CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
A security analyst was transferred to an organization's threat-hunting team to track specific activity throughout the enterprise environment The analyst must observe and assess the number ot times this activity occurs and aggregate the results. Which of the following is the BEST threat-hunting method for the analyst to use?

A. Stack counting
B. Searching
C. Clustering
D. Grouping

Answer: A

Explanation:
Stack counting is the best threat-hunting method for the analyst to use to observe and assess the number of times a specific activity occurs and aggregate the results. Stack counting is a technique that involves collecting data from multiple sources, such as logs, events, or alerts, and grouping them by a common attribute, such as an IP address, a user name, or a process name. Stack counting can help identify patterns, trends, outliers, or anomalies in the data that may indicate malicious activity or compromise.

NEW QUESTION 2
A computer hardware manufacturer developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?

A. Encryption
B. eFuse
C. Secure Enclave
D. Trusted execution

Answer: B

Explanation:
An eFuse, or electronic fuse, is a microscopic fuse put into a computer chip that can be blown by applying a high voltage or current. Once blown, an eFuse cannot be reset or repaired, and its state can be read by software or hardware2
An eFuse can be used by a hardware manufacturer to prevent firmware downgrades on a
system-on-chip (SoC) that will be used by mobile devices. An eFuse can store information such as the firmware version, security level, or device configuration on the chip. When a newer firmware is installed, an eFuse can be blown to indicate the update and prevent reverting to an older firmware. This can help protect the device from security vulnerabilities, compatibility issues, or unauthorized modifications.

NEW QUESTION 3
A security analyst is reviewing a new Internet portal that will be used for corporate employees to obtain their pay statements. Corporate policy classifies pay statement information as confidential, and it must be protected by MFA. Which of the following would best fulfill the MFA requirement while keeping the portal accessible from the internet?

A. Obtaining home public IP addresses of corporate employees to implement source IP restrictions and requiring a username and password
B. Requiring the internet portal to be accessible from only the corporate SSO internet endpoint and requiring a smart card and PIN
C. Moving the internet portal server to a DMZ that is only accessible from the corporate VPN and requiring a username and password
D. Distributing a shared password that must be provided before the internet portal loads and requiring a username and password

Answer: B

Explanation:
Requiring the internet portal to be accessible from only the corporate SSO internet endpoint and requiring a smart card and PIN. This option provides the best MFA requirement because it uses two factors of authentication: something you have (smart card) and something you know (PIN). It also restricts access to the portal from a trusted source (corporate SSO internet endpoint).

NEW QUESTION 4
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.
B. The disclosure section should contain the organization's legal and regulatory requirements regardingdisclosures.
C. The disclosure section should include the names and contact information of key employees who are needed for incident resolution
D. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening m the future.

Answer: B

Explanation:
The disclosure section of an organization’s incident response plan should cover how the organization handles public or private disclosures of an incident. The disclosure section should contain the organization’s legal and regulatory requirements regarding disclosures, such as the type, content, format, timing, and recipients of the disclosures. The disclosure section should also specify the roles and responsibilities of the personnel involved in the disclosure process, such as who is authorized to make or approve disclosures, who is responsible for communicating with internal and external stakeholders, and who is accountable for ensuring compliance with the disclosure requirements. The disclosure section should not focus on how to reduce the likelihood customers will leave due to the incident (A), as this is a business objective rather than a disclosure requirement. The disclosure section should not include the names and contact information of key employees who are needed for incident resolution ©, as this is an operational detail rather than a disclosure requirement. The disclosure section should not contain language explaining how the organization will reduce the likelihood of the incident from happening in the future (D), as this is a remediation action rather than a disclosure requirement.

NEW QUESTION 5

Which of the following data exfiltration discoveries would most likely require communicating a breach to regulatory agencies?

A. CRM data
B. PHI files
C. SIEM logs
D. UEBA metrics

Answer: B

Explanation:
PHI stands for protected health information, which is any information that relates to the health or health care of an individual and can be used to identify that person. PHI is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which sets national standards for the privacy and security of health information. HIPAA requires covered entities, such as health care providers, health plans, and health care clearinghouses, to notify individuals and regulatory agencies of any breach of unsecured PHI. A breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI that compromises the privacy or security of the information

