CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
A company has alerted planning the implemented a vulnerability management procedure. However, to security maturity level is low, so there are some prerequisites to complete before risk calculation and prioritization.
Which of the following should be completed FIRST?

A. A business Impact analysis
B. A system assessment
C. Communication of the risk factors
D. A risk identification process

Answer: A

Explanation:
A business impact analysis (BIA) should be completed first before risk calculation and prioritization. A BIA is a process that identifies and evaluates the potential effects of disruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization's assets and resources1. A BIA is a prerequisite for risk calculation and prioritization because it provides the basis for estimating the impact and likelihood of various threats and vulnerabilities on the organization's operations, reputation, and finances2.

NEW QUESTION 2
Due to a rise m cyberattackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally Which of the following countermeasures can BEST prevent the loss of customers' sensitive data?

A. Implement privileged access management
B. Implement a risk management process
C. Implement multifactor authentication
D. Add more security resources to the environment

Answer: A

Explanation:
Implementing privileged access management (PAM) would be the best countermeasure to prevent the loss of customers' sensitive data due to a rise in cyberattackers seeking PHI (Protected Health Information). PAM is a solution that helps to control and monitor the access and use of privileged accounts, such as administrator or root accounts, that have elevated permissions or access to sensitive data. PAM can help prevent unauthorized or accidental use of privileged accounts by enforcing strict access policies, such as requiring approval, authentication, or auditing for each access request. PAM can also help rotate or expire the passwords of privileged accounts to reduce the risk of compromise2. PAM can help protect PHI from cyberattackers who may try to exploit privileged accounts to access or exfiltrate sensitive data.

NEW QUESTION 3
Which of the following is a vulnerability associated with the Modbus protocol?

A. Weak encryption
B. Denial of service
C. Unchecked user input
D. Lack of authentication

Answer: D

Explanation:
Modbus is a communication protocol that is widely used in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. However, Modbus was not designed to provide security and it is vulnerable to various cyberattacks. One of the main vulnerabilities of Modbus is the lack of authentication, which means that any device on the network can send or receive commands without verifying its identity or authority. This can lead to unauthorized access, data manipulation, or denial of service attacks on the ICS or SCADA system.
Some examples of attacks that exploit the lack of authentication in Modbus are:

- Detection attack: An attacker can scan the network and discover the devices and their addresses, functions, and registers by sending Modbus requests and observing the responses. This can reveal sensitive information about the system configuration and operation1.
- Command injection attack: An attacker can send malicious commands to the devices and modify their settings, values, or outputs. For example, an attacker can change the speed of a motor, open or close a valve, or turn off a switch23.
- Response injection attack: An attacker can intercept and alter the responses from the devices and deceive the master or other devices about the true state of the system. For example, an attacker can fake a normal response when there is an error or an alarm23.
- Denial of service attack: An attacker can flood the network with Modbus requests or commands and overload the devices or the communication channel. This can prevent legitimate requests or commands from being processed and disrupt the normal operation of the system14.

To mitigate these attacks, some security measures that can be applied to Modbus are:

- Encryption: Encrypting the Modbus messages can prevent eavesdropping and tampering by unauthorized parties. However, encryption can also introduce additional overhead and latency to the communication56.
- Authentication: Adding authentication mechanisms to Modbus can ensure that only authorized devices can send or receive commands. Authentication can be based on passwords, certificates, tokens, or other methods56.
- Firewall: Installing a firewall between the Modbus network and other networks can filter out unwanted traffic and block unauthorized access. A firewall can also enforce rules and policies for Modbus communication24.
- Intrusion detection system: Deploying an intrusion detection system (IDS) on the Modbus network can monitor the traffic and detect anomalous or malicious activities. An IDS can also alert the operators or trigger countermeasures when an attack is detected24.

NEW QUESTION 4
A security technician configured a NIDS to monitor network traffic. Which of the following is a condition in which harmless traffic is classified as a potential network attack?

A. True positive
B. True negative
C. False positive
D. False negative

Answer: C

Explanation:
A false positive is a condition in which harmless traffic is classified as a potential network attack by a NIDS. A NIDS is a network intrusion detection system that monitors network traffic for any signs of malicious or anomalous activity. A false positive can result in unnecessary alerts or actions by the NIDS, such as blocking legitimate traffic or generating false alarms. False positives can be caused by various factors, such as misconfigured rules, outdated signatures, noisy network traffic or benign anomalies3 .

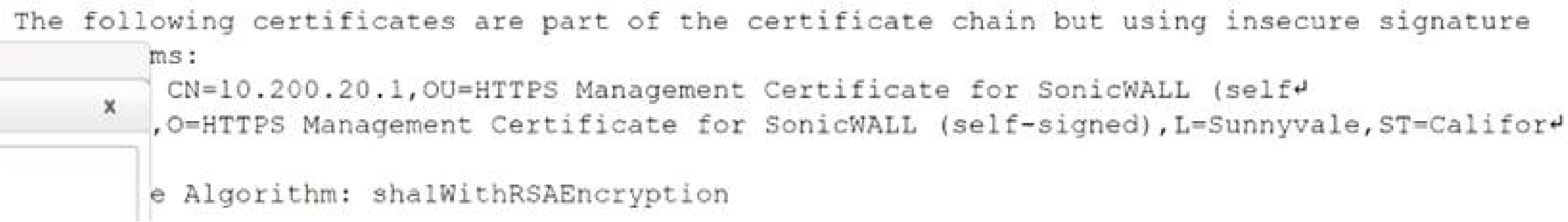
NEW QUESTION 5
An analyst reviews the most recent vulnerability management report and notices a firewall with 99.98% required uptime is reporting different firmware versions on scans than were reported in previous scans. The vendor released new firewall firmware a few months ago. Which of the following will the analyst most likely do next given the requirements?

A. Request to route traffic through a secondary firewall
B. Check for change tickets.
C. Perform a credentialed scan
D. Request an exception to the uptime policy.

Answer: B

Explanation:
The analyst should check for change tickets as the next step, given that the firewall is reporting different firmware versions on scans than were reported in previous scans. Change tickets are records of any authorized changes made to a system or a network, such as updating firmware, installing patches, or modifying configurations. Checking for change tickets can help verify if the firmware change was intentional and approved, or if it was unauthorized or malicious.

NEW QUESTION 6
While reviewing a vulnerability assessment, an analyst notices the following issue is identified in the report: this finding, which of the following would be most appropriate for the analyst to recommend to the network engineer?



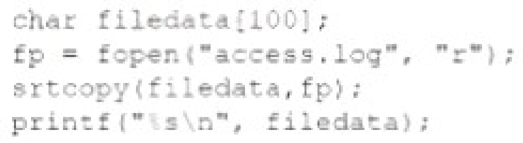
```
 The following certificates are part of the certificate chain but using insecure signature
              ms:
               CN=10.200.20.1,OU=HTTPS Management Certificate for SonicWALL (self↵
              ,O=HTTPS Management Certificate for SonicWALL (self-signed),L=Sunnyvale,ST=Califor↵

              e Algorithm: sha1WithRSAEncryption
```

A. Reconfigure the device to support only connections leveraging TLSv1.2.
B. Obtain a new self-signed certificate and select AES as the hashing algorithm.
C. Replace the existing certificate with a certificate that uses only MD5 for signing.
D. Use only signed certificates with cryptographically secure certificate sources.

Answer: A

Explanation:
The vulnerability assessment report shows that the device is using SSLv3, which is an outdated and insecure protocol for secure communication over a network. SSLv3 has several known vulnerabilities, such as POODLE, that allow attackers to decrypt or modify the encrypted data. To remediate this issue, the analyst should recommend reconfiguring the device to support only connections leveraging TLSv1.2, which is a newer and more secure protocol that provides stronger encryption, authentication, and integrity protection for the data transmitted over the network.

NEW QUESTION 7
An internally developed file-monitoring system identified the following except as causing a program to crash often:



```
char filedata[100];
fp = fopen("access.log", "r");
srtcopy(filedata,fp);
printf("%s\n", filedata);
```

Which of the following should a security analyst recommend to fix the issue?

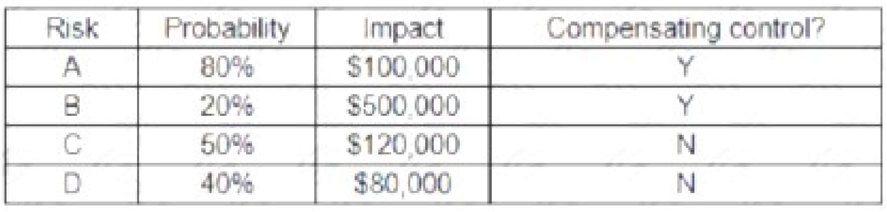
A. Open the access.log file ri read/write mode.
B. Replace the strcpv function.
C. Perform input samtizaton
D. Increase the size of the file data buffer

Answer: B

Explanation:
The security analyst should recommend replacing the strcpy function with a safer alternative. The strcpy function is a C library function that copies a string from one buffer to another. However, this function does not check the size of the destination buffer, which can lead to buffer overflow vulnerabilities if the source string is longer than the destination buffer. Buffer overflow vulnerabilities can allow attackers to execute arbitrary code or crash the program. A safer alternative to strcpy is strncpy, which limits the number of characters copied to the size of the destination buffer.

NEW QUESTION 8
An organization has the following risk mitigation policies

- Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000
- Other nsk mitigation will be pnontized based on risk value. The following risks have been identified:



Risk	Probability	Impact	Compensating control?
A	80%	$100 000	Y
B	20%	$500 000	Y
C	50%	$120,000	N
D	40%	$80,000	N

Which of the following is the ordei of priority for risk mitigation from highest to lowest?

A. A, C, D, B
B. B, C, D, A
C. C, B, A, D
D. D, A, B
E. D, C, B, A

Answer: C

Explanation:
The order of priority for risk mitigation from highest to lowest is C, B, A, D. This order is based on applying the risk mitigation policies of the organization. According to the first policy, risks without compensating controls will be mitigated first if the risk value is greater than $50,000. Risk C has no compensating controls and a risk value of $75,000, so it is the highest priority. Risk B also has no compensating controls, but a risk value of $40,000, so it is the second priority. According to the second policy, other risk mitigation will be prioritized based on risk value. Risk A has a risk value of $60,000 and a compensating control of encryption, so it is the third priority. Risk D has a risk value of $50,000 and a compensating control of backup power supply, so it is the lowest priority.

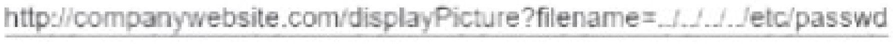
NEW QUESTION 9
A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse
non-business-related websites?

A. Implement a virtual machine alternative.
B. Develop a new secured browser.
C. Configure a personal business VLAN.
D. Install kiosks throughout the building.

Answer: A

Explanation:
A virtual machine alternative is a solution that allows employees to access non-business-related websites on a separate virtual machine that is isolated from the company's network and data. This way, the employees can browse the internet without compromising the security or performance of the company's systems3

NEW QUESTION 10
A SIEM analyst receives an alert containing the following URL:



http://companywebsite.com/displayPicture?filename=../../../../etc/passwd

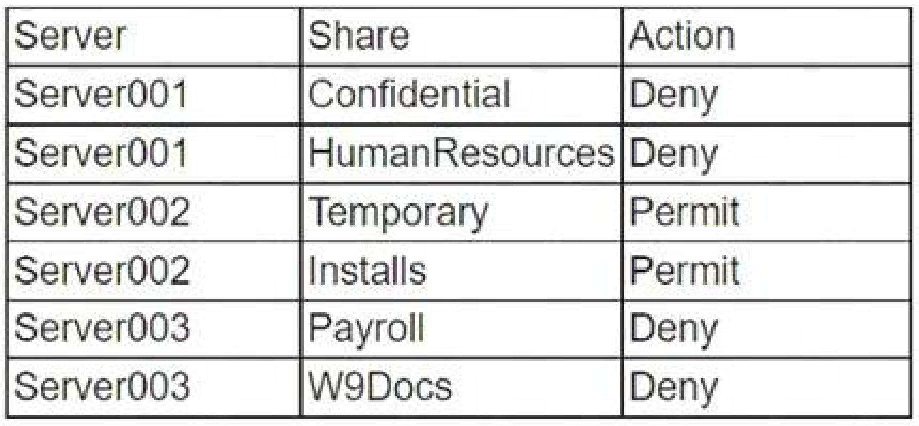
Which of the following BEST describes the attack?

