files are individualized for each employee and are used in tracking various customer orders, inquiries, and issues. The files are not encrypted and can be accessed by anyone. The senior management team would like to address these issues without interrupting existing processes.
Which of the following should a security architect recommend?

A. A DLP program to identify which files have customer data and delete them
B. An ERP program to identify which processes need to be tracked
C. A CMDB to report on systems that are not configured to security baselines
D. A CRM application to consolidate the data and provision access based on the process and need

Correct Answer: D
Section:

QUESTION 66
A security analyst observes the following while looking through network traffic in a company's cloud log:

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

Which of the following steps should the security analyst take FIRST?

A. Quarantine 10.0.5.52 and run a malware scan against the host.
B. Access 10.0.5.52 via EDR and identify processes that have network connections.
C. Isolate 10.0.50.6 via security groups.
D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Correct Answer: D
Section:

QUESTION 67
Which of the following is the MOST important cloud-specific risk from the CSP's viewpoint?

A. Isolation control failure
B. Management plane breach
C. Insecure data deletion
D. Resource exhaustion

Correct Answer: B
Section:

QUESTION 68
An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment's notice.
Which of the following should the organization consider FIRST to address this requirement?

A. Implement a change management plan to ensure systems are using the appropriate versions.
B. Hire additional on-call staff to be deployed if an event occurs.

C. Design an appropriate warm site for business continuity.
D. Identify critical business processes and determine associated software and hardware requirements.

Correct Answer: D
Section:

QUESTION 69
Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:

A. when it is passed across a local network.
B. in memory during processing
C. when it is written to a system's solid-state drive.
D. by an enterprise hardware security module.

Correct Answer: B
Section:

QUESTION 70
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

Correct Answer: D
Section:

QUESTION 71
A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.
Which of the following BEST describes the type of malware the solution should protect against?

A. Worm
B. Logic bomb
C. Fileless
D. Rootkit

Correct Answer: C
Section:

QUESTION 72

A development team created a mobile application that contacts a company's back-end APIs housed in a PaaS environment. The APIs have been experiencing high processor utilization due to scraping activities. The security engineer needs to recommend a solution that will prevent and remedy the behavior.
Which of the following would BEST safeguard the APIs? (Choose two.)

A. Bot protection
B. OAuth 2.0
C. Input validation
D. Autoscaling endpoints
E. Rate limiting
F. CSRF protection

Correct Answer: D, E
Section:

QUESTION 73
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

Correct Answer: A
Section:
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.

QUESTION 74
Which of the following technologies allows CSPs to add encryption across multiple data storages?

A. Symmetric encryption
B. Homomorphic encryption
C. Data dispersion
D. Bit splitting

Correct Answer: D
Section:

QUESTION 75
A vulnerability scanner detected an obsolete version of an open-source file-sharing application on one of a company's Linux servers. While the software version is no longer supported by the OSS community, the company's Linux vendor backported fixes, applied them for all current vulnerabilities, and agrees to support the software in the future.
Based on this agreement, this finding is BEST categorized as a:

A. true positive.

B. true negative.
C. false positive.
D. false negative.

Correct Answer: C
Section:

QUESTION 76
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

Correct Answer: B
Section:

QUESTION 77
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.

Correct Answer: A
Section:

QUESTION 78
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

Correct Answer: A
Section:

QUESTION 79
An organization's assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API.
Given this information, which of the following is a noted risk?

A. Feature delay due to extended software development cycles
B. Financial liability from a vendor data breach
C. Technical impact to the API configuration
D. The possibility of the vendor's business ceasing operations

Correct Answer: A
Section:

QUESTION 80
A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?

A. HSTS
B. CRL
C. CSRs
D. OCSP

Correct Answer: C
Section:

QUESTION 81
A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:
Must have a minimum of 15 characters
Must use one number
Must use one capital letter
Must not be one of the last 12 passwords used
Which of the following policies should be added to provide additional security?

A. Shared accounts
B. Password complexity
C. Account lockout
D. Password history
E. Time-based logins

Correct Answer: C
Section:

QUESTION 82
A security architect for a large, multinational manufacturer needs to design and implement a security solution to monitor traffic.
When designing the solution, which of the following threats should the security architect focus on to prevent attacks against the network?

A. Packets that are the wrong size or length
B. Use of any non-DNP3 communication on a DNP3 port
C. Multiple solicited responses over time
D. Application of an unsupported encryption algorithm

Correct Answer: C
Section:

QUESTION 83
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

Correct Answer: B
Section:

QUESTION 84
As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents.
Which of the following BEST describes this kind of risk response?

A. Risk rejection
B. Risk mitigation
C. Risk transference
D. Risk avoidance

Correct Answer: C
Section:

QUESTION 85
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

Correct Answer: C
Section:

QUESTION 86
An auditor Is reviewing the logs from a web application to determine the source of an Incident. The web application architecture Includes an Internet-accessible application load balancer, a number of web servers In a private subnet, application servers, and one database server In a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

```
Web server logs
192.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET /../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/ HTTP/1.1" 200 453 Safari/536.36

Application server logs
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing

Database server logs
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size' unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is self signed.
```

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

A. Enable the x-Forwarded-For header al the load balancer.
B. Install a software-based HIDS on the application servers.
C. Install a certificate signed by a trusted CA.
D. Use stored procedures on the database server.
E. Store the value of the $_server (' REMOTE_ADDR '] received by the web servers.

Correct Answer: C
Section:

QUESTION 87
A help desk technician just informed the security department that a user downloaded a suspicious file from internet explorer last night. The user confirmed accessing all the files and folders before going home from work. the next morning, the user was no longer able to boot the system and was presented a screen with a phone number. The technician then tries to boot the computer using wake-on-LAN, but the system would not come up. which of the following explains why the computer would not boot?

A. The operating system was corrupted.
B. SElinux was in enforced status.
C. A secure boot violation occurred.
D. The disk was encrypted.

Correct Answer: A
Section:

QUESTION 88
A small business would like to provide guests who are using mobile devices encrypted WPA3 access without first distributing PSKs or other credentials. Which of the following features will enable the business to meet this objective?

A. Simultaneous Authentication of Equals
B. Enhanced open
C. Perfect forward secrecy
D. Extensible Authentication Protocol

Correct Answer: A
Section:

QUESTION 89
Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts partial responsibility for application-level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

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

Correct Answer: D
Section:

QUESTION 90
A large telecommunications equipment manufacturer needs to evaluate the strengths of security controls in a new telephone network supporting first responders. Which of the following techniques would the company use to evaluate data confidentiality controls?

A. Eavesdropping
B. On-path
C. Cryptanalysis
D. Code signing
E. RF sidelobe sniffing

Correct Answer: A
Section:

QUESTION 91
A company wants to quantify and communicate the effectiveness of its security controls but must establish measures. Which of the following is MOST likely to be included in an effective assessment roadmap for these controls?

A. Create a change management process.
B. Establish key performance indicators.
C. Create an integrated master schedule.
D. Develop a communication plan.
E. Perform a security control assessment.

Correct Answer: C
Section:

QUESTION 92
A company launched a new service and created a landing page within its website network for users to access the service. Per company policy, all websites must utilize encryption for any authentication pages. A junior network administrator proceeded to use an outdated procedure to order new certificates. Afterward, customers are reporting the following error when accessing a new web page: NET:ERR_CERT_COMMON_NAME_INVALID. Which of the following BEST describes what the administrator should do NEXT?

A. Request a new certificate with the correct subject alternative name that includes the new websites.
B. Request a new certificate with the correct organizational unit for the company's website.
C. Request a new certificate with a stronger encryption strength and the latest cipher suite.
D. Request a new certificate with the same information but including the old certificate on the CRL.

Correct Answer: D
Section:

QUESTION 93
An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:
* Some developers can directly publish code to the production environment.
* Static code reviews are performed adequately.
* Vulnerability scanning occurs on a regularly scheduled basis per policy.
Which of the following should be noted as a recommendation within the audit report?

A. Implement short maintenance windows.
B. Perform periodic account reviews.
C. Implement job rotation.
D. Improve separation of duties.

Correct Answer: D
Section:

QUESTION 94
An organization requires a contractual document that includes
* An overview of what is covered
* Goals and objectives
* Performance metrics for each party
* A review of how the agreement is managed by all parties
Which of the following BEST describes this type of contractual document?

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

Correct Answer: A
Section:
Explanation:
A Service Level Agreement is a contract between a service provider and a customer that outlines the level of services to be provided, the metrics by which those services will be measured, and how the agreement will be managed by both parties. SLAs also include provisions for dispute resolution and for the termination of the agreement.

QUESTION 95
Based on PCI DSS v3.4, One Particular database field can store data, but the data must be unreadable. which of the following data objects meets this requirement?

A. PAN
B. CVV2
C. Cardholder name
D. expiration date

Correct Answer: A
Section:

QUESTION 96
A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems.

Which of the following now describes the level of risk?

A. Inherent
B. Low
C. Mitigated
D. Residual.
E. Transferred

Correct Answer: D
Section:

QUESTION 97
A developer wants to develop a secure external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of web-application security Which of the following is the BEST option?