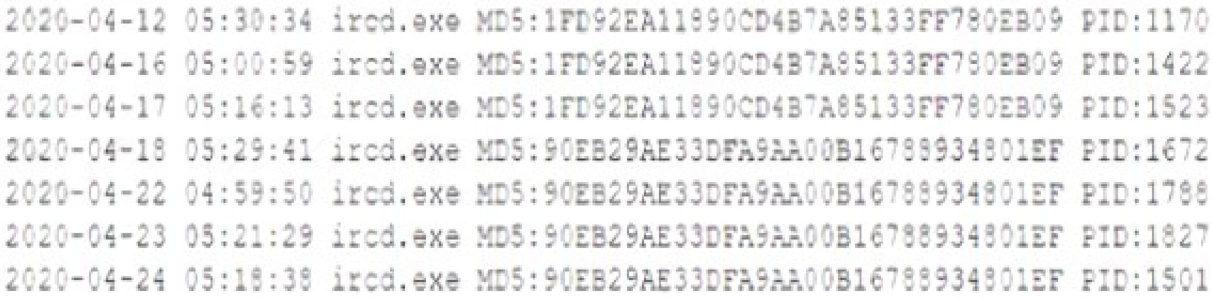
NEW QUESTION 6
As part of the senior leadership team's ongoing nsk management activities the Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones The management team wants to examine a new business process that would use existing infrastructure to process and store sensitive data Which of the following would be appropnate for the security analyst to coordinate?

A. A black-box penetration testing engagement
B. A tabletop exercise
C. Threat modeling
D. A business impact analysis

Answer: C

Explanation:
Threat modeling is a process that helps identify and analyze the potential threats and vulnerabilities of a system or process. It can help evaluate the security risks and mitigation strategies of a new business process that would use existing infrastructure to process and store sensitive data. A black-box penetration testing engagement, a tabletop exercise, or a business impact analysis are other methods that can be used to assess the security or resilience of a system or process, but they are not as appropriate as threat modeling for coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones. Reference: https://owasp.org/www-community/Application_Threat_Modeling

NEW QUESTION 7
During a routine review of service restarts a security analyst observes the following in a server log:



```
2020-04-12 05:30:34 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1170
2020-04-16 05:00:59 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1422
2020-04-17 05:16:13 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1523
2020-04-18 05:29:41 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1672
2020-04-22 04:59:50 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1788
2020-04-23 05:21:29 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1827
2020-04-24 05:18:38 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1501
```

Which of the following is the GREATEST security concern?

A. The daemon's binary was AChanged
B. Four consecutive days of monitoring are skipped in the tog
C. The process identifiers for the running service change
D. The PIDs are continuously changing

Answer: A

Explanation:
A daemon is a program that runs in the background on a system and performs certain tasks or services without user intervention. A daemon's binary is the executable file that contains the code and instructions for the daemon to run. The server log shows that the daemon's binary was changed on Aug 1 2020 at 00:00:01 by an unknown user with UID 0 (root). This is the greatest security concern, because it could indicate that an attacker has gained root access to the system and modified the daemon's binary with malicious code that could compromise the system's security or functionality. Four consecutive days of monitoring being skipped in the log, the process identifiers for the running service changing, or the PIDs continuously changing are not security concerns, but rather normal events that could occur due to system maintenance, updates, restarts, or scheduling. Reference: https://www.linux.com/training-tutorials/what-are-linux-daemons/

NEW QUESTION 8
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

A. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.
B. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.
C. Unsupervised algorithms are not suitable for IDS systems, white supervised algorithms are
D. Unsupervised algorithms produce more false positive
E. Than supervised algorithms.

Answer: B

Explanation:
Supervised and unsupervised machine-learning algorithms are two types of machine-learning methods that are used in cybersecurity applications. Machine learning is a branch of artificial intelligence that enables systems to learn from data and improve their performance without explicit programming.

Supervised machine-learning algorithms are trained on labeled data, which means that each data point has a known outcome or class. Supervised algorithms learn to map input data to output data by finding patterns or rules from the training data. Supervised algorithms require security analyst feedback to provide labels for the data and evaluate the accuracy of the algorithm's predictions. Examples of supervised machine-learning algorithms are classification and regression. Unsupervised machine-learning algorithms are trained on unlabeled data, which means that each data point has no known outcome or class. Unsupervised algorithms learn to discover hidden structures or patterns from the data without any guidance or feedback. Unsupervised algorithms do not require security analyst feedback, as they do not rely on predefined labels or outcomes. Examples of unsupervised machine-learning algorithms are clustering and anomaly detection.

NEW QUESTION 9
An organization discovers motherboards within the environment that appear to have been physically altered during the manufacturing process. Which of the following is the BEST course of action to mitigate the risk of this reoccurring?