A. Password spraying
B. Buffer overflow
C. insecure object access
D. Directory traversal

Answer: D

Explanation:
A directory traversal attack is a type of web application attack that exploits insufficient input validation or filtering to access files or directories that are outside of the web root folder. A directory traversal attack can allow an attacker to read, modify, or execute files on the target server that are not intended to be accessible via web requests. The URL in the alert contains an example of a directory traversal attack, as indicated by the use of "…/" sequences in the query string. These sequences are used to navigate up one level in the directory hierarchy, potentially reaching sensitive files or folders on the server. In this case, the attacker is trying to access /etc/passwd file, which contains user account information on Linux systems.

NEW QUESTION 10
While reviewing abnormal user activity, a security analyst notices a user has the following fileshare activities:



Server	Share	Action
Server001	Confidential	Deny
Server001	HumanResources	Deny
Server002	Temporary	Permit
Server002	Installs	Permit
Server003	Payroll	Deny
Server003	W9Docs	Deny

Which of the following should the analyst do first?

A. Initiate the security incident response process for unauthorized access.
B. Shut down the servers while the access is investigated.
C. Remove the user's access for all fileshares.
D. Lock the user account until the access can be explained.

Answer: A

Explanation:
The security incident response process is a set of procedures and guidelines that define how to identify, contain, analyze, and recover from security incidents that compromise the confidentiality, integrity, or availability of an organization’s assets or operations. Initiating the security incident response process for unauthorized access is the first and most appropriate action that the analyst should take, as it would allow the analyst to follow a structured and consistent approach to handle the situation and mitigate the impact of the incident1.

NEW QUESTION 12
A help desk technician inadvertently sent the credentials of the company's CRM n clear text to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident According to the incident response procedure, which of the following should the security team do NEXT?

A. Contact the CRM vendor.
B. Prepare an incident summary report.
C. Perform postmortem data correlation.
D. Update the incident response plan.

Answer: C

Explanation:
The security team should perform postmortem data correlation next after receiving notification of the incident from the help desk technician. Postmortem data correlation is an activity that involves analyzing data from various sources (such as logs, alerts, reports, etc.) to identify root causes, impacts, indicators of compromise (IoCs), lessons learned, and recommendations for improvement after an incident3. Postmortem data correlation can help the security team to:

- Determine how the incident occurred and how it was detected and resolved
- Identify any gaps or weaknesses in security controls or processes that contributed to the incident
- Develop action plans or remediation strategies to prevent recurrence or mitigate future incidents

NEW QUESTION 13
During a review of SIEM alerts, a securrty analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring toot about files from a newly deployed application that should not change. Which of the following steps should the analyst complete FIRST to respond to the issue7

A. Warn the incident response team that the server can be compromised
B. Open a ticket informing the development team about the alerts
C. Check if temporary files are being monitored
D. Dismiss the alert, as the new application is still being adapted to the environment

Answer: C

Explanation:
The analyst should check if temporary files are being monitored first to respond to the issue. Temporary files are files that are created and used by applications for various purposes, such as storing data temporarily or caching data for faster access. However, temporary files are not meant to be permanent and are usually deleted when they are no longer needed or when the application is closed. Therefore, monitoring temporary files can generate many alerts from the file-integrity monitoring tool that are not relevant or useful for security purposes. The analyst should check if temporary files are being monitored and exclude them from the monitoring scope to reduce the number of alerts and focus on the files that should not change.

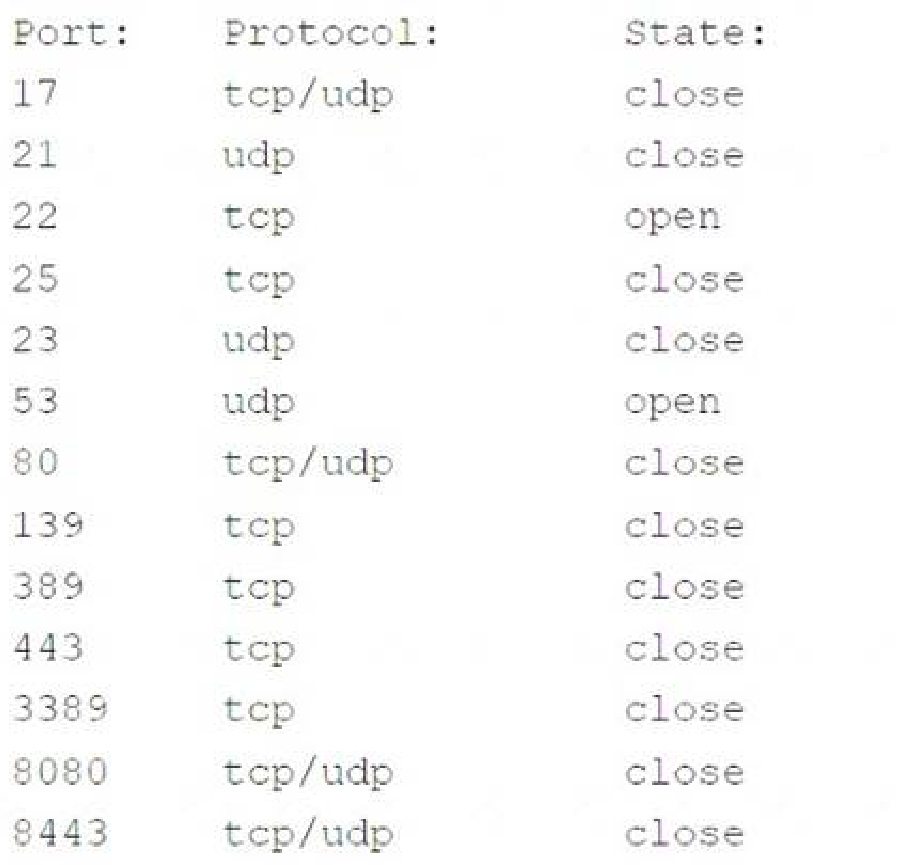
NEW QUESTION 16
After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

A. Header analysis
B. File carving
C. Metadata analysis
D. Data recovery

Answer: B

Explanation:
File carving is a technique that involves scanning the raw data bytes of a hard disk and rebuilding files by using information found in file headers and footers. File carving can help recover files that have been deleted or corrupted or that are not recognized by the file system. File carving does not rely on metadata or directory structures to locate files, but rather on file signatures or patterns that indicate the start and end of files. File carving can be performed manually or automatically using tools or software that support various file formats. Header analysis (A) is a technique that involves examining file headers to determine file types or formats. Header analysis can help identify files that have been renamed or disguised or that have unknown extensions. Header analysis does not involve reconstructing files by scanning raw data bytes. Metadata analysis © is a technique that involves examining metadata to extract information about files or file systems. Metadata analysis can help determine file attributes such as name, size, date, location, owner, etc. Metadata analysis does not involve reconstructing files by scanning raw data bytes

NEW QUESTION 18
A security analyst scans the company's external IP range and receives the following results from one of the hosts:



```
Port:    Protocol:       State:
17       tcp/udp         close
21       udp             close
22       tcp             open
25       tcp             close
23       udp             close
53       udp             open
80       tcp/udp         close
139      tcp             close
389      tcp             close
443      tcp             close
3389     tcp             close
8080     tcp/udp         close
8443     tcp/udp         close
```

Which of the following best represents the security concern?

A. A remote communications port is exposed.
B. The FTP port should be using TCP only.
C. Microsoft RDP is accepting connections on TCP.
D. The company's DNS server is exposed to everyone.

Answer: C

Explanation:
The correct answer is C. Microsoft RDP is accepting connections on TCP. Microsoft RDP stands for Microsoft Remote Desktop Protocol, and it is a protocol that allows users to remotely access and control a Windows computer or server. RDP uses TCP port 3389 by default, and this port is open on the host according to the results. This indicates that the host is allowing RDP connections from anyone on the internet, which poses a security concern. An attacker could exploit vulnerabilities in RDP or use brute force attacks to gain unauthorized access to the host and compromise its data or resources1.
* A. A remote communications port is exposed is not correct. A remote communications port is a generic term for any port that allows remote access or communication with a host. There are many types of remote communications ports, such as SSH, Telnet, FTP, or RDP, and each one has its own security implications. The results do not specify which remote communications port is exposed, so this answer is too vague and inaccurate.
* B. The FTP port should be using TCP only is not correct. FTP stands for File Transfer Protocol, and it is a protocol that allows users to transfer files between hosts. FTP uses TCP ports 20 and 21 by default, and these ports are closed on the host according to the results. However, FTP can also use UDP ports 20 and 21 for data transfer in some cases, such as when using passive mode or extended passive mode2. Therefore, it is not true that FTP should be using TCP only, and this answer does not represent a security concern.
* D. The company's DNS server is exposed to everyone is not correct. DNS stands for Domain Name System, and it is a system that translates domain names into IP addresses. DNS uses UDP port 53 by default, and this port is open on the host according to the results. This indicates that the host is providing DNS services to anyone on the internet, which may or may not be a security concern depending on the configuration and purpose of the host. For example, if the host is a public DNS server that is intended to serve DNS queries from anyone, then this answer does not represent a security concern. However, if the host is a private DNS server that is meant to serve DNS queries only from authorized users or devices, then this answer could represent a security concern.
* 1: What Is Remote Desktop Protocol (RDP)? 2: FTP - File Transfer Protocol : [What Is Domain Name S (DNS)?]

NEW QUESTION 23
A security analyst is concerned the number of security incidents being reported has suddenly gone down. Daily business interactions have not changed, and no following should the analyst review FIRST?

A. The DNS configuration
B. Privileged accounts
C. The IDS rule set
D. The firewall ACL

Answer: C

Explanation:
The security analyst should review the IDS rule set first. The IDS (Intrusion Detection System) is a tool that monitors network traffic and alerts on any suspicious or malicious activity. The IDS rule set is a set of conditions or patterns that define what constitutes normal or abnormal behavior on the network. The IDS rule set can affect the number of security incidents being reported, as it determines what triggers an alert or not3. The security analyst should review the IDS rule set to check if it is up to date, accurate, and comprehensive. If the IDS rule set is outdated, inaccurate, or incomplete, it may miss some incidents or generate false positives or negatives.

NEW QUESTION 28
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 31
An organizational policy requires one person to input accounts payable and another to do accounts receivable. A separate control requires one person to write a check and another person to sign all checks greater than $5,000 and to get an additional signature for checks greater than $10,000. Which of the following controls has the organization implemented?

A. Segregation of duties
B. Job rotation
C. Non-repudiaton
D. Dual control

Answer: A

Explanation:
Segregation of duties is a security control that requires multiple people to be involved with completing a task. This helps prevent fraud, as it ensures that no one individual has the ability to commit fraud or make mistakes without other people being aware of it

NEW QUESTION 33
A security analyst discovers the company's website is vulnerable to cross-site scripting. Which of the following solutions will best remedy the vulnerability?

A. Prepared statements
B. Server-side input validation
C. Client-side input encoding
D. Disabled JavaScript filtering

Answer: B

Explanation:
Server-side input validation is a solution that can prevent cross-site scripting (XSS) vulnerabilities by checking and filtering any user input that is sent to the server before rendering it on a web page. Server-side input validation can help to ensure that the user input conforms to the expected format, length and type, and does not contain any malicious characters or syntax that may alter the logic or behavior of the web page. Server-side input validation can also reject or sanitize any input that does not meet the validation criteria .

NEW QUESTION 36
An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?

