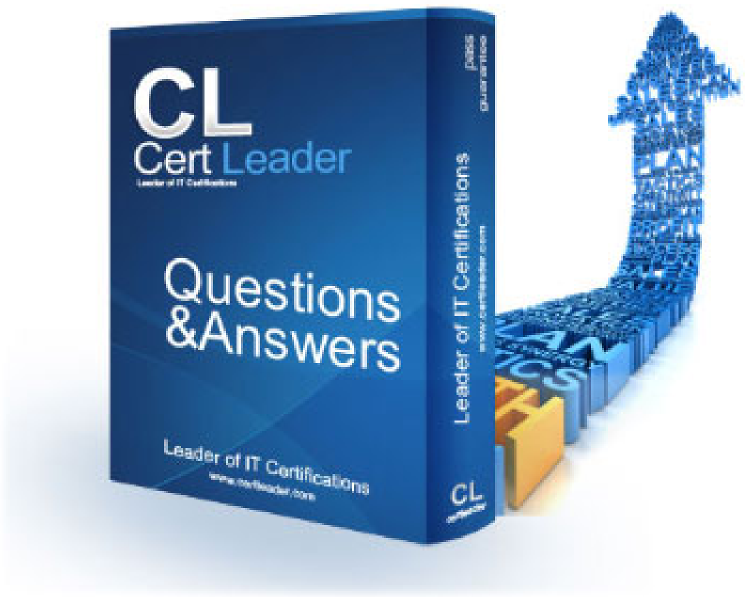
CS0-002 Dumps

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

https://www.certleader.com/CS0-002-dumps.html



NEW QUESTION 1
During an audit, several customer order forms were found to contain inconsistencies between the actual price of an item and the amount charged to the customer. Further investigation narrowed the cause of the issue to manipulation of the public-facing web form used by customers to order products. Which of the following would be the best way to locate this issue?

A. Reduce the session timeout threshold
B. Deploy MFA for access to the web server.
C. Implement input validation.
D. Run a dynamic code analysis.

Answer: C

Explanation:
Implementing input validation is the best way to locate and prevent the issue of manipulation of the
public-facing web form used by customers to order products. Input validation is a technique that checks and filters any user input that is sent to an application before processing it. 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 application. Input validation can also reject or sanitize any input that does not meet the validation criteria .

NEW QUESTION 2
An application has been updated to fix a vulnerability. Which of the following would ensure that previously patched vulnerabilities have not been reintroduced?

A. Stress testing
B. Regression testing
C. Code review
D. Peer review

Answer: B

Explanation:
Regression testing is a type of software testing that ensures that a recent program or code change has not adversely affected existing features123 Regression testing is useful for checking if previously patched vulnerabilities have not been reintroduced by the new update.
Stress testing is a type of software testing that evaluates the performance and reliability of a system under extreme conditions, such as high load, limited resources, or concurrent users. Stress testing is not directly related to checking for vulnerabilities.
Code review is a process of examining the source code of a software program to find and fix errors, improve quality, and ensure compliance with standards and best practices. Code review can help prevent vulnerabilities from being introduced in the first place, but it does not verify that existing features are working as expected after a code change.
Peer review is a process of evaluating the work of another person or group of people, such as a research paper, a report, or a design. Peer review can provide feedback and suggestions for improvement, but it does not test the functionality or security of a software product.

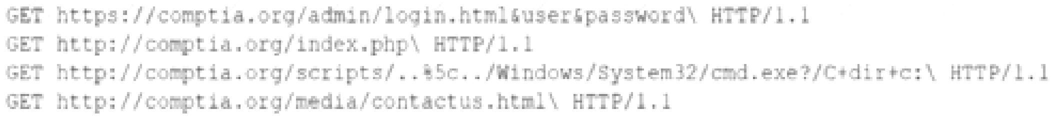
NEW QUESTION 3
Due to a rise m cyberattackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally Which of the following countermeasures 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 4
A security analyst is reviewing the following log entries to identify anomalous activity:



```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/..%5c../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

A. Directory traversal
B. SQL injection
C. Buffer overflow
D. Cross-site scripting

Answer: A

Explanation:
A directory traversal attack is a type of web application attack that exploits insufficient input validation or improper configuration to access files or directories that are outside the intended scope of the web server. The log entries given in the question show several requests that contain "…/" sequences in the URL, which

indicate an attempt to move up one level in the directory structure. For example, the request "/images/…/…/etc/passwd" tries to access the /etc/passwd file, which contains user account information on Linux systems. If successful, this attack could allow an attacker to read, modify, or execute files on the web server that are not meant to be accessible.

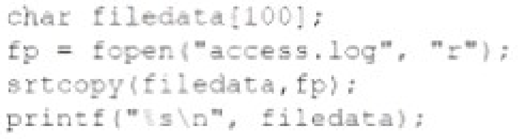
NEW QUESTION 5
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

A. To identify weaknesses in an organization's security posture
B. To identify likely attack scenarios within an organization
C. To build a business security plan for an organization
D. To build a network segmentation strategy

Answer: B

Explanation:
Threat intelligence can be used to identify likely attack scenarios within an organization based on the organization's specific vulnerabilities, assets, and threat landscape. Threat intelligence can help security teams anticipate and prepare for potential attacks, as well as detect and respond to ongoing attacks more effectively1. Threat intelligence can also provide insights into the threat actors, their motivations, and their tactics, techniques, and procedures (TTPs)2.

NEW QUESTION 6
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);
```