A. ICANN
B. PCI DSS
C. OWASP
D. CSA
E. NIST

Correct Answer: C
Section:

QUESTION 98
Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

A. Remote provider BCDR
B. Cloud provider BCDR
C. Alternative provider BCDR
D. Primary provider BCDR

Correct Answer: B
Section:

QUESTION 99
A product development team has submitted code snippets for review prior to release.
INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.
Code Snippet 1

Code Snippet 1 | Code Snippet 2

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103


Web server code:
…
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
…
```

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                          -h loginserver.comptia.org
                          -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

Vulnerability 1:
SQL injection
Cross-site request forgery
Server-side request forgery
Indirect object reference
Cross-site scripting
Fix 1:
Perform input sanitization of the userid field.
Perform output encoding of queryResponse,
Ensure usex:ia belongs to logged-in user.
Inspect URLS and disallow arbitrary requests.
Implement anti-forgery tokens.
Vulnerability 2
1) Denial of service

2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind variables.
B) Remove the serve_forever instruction.
C) Prevent the 'authenticated' value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

A. See below explanation

Correct Answer: A
Section:
Explanation:

Code Snippet 1
Vulnerability 1:SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1:Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2
Vulnerability 2:Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2:Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

QUESTION 100
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.

Correct Answer: D
Section:
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.

QUESTION 101
A software company is developing an application in which data must be encrypted with a cipher that requires the following:
* Initialization vector
* Low latency
* Suitable for streaming
Which of the following ciphers should the company use?

A. Cipher feedback
B. Cipher block chaining message authentication code
C. Cipher block chaining
D. Electronic codebook

Correct Answer: A
Section:
Explanation:
Cipher feedback (CFB) is a mode of operation for block ciphers that allows them to encrypt streaming data. CFB uses an initialization vector (IV) and a block cipher to generate a keystream that is XORed with the plaintext to produce the ciphertext. CFB has low latency because it can encrypt each byte or bit of plaintext as soon as it arrives, without waiting for a full block. CFB is suitable for streaming data because it does not require padding or block synchronization.
B. Cipher block chaining message authentication code (CBC-MAC) is a mode of operation for blockciphers that provides both encryption and authentication. CBC-MAC uses an IV and a block cipher toencrypt the plaintext and generate a MAC value that is appended to the ciphertext. CBC-MAC hashigh latency because it requires the entire message to be processed before generating the MACvalue. CBC-MAC is not suitable for streaming data because it requires padding and blocksynchronization.C. Cipher block chaining (CBC) is a mode of operation for block ciphers that provides encryption only.CBC uses an IV and a block cipher to encrypt each block of plaintext by XORing it with the previousciphertext block. CBC has high latency because it requires a full block of plaintext before encryption.CBC is not suitable for streaming data because it requires padding and block synchronization.D. Electronic codebook (ECB) is a mode of operation for block ciphers that provides encryption only.ECB uses a block cipher to encrypt each block of plaintext independently. ECB has low latencybecause it can encrypt each block of plaintext as soon as it arrives. However, ECB is not suitable forstreaming data because it requires padding and block synchronization. Moreover, ECB is insecurebecause it does not use an IV and produces identical ciphertext blocks for identical plaintext blocks.

QUESTION 102
To save time, a company that is developing a new VPN solution has decided to use the OpenSSL library within Its proprietary software. Which of the following should the company consider to maximize risk reduction from vulnerabilities introduced by OpenSSL?

A. Include stable, long-term releases of third-party libraries instead of using newer versions.
B. Ensure the third-party library implements the TLS and disable weak ciphers.
C. Compile third-party libraries into the main code statically instead of using dynamic loading.
D. Implement an ongoing, third-party software and library review and regression testing.

Correct Answer: D
Section:
Explanation:
Implementing an ongoing, third-party software and library review and regression testing is the best way to maximize risk reduction from vulnerabilities introduced by OpenSSL. Third-party software and libraries are often used by developers to save time and resources, but they may also introduce security risks if they are not properly maintained and updated. By reviewing and testing the third-party software and library regularly, the company can ensure that they are using the latest and most secure version of OpenSSL, and that their proprietary software is compatible and functional with it.

QUESTION 103
Which of the following testing plans is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions?

A. Disaster recovery checklist
B. Tabletop exercise
C. Full interruption test
D. Parallel test

Correct Answer: B
Section:
Explanation:
A tabletop exercise is a type of testing plan that is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions. A tabletop exercise is a simulation of a potential disaster or incident that involves a verbal or written discussion of how each department would respond to it. The purpose of a tabletop exercise is to identify gaps, weaknesses, or conflicts in the disaster recovery plan, and to improve communication and coordination among the team members.

QUESTION 104
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

Correct Answer: A
Section:
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.

QUESTION 105
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

Correct Answer: B
Section:
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.

QUESTION 106
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

Correct Answer: D
Section:
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.

QUESTION 107
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

Correct Answer: B
Section:
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.

QUESTION 108
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

Correct Answer: A, E
Section:
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.

QUESTION 109
An organization is running its e-commerce site in the cloud. The capacity is sufficient to meet the organization's needs throughout most of the year, except during the holidays when the organization plans to introduce a new line of products and expects an increase in traffic. The organization is not sure how well its products will be received. To address this issue, the organization needs to ensure that:
* System capacity is optimized.
* Cost is reduced.
Which of the following should be implemented to address these requirements? (Select TWO).

A. Containerization
B. Load balancer
C. Microsegmentation
D. Autoscaling
E. CDN
F. WAF

Correct Answer: B, D
Section:
Explanation:
Load balancer and autoscaling are the solutions that should be implemented to address the requirements of optimizing system capacity and reducing cost for an e-commerce site in the cloud. A load balancer is a device or service that distributes incoming network traffic across multiple servers or instances based on various criteria, such as availability, performance, or location. A load balancer can improve system capacity by balancing the workload and preventing overloading or underutilization of resources. Autoscaling is a feature that allows cloud services to automatically adjust the number of servers or instances based on the demand or predefined rules. Autoscaling can reduce cost by scaling up or down the resources as needed, avoiding unnecessary expenses or wastage.

QUESTION 110
A cloud security engineer is setting up a cloud-hosted WAF. The engineer needs to implement a solution to protect the multiple websites the organization hosts. The organization websites are:
* www.mycompany.org
* www.mycompany.com
* campus.mycompany.com
* wiki. mycompany.org
The solution must save costs and be able to protect all websites. Users should be able to notify the cloud security engineer of any on-path attacks. Which of the following is the BEST solution?

A. Purchase one SAN certificate.
B. Implement self-signed certificates.
C. Purchase one certificate for each website.
D. Purchase one wildcard certificate.

Correct Answer: D
Section:
Explanation:

Purchasing one wildcard certificate is the best solution to protect multiple websites hosted by an organization in a cloud-hosted WAF. A wildcard certificate is a type of SSL/TLS certificate that can secure a domain name and any number of its subdomains with a single certificate. For example, a wildcard certificate for *.mycompany.com can secure www.mycompany.com, campus.mycompany.com, and any other subdomain under mycompany.com. A wildcard certificate can save costs and simplify management compared to purchasing individual certificates for each website.

QUESTION 111
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

Correct Answer: D
Section:
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.

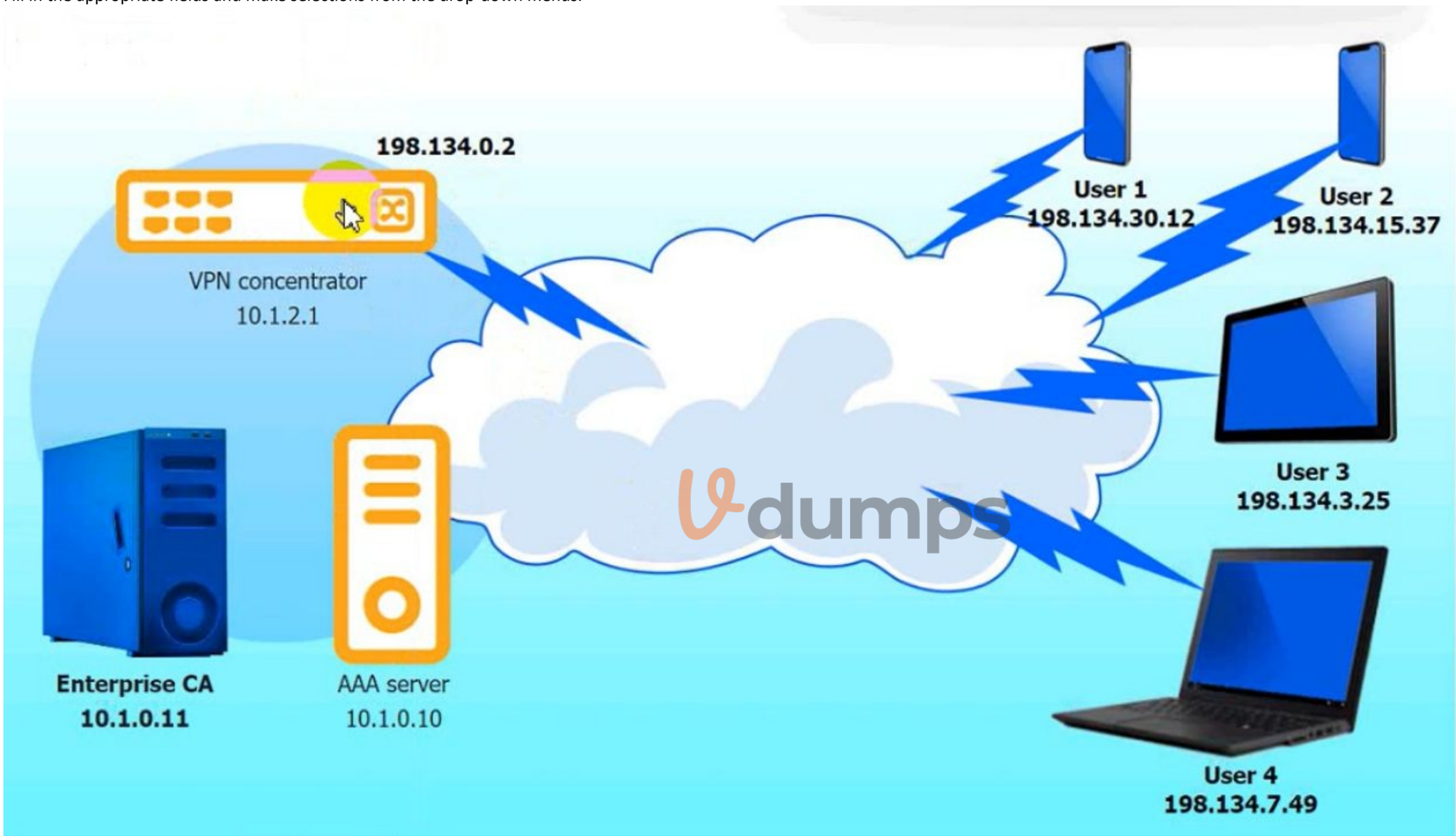
QUESTION 112
A security manager has written an incident response playbook for insider attacks and is ready to begin testing it. Which of the following should the manager conduct to test the playbook?

A. Automated vulnerability scanning
B. Centralized logging, data analytics, and visualization
C. Threat hunting
D. Threat emulation

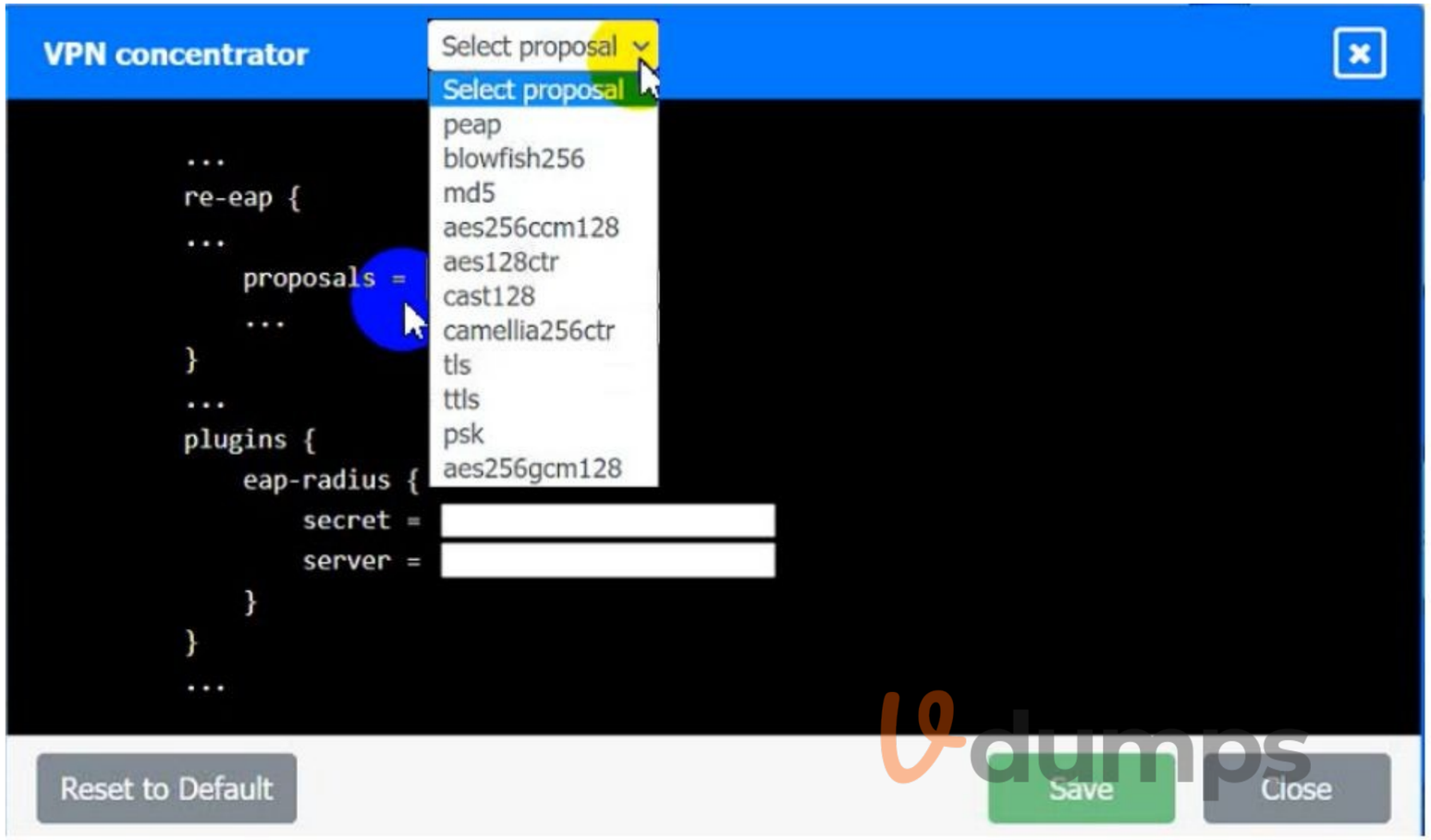
Correct Answer: D
Section:
Explanation:
Threat emulation is the method that should be used to test an incident response playbook for insider attacks. Threat emulation is a technique that simulates real-world attacks using realistic scenarios, tactics, techniques, and procedures (TTPs) of threat actors. Threat emulation can help evaluate the effectiveness of an incident response plan by testing how well it can detect, respond to, contain, eradicate, recover from, and learn from an attack.

QUESTION 113
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.
Complete the configuration files to meet the following requirements:
* The EAP method must use mutual certificate-based authentication (With issued client certificates).
* The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

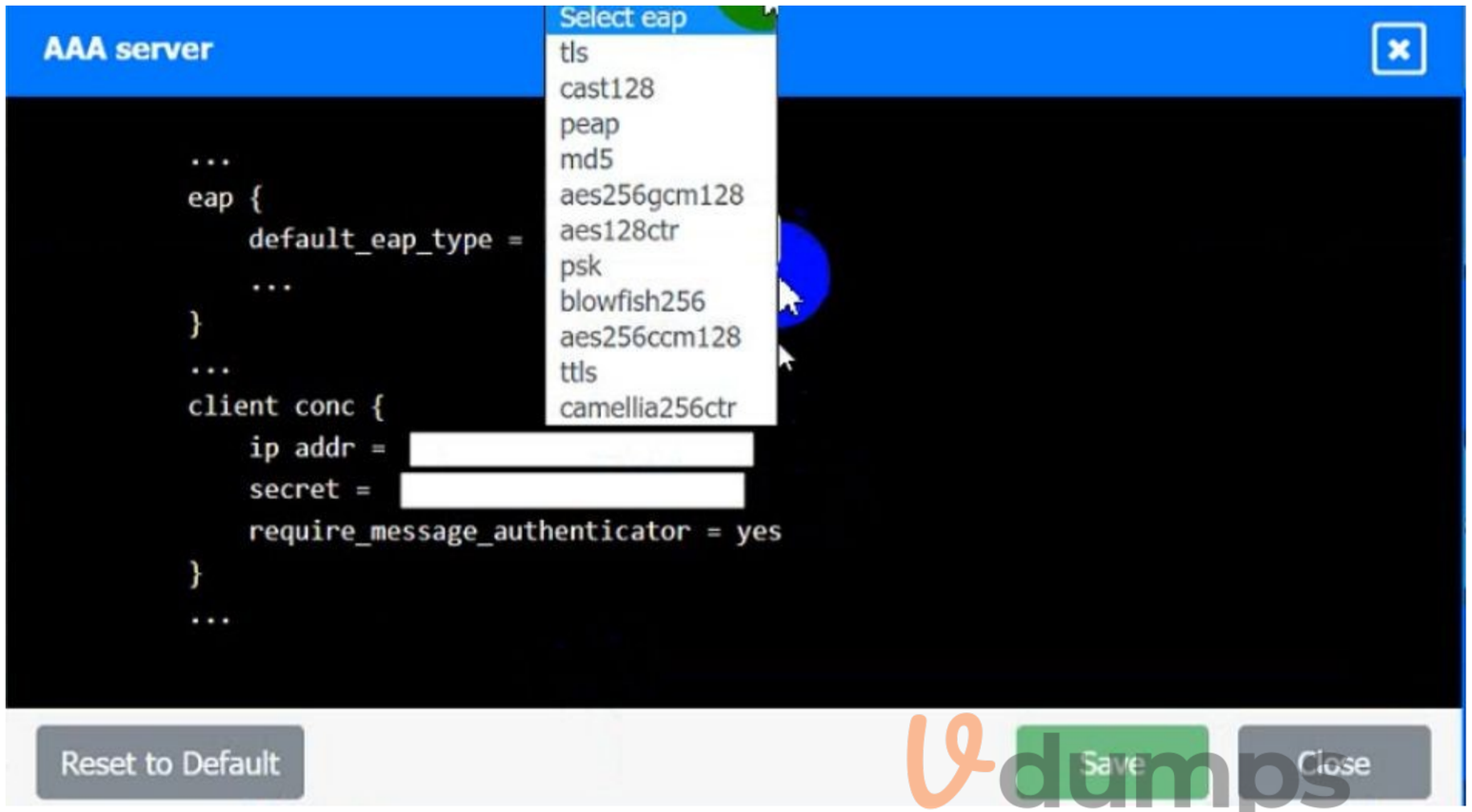
INSTRUCTIONS
Click on the AAA server and VPN concentrator to complete the configuration.
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:


VPN concentrator
Select proposal
Select proposal
peap
blowfish256
md5
aes256ccm128
aes128ctr
cast128
camellia256ctr
tls
ttls
psk
aes256gcm128
...
re-eap {
...
proposals =
...
}
...
plugins {
eap-radius {
secret =
server =
}
}
...
Reset to Default
Save
Close

AAA Server:

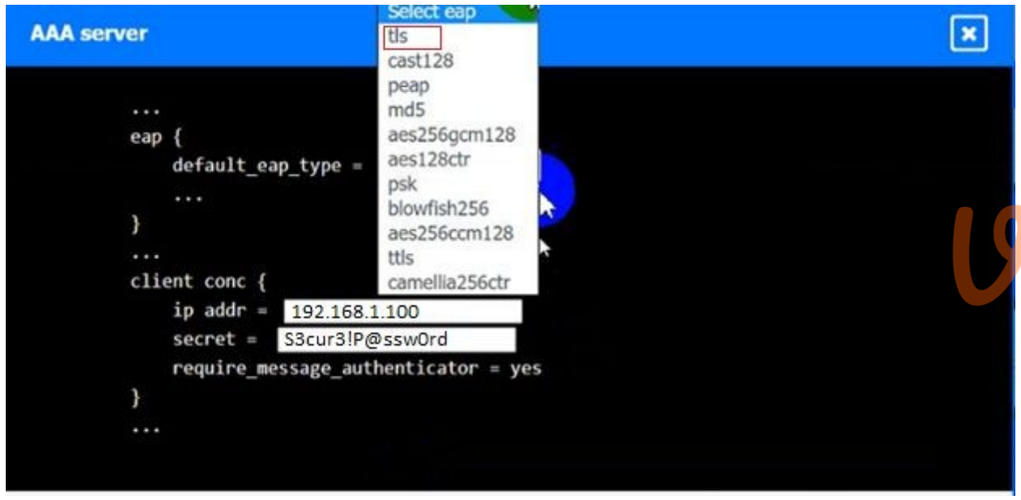


A. See the Explanation below for the solution.

Correct Answer: A
Section:
Explanation:

VPN Concentrator:

AAA Server:



QUESTION 114
In a cloud environment, the provider offers relief to an organization's teams by sharing in many of the operational duties. In a shared responsibility model, which of the following responsibilities belongs to the provider in a Paas implementation?

A. Application-specific data assets
B. Application user access management
C. Application-specific logic and code
D. Application/platform software

Correct Answer: D
Section:
Explanation:

A) Application-specific data assets are the responsibility of the organization in a PaaS implementation. The organization owns and controls its own data and must ensure its confidentiality, integrity, and availability. The organization must also comply with any applicable data protection laws and regulations.
B) Application user access management is the responsibility of the organization in a PaaS implementation. The organization must define and enforce its own policies and procedures for granting, revoking, and monitoring

access to its applications and data. The organization must also ensure that its users follow security best practices such as strong passwords and multifactor authentication.