A. A DLP system
B. DNS sinkholing
C. IP address allow list
D. An inline IDS

Answer: B

Explanation:
DNS sinkholing is a mechanism that can prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains by returning a false or controlled IP address for those domains. This can reduce the load on the firewall by intercepting the DNS requests before they reach the firewall and diverting them to a sinkhole server. The other options are not relevant or effective for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://www.enisa.europa.eu/topics/incident-response/glossary/dns-sinkhole

NEW QUESTION 40
A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

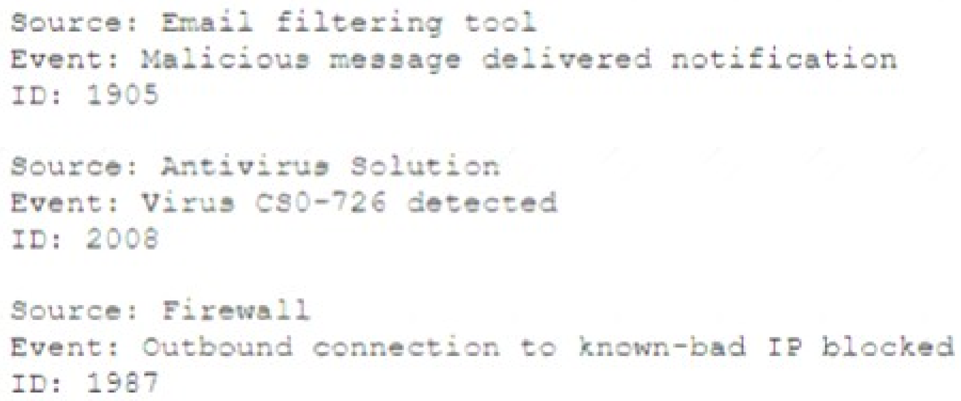
A. Deterrent
B. Preventive
C. Compensating
D. Detective

Answer: C

Explanation:
A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.
"Compensating controls are additional security measures that you take to address a vulnerability without remediating the underlying issue."
A compensating control is a control that reduces the risk of an existing or potential control weakness2
In this case, the lack of segregation of duties in the accounting department is a control weakness that increases the risk of fraud or error. The quarterly reviews by a different officer are a compensating control that reduces this risk by providing an independent verification of the transactions recorded by the controller.

NEW QUESTION 43

A security analyst needs to automate the incident response process for malware infections. When the following logs are generated, an alert email should automatically be sent within 30 minutes:



```
Source: Email filtering tool
Event: Malicious message delivered notification
ID: 1905

Source: Antivirus Solution
Event: Virus CS0-726 detected
ID: 2008

Source: Firewall
Event: Outbound connection to known-bad IP blocked
ID: 1987
```

Which of the following is the best way for the analyst to automate alert generation?

A. Deploy a signature-based IDS
B. Install a UEBA-capable antivirus
C. Implement email protection with SPF
D. Create a custom rule on a SIEM

Answer: D

Explanation:
A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A security analyst can create a custom rule on a SIEM system to automate the incident response process for malware infections. For example, the analyst can create a rule that triggers an alert email when the SIEM system detects logs that match the criteria of malware infection, such as process name, file name, file hash, etc. The alert email can be sent within 30 minutes or any other desired time frame. The other options are not suitable or sufficient for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15; https://www.sans.org/reading-room/whitepapers/analyst/security-information-event-management-siem-impleme

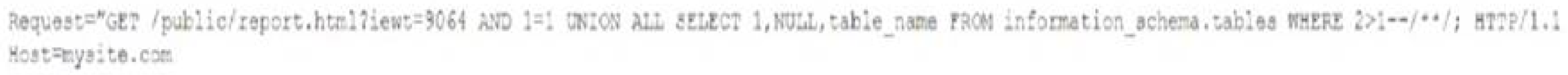
NEW QUESTION 45
To prioritize the morning's work, an analyst is reviewing security alerts that have not yet been investigated. Which of the following assets should be investigated FIRST?

A. The workstation of a developer who is installing software on a web server
B. A new test web server that is in the process of initial installation
C. An accounting supervisor's laptop that is connected to the VPN
D. The laptop of the vice president that is on the corporate LAN

Answer: D

Explanation:
The laptop of the vice president that is on the corporate LAN should be investigated first. According to the CompTIA CySA+ Certification Exam (CS0-002) study guide, when prioritizing security alerts, the analyst should prioritize assets based on the potential impact of a successful attack or compromise. Therefore, the laptop of the vice president, which is connected to the corporate LAN, should be investigated first, as it has the highest potential impact.

NEW QUESTION 50
A security analyst is reviewing WAF alerts and sees the following request:



```
Request="GET /public/report.html?iewt=9064 AND 1=1 UNION ALL SELECT 1,NULL,table_name FROM information_schema.tables WHERE 2>1--/**/; HTTP/1.1
Host=mysite.com
```

Which of the following BEST describes the attack?

A. SQL injection
B. LDAP injection
C. Command injection
D. Denial of service

Answer: A

Explanation:
The attack is a SQL injection attack. SQL injection is a type of attack that exploits a security vulnerability in an application's software that allows user input to be executed as SQL commands by the underlying database3. SQL injection can enable an attacker to perform various malicious actions on the database, such as reading, modifying, deleting or creating data; executing commands; or bypassing authentication. The request shows that the attacker has entered a malicious SQL statement in the username parameter that attempts to drop (delete) all tables in the database.

NEW QUESTION 54
A security analyst observes a large amount of scanning activity coming from an IP address outside the organization's environment. Which of the following should the analyst do to block this activity?

A. Create an IPS rule to block the subnet.
B. Sinkhole the IP address.
C. Create a firewall rule to block the IP address.
D. Close all unnecessary open ports.

Answer: C

Explanation:

A firewall is a device or software that controls the incoming and outgoing network traffic based on predefined rules. Creating a firewall rule to block the IP address that is scanning the organization’s environment is an effective way to stop this activity and prevent potential attacks. Creating an IPS rule to block the subnet, sinkholing the IP address, or closing all unnecessary open ports are other possible actions, but they are not as specific or efficient as creating a firewall rule to block the IP address. Reference: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/firewall.html

NEW QUESTION 55
A security analyst identified one server that was compromised and used as a data making machine, and a few of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?

A. System timeline reconstruction
B. System registry extraction
C. Data carving
D. Volatile memory analysts

Answer: A

Explanation:
System timeline reconstruction is a forensic analysis technique that involves creating a chronological record of events that occurred on a system based on various sources of evidence such as log files, registry entries, file timestamps, network traffic, etc. System timeline reconstruction can provide information about when and how the machine was compromised and where the malware is located by showing when suspicious activities or changes took place on the system, such as unauthorized access attempts, file creation or modification, process execution, network connections, etc.

NEW QUESTION 56
Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

A. Message queuing telemetry transport does not support encryption.
B. The devices may have weak or known passwords.
C. The devices may cause a dramatic Increase in wireless network traffic.
D. The devices may utilize unsecure network protocols.
E. Multiple devices may interface with the functions of other loT devices.
F. The devices are not compatible with TLS 12.

Answer: BD

Explanation:
Consumer IoT devices are devices that connect to the internet and provide various functions or services for personal or home use, such as smart speakers, cameras, thermostats, etc. Consumer IoT devices should be avoided in an enterprise environment because they may pose security risks or challenges for the organization’s network and data. Some of the reasons why consumer IoT devices should be avoided are:

➢ The devices may have weak or known passwords: Many consumer IoT devices come with default or hardcoded passwords that are easy to guess or find online. Some devices may not allow users to change their passwords or enforce strong password policies. This can make them vulnerable to brute-force attacks or unauthorized access by attackers.

➢ The devices may utilize unsecure network protocols: Many consumer IoT devices use unsecure network protocols to communicate with other devices or servers, such as HTTP, FTP, Telnet, etc. These protocols do not encrypt or authenticate the data they transmit or receive, which can expose them to interception, modification, or spoofing by attackers.

NEW QUESTION 59
During an Incident, it Is determined that a customer database containing email addresses, first names, and last names was exfiltrated. Which ot the following should the security analyst do NEXT?

A. Consult with the legal department for regulatory impact.
B. Encrypt the database with available tools.
C. Email the customers to inform them of the breach.
D. Follow the incident communications process.

Answer: D

Explanation:
An incident communications process is a set of procedures that defines how to communicate with internal and external stakeholders during and after an incident, such as customers, employees, management, regulators and media. An incident communications process can help to provide accurate, timely and consistent information about the incident, its impact and the actions taken to resolve it. An incident communications process can also help to maintain trust and reputation, comply with legal obligations and prevent misinformation or confusion3.

NEW QUESTION 64
A network appliance manufacturer is building a new generation of devices and would like to include chipset security improvements. The management team wants the security team to implement a method to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. Which of the following would meet this objective?

A. UEFI
B. A hardware security module
C. eFUSE
D. Certificate signed updates

Answer: C

Explanation:
The correct answer is C. eFUSE. An eFUSE is a type of electronic fuse that can be programmed to permanently alter the functionality or configuration of a chipset. An eFUSE can be used to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset, by locking the firmware to a specific version or preventing unauthorized modifications. An eFUSE can also provide other benefits, such as anti-tampering, anti-counterfeiting, and device

authentication1.
* A. UEFI is not correct. UEFI stands for Unified Extensible Firmware Interface, and it is a standard that defines the software interface between an operating system and a platform firmware. UEFI can provide security features, such as secure boot, which verifies the integrity of the boot loader and prevents unauthorized code execution during the boot process. However, UEFI does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset2.
* B. A hardware security module is not correct. A hardware security module (HSM) is a physical device that provides secure storage and processing of cryptographic keys and operations. An HSM can protect sensitive data and transactions, such as encryption, decryption, signing, or verification, from unauthorized access or tampering. However, an HSM does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset3.
* D. Certificate signed updates are not correct. Certificate signed updates are a method of ensuring the authenticity and integrity of firmware updates by using digital certificates and signatures. Certificate signed updates can prevent malicious or corrupted firmware updates from being installed on the chipset, but they do not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. 1: What Is an eFUSE? 2: What Is UEFI? 3: What Is a Hardware Security Module (HSM)?

NEW QUESTION 68
A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance.
B. Implement blacklisting lor IP addresses from outside the county.
C. Implement strong authentication controls for at contractors.
D. Implement user behavior analytics tor key staff members.

Answer: A

Explanation:
A secure supply chain program is a set of processes and practices that aim to protect the supply chain from various risks, such as cyberattacks, data breaches, fraud, theft, sabotage, or natural disasters1. A secure supply chain program can help to ensure the integrity, availability, and confidentiality of the products, services, data, and systems involved in the supply chain. A secure supply chain program with governance means that there are clear roles, responsibilities, policies, procedures, and controls for managing the security of the supply chain. This can help to monitor and enforce the compliance of the third-party service provider with the requirement to source talent from its own country. A secure supply chain program with governance can also help to identify and mitigate any potential threats or vulnerabilities in the supply chain. Implementing blacklisting for IP addresses from outside the country (B) may not be sufficient or effective, as IP addresses can be spoofed or bypassed by attackers. Implementing strong authentication controls for all contractors © may not be relevant or adequate, as authentication controls do not prevent the sourcing of talent from other countries. Implementing user behavior analytics for key staff members (D) may not be applicable or useful, as user behavior analytics do not verify the origin or location of the talent.

NEW QUESTION 70
An incident response plan requires systems that contain critical data to be triaged first in the event of a compromise. Which of the following types of data would most likely be classified as critical?

A. Encrypted data
B. data
C. Masked data
D. Marketing data

Answer: B

Explanation:
PII stands for personally identifiable information, and it is any data that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, or biometric data. PII data is considered critical because it can be used by attackers to commit identity theft, fraud, or other crimes. PII data is also subject to various laws and regulations that require organizations to protect it from unauthorized access, use, or disclosure1.

NEW QUESTION 72
An organization announces that all employees will need to work remotely for an extended period of time. All employees will be provided with a laptop and supported hardware to facilitate this requirement. The organization asks the information security division to reduce the risk during this time. Which of the following is a technical control that will reduce the risk of data loss if a laptop is lost or stolen?

A. Requiring the use of the corporate VPN
B. Requiring the screen to be locked after five minutes of inactivity
C. Requiring the laptop to be locked in a cabinet when not in use
D. Requiring full disk encryption

Answer: D

Explanation:
Full disk encryption (FDE) is a technical control that encrypts all the data on a disk drive, including the operating system and applications. FDE prevents unauthorized access to the data if the disk drive is lost or stolen, as it requires a password or key to decrypt the data. FDE can be implemented using software or hardware solutions and can protect data at rest on laptops and other devices. The other options are not technical controls or do not reduce the risk of data loss if a laptop is lost or stolen. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

NEW QUESTION 76
A security analyst responds to a series of events surrounding sporadic bandwidth consumption from an endpoint device. The security analyst then identifies the following additional details:
• Bursts of network utilization occur approximately every seven days.
• The content being transferred appears to be encrypted or obfuscated.
• A separate but persistent outbound TCP connection from the host to infrastructure in a third-party cloud is in place.
• The HDD utilization on the device grows by 10GB to 12GB over the course of every seven days.
• Single file sizes are 10GB.

Which of the following describes the most likely cause of the issue?