A. Perform an assessment of the firmware to determine any malicious modifications.
B. Conduct a trade study to determine if the additional risk constitutes further action.
C. Coordinate a supply chain assessment to ensure hardware authenticity.
D. Work with IT to replace the devices with the known-altered motherboards.

Answer: C

Explanation:
A supply chain assessment is a process that evaluates the security and integrity of the suppliers and vendors that provide hardware or software to an organization. It can help identify and mitigate the risk of tampered or counterfeit products that could compromise the organization's security or performance. Coordinating a supply chain assessment to ensure hardware authenticity is the best course of action to mitigate the risk of motherboards that have been physically altered during the manufacturing process. Performing an assessment of the firmware, conducting a trade study, or working with IT to replace the devices are other possible actions, but they are not as effective or proactive as coordinating a supply chain assessment. Reference:
https://www.nist.gov/system/files/documents/2017/04/28/sp800-161.pdf

NEW QUESTION 10
An analyst is performing a BIA and needs to consider measures and metrics. Which of the following would help the analyst achieve this objective? (Select two).

A. Time to reimage the server
B. Minimum data backup volume
C. Disaster recovery plan for non-critical services
D. Maximum downtime before impact is unacceptable
E. Time required to inform stakeholders about outage
F. Total time accepted for business process outage

Answer: DF

Explanation:
The objective of a BIA is to determine the potential impacts of various disruptions on the business processes and functions, and to establish the recovery priorities and objectives for each process and function. To achieve this objective, the analyst needs to consider various measures and metrics that can quantify the impacts and the recovery requirements. Some of the common measures and metrics that are used in a BIA are:

- Maximum downtime before impact is unacceptable: This metric defines the maximum amount of time that a business process or function can be disrupted without causing significant or irreversible damage to the organization's reputation, operations, finances, or legal obligations. This metric is also known as the maximum tolerable downtime (MTD) or maximum tolerable period of disruption (MTPD). It helps to determine the recovery time objective (RTO), which is the target time for restoring the process or function to an acceptable level of service after a disruption1.
- Total time accepted for business process outage: This metric defines the total amount of time that a business process or function can be out of service within a given period, such as a day, a week, or a month. This metric is also known as the recovery point objective (RPO), which is the maximum amount of data loss or corruption that can be tolerated after a disruption1. It helps to determine the backup frequency and retention policy for the data and systems that support the process or function.
- Time required to inform stakeholders about outage: This metric defines the time frame for communicating with the internal and external stakeholders who are affected by or involved in the disruption and recovery of a business process or function. This metric helps to establish the crisis communication plan and protocol, which specifies who, what, when, where, why, and how to communicate during and after a disruption2. It also helps to manage the expectations and perceptions of the stakeholders and to maintain their trust and confidence in the organization.
- Time to reimage the server: This metric defines the time needed to restore a server to its original or desired state after a disruption. This metric helps to estimate the resources and efforts required for recovering the server and its applications. It also helps to evaluate the feasibility and effectiveness of different recovery strategies, such as restoring from backup, rebuilding from scratch, or replacing with a spare3.
- Minimum data backup volume: This metric defines the minimum amount of data that needs to be backed up regularly to ensure the continuity and integrity of a business process or function. This metric helps to optimize the backup process and reduce the storage costs and bandwidth consumption. It also helps to identify the critical data elements and sources that are essential for the process or function4.

NEW QUESTION 11
Which of the following is a reason for correctly identifying APTs that might be targeting an organization?

A. APTs' passion for social justice will make them ongoing and motivated attackers.
B. APTs utilize methods and technologies differently than other threats
C. APTs are primarily focused on financial gam and are widely available over the internet.
D. APTs lack sophisticated methods, but their dedication makes them persistent.

Answer: B

Explanation:
APTs utilize methods and technologies differently than other threats. APTs stand for Advanced Persistent Threats, and they are sophisticated and stealthy attacks that target specific organizations or networks over a long period of time, often with political or financial motives. APTs utilize methods and technologies differently than other threats, such as using custom-made malware, exploiting zero-day vulnerabilities, leveraging social engineering techniques, or employing multiple vectors of attack. APTs can also evade detection by existing security tools or controls, by using encryption, obfuscation, proxy servers, or other techniques to hide their activities or communications.

NEW QUESTION 12
A Chief Information Security Officer has asked for a list of hosts that have critical and high-severity findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?