C) Application-specific logic and code are the responsibility of the organization in a PaaS implementation. The organization must develop, test, deploy, and manage its own applications using the tools and services provided by the platform. The organization must also ensure that its applications are secure, reliable, and performant. https://www.techtarget.com/searchcloudcomputing/feature/The-cloud-shared-responsibility-model-for-IaaS-PaaS-and-SaaS

In a PaaS implementation, the provider offers relief to the organization's teams by sharing in many of the operational duties related to the application/platform software. The provider is responsible for securing and maintaining the underlying infrastructure, operating systems, middleware, runtime environments, and other software components that support the platform and the applications running on it. The provider also handles tasks such as patching, updating, scaling, and backing up the platform software.

QUESTION 115
A security architect recommends replacing the company's monolithic software application with a containerized solution. Historically, secrets have been stored in the application's configuration files. Which of the following changes should the security architect make in the new system?

A. Use a secrets management tool.
B. 'Save secrets in key escrow.
C. Store the secrets inside the Dockerfiles.
D. Run all Dockerfles in a randomized namespace.

Correct Answer: A
Section:
Explanation:

B) Saving secrets in key escrow is not a recommended solution for replacing the company's monolithic software application with a containerized solution, because it does not address the operational challenges of managing secrets for containers. Key escrow is a process of storing cryptographic keys with a trusted third party that can release them under certain conditions. Key escrow can be useful for backup or recovery purposes, but it does not provide the same level of security and automation as a secrets management tool.
C) Storing the secrets inside the Dockerfiles is not a recommended solution for replacing the company's monolithic software application with a containerized solution, because it exposes the secrets to anyone who can access the Dockerfiles or the images built from them. Storing secrets inside the Dockerfiles is equivalent to hardcoding them into the application code, which is a bad practice that violates the principle of least privilege and increases the risk of secrets leakage or compromise.
D) Running all Dockerfiles in a randomized namespace is not a recommended solution for replacing the company's monolithic software application with a containerized solution, because it does not address the issue of storing and managing secrets for containers. Running Dockerfiles in a randomized namespace is a technique to avoid name conflicts and collisions between containers, but it does not provide any security benefits for secrets.

A secrets management tool is a tool that helps companies securely store, transmit, and manage sensitive digital authentication credentials such as passwords, keys, tokens, certificates, and other secrets. A secrets management tool can help prevent secrets sprawl, enforce business policies, and inject secrets into pipelines. A secrets management tool can also help protect secrets from unauthorized access, leakage, or compromise by using encryption, tokenization, access control, auditing, and rotation. A secrets management tool is a recommended solution for replacing the company's monolithic software application with a containerized solution, because it can provide a centralized and consistent way to manage secrets across multiple containers and environments.

QUESTION 116
The CI/CD pipeline requires code to have close to zero defects and zero vulnerabilities. The current process for any code releases into production uses two-week Agile sprints. Which of the following would BEST meet the requirement?

A. An open-source automation server
B. A static code analyzer
C. Trusted open-source libraries
D. A single code repository for all developers

Correct Answer: B
Section:
Explanation:

A) An open-source automation server is not a tool that can help ensure that the code has close to zero defects and zero vulnerabilities. An open-source automation server is a tool that automates various tasks related to software development and delivery, such as building, testing, deploying, and monitoring. An open-source automation server can help speed up the CI/CD pipeline, but it does not analyze or improve the code itself.
C) Trusted open-source libraries are not tools that can help ensure that the code has close to zero defects and zero vulnerabilities. Trusted open-source libraries are collections of reusable code that developers can use to implement common or complex functionalities in their applications. Trusted open-source libraries can help save time and effort for developers, but they do not guarantee that the code is free of defects or vulnerabilities.
D) A single code repository for all developers is not a tool that can help ensure that the code has close to zero defects and zero vulnerabilities. A single code repository for all developers is a centralized storage location where developers can access and manage their source code files. A single code repository for all developers can help facilitate collaboration and version control, but it does not analyze or improve the code itself.
https://www.comparitech.com/net-admin/best-static-code-analysis-tools/ https://www.perforce.com/blog/sca/what-static-analysis

A static code analyzer is a tool that analyzes computer software without actually running the software. A static code analyzer can help developers find and fix vulnerabilities, bugs, and security risks in their new applications while the source code is in its 'static' state. A static code analyzer can help ensure that the code has close to zero defects and zero vulnerabilities by checking the code against a set of coding rules, standards, and best practices. A static code analyzer can also help improve the code quality, performance, and maintainability.

QUESTION 117
Which of the following BEST describes a common use case for homomorphic encryption?

A. Processing data on a server after decrypting in order to prevent unauthorized access in transit
B. Maintaining the confidentiality of data both at rest and in transit to and from a CSP for processing
C. Transmitting confidential data to a CSP for processing on a large number of resources without revealing information
D. Storing proprietary data across multiple nodes in a private cloud to prevent access by unauthenticated users

Correct Answer: C
Section:
Explanation:

A) Processing data on a server after decrypting in order to prevent unauthorized access in transit is not a common use case for homomorphic encryption, because it does not take advantage of the main feature of homomorphic encryption, which is computing over encrypted data. This use case can be achieved by using any standard encryption method that provides confidentiality for data in transit.
B) Maintaining the confidentiality of data both at rest and in transit to and from a CSP for processing is not a common use case for homomorphic encryption, because it does not take advantage of the main feature of homomorphic encryption, which is computing over encrypted data. This use case can be achieved by using any standard encryption method that provides confidentiality for data at rest and in transit.
D) Storing proprietary data across multiple nodes in a private cloud to prevent access by unauthenticated users is not a common use case for homomorphic encryption, because it does not involve any computation over encrypted data. This use case can be achieved by using any standard encryption method that provides confidentiality for data at rest. https://www.splunk.com/en_us/blog/learn/homomorphic-encryption.html https://research.aimultiple.com/homomorphic-encryption/

Homomorphic encryption is a type of encryption method that allows computations to be performed on encrypted data without first decrypting it with a secret key. The results of the computations also remain encrypted and can only be decrypted by the owner of the private key. Homomorphic encryption can be used for privacy-preserving outsourced storage and computation. This means that data can be encrypted and sent to a cloud service provider (CSP) for processing, without revealing any information to the CSP or anyone else who might intercept the data. Homomorphic encryption can enable new services and applications that require processing confidential data on a large number of resources, such as machine learning, data analytics, health care, finance, and voting.

QUESTION 118
Which of the following describes the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely?

A. Key escrow
B. TPM
C. Trust models
D. Code signing

Correct Answer: A
Section:
Explanation:

B) TPM is not the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. TPM stands for Trusted Platform Module, which is a hardware device that provides secure storage and generation of cryptographic keys on a computer. TPM does not involve any third party or escrow service.
C) Trust models are not the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. Trust models are frameworks that define how entities can establish and maintain trust relationships in a network or system. Trust models do not necessarily involve any third party or escrow service.
D) Code signing is not the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. Code signing is a process of using digital signatures to verify the authenticity and integrity of software code. Code signing does not involve any third party or escrow service.

Key escrow is the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow by a trusted third party that can release them under certain conditions. Key escrow can be useful for backup or recovery purposes, or for complying with legal or regulatory requirements that may demand access to encrypted data.

QUESTION 119
An organization is looking to establish more robust security measures by implementing PKI. Which of the following should the security analyst implement when considering mutual authentication?

A. Perfect forward secrecy on both endpoints
B. Shared secret for both endpoints
C. Public keys on both endpoints
D. A common public key on each endpoint
E. A common private key on each endpoint

Correct Answer: C
Section:
Explanation:

A) Perfect forward secrecy on both endpoints is not required for implementing PKI-based mutual authentication. Perfect forward secrecy (PFS) is a property of encryption protocols that ensures that the compromise of a long-term secret key (such as a private key) does not affect the security of past or future session keys (such as symmetric keys). PFS can enhance the security and privacy of encrypted communications, but it does not provide authentication by itself.
B) Shared secret for both endpoints is not required for implementing PKI-based mutual authentication. Shared secret is a method of authentication that relies on a pre-shared piece of information (such as a password or a passphrase) that is known only to both parties. Shared secret can provide simple and fast authentication, but it does not provide non-repudiation or identity verification.
D) A common public key on each endpoint is not required for implementing PKI-based mutual authentication. A common public key on each endpoint would imply that both parties share the same certificate and private key, which would defeat the purpose of PKI-based mutual authentication. Each party should have its own unique certificate and private key that proves its identity and authenticity.
E) A common private key on each endpoint is not required for implementing PKI-based mutual authentication. A common private key on each endpoint would imply that both parties share the same certificate and public key, which would defeat the purpose of PKI-based mutual authentication. Each party should have its own unique certificate and private key that proves its identity and authenticity.

Public keys on both endpoints are required for implementing PKI-based mutual authentication. PKI stands for Public Key Infrastructure, which is a system that manages the creation, distribution, and verification of certificates. Certificates are digital documents that contain public keys and identity information of their owners. Certificates are issued by trusted authorities called Certificate Authorities (CAs), and can be used to prove the identity and authenticity of the certificate holders. Mutual authentication is a process in which two parties authenticate each other at the same time using certificates. Mutual authentication can provide stronger security and privacy than one-way authentication, where only one party is authenticated. In PKI-based mutual authentication, each party has a certificate that contains its public key and identity information, and a private key that corresponds to its public key. The private key is kept secret and never shared with anyone, while the public key is shared and used to verify the identity and signature of the certificate holder. The basic steps of PKI-based mutual authentication are as follows:
Party A sends its certificate to Party B.
Party B verifies Party A's certificate by checking its validity, signature, and trust chain. If the certificate is valid and trusted, Party B extracts Party A's public key from the certificate.
Party B generates a random challenge (such as a nonce or a timestamp) and encrypts it with Party A's public key. Party B sends the encrypted challenge to Party A.
Party A decrypts the challenge with its private key and sends it back to Party B.
Party B compares the received challenge with the original one. If they match, Party B confirms that Party A is the legitimate owner of the certificate and has possession of the private key.
The same steps are repeated in reverse, with Party A verifying Party B's certificate and sending a challenge encrypted with Party B's public key.

QUESTION 120
A security manager wants to transition the organization to a zero trust architecture. To meet this requirement, the security manager has instructed administrators to remove trusted zones, role-based access, and one-time

authentication. Which of the following will need to be implemented to achieve this objective? (Select THREE).

A. Least privilege
B. VPN
C. Policy automation
D. PKI
E. Firewall
F. Continuous validation
G. Continuous integration
H. laas

Correct Answer: A, C, F
Section:
Explanation:

A) Least privilege is a principle that states that every entity or resource should only have the minimum level of access or permissions necessary to perform its function. Least privilege can help enforce granular and dynamic policies that limit the exposure and impact of potential breaches. Least privilege can also help prevent privilege escalation and abuse by malicious insiders or compromised accounts.
C) Policy automation is a process that enables the creation, enforcement, and management of security policies using automated tools and workflows. Policy automation can help simplify and streamline the implementation of zero trust architecture by reducing human errors, inconsistencies, and delays. Policy automation can also help adapt to changing conditions and requirements by updating and applying policies in real time.
F) Continuous validation is a process that involves verifying the identity, context, and risk level of every request and transaction throughout its lifecycle. Continuous validation can help ensure that only authorized and legitimate requests and transactions are allowed to access or transfer data. Continuous validation can also help detect and respond to anomalies or threats by revoking access or terminating sessions if the risk level changes.
B) VPN is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. VPN stands for Virtual Private Network, which is a technology that creates a secure tunnel between a device and a network over the internet. VPN can provide confidentiality, integrity, and authentication for network communications, but it does not provide zero trust security by itself. VPN still relies on network-based perimeters and does not verify every request or transaction at a granular level.
D) PKI is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. PKI stands for Public Key Infrastructure, which is a system that manages the creation, distribution, and verification of certificates. Certificates are digital documents that contain public keys and identity information of their owners. Certificates can be used to prove the identity and authenticity of the certificate holders, as well as to encrypt and sign data. PKI can provide encryption and authentication for data communications, but it does not provide zero trust security by itself. PKI still relies on trusted authorities and does not verify every request or transaction at a granular level.
E) Firewall is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. Firewall is a device or software that monitors and controls incoming and outgoing network traffic based on predefined rules. Firewall can provide protection against unauthorized or malicious network access, but it does not provide zero trust security by itself. Firewall still relies on network-based perimeters and does not verify every request or transaction at a granular level.
G) Continuous integration is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. Continuous integration is a software development practice that involves merging code changes from multiple developers into a shared repository frequently and automatically. Continuous integration can help improve the quality, reliability, and performance of software products, but it does not provide zero trust security by itself. Continuous integration still relies on code-based quality assurance and does not verify every request or transaction at a granular level.
H) IaaS is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources over the internet. IaaS can provide scalability, flexibility, and cost-efficiency for IT infrastructure, but it does not provide zero trust security by itself. IaaS still relies on cloud-based security controls and does not verify every request or transaction at a granular level. (Need Quick help to double verify the Answers that based on CompTIA CASP+ documents and resources) Give me following format: Question no: (Number only) Correct Answer: (Answer option in bold)

Least privilege, policy automation, and continuous validation are some of the key elements that need to be implemented to achieve the objective of transitioning to a zero trust architecture. Zero trust architecture is a security model that assumes no implicit trust for any entity or resource, regardless of their location or ownership. Zero trust architecture requires verifying every request and transaction before granting access or allowing data transfer. Zero trust architecture also requires minimizing the attack surface and reducing the risk of lateral movement by attackers.
Short but Comprehensive Explanation of Correct Answer Only: (Short Explanation based on CompTIA CASP+ documents and resources)
Verified
Reference: (Related URLs AND Make sure Links are working and verified references)

QUESTION 121
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

Correct Answer: B, C
Section:
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
Reference:
https://en.wikipedia.org/wiki/Email_spoofing
https://en.wikipedia.org/wiki/DMARC
https://en.wikipedia.org/wiki/Sender_Policy_Framework

QUESTION 122
During a recent security incident investigation, a security analyst mistakenly turned off the infected machine prior to consulting with a forensic analyst. upon rebooting the machine, a malicious script that was running as a background process was no longer present. As a result, potentially useful evidence was lost. Which of the following should the security analyst have followed?

A. Order of volatility
B. Chain of custody
C. Verification
D. Secure storage

Correct Answer: A
Section:
Explanation:
Order of volatility is a procedure that a computer forensics examiner must follow during evidence collection. It refers to the order in which digital evidence is collected, starting with the most volatile and moving to the least volatile. Volatile data is data that is not permanent and is easily lost, such as data in memory when you turn off a computer. The security analyst should have followed the order of volatility to preserve the most fragile evidence first, such as the malicious script running as a background process, before turning off the infected machine. Verified
Reference:
https://www.computer-forensics-recruiter.com/order-of-volatility/
https://www.sans.org/blog/best-practices-in-digital-evidence-collection/
https://blogs.getcertifiedgetahead.com/order-of-volatility/

QUESTION 123
Some end users of an e-commerce website are reporting a delay when browsing pages. The website uses TLS 1.2. A security architect for the website troubleshoots by connecting from home to the website and capturing tramc via Wire-shark. The security architect finds that the issue is the time required to validate the certificate. Which of the following solutions should the security architect recommend?

A. Adding more nodes to the web server clusters
B. Changing the cipher algorithm used on the web server
C. Implementing OCSP stapling on the server
D. Upgrading to TLS 1.3

Correct Answer: C
Section:
Explanation:
OCSP stapling is a solution that allows the web server to provide a time-stamped OCSP response signed by the CA along with the certificate during the TLS handshake, eliminating the need for the client to contact the CA separately to validate the certificate. OCSP stapling can reduce the delay caused by the certificate validation process by saving a round-trip between the client and the CA. It can also improve the security and privacy of the certificate validation by preventing potential attacks or tracking by malicious third parties. Verified
Reference:
https://en.wikipedia.org/wiki/OCSP_stapling
https://www.digicert.com/knowledgebase/ssl-certificates/ssl-general-topics/what-is-ocsp-stapling.html
https://www.entrust.com/knowledgebase/ssl/online-certificate-status-protocol-ocsp-stapling

QUESTION 124
A pharmaceutical company was recently compromised by ransomware. Given the following EDR output from the process investigation:

Event ID	Device	Process	Classification	Threat type	Action
2142773	cpt-ws002	DearCry.exe	Inconclusive	Create	Allowed
2142755	cpt-ws002	userinit.exe	Inconclusive	Connect	Allowed
2142734	cpt-ws002	NO-AV.exe	Suspicious	Halt process	Allowed
2152118	cpt-ws018	explorer.exe	Inconclusive	Create process	Allowed
2152101	cpt-ws018	powershell.exe	Likely safe	Connect	Allowed
2142696	cpt-ws002	notepad.exe	Likely safe	Process execution	Allowed
2152773	cpt-ws026	DearCry.exe	Malicious	Create	Blocked
2152755	cpt-ws026	userinit.exe	Inconclusive	Connect	Allowed
2152734	cpt-ws026	NO-AV.exe	Suspicious	Halt process	Quarantined
2142685	cpt-ws002	userinit.exe	Malicious	Create process	Blocked
2153855	cpt-ws026	javaw.exe	Likely safe	Connect	Allowed

On which of the following devices and processes did the ransomware originate?

A. cpt-ws018, powershell.exe
B. cpt-ws026, DearCry.exe
C. cpt-ws002, NO-AV.exe
D. cpt-ws026, NO-AV.exe

E. cpt-ws002, DearCry.exe

Correct Answer: D
Section:
Explanation:
The EDR output shows the process tree of the ransomware infection. The root node is NO-AV.exe, which is a malicious executable that disables antivirus software and downloads the DearCry ransomware. The NO-AV.exe process was launched on cpt-ws026 by a user named John. The DearCry.exe process was then launched on cpt-ws026 by NO-AV.exe and propagated to other devices via SMB. Therefore, the ransomware originated from cpt-ws026 and NO-AV.exe. Verified
Reference:
https://www.microsoft.com/security/blog/2021/03/12/analyzing-dearcry-ransomware-the-first-attack-to-exploit-exchange-server-vulnerabilities/
https://www.crowdstrike.com/blog/dearcry-ransomware-analysis/

QUESTION 125
A security architect is tasked with securing a new cloud-based videoconferencing and collaboration platform to support a new distributed workforce. The security architect's key objectives are to:
* Maintain customer trust
* Minimize data leakage
* Ensure non-repudiation
Which of the following would be the BEST set of recommendations from the security architect?

A. Enable the user authentication requirement, enable end-to-end encryption, and enable waiting rooms.
B. Disable file exchange, enable watermarking, and enable the user authentication requirement.
C. Enable end-to-end encryption, disable video recording, and disable file exchange.
D. Enable watermarking, enable the user authentication requirement, and disable video recording.

Correct Answer: B
Section:
Explanation:
Disabling file exchange can help to minimize data leakage by preventing users from sharing sensitive documents or data through the videoconferencing platform. Enabling watermarking can help to maintain customer trust and ensure non-repudiation by adding a visible or invisible mark to the video stream that identifies the source or owner of the content. Enabling the user authentication requirement can help to secure the videoconferencing sessions by verifying the identity of the participants and preventing unauthorized access. Verified
Reference:
https://www.rev.com/blog/marketing/follow-these-7-video-conferencing-security-best-practices
https://www.paloaltonetworks.com/blog/2020/04/network-video-conferencing-security/