A. Memory consumption
B. Non-standard port usage
C. Data exfiltration
D. System update
E. Botnet participant

Answer: C

Explanation:
data exfiltration is the unauthorized transfer of data from an organization's network to an external destination, usually for malicious purposes such as espionage, sabotage, or theft. The details given in the question suggest that data exfiltration is occurring from an endpoint device. The bursts of network utilization every seven days indicate periodic data transfers. The content being transferred appears to be encrypted or obfuscated to avoid detection or analysis. The persistent outbound TCP connection from the host to infrastructure in a third-party cloud indicates a possible command and control channel for an attacker. The HDD utilization on the device grows by 10GB to 12GB over the course of every seven days, and single file sizes are 10GB, indicating that large amounts of data are being collected and compressed before being exfiltrated.

NEW QUESTION 77
During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideralion Wtiich of the following are part of a known threat modeling method?

A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans
B. Purpose, objective, scope, (earn management, cost, roles and responsibilities
C. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege
D. Human impact, adversary's motivation, adversary's resources, adversary's methods

Answer: C

Explanation:
Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege are part of a known threat modeling method called STRIDE. STRIDE is a mnemonic that stands for six categories of threats that can affect the security of a system or application. STRIDE was developed by Microsoft in 1999 and has been widely adopted as a threat modeling method by many organizations. STRIDE can help identify and prioritize potential threats based on their impact and likelihood1.

NEW QUESTION 81
A company's Chief Information Security Officer [CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the best technique to address the ClSO's concerns?

A. Configure DLP to reject all changes to the files without pre-authorizatio
B. Monitor the files for unauthorized changes.
C. Regularly use SHA-256 to hash the directory containing the sensitive informatio
D. Monitor the files for unauthorized changes.
E. Place a legal hold on the files Require authorized users to abide by a strict time context access policy.Monitor the files for unauthorized changes.
F. Use Wireshark to scan all traffic to and from the director
G. Monitor the files for unauthorized changes.

Answer: B

Explanation:
Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes. This option is the best technique to ensure the integrity of the files and tie any changes to a specific user session. Hashing is a process that generates a unique value for a given input, and any modification to the input will result in a different hash value. By using SHA-256, which is a secure hashing algorithm, the analyst can compare the hash values of the files before and after each user session and detect any unauthorized changes.

NEW QUESTION 82
A Chief Executive Officer (CEO) is concerned the company will be exposed to data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

A. Data masking procedures
B. Enhanced encryption functions
C. Regular business impact analysis functions
D. Geographic access requirements

Answer: D

Explanation:
Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner. You're only worried about that if you're in multiple locations. .
https://www.virtru.com/blog/gdpr-data-sovereignty-matters-globally
Geographic access requirements are an appropriate technical control to implement to mitigate data sovereignty issues. Data sovereignty issues arise when data is subject to different laws and regulations depending on where it is stored or processed. For example, some countries may have stricter data protection or privacy laws than others, or may impose restrictions on cross-border data transfers. Geographic access requirements can help ensure that data is only accessed from locations that comply with the applicable laws and regulations, and prevent unauthorized access from locations that do not.

NEW QUESTION 86
A security analyst who works in the SOC receives a new requirement to monitor for indicators of compromise. Which of the following is the first action the analyst should take in this situation?

A. Develop a dashboard to track the indicators of compromise.
B. Develop a query to search for the indicators of compromise.
C. Develop a new signature to alert on the indicators of compromise.
D. Develop a new signature to block the indicators of compromise.

Answer: B

Explanation:
Developing a query to search for the indicators of compromise is the first action the analyst should take in this situation. Indicators of compromise (IOCs) are pieces of information that suggest a system or network has been compromised by an attacker. IOCs can include IP addresses, domain names, file hashes, URLs, or other artifacts that are associated with malicious activity. Developing a query to search for IOCs can help to identify any potential incidents or threats in the environment and initiate further investigation or response .

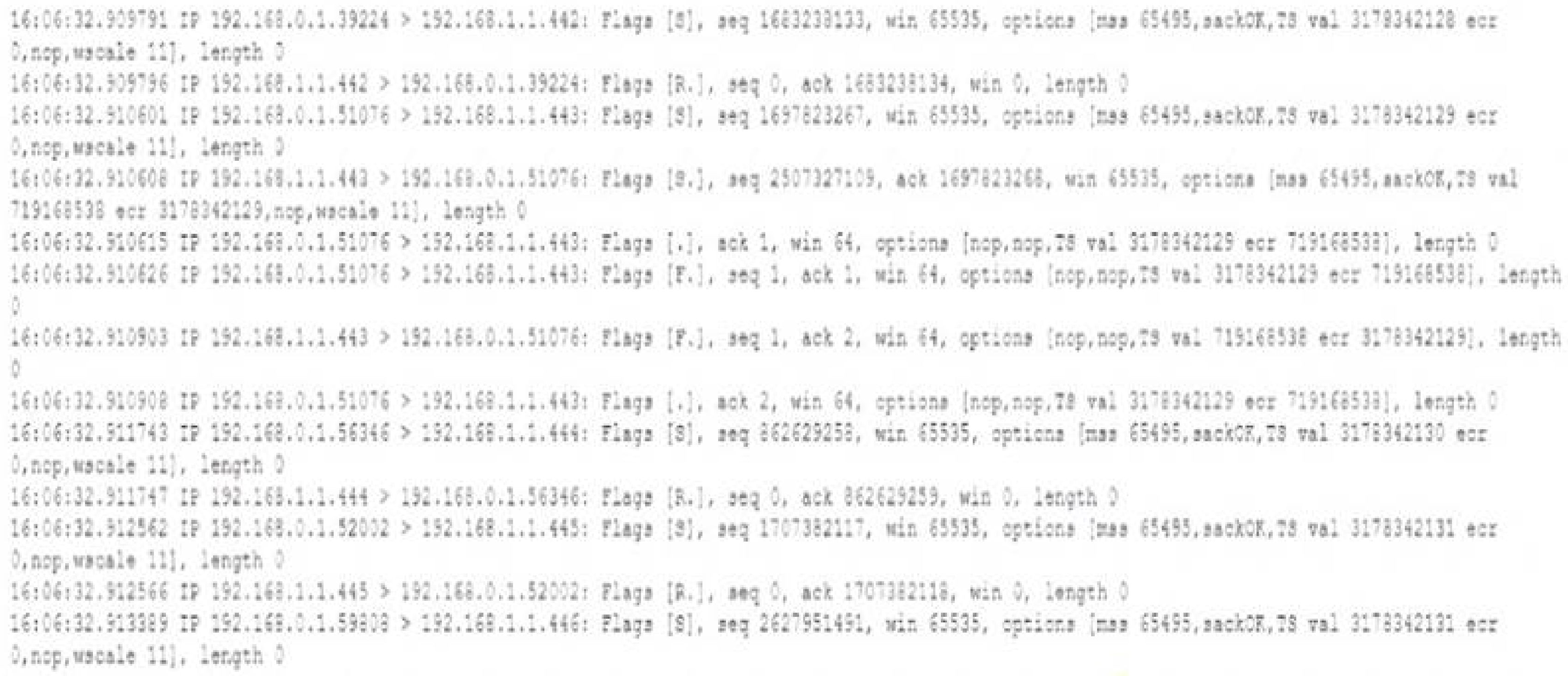
NEW QUESTION 89
A security analyst notices the following entry while reviewing the server togs OR 1=1' ADD USER attacker' PW 1337password' ---Which of the following events occurred?

A. CSRF
B. XSS
C. SQLi
D. RCE

Answer: C

Explanation:
SQLi stands for SQL injection, which is a type of attack that injects malicious SQL statements into a web application’s input fields or parameters. The attacker can use SQLi to execute unauthorized commands on the database server, such as adding a new user or retrieving sensitive data. The entry in the server logs shows an example of a SQLi attack that tries to add a new user named attacker with the password 1337password. CSRF, XSS, and RCE are other types of attacks, but they do not match the description of the entry in the server logs. Reference: https://owasp.org/www-community/attacks/SQL_Injection

NEW QUESTION 93
A security analyst is reviewing the output of tcpdump to analyze the type of activity on a packet capture:



```
16:06:32.909791 IP 192.168.0.1.39224 > 192.168.1.1.442: Flags [S], seq 1683238133, win 65535, options [mss 65495,sackOK,TS val 3178342128 ecr
0,nop,wscale 11], length 0
16:06:32.909796 IP 192.168.1.1.442 > 192.168.0.1.39224: Flags [R.], seq 0, ack 1683238134, win 0, length 0
16:06:32.910601 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [S], seq 1697823267, win 65535, options [mss 65495,sackOK,TS val 3178342129 ecr
0,nop,wscale 11], length 0
16:06:32.910608 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [S.], seq 2507327109, ack 1697823268, win 65535, options [mss 65495,sackOK,TS val
719168538 ecr 3178342129,nop,wscale 11], length 0
16:06:32.910615 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.910626 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [F.], seq 1, ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length
0
16:06:32.910903 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [F.], seq 1, ack 2, win 64, options [nop,nop,TS val 719168538 ecr 3178342129], length
0
16:06:32.910908 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 2, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.911743 IP 192.168.0.1.56346 > 192.168.1.1.444: Flags [S], seq 862629258, win 65535, options [mss 65495,sackOK,TS val 3178342130 ecr
0,nop,wscale 11], length 0
16:06:32.911747 IP 192.168.1.1.444 > 192.168.0.1.56346: Flags [R.], seq 0, ack 862629259, win 0, length 0
16:06:32.912562 IP 192.168.0.1.52002 > 192.168.1.1.445: Flags [S], seq 1707382117, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr
0,nop,wscale 11], length 0
16:06:32.912566 IP 192.168.1.1.445 > 192.168.0.1.52002: Flags [R.], seq 0, ack 1707382118, win 0, length 0
16:06:32.913389 IP 192.168.0.1.59808 > 192.168.1.1.446: Flags [S], seq 2627951491, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr
0,nop,wscale 11], length 0
```

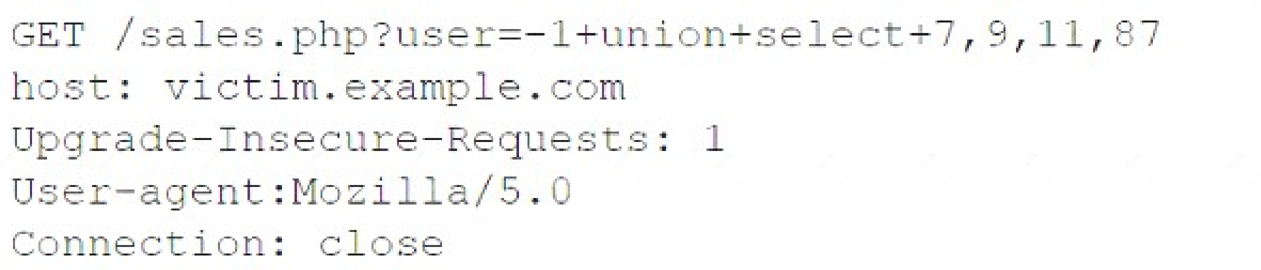
Which of the following generated the above output?

A. A port scan
B. A TLS connection
C. A vulnerability scan
D. A ping sweep

Answer: B

Explanation:
A port scan generated the output. A port scan is a type of attack that probes a host or a network for open ports or services. A port scan can help an attacker discover potential vulnerabilities or entry points for further exploitation. The output shows that tcpdump captured packets with different flags, such as SYN, ACK, RST, and FIN, which indicate different stages of the TCP three-way handshake or connection termination. The output also shows that the source IP address 192.168.1.100 sent packets to different destination ports on the target IP address 192.168.1.101, such as 22, 23, 25, 80, and 443. These are common ports that an attacker would scan to find out what services are running on the target.

NEW QUESTION 97
A security analyst is investigating a data leak on a corporate website. The attacker was able to dump data by sending a crafted HTTP request with the following payload:



```
GET /sales.php?user=-1+union+select+7,9,11,87
host: victim.example.com
Upgrade-Insecure-Requests: 1
User-agent:Mozilla/5.0
Connection: close
```

Which of the following systems would most likely have logs with details regarding the threat actor's requests?