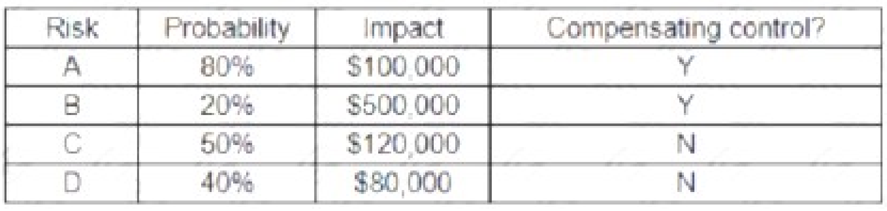
Which of the following should a security analyst recommend to fix the issue?

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 7
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.

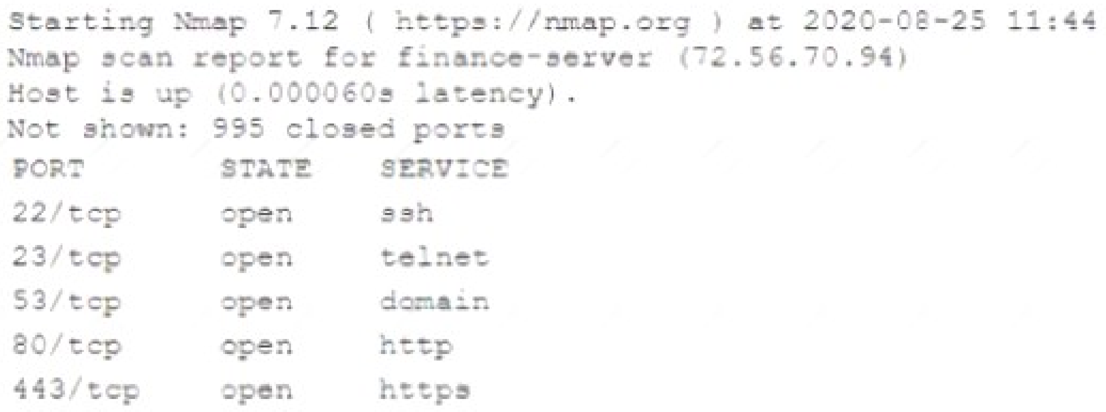
NEW QUESTION 8
While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the
certAcate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Select TWO)

A. On a private VLAN
B. Full disk encrypted
C. Powered off
D. Backed up hourly
E. VPN accessible only
F. Air gapped

Answer: CF

Explanation:
The most secure states for the certificate authority server when it is not in use are powered off and air gapped. Powering off the server will prevent any unauthorized access or tampering with the server while it is idle. Air gapping the server will isolate it from any network connections, making it inaccessible to remote attackers or malware. These measures will help to protect the integrity and confidentiality of the certificate authority server and its keys.

NEW QUESTION 9
A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:



```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
Not shown: 995 closed ports
PORT        STATE    SERVICE
22/tcp      open     ssh
23/tcp      open     telnet
53/tcp      open     domain
80/tcp      open     http
443/tcp     open     https
```

Which of the following should the cybersecunty analyst recommend to harden the server? (Select TWO).