https://www.megameeting.com/news/best-practices-secure-video-conferencing/

QUESTION 126
A security consultant has been asked to identify a simple, secure solution for a small business with a single access point. The solution should have a single SSID and no guest access. The customer facility is located in a crowded area of town, so there is a high likelihood that several people will come into range every day. The customer has asked that the solution require low administrative overhead and be resistant to offline password attacks. Which of the following should the security consultant recommend?

A. WPA2-Preshared Key
B. WPA3-Enterprise
C. WPA3-Personal
D. WPA2-Enterprise

Correct Answer: C
Section:
Explanation:

WPA3-Personal is a simple, secure solution for a small business with a single access point. It uses a new security protocol called Simultaneous Authentication of Equals (SAE), which replaces the Pre-Shared Key (PSK) exchange with a more secure way to do initial key exchange. SAE also provides forward secrecy, which means that even if the password is compromised, the attacker cannot decrypt past or future data. WPA3-Personal also uses AES-128 in CCM mode as the minimum encryption algorithm, which is resistant to offline password attacks. WPA3-Personal requires low administrative overhead and supports a single SSID with no guest access. Verified Reference:
https://www.diffen.com/difference/WPA2_vs_WPA3
https://www.thewindowsclub.com/wpa3-personal-enterprise-wi-fi-encryption
https://www.teldat.com/blog/wpa3-wi-fi-network-security-wpa3-personal-wpa3-enterprise/

QUESTION 127
A network administrator who manages a Linux web server notices the following traffic:
http://corr.ptia.org/.../.../.../... /etc./shadow
Which of the following Is the BEST action for the network administrator to take to defend against this type of web attack?

A. Validate the server certificate and trust chain.
B. Validate the server input and append the input to the base directory path.
C. Validate that the server is not deployed with default account credentials.
D. Validate that multifactor authentication is enabled on the server for all user accounts.

Correct Answer: B
Section:
Explanation:
The network administrator is noticing a web attack that attempts to access the /etc/shadow file on a Linux web server. The /etc/shadow file contains the encrypted passwords of all users on the system and is a common target for attackers. The attack uses a technique called directory traversal, which exploits a vulnerability in the web application that allows an attacker to access files or directories outside of the intended scope by manipulating the file path.
Validating the server input and appending the input to the base directory path would be the best action for the network administrator to take to defend against this type of web attack, because it would:
Check the user input for any errors, malicious data, or unexpected values before processing it by the web application.
Prevent directory traversal by ensuring that the user input is always relative to the base directory path of the web application, and not absolute to the root directory of the web server.
Deny access to any files or directories that are not part of the web application's scope or functionality.

QUESTION 128
In comparison with traditional on-premises infrastructure configurations, defining ACLs in a CSP relies on:

A. cloud-native applications.
B. containerization.
C. serverless configurations.
D. software-defined netWorking.
E. secure access service edge.

Correct Answer: D
Section:
Explanation:
Defining ACLs in a CSP relies on software-defined networking. Software-defined networking (SDN) is a network architecture that decouples the control plane from the data plane, allowing for centralized and programmable network management. SDN can enable dynamic and flexible network configuration and optimization, as well as improved security and performance. In a CSP, SDN can be used to define ACLs that can apply to virtual networks, subnets, or interfaces, regardless of the physical infrastructure. SDN can also allow for granular and consistent ACL enforcement across different cloud services and regions. Verified
Reference:
https://www.techtarget.com/searchsdn/definition/software-defined-networking-SDN
https://learn.microsoft.com/en-us/azure/architecture/guide/networking/network-security
https://www.techtarget.com/searchcloudcomputing/definition/cloud-networking

QUESTION 129
A systems administrator at a web-hosting provider has been tasked with renewing the public certificates of all customer sites. Which of the following would BEST support multiple domain names while minimizing the amount of certificates needed?

A. ocsp
B. CRL
C. SAN
D. CA

Correct Answer: C
Section:
Explanation:
The administrator should use SAN certificates to support multiple domain names while minimizing the amount of certificates needed. SAN stands for Subject Alternative Name, which is an extension of a certificate that allows it to include multiple fully-qualified domain names (FQDNs) within the same certificate. For example, a SAN certificate can secure www.example.com, www.example.net, and mail.example.org with one certificate. SAN certificates can reduce the cost and complexity of managing multiple certificates for different domains. SAN certificates can also support wildcard domains, such as *.example.com, which can cover any subdomain under that domain. Verified Reference:
https://www.techtarget.com/searchsecurity/definition/Subject-Alternative-Name
https://www.techtarget.com/searchsecurity/definition/wildcard-certificate
https://www.nexcess.net/help/what-is-a-multi-domain-ssl-certificate/

QUESTION 130
A new, online file hosting service is being offered. The service has the following security requirements:
• Threats to customer data integrity and availability should be remediated first.
• The environment should be dynamic to match increasing customer demands.
• The solution should not interfere with customers" ability to access their data at anytime.
• Security analysts should focus on high-risk items.
Which of the following would BEST satisfy the requirements?

A. Expanding the use of IPS and NGFW devices throughout the environment
B. Increasing the number of analysts to Identify risks that need remediation
C. Implementing a SOAR solution to address known threats
D. Integrating enterprise threat feeds in the existing SIEM

Correct Answer: C
Section:
Explanation:
A SOAR (Security Orchestration, Automation, and Response) solution is a software platform that can automate the detection and response of known threats, such as ransomware, phishing, or denial-ofservice attacks. A SOAR solution can also integrate with other security tools, such as IPS, NGFW,
SIEM, and threat feeds, to provide a comprehensive and dynamic security posture. A SOAR solution would best satisfy the requirements of the online file hosting service, because it would:
Remediate threats to customer data integrity and availability first, by automatically applying predefined actions or workflows based on the severity and type of the threat.
Allow the environment to be dynamic to match increasing customer demands, by scaling up or down the security resources and processes as needed.
Not interfere with customers' ability to access their data at anytime, by minimizing the human intervention and downtime required for threat response.
Enable security analysts to focus on high-risk items, by reducing the manual tasks and alert fatigue associated with threat detection and response.
Reference: CASP+ (Plus) CompTIA Advanced Security Practitioner Certification …

QUESTION 131
A security consultant has been asked to recommend a secure network design that would:
• Permit an existing OPC server to communicate with a new Modbus server that is controlling electrical relays.
• Limit operational disruptions.

Due to the limitations within the Modbus protocol, which of the following configurations should the security engineer recommend as part of the solution?

A. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 135.
B. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 102.
C. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 5000.
D. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502.

Correct Answer: D
Section:
Explanation:
OPC (Open Platform Communications) and Modbus are two common protocols used for industrial control systems (ICS). OPC is a standard that allows different devices and applications to exchange data in a vendor-neutral way. Modbus is a serial communication protocol that enables devices to send and receive commands and data over a network. Modbus has two variants: Modbus TCP/IP, which uses TCP port 502 for communication, and Modbus RTU/ASCII, which uses serial ports.
To allow an OPC server to communicate with a Modbus server that is controlling electrical relays, the security engineer should recommend restricting inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502. This configuration would:
Permit the OPC server to send commands and data to the Modbus server using Modbus TCP/IP protocol over port 502.
Limit operational disruptions, by preventing unauthorized or malicious access to the Modbus server from other sources.
Due to the limitations within the Modbus protocol, such as lack of encryption and authentication, restricting inbound traffic is a necessary security measure to protect the integrity and availability of the ICS.
Reference: CASP+ (Plus) Certification Training | CompTIA IT Certifications

QUESTION 132
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.

Correct Answer: C
Section:
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.

QUESTION 133
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

Correct Answer: A
Section:
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.

QUESTION 134
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 Tool. *
B. www\. malicious\. com\/malicious. php
C. POST /malicious\. php
D. Hose: [a-2] *\.malicious\.com
E. malicious. *

Correct Answer: D
Section:
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-andcontrol 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.

QUESTION 135
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.

Correct Answer: C
Section:
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-themiddle (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).

QUESTION 136
A security architect for a large, multinational manufacturer needs to design and implement a security solution to monitor traffic.
When designing the solution, which of the following threats should the security architect focus on to prevent attacks against the network?

A. Packets that are the wrong size or length
B. Use of any non-DNP3 communication on a DNP3 port
C. Multiple solicited responses over time
D. Application of an unsupported encryption algorithm

Correct Answer: C
Section:

QUESTION 137
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

Correct Answer: A
Section:

QUESTION 138
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

Correct Answer: A
Section:
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. Reference: [CompTIA Advanced Security
Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.1: Apply cryptographic techniques

QUESTION 139
A DevOps team has deployed databases, event-driven services, and an API gateway as PaaS solution that will support a new billing system. Which of the following security responsibilities will the DevOps team need to perform?

A. Securely configure the authentication mechanisms
B. Patch the infrastructure at the operating system
C. Execute port scanning against the services
D. Upgrade the service as part of life-cycle management

Correct Answer: A
Section:

QUESTION 140
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

Correct Answer: A, C
Section:

QUESTION 141
Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage. Which of the following should be created to prevent this type of issue in the future?

A. SLA
B. BIA
C. BCM
D. BCP
E. RTO

Correct Answer: D
Section:
Explanation:
A Business Continuity Plan (BCP) is a set of policies and procedures that outline how an organization should respond to and recover from disruptions[1]. It is designed to ensure that critical operations and services can be quickly restored and maintained, and should include steps to identify risks, develop plans to mitigate those risks, and detail the procedures to be followed in the event of a disruption. Resources:
CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 4: ''Business Continuity Planning,'' Wiley, 2018.https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition-p-9781119396582

QUESTION 142
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:

```
(&(objectClass=*)(objectClass=*))(&(objectClass=void)(type=admin))
```

Which of the following would BEST mitigate this vulnerability?

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

Correct Answer: C
Section:

QUESTION 143
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

Correct Answer: A, C
Section:

QUESTION 144
A company Is adopting a new artificial-intelligence-based analytics SaaS solution. This Is the company's first attempt at using a SaaS solution, and a security architect has been asked to determine any future risks. Which of the following would be the GREATEST risk In adopting this solution?

A. The inability to assign access controls to comply with company policy
B. The inability to require the service provider process data in a specific country
C. The inability to obtain company data when migrating to another service
D. The inability to conduct security assessments against a service provider

Correct Answer: C
Section:

QUESTION 145
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

Correct Answer: B
Section:

QUESTION 146
A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability. Which of the following would BEST resolve and mitigate the issue? (Select TWO).

A. Deploying a WAF signature
B. Fixing the PHP code
C. Changing the web server from HTTPS to HTTP
D. UsingSSLv3
E. Changing the code from PHP to ColdFusion
F. Updating the OpenSSL library

Correct Answer: A, F
Section:
Explanation:

B) Fixing the PHP code is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not in the PHP code, but in the OpenSSL library that handles the SSL/TLS encryption for the web server.
C) Changing the web server from HTTPS to HTTP is not a way to resolve or mitigate the Heartbleed vulnerability, because it would expose all the web traffic to eavesdropping and tampering by attackers. HTTPS provides confidentiality, integrity, and authentication for web communications, and should not be disabled for security reasons.
D) Using SSLv3 is not a way to resolve or mitigate the Heartbleed vulnerability, because SSLv3 is an outdated and insecure protocol that has been deprecated and replaced by TLS. SSLv3 does not support modern cipher suites, encryption algorithms, or security features, and is vulnerable to various attacks, such as POODLE.
E) Changing the code from PHP to ColdFusion is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not related to the programming language of the web application, but to the OpenSSL library that handles the SSL/TLS encryption for the web server. https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug https://heartbleed.com/
Deploying a web application firewall (WAF) signature is a way to detect and block attempts to exploit the Heartbleed vulnerability on the web server. A WAF signature is a pattern that matches a known attack vector, such as a malicious heartbeat request. By deploying a WAF signature, the company can protect its web application from Heartbleed attacks until the underlying vulnerability is fixed.
Updating the OpenSSL library is the ultimate way to fix and mitigate the Heartbleed vulnerability. The OpenSSL project released version 1.0.1g on April 7, 2014, which patched the bug by adding a bounds check to the heartbeat function. By updating the OpenSSL library on the web server, the company can eliminate the vulnerability and prevent any future exploitation.

QUESTION 147
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.

Correct Answer: B
Section:
Explanation:

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
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.

QUESTION 148

A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

* The PostgreSQL server must only allow connectivity in the 10.1.2.0/24

subnet.

* The SSH daemon on the database server must be configured to listen

to port 4022.

* The SSH daemon must only accept connections from a Single

workstation.

* All host-based firewalls must be disabled on all workstations.

* All devices must have the latest updates from within the past eight

days.

* All HDDs must be configured to secure data at rest.

* Cleartext services are not allowed.

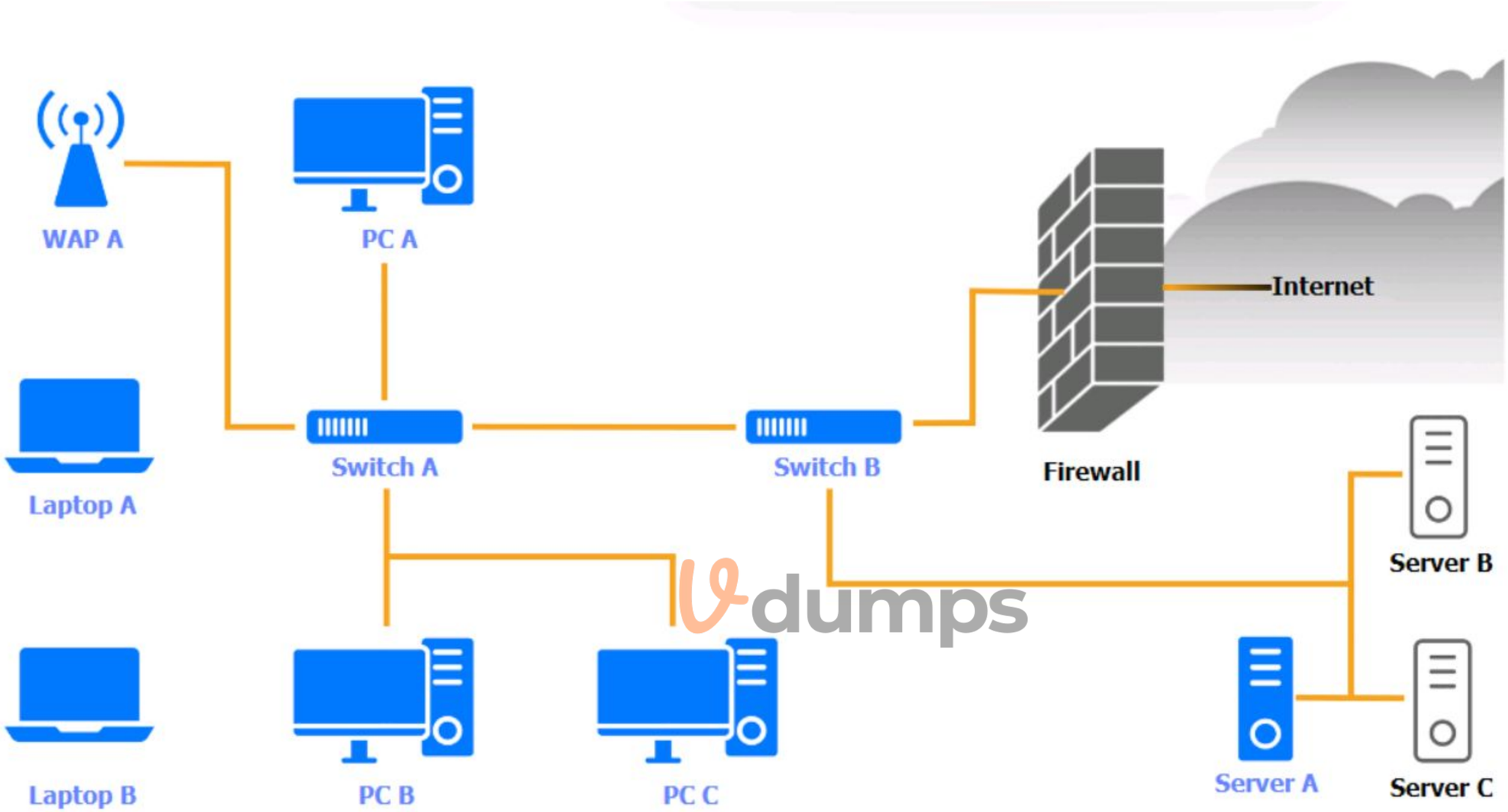
* All devices must be hardened when possible.

Instructions:

Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.

Click on Server A to review output dat

a. Select commands in the appropriate tab to remediate connectivity problems to the pOSTGREsql DATABASE VIA ssh



WAP A

WAP A

Finding	Status	Remediation
Firmware	Updated 5 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
SSID broadcast	Disabled	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ Enable port security on network device
		☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

PC A

PC A

OS updates	Updated 2 days ago, last checked 5:08 a.m.
Endpoint protection	Last checked 6:11 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Normal
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Disabled

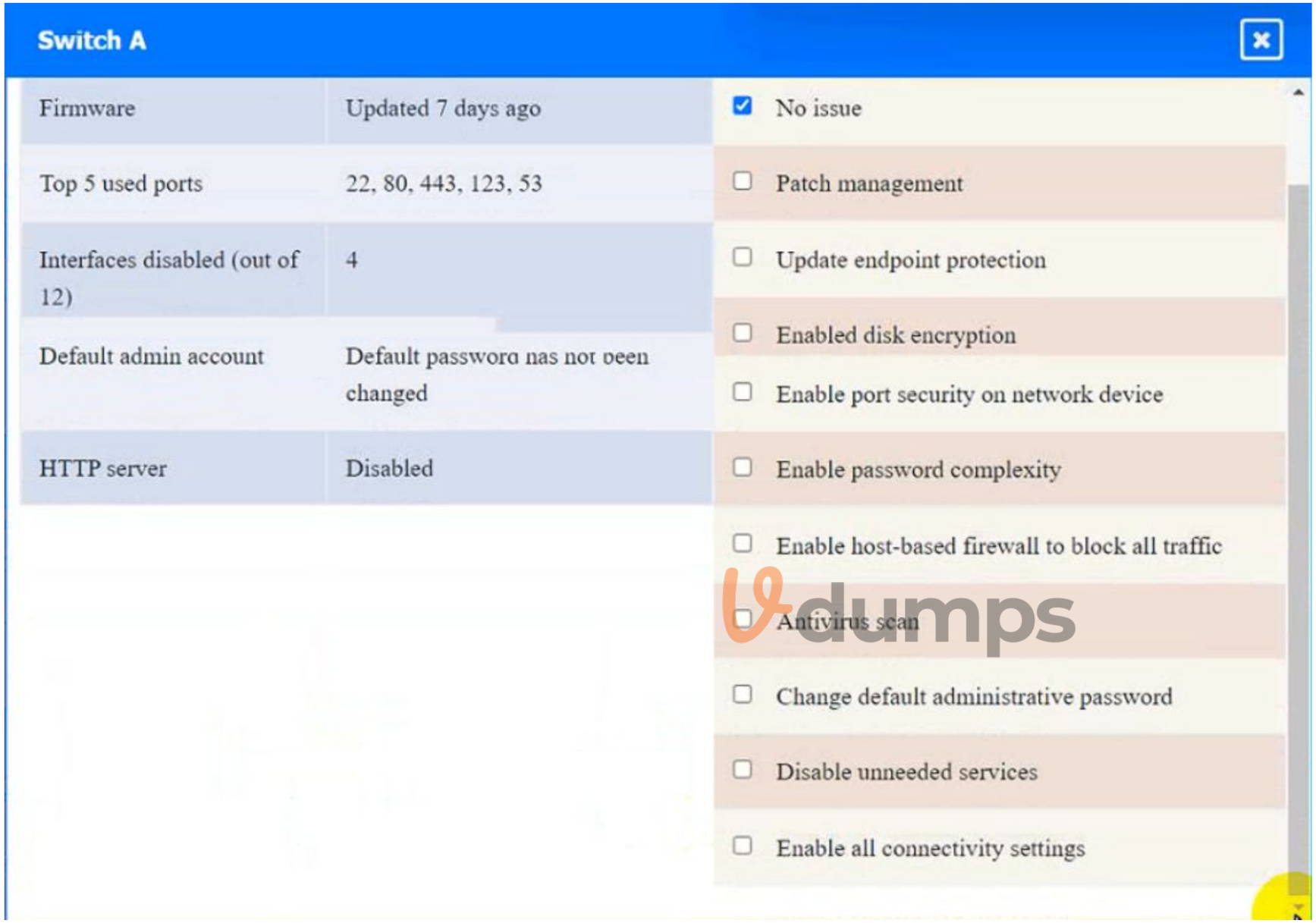
- [x] No issue
- [ ] Patch management
- [ ] Update endpoint protection
- [ ] Enabled disk encryption
- [ ] Enable port security on network device
- [ ] Enable password complexity
- [ ] Enable host-based firewall to block all traffic
- [ ] Antivirus scan
- [ ] Change default administrative password
- [ ] Disable unneeded services
- [ ] Enable all connectivity settings

Laptop A

Laptop A

OS updates	Updated 3 days ago, last checked 6:08 a.m.	☑	No issue
Endpoint protection	Last checked in 6:13 a.m.	☐	Patch management
Browser version	91.2.5 (7/31/2023)	☐	Update endpoint protection
Disk encryption	Enabled	☐	Enabled disk encryption
Password complexity	Enabled	☐	Enable port security on network device
Host-based firewall	Disabled	☐	Enable password complexity
CPU & memory usage	Medium	☐	Enable host-based firewall to block all traffic
		☐	Antivirus scan
Screensaver	Enabled	☐	Change default administrative password
Top 5 used ports	22, 80, 443, 389, 53	☐	Disable unneeded services
Wireless	Enabled	☐	Enable all connectivity settings

Switch A


Switch A
Firmware
Updated 7 days ago
No issue
Top 5 used ports
22, 80, 443, 123, 53
Patch management
Interfaces disabled (out of 12)
4
Update endpoint protection
Enabled disk encryption
Default admin account
Default password has not been changed
Enable port security on network device
HTTP server
Disabled
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

Switch B:

Switch B

Firmware	Updated 7 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 6)	1	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ Enable port security on network device
		☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

Laptop B

Laptop B

OS updates	Updated 3 days ago, last checked 8:08 a.m.
Endpoint protection	Last checked in 8:11 a.m.
Browser version	81.2.5 (7/31/2023)
Disk encryption	Disabled
Password Complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Normal
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 8080, 53
Wireless	Enabled

- [x] No issue
- [ ] Patch management
- [ ] Update endpoint protection
- [ ] Enabled disk encryption
- [ ] Enable port security on network device
- [ ] Enable password complexity
- [ ] Enable host-based firewall to block all traffic
- [ ] Antivirus scan
- [ ] Change default administrative password
- [ ] Disable unneeded services
- [ ] Enable all connectivity settings

PC B

PC B

OS updates	Updated 2 days ago, last checked 5:10 a.m.
Endpoint protection	Last checked in 6:13 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Medium
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Disabled

- [x] No issue
- [ ] Patch management
- [ ] Update endpoint protection
- [ ] Enabled disk encryption
- [ ] Enable port security on network device
- [ ] Enable password complexity
- [ ] Enable host-based firewall to block all traffic
- [ ] Antivirus scan
- [ ] Change default administrative password
- [ ] Disable unneeded services
- [ ] Enable all connectivity settings

PC C

PC C

OS updates	Updated 22 days ago	☑ No issue
Endpoint protection	Last checked 6:19 a.m.	☐ Patch management
Browser version	91.2.5 (7/18/2022)	☐ Update endpoint protection
Disk encryption	Enabled	☐ Enabled disk encryption
Password complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	High	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 23, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

Server A

Server A

Nmap | IP Tables