A. Cloud WAF
B. Internal proxy
C. TAXII server
D. Hardware security module

Answer: A

Explanation:
The correct answer is A. Cloud WAF. A cloud WAF stands for a cloud-based web application firewall, and it is a service that protects web applications from common attacks, such as SQL injection, cross-site scripting, or denial-of-service. A cloud WAF can inspect and filter HTTP requests and responses between the web application and the internet, and block or allow them based on predefined or custom rules. A cloud WAF can also generate logs with details regarding the threat actor's requests, such as the source IP address, the destination URL, the payload, the rule triggered, and the action taken1.
* B. Internal proxy is not correct. An internal proxy is a server that acts as an intermediary between internal clients and external servers. An internal proxy can provide various functions, such as caching, filtering, authentication, or encryption. An internal proxy can also generate logs with details regarding the client's requests, such as the source IP address, the destination URL, the protocol used, and the response received2. However, an internal proxy would not have logs with details regarding the threat actor's requests, as they are directed to the web application, not to the internal proxy.
* C. TAXII server is not correct. TAXII stands for Trusted Automated eXchange of Intelligence Information, and it is a standard that defines how to exchange cyber threat intelligence (CTI) between different systems or organizations. TAXII uses a client-server model, where a TAXII client can request or send CTI to a TAXII server using predefined services and messages. A TAXII server can store and provide CTI in a structured and standardized format3. However, a TAXII server would not have logs with details regarding the threat actor's requests, as they are not related to CTI exchange.
* D. Hardware security module is not correct. A hardware security module (HSM) is a physical device that provides secure storage and processing of cryptographic keys and operations. An HSM can protect sensitive data and transactions, such as encryption, decryption, signing, or verification, from unauthorized access or tampering. However, an HSM would not have logs with details regarding the threat actor's requests, as they are not related to cryptographic operations.
* 1: What Is a Cloud-Based Web Application Firewall (WAF)? 2: What Is a Proxy Server? 3: What Is T
[What Is a Hardware Security Module (HSM)?]

NEW QUESTION 99
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issued mobile device while connected to the network. Which of the following actions would help during the forensic analysis of the mobile device? (Select TWO).

A. Resetting the phone to factory settings
B. Rebooting the phone and installing the latest security updates
C. Documenting the respective chain of custody
D. Uninstalling any potentially unwanted programs
E. Performing a memory dump of the mobile device for analysis
F. Unlocking the device by browsing the eFuse

Answer: CE

Explanation:
Documenting the chain of custody is an important step in the forensic analysis of any device, as it helps to ensure that all evidence is collected and preserved correctly. A memory dump is also essential, as it can provide information about the state of the device when the attack occurred and can be used for further analysis.
Documenting the respective chain of custody can help to preserve the integrity and admissibility of the evidence collected from the mobile device during the forensic analysis. Chain of custody is a record of who handled, accessed or modified the evidence, when, where, how and why . Performing a memory dump of the mobile device for analysis can help to extract volatile data from the mobile device that may contain valuable information about the ransomware attack, such as processes, network connections or encryption keys. Memory dump is a process of copying the contents of the memory (RAM) to a file or storage device .
References: https://www.techopedia.com/definition/23371/chain-of-custody https://www.techopedia.com/definition/10339/memory-dump

NEW QUESTION 104
A manufacturing company uses a third-party service provider lor Tier 1 security support One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance
B. Implement blacklisting for IP addresses from outside the country
C. Implement strong authentication controls for all contractors
D. Implement user behavior analytics for key staff members

Answer: A

Explanation:
Implementing a secure supply chain program with governance would be the best way to ensure the third-party service provider meets the requirement of only sourcing talent from its own country. A secure supply chain program is a set of policies, procedures, and controls that aim to protect the integrity and security of the products and services delivered by third-party vendors. A secure supply chain program can help mitigate the risks of geopolitical and national security interests by verifying the origin, identity, and trustworthiness of the vendors and their employees1. Governance is a key component of a secure supply chain program, as it provides oversight, accountability, and enforcement of the policies and procedures.

NEW QUESTION 105

To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

A. SCAP
B. SAST
C. DAST
D. DACS

Answer: A

Explanation:
SCAP is a protocol designed to assess the security compliance of computers and other devices. It works by scanning systems against security policies, and can help verify that the scanned device meets security requirements. Here is a link to the CompTIA CySA+ Guide's Chapter 5 - Access Controls for more information: https://certification.comptia.org/docs/default-source/exam-objectives/cs0-002.pdf

NEW QUESTION 108
A company's application development has been outsourced to a third-party development team. Based on the SLA. The development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

A. Input validation
B. Security regression testing
C. Application fuzzing
D. User acceptance testing
E. Stress testing

Answer: B

Explanation:
Detailed
Security regression testing is a type of testing that verifies that the security features and functionality of an application are not compromised or broken by any changes or updates in the code2. Security regression testing can help to ensure that the application follows industry best practices for secure coding and does not introduce any new vulnerabilities or weaknesses. Security regression testing can be performed manually or automatically using tools or scripts that check for common security flaws and compliance with security standards. Security regression testing can also help to validate the error-handling capabilities of an application by testing how it responds to different types of inputs and scenarios. Input validation (A) is a technique that checks whether the inputs to an application are valid and expected before processing them3. Input validation can help to prevent some types of security attacks, such as injection attacks or buffer overflows, but it is not a way to verify that an application follows industry best practices for secure
coding. Input validation is part of secure coding, not a way to test it. Application fuzzing © is a technique that tests an application by sending random or malformed inputs to it and observing its behavior4. Application fuzzing can help to discover some types of security vulnerabilities, such as memory leaks or crashes, but it is not a comprehensive way to verify that an application follows industry best practices for secure coding. Application fuzzing may not cover all possible inputs and scenarios and may not check for compliance with security standards. User acceptance testing (D) is a technique that tests an application by involving end users or customers in evaluating its functionality and usability. User acceptance testing can help to ensure that an application meets the user requirements and expectations, but it is not a reliable way to verify that an application follows industry best practices for secure coding. User acceptance testing may not focus on security aspects and may not detect subtle or hidden security flaws. Stress testing (E) is a technique that tests an application by subjecting it to high levels of load or demand. Stress testing can help to evaluate the performance and reliability of an application under extreme conditions, but it is not a relevant way to verify that an application follows industry best practices for secure coding. Stress testing does not check for security issues and may not reflect normal usage patterns.
References: 2: https://www.techopedia.com/definition/31686/resource-exhaustion 3: https://www.techopedia.com/definition/13493/penetration-testing 4: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl : https://www.techopedia.com/definition/24771/technical-controls : https://www.techopedia.com/definition/32088/vm-escape

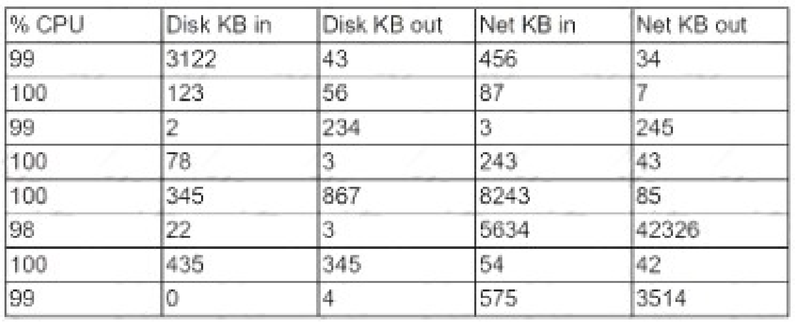
NEW QUESTION 111
The Chief Information Security Officer (CISO) of a large financial institution is seeking a solution that will block a predetermined set of data points from being transferred or downloaded by employees. The CISO also wants to track the data assets by name, type, content, or data profile.
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 112
A security analyst is reviewing the following server statistics:



% CPU	Disk KB in	Disk KB out	Net KB in	Net KB out
99	3122	43	456	34
100	123	56	87	7
99	2	234	3	245
100	78	3	243	43
100	345	867	8243	85
98	22	3	5634	42326
100	435	345	54	42
99	0	4	575	3514

Which of the following Is MOST likely occurring?

A. Race condition
B. Privilege escalation
C. Resource exhaustion
D. VM escape

Answer: C

Explanation:
Resource exhaustion occurs when a system runs out of resources such as memory, CPU, disk space, or network bandwidth due to excessive demand or poor management1. In this case, the server statistics show that the CPU usage is 100%, the memory usage is 99%, and the disk usage is 98%, indicating that the system is suffering from resource exhaustion. This can affect the performance and availability of the system and its applications. A race condition (A) is a condition where the system's behavior depends on the sequence or timing of other uncontrollable events2. Privilege escalation (B) is a situation where an attacker gains unauthorized access to higher privileges or permissions on a system3. VM escape (D) is a technique where an attacker breaks out of a virtual machine and interacts with the host operating system.
References: 1: https://www.techopedia.com/definition/31686/resource-exhaustion 2: https://en.wikipedia.org/wiki/Race_condition 3: https://www.techopedia.com/definition/4111/privilege-escalation : https://www.techopedia.com/definition/32088/vm-escape

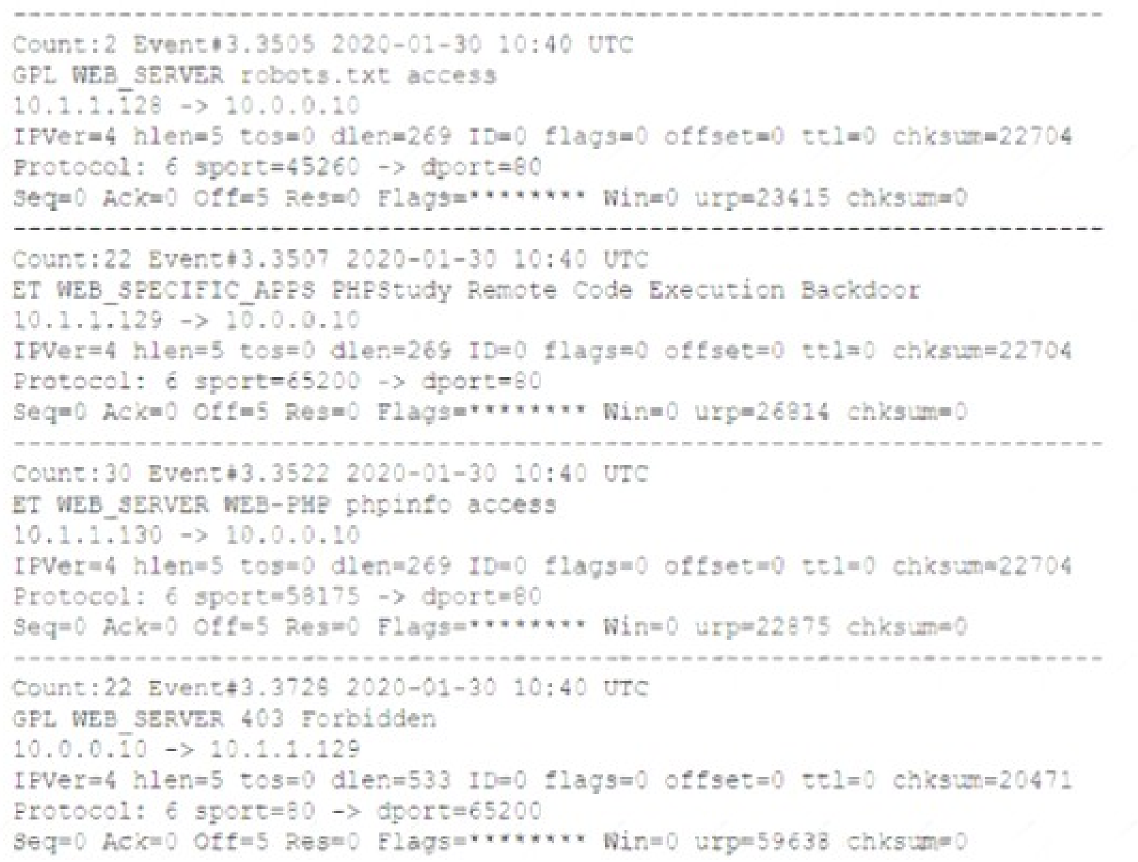
NEW QUESTION 116
In web application scanning, static analysis refers to scanning:

A. the system for vulnerabilities before installing the application.
B. the compiled code of the application to detect possible issues.
C. an application that is installed and active on a system.
D. an application that is installed on a system that is assigned a static IP.