A. Uninstall the DNS service
B. Perform a vulnerability scan
C. Change the server's IP to a private IP address
D. Disable the Telnet service
E. Block port 80 with the host-based firewall
F. Change the SSH port to a non-standard port

Answer: DF

Explanation:
Disabling the Telnet service would harden the server by removing an insecure protocol that transmits data in cleartext and could allow unauthorized access to the server. Changing the SSH port to a non-standard port would harden the server by reducing the exposure to brute-force attacks or port scans that target the default SSH port (22). Uninstalling the DNS service, performing a vulnerability scan, changing the server's IP to a private IP address, or blocking port 80 with the host-based firewall would not harden the server or could affect its functionality as a web server. Reference:
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

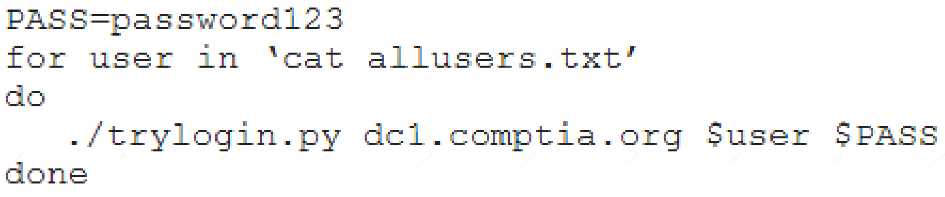
NEW QUESTION 10
An analyst is working on a method to allow secure access to a highly sensi-tive server. The solution must allow named individuals remote access to data contained on the box and must limit access to a single IP address. Which of the following solutions would best meet these requirements?

A. Jump box
B. Software-defined networking
C. VLAN
D. ACL

Answer: A

Explanation:
A jump box is a secure computer that can be used to access a remote server or network. It acts as an intermediary between the user and the target system, and can limit access to specific IP addresses. A jump box can also provide logging and auditing of the user's actions on the remote system. A jump box is a common solution for accessing highly sensitive servers or networks1.

NEW QUESTION 10
When investigating a compromised system, a security analyst finds the following script in the /tmp directory:



```
PASS=password123
for user in 'cat allusers.txt'
do
   ./trylogin.py dc1.comptia.org $user $PASS
done
```

Which of the following attacks is this script attempting, and how can it be mitigated?

A. This is a password-hijacking attack, and it can be mitigated by using strong encryption protocols.
B. This is a password-spraying attack, and it can be mitigated by using multifactor authentication.
C. This is a password-dictionary attack, and it can be mitigated by forcing password changes every 30 days.
D. This is a credential-stuffing attack, and it can be mitigated by using multistep authentication.

Answer: B

Explanation:
https://owasp.org/www-community/attacks/Password_Spraying_Attack
A credential stuffing attack would be using the full credentials and most likely being used across many common platforms. A credential stuffing attack depends on the reuse of passwords. With so many people reusing their passwords for multiple accounts, just one set of credentials is enough to expose most or all of their accounts.

NEW QUESTION 14
An organization is concerned about the security posture of vendors with access to its facilities and systems. The organization wants to implement a vendor review process to ensure \hi> policies implemented by vendors are in line with its own. Which of the following will provide the highest assurance of compliance?

A. An in-house red-team report
B. A vendor self-assessment report
C. An independent third-party audit report
D. Internal and external scans from an approved third-party vulnerability vendor

Answer: C

Explanation:
An independent third-party audit report can provide the highest assurance of compliance with the organization's policies by vendors, as it involves an objective and unbiased evaluation of the vendor's security posture and practices by an external auditor who follows established standards and criteria. An independent third-party audit report can help verify if the vendor meets the organization's requirements and expectations, as well as identify any gaps or weaknesses that need to be addressed.

NEW QUESTION 15
A security analyst was transferred to an organization's threat-hunting team to track specific activity throughout the enterprise environment The analyst must observe and assess the number ot times this activity occurs and aggregate the results. Which of the following is the BEST threat-hunting method for the analyst to use?

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

Answer: A

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

NEW QUESTION 17
A financial institution's business unit plans to deploy a new technology in a manner that violates existing information security standards. Which of the following actions should the Chief Information Security Officer (CISO) take to manage any type of violation?

A. Enforce the existing security standards and controls.
B. Perform a risk analysis and qualify the risk with legal.
C. Perform research and propose a better technology.
D. Enforce the standard permits.

Answer: B

Explanation:
The International Standards Organization, or ISO, develops standards for businesses around the world so that they may operate using a uniform set of best practices. These standards are not enforceable laws, but companies who choose to follow them stand to gain international credibility from their compliance; standards are set as guidance for best practices but are not enforceable laws

NEW QUESTION 19
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 21
An application developer needs help establishing a digital certificate for a new application. Which of the following illustrates a certificate management best practice?

A. Ensure the certificate Is applied to the certificate revocation list.
B. Ensure the certificate key algorithm is SHA-1 compliant.
C. Ensure the certificate is requested from a trusted CA.