A. Nessus
B. Nikto
C. Fuzzer
D. Wireshark
E. Prowler

Answer: A

Explanation:
Nessus is a vulnerability scanning and assessment tool that can be used to scan systems for potential vulnerabilities and weaknesses. It provides detailed reports on any critical and high-severity findings as referenced in the CVE database, making it the ideal tool for fulfilling the Chief Information Security Officer's request. Nikto, fuzzer, wireshark, and prowler are all security tools, but they are not applicable for the scenario described in the question. Here is a link to an article from CompTIA's website about Nessus for your reference: https://www.comptia.org/content/nessus-vulnerability-scanning-and-assessment-tool.

NEW QUESTION 13
A user receives a potentially malicious attachment that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review. Which of the following commands would most likely indicate if the email is malicious?

A. sha256sum ~/Desktop/fi1e.pdf
B. /bin/;s -1 ~/Desktop/fi1e.pdf
C. strings ~/Desktop/fi1e.pdf | grep -i “<script”
D. cat < ~/Desktop/file.pdf | grep —i .exe

Answer: C

Explanation:
This command would most likely indicate if the email attachment is malicious, as it would display any JavaScript code embedded in the PDF file. JavaScript code can be used by attackers to execute malicious commands or scripts on the victim’s system when the PDF file is opened1. The strings command extracts the printable characters from a binary file, such as a PDF file, and the grep -i “<script” option searches for the presence of JavaScript code in a case-insensitive manner2.

NEW QUESTION 14
A company frequently expenences issues with credential stuffing attacks Which of the following is the BEST control to help prevent these attacks from being successful?

A. SIEM
B. IDS
C. MFA
D. TLS

Answer: C

Explanation:
MFA stands for multi-factor authentication, which is a method of verifying a user’s identity by requiring two or more pieces of evidence, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., fingerprint). MFA is the best control to help prevent credential stuffing attacks from being successful, because even if an attacker obtains a valid username and password from a breached site, they would still need another factor to access the target site. SIEM, IDS, and TLS are other security controls, but they are not as effective as MFA for preventing credential stuffing attacks.
Reference: https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

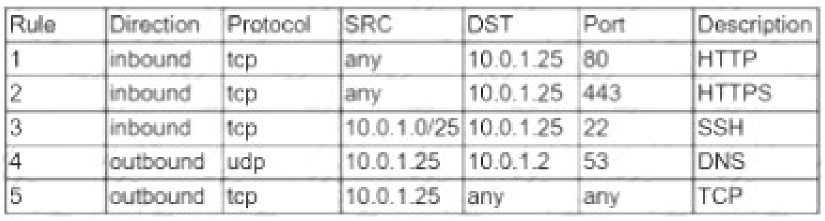
NEW QUESTION 15
A company wants to run a leaner team and needs to deploy a threat management system with minimal human Interaction. Which of the following is the server component of the threat management system that can accomplish this goal?

A. STIX
B. OpenIOC
C. CVSS
D. TAXll

Answer: D

Explanation:
TAXII stands for Trusted Automated eXchange of Indicator Information, and it is a server component of a threat management system that can facilitate the exchange of threat intelligence data between different sources and consumers, using a standard protocol and format. TAXII can help deploy a threat management system with minimal human interaction, by automating the collection, processing, and dissemination of threat intelligence data.

NEW QUESTION 16
A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0 1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.
The network rules for the instance are the following:



Rule	Direction	Protocol	SRC	DST	Port	Description
1	inbound	tcp	any	10.0.1.25	80	HTTP
2	inbound	tcp	any	10.0.1.25	443	HTTPS
3	inbound	tcp	10.0.1.0/25	10.0.1.25	22	SSH
4	outbound	udp	10.0.1.25	10.0.1.2	53	DNS
5	outbound	tcp	10.0.1.25	any	any	TCP

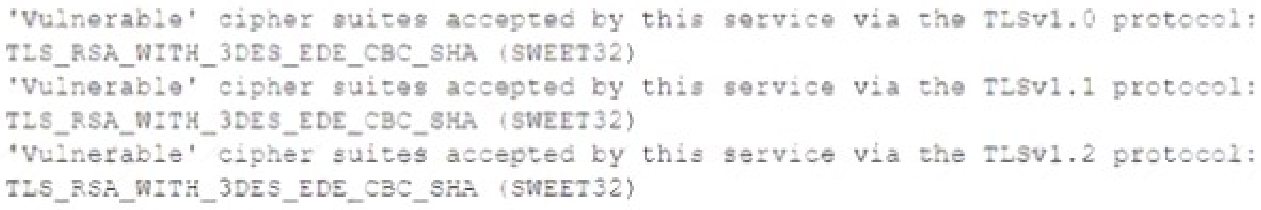
Which of the following is the BEST way to isolate and triage the host?