Answer: B

Explanation:
This type of analysis is performed before the application is installed and active on a system, and it involves
examining the code without actually executing it in order to identify potential vulnerabilities or security risks.
As per CYSA+ 002 Study Guide: Static analysis is conducted by reviewing the code for an application. Static analysis does not run the program; instead, it focuses on understanding how the program is written and what the code is intended to do.
Static analysis refers to scanning the source code or the compiled code of an application without executing it, to identify potential vulnerabilities, errors, or bugs. Static analysis can help improve the quality and security of the code before it is deployed or run4

NEW QUESTION 117
A security analyst is reviewing the network security monitoring logs listed below:



```
------------------------------------------------------------------------
Count:2 Event#3.3505 2020-01-30 10:40 UTC
GPL WEB_SERVER robots.txt access
10.1.1.128 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=45260 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=23415 chksum=0
------------------------------------------------------------------------
Count:22 Event#3.3507 2020-01-30 10:40 UTC
ET WEB_SPECIFIC_APPS PHPStudy Remote Code Execution Backdoor
10.1.1.129 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=65200 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=26814 chksum=0
------------------------------------------------------------------------
Count:30 Event#3.3522 2020-01-30 10:40 UTC
ET WEB_SERVER WEB-PHP phpinfo access
10.1.1.130 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=58175 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=22875 chksum=0
------------------------------------------------------------------------
Count:22 Event#3.3728 2020-01-30 10:40 UTC
GPL WEB_SERVER 403 Forbidden
10.0.0.10 -> 10.1.1.129
IPVer=4 hlen=5 tos=0 dlen=533 ID=0 flags=0 offset=0 ttl=0 chksum=20471
Protocol: 6 sport=80 -> dport=65200
Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=59638 chksum=0
```

Which of the following is the analyst most likely observing? (Select two).

A. 10.1.1.128 sent potential malicious traffic to the web server.
B. 10.1.1.128 sent malicious requests, and the alert is a false positive
C. 10.1.1.129 successfully exploited a vulnerability on the web server
D. 10.1.1.129 sent potential malicious requests to the web server
E. 10.1.1.129 can determine mat port 443 is being used
F. 10.1.1.130 can potentially obtain information about the PHP version

Answer: DF

Explanation:
A security analyst is reviewing the network security monitoring logs listed below and is most likely observing that 10.1.1.129 sent potential malicious requests to the web server and that 10.1.1.130 can potentially obtain information about the PHP version. The logs show that 10.1.1.129 sent two requests to the web server with suspicious parameters, such as "union select" and "or 1=1", which are commonly used for SQL injection attacks. The logs also show that 10.1.1.130 sent a request to the web server with a parameter "phpinfo", which is a function that displays information about the PHP configuration and environment, which can be useful for attackers to find vulnerabilities or exploit them. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://owasp.org/www-community/attacks/SQL_Injection; https://www.php.net/manual/en/function.phpinfo.php

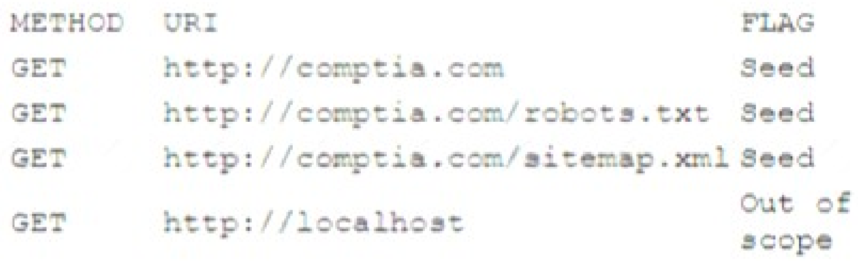
NEW QUESTION 122
A forensics investigator is analyzing a compromised workstation. The investigator has cloned the hard drive and needs to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive that was collected as evidence. Which of the following should the investigator 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 124
A security analyst is analyzing the following output from the Spider tab of OWASP ZAP after a vulnerability scan was completed:



METHOD	URI	FLAG
GET	http://comptia.com	Seed
GET	http://comptia.com/robots.txt	Seed
GET	http://comptia.com/sitemap.xml	Seed
GET	http://localhost	Out of scope

Which of the following options can the analyst conclude based on the provided output?

A. The scanning vendor used robots to make the scanning job faster
B. The scanning job was successfully completed, and no vulnerabilities were detected
C. The scanning job did not successfully complete due to an out of scope error
D. The scanner executed a crawl process to discover pages to be assessed

Answer: D

Explanation:
The output shows the result of using OWASP ZAP’s Spider tab after a vulnerability scan was completed. The Spider tab allows users to crawl web applications and discover pages and resources that can be assessed for vulnerabilities. The output shows that the scanner discovered various pages under different directories, such as /admin/, /blog/, /contact/, etc., as well as some parameters and forms that can be used for testing inputs and outputs. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://www.zaproxy.org/docs/desktop/start/features/spider/

NEW QUESTION 127
Which of the following is the BEST option to protect a web application against CSRF attacks?

A. Update the web application to the latest version.
B. Set a server-side rate limit for CSRF token generation.
C. Avoid the transmission of CSRF tokens using cookies.
D. Configure the web application to only use HTTPS and TLS 1.3.

Answer: C

Explanation:
CSRF tokens are random values that are generated by the server and included in requests that perform
state-changing actions. They are used to prevent CSRF attacks by verifying that the request originates from a legitimate source. However, if the CSRF tokens are transmitted using cookies, they are vulnerable to being stolen or forged by an attacker who can exploit other vulnerabilities, such as cross-site scripting (XSS) or cookie injection. Therefore, a better option is to avoid the transmission of CSRF tokens using cookies and use other methods, such as hidden form fields or custom HTTP headers. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 11;
https://owasp.org/www-community/attacks/csrf

NEW QUESTION 129
A security analyst is designing firewall rules to prevent external IP spoofing Which of the following explains the firewall rule for mitigation?

A. Packets with external source IP addresses do not enter the network from either direction.
B. Packets with internal source IP addresses do not enter the network from the outside.
C. Packets with internal source IP addresses do not exit the network from the inside.
D. Packets with public IP addresses do not pass through the router in either direction.

Answer: B

Explanation:
Packets with internal source IP addresses do not enter the network from the outside. This firewall rule can prevent external IP spoofing, which is an attack technique that involves forging the source IP address of a packet to impersonate another host or network. By blocking packets with internal source IP addresses from entering the network from the outside, the firewall can filter out spoofed packets that claim to originate from the internal network.

NEW QUESTION 134

Which of the following would best protect sensitive data If a device is stolen?

A. Remote wipe of drive
B. Self-encrypting drive
C. Password-protected hard drive
D. Bus encryption

Answer: B

Explanation:
A self-encrypting drive is a type of hard drive that automatically encrypts and decrypts data using a hardware-based mechanism. A self-encrypting drive can best protect sensitive data if a device is stolen, because it prevents unauthorized access to the data without the proper encryption key or password.

NEW QUESTION 137
Which of the following software assessment methods world peak times?

A. Security regression testing
B. Stress testing
C. Static analysis testing
D. Dynamic analysis testing
E. User acceptance testing

Answer: B

Explanation:
Stress testing is a software assessment method that tests how an application performs under peak times or extreme workloads. Stress testing can help to identify any performance issues, bottlenecks, errors or crashes that may occur when an application faces high demand or concurrent users. Stress testing can also help to determine the maximum capacity and scalability of an application .

NEW QUESTION 138
Wncn ol the following provides an automated approach 10 checking a system configuration?

A. SCAP
B. CI/CD
C. OVAL
D. Scripting
E. SOAR

Answer: A

Explanation:
SCAP stands for Security Content Automation Protocol, which is a set of standards and specifications that allows automated configuration and vulnerability management of systems. SCAP provides an automated approach to checking a system configuration by using standardized expressions and formats to evaluate the system’s compliance with predefined policies or benchmarks. CI/CD, OVAL, scripting, or SOAR are other terms related to automation or security, but they do not provide an automated approach to checking a system configuration. Reference: https://csrc.nist.gov/projects/security-content-automation-protocol

NEW QUESTION 141
A business recently acquired a software company. The software company's security posture is unknown. However, based on an assessment, there are limited security controls. No significant security monitoring exists. Which of the following is the NEXT step that should be completed to obtain information about the software company's security posture?

A. Develop an asset inventory to determine the systems within the software company
B. Review relevant network drawings, diagrams and documentation
C. Perform penetration tests against the software company's Internal and external networks
D. Baseline the software company's network to determine the ports and protocols in use.

Answer: A

Explanation:
An asset inventory is a list of all the hardware, software, data, and other resources that an organization owns or uses. An asset inventory helps to identify what systems are present in an organization, where they are located, what they do, and how they are configured2
Developing an asset inventory is the next step that should be completed to obtain information about the software company’s security posture, as it provides a baseline for further analysis and assessment of the systems’ vulnerabilities and risks.

NEW QUESTION 142
Which of the following are important reasons for performing proactive threat-hunting activities7 (Select two).

A. To ensure all alerts are fully investigated
B. To test incident response capabilities
C. To uncover unknown threats
D. To allow alerting rules to be more specific
E. To create a new security baseline
F. To improve user awareness about security threats

Answer: CE

Explanation:
Proactive threat-hunting is the process of actively searching for unknown threats in the network, rather than waiting for alerts or indicators of compromise. Some of

the important reasons for performing proactive
threat-hunting activities are:

- To uncover unknown threats that may have evaded detection by existing security tools or controls, and to mitigate them before they cause damage or data loss.
- To create a new security baseline that reflects the current state of the network, and to identify any anomalies or deviations from the normal behavior or activity.

NEW QUESTION 143

A company uses an FTP server to support its critical business functions The FTP server is configured as follows:

• The FTP service is running with (he data duectory configured in /opt/ftp/data.
• The FTP server hosts employees' home aVectories in /home
• Employees may store sensitive information in their home directories

An loC revealed that an FTP director/ traversal attack resulted in sensitive data loss Which of the following should a server administrator implement to reduce the risk of current and future directory traversal attacks targeted at the FTP server?

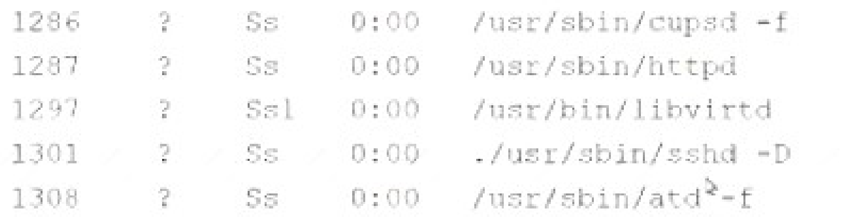
A. Implement file-level encryption of sensitive files
B. Reconfigure the FTP server to support FTPS
C. Run the FTP server n a chroot environment
D. Upgrade the FTP server to the latest version

Answer: C

Explanation:
This would limit the FTP server’s access to a specific directory tree and prevent directory traversal attacks that could access files outside of that tree. Implementing file-level encryption, supporting FTPS, or upgrading the FTP server would not prevent directory traversal attacks.

NEW QUESTION 144

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output:



```
1286    ?    Ss     0:00   /usr/sbin/cupsd -f
1287    ?    Ss     0:00   /usr/sbin/httpd
1297    ?    Ssl    0:00   /usr/bin/libvirtd
1301    ?    Ss     0:00   ./usr/sbin/sshd -D
1308    ?    Ss     0:00   /usr/sbin/atd-f
```

Which of the following commands should the administrator run next to further analyze the compromised system?

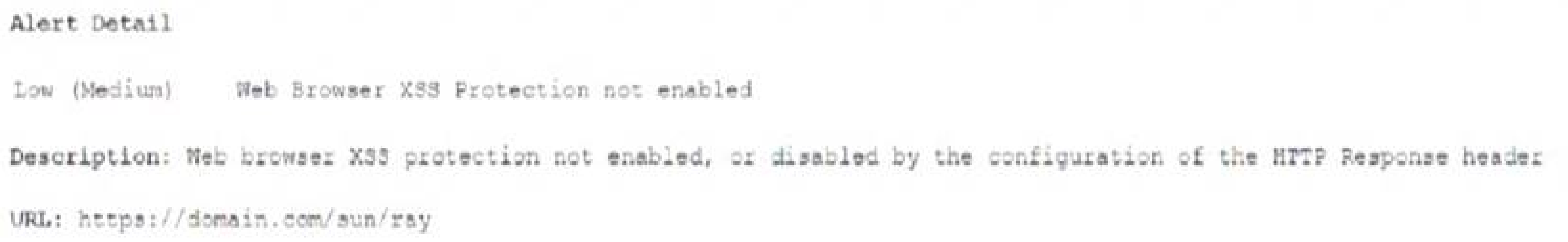
A. gbd /proc/1301
B. rpm -V openssh-server
C. /bin/Is -1 /proc/1301/exe
D. kill -9 1301

Answer: C

Explanation:
/bin/ls -1 /proc/1301/exe is the command that will show the absolute path to the executed binary file associated with the process ID 1301, which is ./usr/sbin/sshd. This information can help the security analyst determine if the binary is an official version and has not been modified, which could be an indicator of a compromise. /proc/1301/exe is a special symbolic link that points to the executable file that was used to start the process 1301 .