```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT            STATE   SERVICE         VERSION
22/tcp          open    ssh             OpenSSH 8.4
80/tcp          closed  http
443/tcp         closed  ssl/http
1433/tcp        closed  mssql
5432/tcp        closed  postgresql
...
```

1 | 2 | 3 | 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 | 2 | 3 | 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

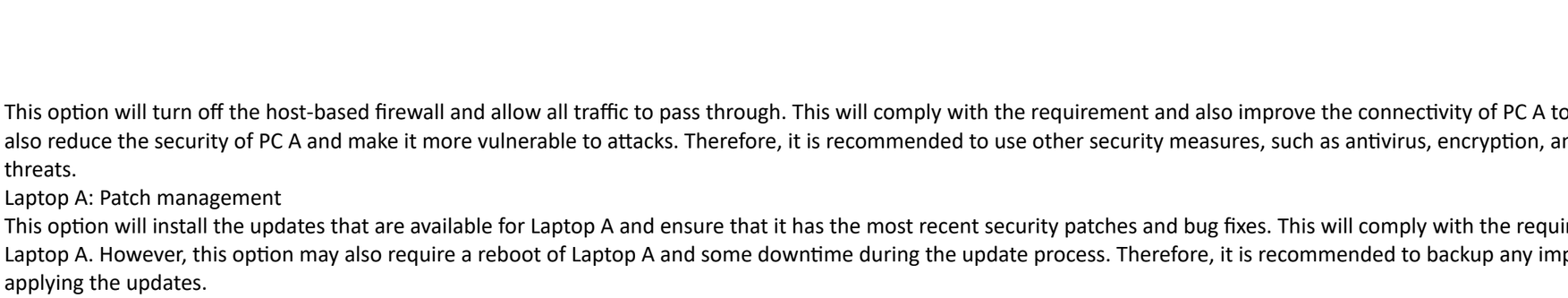
Nmap | IP Tables