A. Remove rules 1.2. and 3.
B. Remove rules 1.2. 4. and 5.
C. Remove rules 1.2. 3.4. and 5.
D. Remove rules 1.2. and 5.
E. Remove rules 1.4. and 5.
F. Remove rules 4 and 5

Answer: C

Explanation:
The best way to isolate and triage the host is to remove rules 1, 2, 3, 4, and 5. These rules allow inbound and outbound traffic on ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) from any source or destination. By removing these rules, the security analyst can block any network communication to or from the host, preventing any further data exfiltration or malware infection. This will also allow the security analyst to perform a forensic analysis on the host without any interference from external sources.

NEW QUESTION 17
During a review of the vulnerability scan results on a server, an information security analyst notices the following:



```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

The MOST appropriate action for the analyst to recommend to developers is to change the web server so:

A. It only accepts TLSvl 2
B. It only accepts cipher suites using AES and SHA
C. It no longer accepts the vulnerable cipher suites
D. SSL/TLS is offloaded to a WAF and load balancer

Answer: C

Explanation:
A cipher suite is a set of algorithms that defines how the encryption, authentication, and integrity of data are performed during a secure communication session. Some cipher suites are considered vulnerable or weak because they use outdated or insecure algorithms that can be easily broken or compromised by attackers. The vulnerability scan results show that the web server accepts several vulnerable cipher suites, such as RC4, MD5, or DES. The best action for the analyst to recommend to developers is to change the web server so it no longer accepts the vulnerable cipher suites and only accepts the secure ones. Changing the web server so it only accepts TLSv1.2, only accepts cipher suites using AES and SHA, or offloading SSL/TLS to a WAF and load balancer are other possible actions, but they are not as specific or effective as changing the web server so it no longer accepts the vulnerable cipher suites. Reference:
https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/

NEW QUESTION 18
The Chief Information Security Officer (CISO) of a large financial institution is seeking a solution that will block a predetermined set of data points from being transferred or downloaded by employees. The CISO also wants to track the data assets by name, type, content, or data profile.
Which of the following BEST describes what the CIS wants to purchase?

A. Asset tagging
B. SIEM
C. File integrity monitor
D. DLP

Answer: D

Explanation:
DLP (Data Loss Prevention) is what the CISO wants to purchase. DLP is a solution that prevents unauthorized or accidental disclosure of sensitive data by monitoring, detecting, and blocking data transfers or downloads that violate predefined policies or rules3. DLP can also track and classify data assets based on various criteria, such as name, type, content, or data profile4. DLP can help protect data from insider threats, external attackers, or human errors.

NEW QUESTION 19
A forensics investigator is analyzing a compromised workstation. The investigator has cloned the hard drive and needs to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive that was collected as evidence. Which of the following should the investigator do?

A. Insert the hard drive on a test computer and boot the computer.
B. Record the serial numbers of both hard drives.
C. Compare the file-directory "sting of both hard drives.
D. Run a hash against the source and the destination.

Answer: D

Explanation:

A hash is a mathematical function that produces a unique value for a given input. A hash can be used to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive by comparing the hash values of both drives. If the hash values match, then the drives are identical. If the hash values differ, then there is some discrepancy between the drives. Inserting the hard drive on a test computer and booting the computer, recording the serial numbers of both hard drives, or comparing the file-directory listing of both hard drives are not reliable methods to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive. Reference: https://www.forensicswiki.org/wiki/Hashing

NEW QUESTION 20
Members of the sales team are using email to send sensitive client lists with contact information to their personal accounts The company's AUP and code of conduct prohibits this practice. Which of the following configuration changes would improve security and help prevent this from occurring?

A. Configure the DLP transport rules to provide deep content analysis.
B. Put employees' personal email accounts on the mail server on a blocklist.
C. Set up IPS to scan for outbound emails containing names and contact information.
D. Use Group Policy to prevent users from copying and pasting information into emails.
E. Move outbound emails containing names and contact information to a sandbox for further examination.

Answer: A

Explanation:
Data loss prevention (DLP) is a set of policies and tools that aim to prevent unauthorized disclosure of sensitive data. DLP transport rules are rules that apply to email messages that are sent or received by an organization’s mail server. These rules can provide deep content analysis, which means they can scan the content of email messages and attachments for sensitive data patterns, such as client lists or contact information. If a rule detects a violation of the DLP policy, it can take actions such as blocking, quarantining, or notifying the sender or recipient. This would improve security and help prevent sales team members from sending sensitive client lists to their personal accounts. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/data-loss-prevention

NEW QUESTION 21
A cybersecurity analyst is concerned about attacks that use advanced evasion techniques. Which of the following would best mitigate such attacks?

A. Keeping IPS rules up to date
B. Installing a proxy server
C. Applying network segmentation
D. Updating the antivirus software

Answer: A

Explanation:
Keeping IPS rules up to date is the best way to mitigate attacks that use advanced evasion techniques. An IPS (intrusion prevention system) is a security device that monitors network traffic and blocks or prevents malicious activity based on predefined rules or signatures. Advanced evasion techniques are cyberattacks that combine various evasion methods to bypass security detection and protection tools, such as IPS. Keeping IPS rules up to date can help to ensure that the IPS can recognize and block the latest advanced evasion techniques and prevent them from compromising the network .

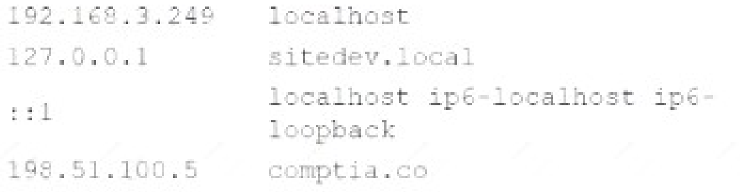
NEW QUESTION 22
While observing several host machines, a security analyst notices a program is overwriting data to a buffer. Which of the following controls will best mitigate this issue?

A. Data execution prevention
B. Output encoding
C. Prepared statements
D. Parameterized queries

Answer: A

Explanation:
Data execution prevention (DEP) is a security feature that prevents code from being executed in memory regions that are marked as data-only. This helps mitigate buffer overflow attacks, which are a type of attack where a program overwrites data to a buffer beyond its allocated size, potentially allowing malicious code to be executed. DEP can be implemented at the hardware or software level and can prevent unauthorized code execution in memory buffers. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/win32/memory/data-execution-prevention

NEW QUESTION 23
An analyst Is reviewing a web developer's workstation for potential compromise. While examining the workstation's hosts file, the analyst observes the following:



```
192.168.3.249    localhost
127.0.0.1        sitedev.local
::1              localhost ip6-localhost ip6-
                 loopback
198.51.100.5     comptia.co
```

Which of the following hosts file entries should the analyst use for further investigation?

A. ::1
B. 127.0.0.1
C. 192.168.3.249
D. 198.51.100.5

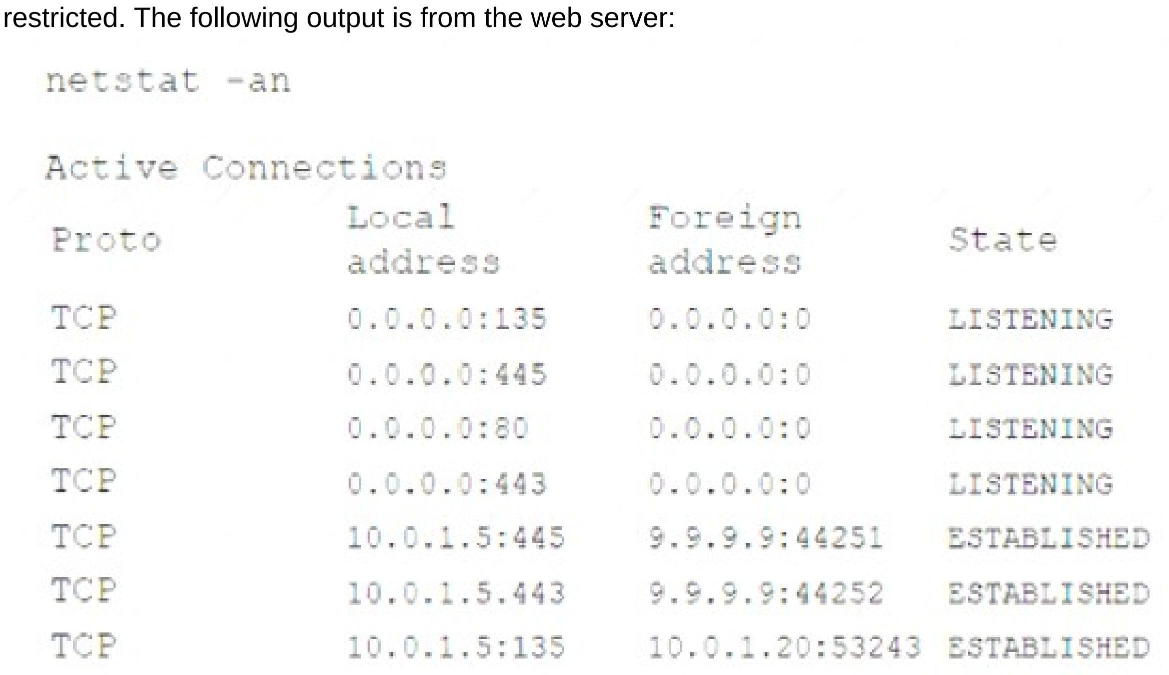
Answer: D

Explanation:

The hosts file is a text file that maps hostnames to IP addresses, and it can be used to override DNS resolution. The hosts file entries that should be used for further investigation are the ones that point to external or suspicious IP addresses, such as 198.51.100.5, which is a reserved IP address for documentation purposes. The other entries are either loopback addresses (::1 and 127.0.0.1) or internal network addresses (192.168.3.249), which are less likely to be malicious.

NEW QUESTION 24

During a routine security review, anomalous traffic from 9.9.9.9 was observed accessing a web server in the corporate perimeter network. The server is mission critical and must remain accessible around the world to serve web content. The Chief Information Security Officer has directed that improper traffic must be restricted. The following output is from the web server:



```
netstat -an

Active Connections
         Local            Foreign
Proto    address          address          State
TCP      0.0.0.0:135      0.0.0.0:0        LISTENING
TCP      0.0.0.0:445      0.0.0.0:0        LISTENING
TCP      0.0.0.0:80       0.0.0.0:0        LISTENING
TCP      0.0.0.0:443      0.0.0.0:0        LISTENING
TCP      10.0.1.5:445     9.9.9.9:44251    ESTABLISHED
TCP      10.0.1.5.443     9.9.9.9:44252    ESTABLISHED
TCP      10.0.1.5:135     10.0.1.20:53243  ESTABLISHED
```

Which of the following is the best method to accomplish this task?

A. Adjusting the IDS to block anomalous activity
B. Implementing port security
C. Adding 9.9.9.9 to the blocklist
D. Adjusting the firewall

Answer: D

Explanation:

Based on the output of the “netstat -an” command, it seems that the web server is listening on port 80 for HTTP traffic and port 443 for HTTPS traffic. The anomalous traffic from 9.9.9.9 is accessing the web server on port 443, which means it is using a secure connection.

The best method to accomplish the task of restricting improper traffic from 9.9.9.9 is D. Adjusting the firewall. A firewall is a device or software that controls the flow of network traffic based on predefined rules. By adjusting the firewall rules, you can block or allow specific IP addresses, ports, protocols, or domains from accessing your web server.

NEW QUESTION 25

Which of the following is the software development process by which function, usability, and scenarios are tested against a known set of base requirements?

A. Security regression testing
B. Code review
C. User acceptance testing
D. Stress testing

Answer: C

Explanation:

"User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications." https://www.plutora.com/blog/uat-user-acceptance-testing

User acceptance testing is the software development process by which function, usability, and scenarios are tested against a known set of base requirements. User acceptance testing (UAT) is the final stage of software development before production. It is used to get feedback from users who test the software and its user interface (UI). UAT is usually done manually, with users creating real-world situations and testing how the software reacts and performs. UAT is used to determine if end-users accept software before it’s made public. Client or business requirements determine whether it fulfills the expectations originally set in its development2.

NEW QUESTION 26

Due to continued support of legacy applications, an organization's enterprise password complexity rules are inadequate for its required security posture. Which of the following is the BEST compensating control to help reduce authentication compromises?

A. Smart cards
B. Multifactor authentication
C. Biometrics
D. Increased password-rotation frequency

Answer: B

Explanation:

Multifactor authentication is a method of verifying a user’s identity by requiring two or more pieces of evidence, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., fingerprint). Multifactor authentication is the best compensating control to help reduce authentication compromises when the organization’s enterprise password complexity rules are inadequate for its required security posture. Smart cards, biometrics, or increased password-rotation frequency are other possible controls, but they are not as effective or comprehensive as multifactor authentication.
Reference:
https://www.csoonline.com/article/3239144/what-is-multifactor-authentication-mfa-how-it-works-and-why-you

NEW QUESTION 27
An organization is developing software to match customers' expectations. Before the software goes into production, it must meet the following quality assurance guidelines
• Uncover all the software vulnerabilities.
• Safeguard the interest of the software's end users.
• Reduce the likelihood that a defective program will enter production.
• Preserve the Interests of me software producer Which of me following should be performed FIRST?

A. Run source code against the latest OWASP vulnerabilities.
B. Document the life-cycle changes that look place.
C. Ensure verification and vacation took place during each phase.
D. Store the source code in a s oftware escrow.
E. Conduct a static analysis of the code.

Answer: E

Explanation:
Static analysis of the code is a technique that scans the source code or the compiled code of an application without executing it, to identify potential vulnerabilities, errors, or bugs. Static analysis can help uncover all the software vulnerabilities, safeguard the interest of the software’s end users, reduce the likelihood that a defective program will enter production, and preserve the interests of the software producer by improving the quality and security of the code before it is deployed or run1