NEW QUESTION 146

A security analyst sees the following OWASP ZAP output from a scan that was performed against a modern version of Windows while testing for client-side vulnerabilities:



```
Alert Detail

Low (Medium)     Web Browser XSS Protection not enabled

Description: Web browser XSS protection not enabled, or disabled by the configuration of the HTTP Response header

URL: https://domain.com/sun/ray
```

Which of the following is the MOST likely solution to the listed vulnerability?

A. Enable the browser's XSS filter.
B. Enable Windows XSS protection
C. Enable the browser's protected pages mode
D. Enable server-side XSS protection

Answer: A

Explanation:
Enabling the browser’s XSS filter would be the most likely solution to the listed vulnerability. The vulnerability is a reflected cross-site scripting (XSS) attack, which occurs when a malicious script is injected into a web page that reflects user input back to the browser without proper validation or encoding. The malicious script can then execute in the browser and perform various actions, such as stealing cookies, redirecting to malicious sites, or displaying fake content2. Enabling the browser’s XSS filter can help prevent reflected XSS attacks by detecting and blocking malicious scripts before they execute in the browser3.

NEW QUESTION 150

While monitoring the information security notification mailbox, a security analyst notices several emails were repotted as spam. Which of the following should the analyst do FIRST?

A. Block the sender In the email gateway.
B. Delete the email from the company's email servers.
C. Ask the sender to stop sending messages.
D. Review the message in a secure environment.

Answer: D

Explanation:
The security analyst should review the message in a secure environment first. This will help determine if the message is indeed spam or if it contains any malicious content, such as malware attachments or phishing links. Reviewing the message in a secure environment means using a sandbox or an isolated system that can prevent any potential harm to the analyst’s system or network. If the message is confirmed to be spam or malicious, then the analyst can take further actions, such as blocking the sender, deleting the email, or notifying the users 3.

NEW QUESTION 154
A user reports a malware alert to the help desk. A technician verities the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access. The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do next?

A. Document the procedures and walk through the incident training guide.
B. Reverse engineer the malware to determine its purpose and risk to the organization.
C. Sanitize the workstation and verify countermeasures are restored.
D. Isolate the workstation and issue a new computer to the user.

Answer: C

Explanation:
Sanitizing the workstation and verifying countermeasures are restored are part of the eradication and recovery processes that the security analyst should perform next. Eradication is the process of removing malware or other threats from the affected systems, while recovery is the process of restoring normal operations and functionality to the affected systems. Sanitizing the workstation can involve deleting or wiping any malicious files or programs, while verifying countermeasures are restored can involve checking and updating any security controls or settings that may have been compromised .

NEW QUESTION 159
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.

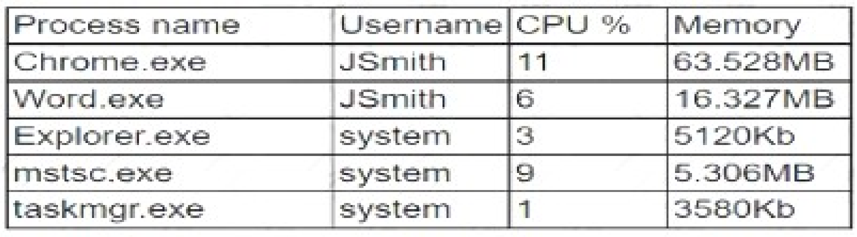
NEW QUESTION 160
Which of the following types of controls defines placing an ACL on a file folder?

A. Technical control
B. Confidentiality control
C. Managerial control
D. Operational control

Answer: A

Explanation:
"Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption."
A technical control is a type of control that uses technology or software to protect data and systems from unauthorized access or misuse3. A technical control can include encryption, authentication, firewalls, antivirus software, and other mechanisms that rely on hardware or software. Placing an ACL (access control list) on a file folder is an example of a technical control. An ACL is a list of permissions that specifies who can access or modify a file or folder4. An ACL can help to enforce confidentiality, integrity, and availability of data by restricting access to authorized users only.

NEW QUESTION 164
A company employee downloads an application from the internet. After the installation, the employee begins experiencing noticeable performance issues, and files are appearing on the desktop.



Process name	Username	CPU %	Memory
Chrome.exe	JSmith	11	63.528MB
Word.exe	JSmith	6	16.327MB
Explorer.exe	system	3	5120Kb
mstsc.exe	system	9	5.306MB
taskmgr.exe	system	1	3580Kb

Which of the following processes will the security analyst Identify as the MOST likely indicator of system compromise given the processes running in Task

Manager?

A. Chrome.exe
B. Word.exe
C. Explorer.exe
D. mstsc.exe
E. taskmgr.exe

Answer: D

Explanation:
mstsc.exe is the process name for Remote Desktop Connection, a program that allows users to connect to remote computers or servers over a network or the Internet12. mstsc.exe is an indicator of system compromise if the user did not initiate or authorize a remote connection, as it may mean that an attacker has gained access to the system and is using it to connect to other systems or exfiltrate data3.

NEW QUESTION 167
A threat intelligence group issued a warning to its members regarding an observed increase in attacks performed by a specific threat actor and the related loCs. Which is of the following is (he best method to operationalize these loCs to detect future attacks?

A. Analyzing samples of associated malware
B. Publishing an internal executive threat report
C. Executing an adversary emulation exercise
D. Integrating the company's SIEM platform

Answer: D

Explanation:
This is the best method to operationalize these loCs to detect future attacks because it allows the company to collect, correlate, analyze, and alert on the indicators of compromise (loCs) from various sources and systems. A SIEM stands for security information and event management, which is a software or service that provides centralized visibility and management of security events and data.

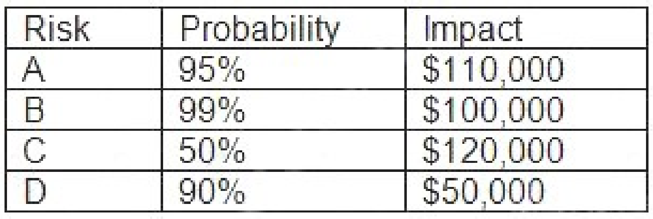
NEW QUESTION 170
An organization is developing software to match customers' expectations. Before the software goes into production, it must meet the following quality assurance guidelines
• Uncover all the software vulnerabilities.
• Safeguard the interest of the software's end users.
• Reduce the likelihood 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 174
An organization has the following risk mitigation policy:
Risks with a probability of 95% or greater will be addressed before all others regardless of the impact. All other prioritization will be based on risk value.
The organization has identified the following risks:



Risk	Probability	Impact
A	95%	$110,000
B	99%	$100,000
C	50%	$120,000
D	90%	$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, B, D, C
B. A, B, C, D
C. D, A, B, C
D. D, A, C, B

Answer: D

Explanation:
According to the risk mitigation policy, risks with a probability of 95% or greater will be addressed first, regardless of the impact. Therefore, risk D is the highest priority, as it has a probability of 95% and an impact of $100,000. The next priority is risk A, which has a probability of 90% and an impact of $200,000. The remaining risks will be prioritized based on their risk value, which is calculated by multiplying the probability and the impact. Risk C has a risk value of $40,000 (80% x $50,000), while risk B has a risk value of $30,000 (60% x $50,000). Therefore, risk C is higher priority than risk B.

NEW QUESTION 176
A company wants to ensure a third party does not take intellectual property and build a competing product. Which of the following is a non-technical data and privacy control that would best protect the company?

A. Data encryption
B. A non-disclosure agreement
C. Purpose limitation
D. Digital rights management

Answer: B

Explanation:
A non-disclosure agreement (NDA) is a legally binding contract that establishes a confidential relationship between two or more parties and prevents them from sharing or using certain information that is deemed sensitive, proprietary, or valuable1. An NDA can be used to protect intellectual property (IP) such as trade secrets, inventions, designs, or business plans from being disclosed to competitors or the public2.
A company that wants to ensure a third party does not take its IP and build a competing product can use an NDA to restrict the access, use, and disclosure of its IP by the third party. For example, if the company hires a contractor to develop a software application, the company can require the contractor to sign an NDA that prohibits the contractor from copying, modifying, selling, or revealing the source code or any other details of the application to anyone else3. The NDA can also specify the duration, scope, and consequences of the confidentiality obligation.

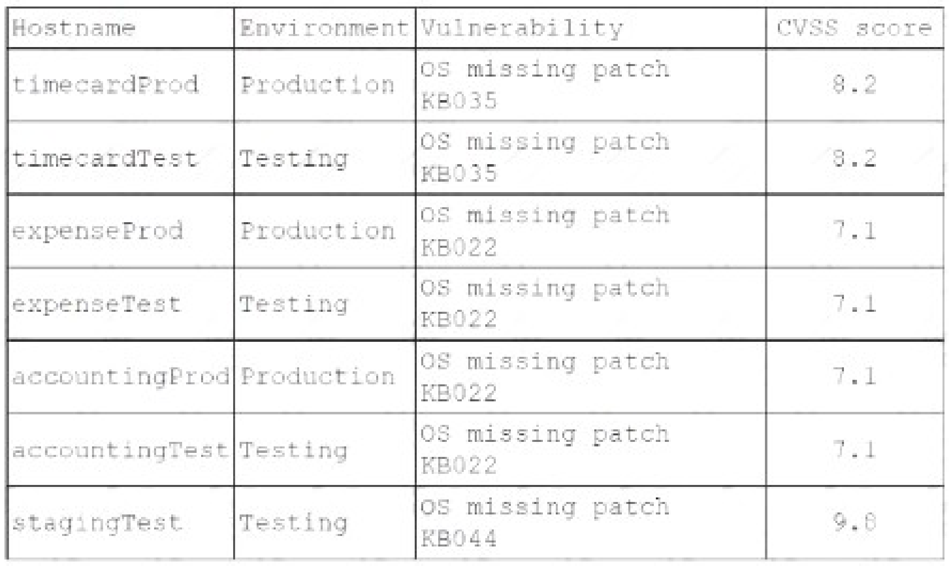
NEW QUESTION 180
White reviewing incident reports from the previous night, a security analyst notices the corporate websites were defaced with po mcai propaganda. Which of the following BEST Describes this type of actor?

A. Hacktivist
B. Nation-state
C. insider threat
D. Organized crime

Answer: A

Explanation:
A hacktivist is a type of actor who uses hacking techniques to promote a political or social cause or agenda. Hacktivists often target websites or systems of organizations or governments that they oppose or disagree with, and deface them with messages or propaganda related to their cause. In this case, the hacktivist defaced the corporate websites with political propaganda.

NEW QUESTION 185
An organization has the following vulnerability remediation policies:
• For production environment servers:
• Vulnerabilities with a CVSS score of 9.0 or greater must be remediated within 48 hours.
• Vulnerabilities with a CVSS score of 5.0 to 8.9 must be remediated within 96 hours.
• Vulnerabilities in lower environments may be left unremediated for up to two weeks.
* All vulnerability remediations must be validated in a testing environment before they are applied in the production environment.
The organization has two environments: production and testing. The accountingProd server is the only server that contains highly sensitive information.
A recent vulnerability scan provided the following report:



Hostname	Environment	Vulnerability	CVSS score
timecardProd	Production	OS missing patch KB035	8.2
timecardTest	Testing	OS missing patch KB035	8.2
expenseProd	Production	OS missing patch KB022	7.1
expenseTest	Testing	OS missing patch KB022	7.1
accountingProd	Production	OS missing patch KB022	7.1
accountingTest	Testing	OS missing patch KB022	7.1
stagingTest	Testing	OS missing patch KB044	9.8

Which of the following identifies the server that should be patched first? (Choose Two)

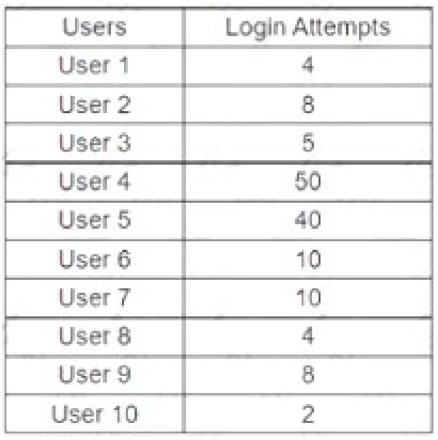
A. timecardProd
B. timecardTesl
C. expense Prod
D. expenseTest
E. accountingProd
F. accountingTest
G. stagingTest

Answer: CE

Explanation:
These servers should be patched first because they have vulnerabilities with CVSS scores of 9.0 and 8.9 respectively, which fall under the policy of remediating within 48 hours and 96 hours for production environment servers. The other servers either have lower CVSS scores, are in lower environments, or do not contain highly sensitive information.