```
#iptables --list --verbose

Chain INPUT (policy DROP 5 packets, 341 bytes)

pkts bytes  target  prot  opt in  out source    destination

0    0      ACCEPT  tcp   --  any any anywhere  anywhere    tcp spts:login:65535 dpt:ssh state NEW,ESTABLISHED

1   28      DROP    all   --  any any anywhere  anywhere


Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

A. See the Explanation below for the solution.

Correct Answer: A
Section:
Explanation:
WAP A: No issue found. The WAP A is configured correctly and meets the requirements.
PC A = Enable host-based firewall to block all traffic

This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.
Laptop A: Patch management
This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.
Switch A: No issue found. The Switch A is configured correctly and meets the requirements.
Switch B: No issue found. The Switch B is configured correctly and meets the requirements.
Laptop B: Disable unneeded services
This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore, it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.
PC B:Enable disk encryption
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B's data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.
PC C: Disable unneeded services
This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is the default and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:
sudo nano /etc/ssh/sshd_config
Server A. Need to select the following:



QUESTION 149
The Chief Information Security Officer is concerned about the possibility of employees downloading 'malicious files from the internet and 'opening them on corporate workstations. Which of the following solutions would be BEST to reduce this risk?

A. Integrate the web proxy with threat intelligence feeds.
B. Scan all downloads using an antivirus engine on the web proxy.
C. Block known malware sites on the web proxy.
D. Execute the files in the sandbox on the web proxy.

Correct Answer: D
Section:
Explanation:
Executing the files in the sandbox on the web proxy is the best solution to reduce the risk of employees downloading and opening malicious files from the internet. A sandbox is a secure and isolated environment that can run untrusted or potentially harmful code without affecting the rest of the system. By executing the files in the sandbox, the web proxy can analyze their behavior and detect any malicious activity before allowing them to reach

the corporate workstations.

QUESTION 150
An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.
Which of the following side-channel attacks did the team use?

A. Differential power analysis
B. Differential fault analysis
C. Differential temperature analysis
D. Differential timing analysis

Correct Answer: B
Section:
Explanation:
'Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults---unexpected environmental conditions---into cryptographic operations, to reveal their internal states.'

QUESTION 151
A SaaS startup is maturing its DevSecOps program and wants to identify weaknesses earlier in the development process in order to reduce the average time to identify serverless application vulnerabilities and the costs associated with remediation The startup began its early security testing efforts with DAST to cover public-facing application components and recently implemented a bug bounty program Which of the following will BEST accomplish the company's objectives?

A. RASP
B. SAST
C. WAF
D. CMS

Correct Answer: B
Section:
Explanation:
Static application security testing (SAST) is a method of analyzing the source code of an application for vulnerabilities and weaknesses before it is deployed. SAST can help identify security issues earlier in the development process, reducing the time and cost of remediation. Dynamic application security testing (DAST) is a method of testing the functionality and behavior of an application at runtime for vulnerabilities and weaknesses. DAST can cover public-facing application components, but it cannot detect issues in the source code or in serverless applications. Runtime application self-protection (RASP) is a technology that monitors and protects an application from attacks in real time by
embedding security features into the application code or runtime environment. RASP can help prevent exploitation of vulnerabilities, but it cannot identify or fix them. 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 protect an application from common attacks, but it cannot detect or fix vulnerabilities in the application code or in serverless applications. Reference: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 3: Enterprise Security Operations, Objective 3.4: Conduct security assessments using appropriate tools

QUESTION 152
A software development company wants to ensure that users can confirm the software is legitimate when installing it. Which of the following is the best way for the company to achieve this security objective?

A. Code signing
B. Non-repudiation
C. Key escrow
D. Private keys

Correct Answer: A
Section:

Explanation:
Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed. This provides users with the assurance that the software is legitimate and safe to install.

QUESTION 153
After installing an unapproved application on a personal device, a Chief Executive Officer reported an incident to a security analyst. This device is not controlled by the MDM solution, as stated in the BYOD policy. However, the device contained critical confidential information. The cyber incident response team performed the analysis on the device and found the following log:

```
Wed 12 Dec 2020 10:00:03 Unknown sources is now enabled on this device.
```

Which of the following is the most likely reason for the successful attack?

A. Lack of MDM controls
B. Auto-join hotspots enabled
C. Sideloading
D. Lack of application segmentation

Correct Answer: A
Section:
Explanation:
A lack of Mobile Device Management (MDM) controls can lead to successful attacks because MDM solutions provide the ability to enforce security policies, remotely wipe sensitive data, and manage software updates, which can prevent unauthorized access and protect corporate data. Without MDM, personal devices are more vulnerable to security risks.

QUESTION 154
A security administrator wants to enable a feature that would prevent a compromised encryption key from being used to decrypt all the VPN traffic. Which of the following should the security administrator use?

A. Salsa20 cipher
B. TLS-based VPN
C. PKI-based IKE IPSec negotiation
D. Perfect forward secrecy

Correct Answer: D
Section:
Explanation:
Perfect Forward Secrecy (PFS) is a feature of certain key agreement protocols that ensures a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. In the context of a VPN, PFS ensures that each session has a unique encryption key, and even if a key is compromised, it will not compromise past or future VPN sessions.