NEW QUESTION 28
An organization wants to ensure the privacy of the data that is on its systems Full disk encryption and DLP are already in use Which of the following is the BEST option?

A. Require all remote employees to sign an NDA
B. Enforce geofencing to limit data accessibility
C. Require users to change their passwords more frequently
D. Update the AUP to restrict data sharing

Answer: B

Explanation:
Enforcing geofencing to limit data accessibility is the best option to ensure the privacy of the data that is on its systems. Geofencing is a technique that uses GPS or RFID technology to create a virtual geographic boundary around a specific location or area. Geofencing can be used to restrict data accessibility based on the location of the device or user that tries to access it. For example, geofencing can prevent employees from accessing sensitive data when they are outside the office premises or in a different country3. Geofencing can help protect data privacy and comply with data protection regulations that may vary across regions or jurisdictions.

NEW QUESTION 29
When of the following techniques can be implemented to safeguard the confidentiality of sensitive information while allowing limited access to authorized individuals?

A. Deidentification
B. Hashing
C. Masking
D. Salting

Answer: C

Explanation:
https://www.techtarget.com/searchsecurity/definition/data-masking
Masking is a technique that involves replacing or hiding some parts of sensitive information with symbols or characters, such as asterisks (*) or Xs. Masking can help safeguard the confidentiality of sensitive information while allowing limited access to authorized individuals, because it obscures the original data without altering its format or structure. For example, masking can be used to hide some digits of a credit card number or a social security number. Deidentification, hashing, or salting are other techniques that involve transforming or modifying sensitive information, but they do not allow limited access to authorized individuals.
Reference: https://www.ibm.com/docs/en/ims/14.1?topic=masking-data

NEW QUESTION 30
A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with acKvare. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

A. Blacklist the hash in the next-generation antivirus system.
B. Manually delete the file from each of the workstations.
C. Remove administrative rights from all developer workstations.
D. Block the download of the fie via the web proxy

Answer: D

Explanation:
Blocking the download of the file via the web proxy is the best change to make to the security tools to remedy the issue. A web proxy is a server that acts as an intermediary between a client and a web server, filtering or modifying requests and responses according to predefined rules1. Blocking the download of the file via the web proxy can prevent developers from accessing and executing the offending file that is bundled with adware. This can reduce the risk of infection or compromise of the developer workstations and improve their performance and security. Blacklisting the hash in the next-generation antivirus system (A) is not the best change to make to the security tools to remedy the issue. Blacklisting is a technique that involves blocking or denying access to known malicious or unwanted entities based on their identifiers, such as hashes, IP addresses, domains, etc2. Blacklisting the hash in the next-generation antivirus system can prevent developers from executing the offending file that is bundled with adware, but it does not prevent them from downloading it. This can still consume network

bandwidth and disk space and expose developers to potential threats. Manually deleting the file from each of the workstations (B) is not the best change to make to the security tools to remedy the issue. Manually deleting the file from each of the workstations can remove the offending file that is bundled with adware, but it does not prevent developers from downloading it again. This can be a time-consuming and inefficient process that requires human intervention and coordination. Removing administrative rights from all developer workstations © is not the best change to make to the security tools to remedy the issue. Removing administrative rights from all developer workstations can limit developers' ability to install or execute unauthorized or malicious applications, such as adware, but it does not prevent them from downloading them. This can also affect developers' productivity and functionality by restricting their access to legitimate applications or settings.
References: 1: https://www.techopedia.com/definition/24771/technical-controls 2: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl

NEW QUESTION 31
......