NEW QUESTION 190

A cybersecurity analyst routinely checks logs, querying for login attempts. While querying for unsuccessful login attempts during a five-day period, the analyst produces the following report:



Users	Login Attempts
User 1	4
User 2	8
User 3	5
User 4	50
User 5	40
User 6	10
User 7	10
User 8	4
User 9	8
User 10	2

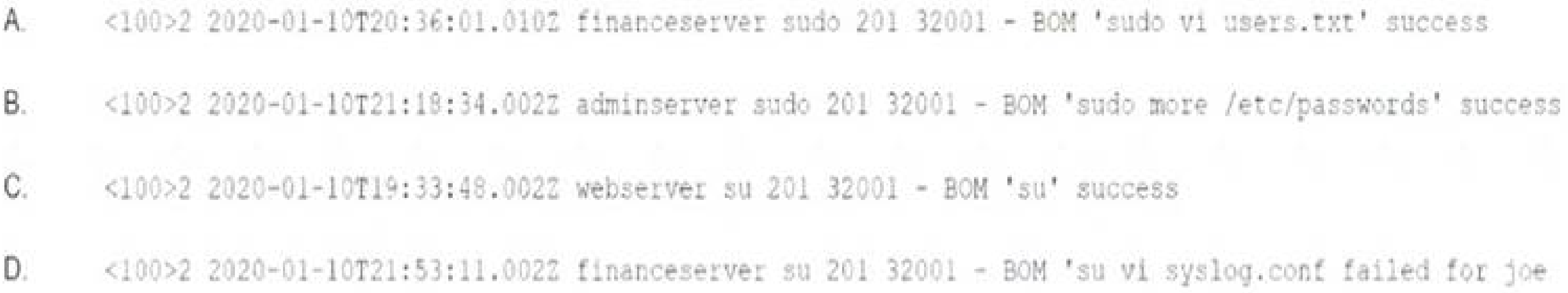
Which of the following BEST describes what the analyst Just found?

A. Users 4 and 5 are using their credentials to transfer files to multiple servers.
B. Users 4 and 5 are using their credentials to run an unauthorized scheduled task targeting some servers In the cloud.
C. An unauthorized user is using login credentials in a script.
D. A bot is running a brute-force attack in an attempt to log in to the domain.

Answer: C

Explanation:
A script is a program that can automate tasks or perform actions on a computer system. A script can be used to attempt multiple login attempts with different credentials, either randomly or from a list of known or guessed usernames and passwords. This can be done to gain unauthorized access to a system or to test its securit1y2.
Users 4 and 5 are not using their credentials to transfer files or run tasks, because the report shows that they have failed login attempts on multiple servers. If they were authorized users, they would not have failed login attempts. Also, transferring files or running tasks does not require multiple login attempts on different servers.
A bot is a software application that runs automated tasks over the Internet. A bot can also be used to perform brute-force attacks, which are repeated attempts to guess a password or other authentication
information. However, a bot would not use login credentials in a script, but rather generate random or common passwords to try3.

NEW QUESTION 192
An organization prohibits users from logging in to the administrator account. If a user requires elevated permissions. the user's account should be part of an administrator group, and the user should escalate permission only as needed and on a temporary basis. The organization has the following reporting priorities when reviewing system activity:
• Successful administrator login reporting priority - high
• Failed administrator login reporting priority - medium
• Failed temporary elevated permissions - low
• Successful temporary elevated permissions - non-reportable
A security analyst is reviewing server syslogs and sees the following: Which of the following events is the HIGHEST reporting priority?



```
A.    <100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success

B.    <100>2 2020-01-10T21:18:34.002Z adminserver sudo 201 32001 - BOM 'sudo more /etc/passwords' success

C.    <100>2 2020-01-10T19:33:48.002Z webserver su 201 32001 - BOM 'su' success

D.    <100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:
Option A shows a successful administrator login from an IP address that is not part of the organization’s network. This is a high reporting priority event, because it violates the organization’s policy that prohibits users from logging in to the administrator account and it could indicate a compromise of the administrator credentials or a malicious insider. Option B shows a failed administrator login from an IP address that is part of the organization’s network. This is a medium reporting priority event, because it could indicate an unauthorized attempt to access the administrator account. Option C shows a failed temporary elevated permission request from a user account that is part of the organization’s network. This is a low reporting priority event, because it could indicate a user error or a legitimate need for elevated permission that was denied. Option D shows a successful temporary elevated permission request from a user account that is part of the organization’s network. This is a non-reportable event, because it complies with the organization’s policy that allows users to escalate permission only as needed and on a temporary basis. Reference: https://www.sans.org/reading-room/whitepapers/logging/detecting-attacks-systems-microsoft-windows-event-lo

NEW QUESTION 193
Which of the following are considered PII by themselves? (Select TWO).

A. Government ID
B. Job title
C. Employment start date
D. Birth certificate

E. Employer address
F. Mother's maiden name

Answer: AD

Explanation:
PII (Personally Identifiable Information) is any information that can be used to identify, contact, or locate a specific individual, either by itself or when combined with other information1. PII by itself is information that can uniquely identify an individual without any additional information. Examples of PII by itself are:

- Government ID. A government ID is a number or code that is issued by a government authority to an individual for identification purposes. Examples of government IDs are social security numbers, passport numbers, driver's license numbers, etc. A government ID can uniquely identify an individual without any additional information.
- Birth certificate. A birth certificate is a document that records the birth of an individual and contains information such as name, date of birth, place of birth, parents' names, etc. A birth certificate can uniquely identify an individual without any additional information.

Other examples of PII by itself are biometric data, DNA profile, fingerprints, etc. Examples of information that are not PII by themselves are:

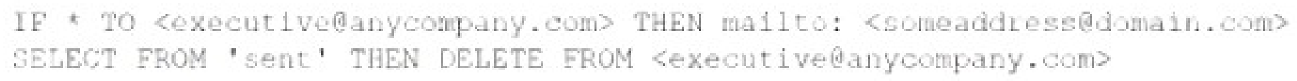
- Job title. A job title is a name or description of a position or role in an organization. A job title does not uniquely identify an individual without any additional information, as many individuals can have the same job title.
- Employment start date. An employment start date is the date when an individual began working for an organization. An employment start date does not uniquely identify an individual without any additional information, as many individuals can have the same employment start date.
- Employer address. An employer address is the location of an organization where an individual works.

An employer address does not uniquely identify an individual without any additional information, as many individuals can work at the same employer address.

- Mother's maiden name. A mother's maiden name is the surname that a woman had before she married.

A mother's maiden name does not uniquely identify an individual without any additional information, as many individuals can have the same mother's maiden name.
Other examples of information that are not PII by themselves are gender, race, ethnicity, age, etc.

NEW QUESTION 197
During an investigation, an analyst discovers the following rule in an executive's email client:



```
IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com>
SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com>
```

The executive is not aware of this rule. Which of the following should the analyst do first to evaluate the potential impact of this security incident?

A. Check the server logs to evaluate which emails were sent to <someaddress@domain,com>.
B. Use the SIEM to correlate logging events from the email server and the domain server.
C. Remove the rule from the email client and change the password.
D. Recommend that the management team implement SPF and DKIM.

Answer: A

Explanation:
Checking the server logs to evaluate which emails were sent to <someaddress@domain,com> is the first action the analyst should do to evaluate the potential impact of this security incident. Server logs are records of events or activities that occur on a server, such as email transactions, web requests, or authentication attempts. Checking the server logs can help to determine how many emails were sent to <someaddress@domain,com>, when they were sent, who sent them, and what they contained. This can help to assess the scope and severity of the incident and plan further actions .

NEW QUESTION 199
Which of the following are the most likely reasons to include reporting processes when updating an incident response plan after a breach? (Select two).

A. To use the SLA to determine when to deliver the report
B. To meet regulatory requirements for timely reporting
C. To limit reputation damage caused by the breach
D. To remediate vulnerabilities that led to the breach
E. To isolate potential insider threats
F. To provide secure network design changes

Answer: BC

Explanation:
According to the CompTIA CySA+ Study Guide Exam CS0-002, 2nd Edition1, reporting is an essential part of the incident response process. It helps communicate the details and impact of the incident to various stakeholders, such as management, customers, regulators, law enforcement, and the public. Reporting also provides valuable feedback and lessons learned that can improve the security posture and readiness of the organization.
Based on this information, the most likely reasons to include reporting processes when updating an incident response plan after a breach are:

- B. To meet regulatory requirements for timely reporting: Many industries and jurisdictions have laws and regulations that mandate reporting of security breaches within a certain time frame. Failing to comply with these requirements can result in fines, penalties, lawsuits, and loss of trust. Therefore, it is important to have a clear and consistent reporting process that ensures timely and accurate disclosure of the breach to the relevant authorities.
- C. To limit reputation damage caused by the breach: A security breach can have a negative impact on the reputation and credibility of the organization. Customers, partners, investors, and the public may lose confidence in the organization's ability to protect their data and interests. Therefore, it is important to have a transparent and honest reporting process that informs the affected parties about the nature, scope, and consequences of the breach, as well as the actions taken to mitigate and prevent future incidents. This can help restore trust and goodwill among the stakeholders.

NEW QUESTION 203
Which of the following are the MOST likely reasons lo include reporting processes when updating an incident response plan after a breach? (Select TWO).

A. To establish a clear chain of command
B. To meet regulatory requirements for timely reporting
C. To limit reputation damage caused by the breach

D. To remediate vulnerabilities that led to the breach
E. To isolate potential insider threats
F. To provide secure network design changes

Answer: BC

Explanation:
Reporting processes are important to include when updating an incident response plan after a breach for several reasons. Two of the most likely reasons are:

- To meet regulatory requirements for timely reporting. Many regulations and standards require organizations to report security incidents or breaches within a certain time frame or face penalties or sanctions. For example, the General Data Protection Regulation (GDPR) requires organizations to report personal data breaches within 72 hours of becoming aware of them. Reporting processes can help organizations to comply with these requirements by defining who, what, when, where, how, and why to report incidents or breaches.
- To limit reputation damage caused by the breach. Security incidents or breaches can have negative impacts on an organization’s reputation, trust, and customer loyalty. Reporting processes can help organizations to limit these impacts by communicating effectively and transparently with internal and external stakeholders, such as employees, customers, partners, regulators, media, and public. Reporting processes can help organizations to provide accurate and consistent information about the breach, its causes, impacts, and remediation actions.

Other possible reasons to include reporting processes when updating an incident response plan after a breach are:

- To establish a clear chain of command (A). Reporting processes can help organizations to establish a clear chain of command for incident response by defining roles and responsibilities, escalation procedures, and decision-making authority.
- To remediate vulnerabilities that led to the breach (D). Reporting processes can help organizations to remediate vulnerabilities that led to the breach by documenting and analyzing the root causes, lessons learned, and best practices for improvement.
- To isolate potential insider threats (E). Reporting processes can help organizations to isolate potential insider threats by monitoring and auditing user activities, behaviors, and access rights before, during, and after the breach.

References: : https://gdpr.eu/data-breach-notification/ : https://www.techopedia.com/definition/13493/penetration-testing : https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl

NEW QUESTION 208
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 211
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CS0-002 Practice Exam Features:

* CS0-002 Questions and Answers Updated Frequently

* CS0-002 Practice Questions Verified by Expert Senior Certified Staff

* CS0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The CS0-002 Practice Test Here