D. Ensure the developer has self-signed the certificate.
E. Ensure the certificate key is less than 1028 bits long.

Answer: C

Explanation:
The best practice for establishing a digital certificate for a new application is to ensure the certificate is requested from a trusted CA. A CA stands for Certificate Authority, and it is an entity that issues and verifies digital certificates, which are electronic documents that contain a public key and a digital signature that prove the identity and authenticity of an application, a website, or a person. Requesting a certificate from a trusted CA can help ensure that the certificate is valid, secure, and recognized by other parties.

NEW QUESTION 24
A team of network security analysts is examining network traffic to determine if sensitive data was exfiltrated. Upon further investigation, the analysts believe confidential data was compromised. Which of the following capabilities would BEST defend against this type of sensitive data exfiltration?

A. Deploy an edge firewall.
B. Implement DLP
C. Deploy EDR.
D. Encrypt the hard drives

Answer: B

Explanation:
DLP, or Data Loss Prevention, is a cybersecurity solution that detects and prevents data breaches. It blocks the extraction of sensitive data and prevents the unauthorized or inappropriate sharing, transfer, or use of data. It also helps organizations comply with data protection regulations and policies1
DLP can help defend against sensitive data exfiltration by monitoring and controlling data movement across networks, devices, applications, and cloud services. DLP can also alert or block users from sending or uploading sensitive data to untrusted destinations or recipients.

NEW QUESTION 28
A new variant of malware is spreading on the company network using TCP 443 to contact its
command-and-control server The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?

A. Implement a sinkhole with a high entropy level
B. Disable TCP/53 at the parameter firewall
C. Block TCP/443 at the edge router
D. Configure the DNS forwarders to use recursion

Answer: A

Explanation:
A sinkhole is a technique that redirects malicious network traffic to a controlled destination, such as a fake server or a black hole. A sinkhole can be used to stop malicious communications with a command-and-control server by preventing the malware from reaching its intended destination. A high entropy level means that the sinkhole can generate random domain names that match the changing domain name used by the malware for callback. Blocking TCP/443 at the edge router, disabling TCP/53 at the perimeter firewall, or configuring the DNS forwarders to use recursion are other possible actions that could stop malicious communications, but they could also disrupt legitimate services that use those protocols or settings. Reference: https://www.cisco.com/c/en/us/about/security-center/dns-sinkholing.html

NEW QUESTION 31
Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?

A. Remote code execution
B. Buffer overflow
C. Unauthenticated commands
D. Certificate spoofing

Answer: C

Explanation:
Modbus is a communication protocol that is widely used in industrial control systems (ICS). Modbus does not have any built-in security features, such as authentication or encryption, which makes it vulnerable to various attacks. One of the most common and effective attack techniques against Modbus assets is to send unauthenticated commands to manipulate or disrupt the operation of the devices. Remote code execution, buffer overflow, and certificate spoofing are other attack techniques, but they have less likelihood of quick success against Modbus assets. Reference:
https://www.sciencedirect.com/science/article/pii/S2405959517300045

NEW QUESTION 35
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 36
A security team has begun updating the risk management plan incident response plan and system security plan to ensure compliance with secunty review guidelines Which of the (olowing can be executed by internal managers to simulate and validate the proposed changes'?

A. Internal management review
B. Control assessment
C. Tabletop exercise
D. Peer review

Answer: C

Explanation:
A tabletop exercise is a simulation of a security incident or scenario that involves the participation of key stakeholders and decision-makers. It can be used to test and validate the effectiveness of the organization’s plans, policies, and procedures, such as the risk management plan, incident response plan, and system security plan. A tabletop exercise can also help identify gaps or weaknesses in the plans and improve the communication and coordination among the participants. An internal management review, a control assessment, a peer review, or a scripting are other possible methods to evaluate and validate a new product’s security capabilities, but they are not as comprehensive or interactive as a tabletop exercise. Reference: https://www.csoonline.com/article/3444488/what-is-a-tabletop-exercise-how-to-run-a-security-scenario-in-6-ste

NEW QUESTION 39
During a risk assessment, a senior manager inquires about what the cost would be if a unique occurrence would impact the availability of a critical service. The service generates $1 ,000 in revenue for the organization. The impact of the attack would affect 20% of the server's capacity to perform jobs. The organization expects that five out of twenty attacks would succeed during the year. Which of the following is the calculated single loss expectancy?

A. $200
B. $800
C. $5,000
D. $20,000

Answer: A

Explanation:
The single loss expectancy (SLE) is a measure of the monetary loss associated with a single occurrence of a risk. The SLE can be calculated by multiplying the asset value (AV) by the exposure factor (EF), which is the percentage of loss that the asset would suffer if the risk occurred. In this case, the asset value is the revenue generated by the service, which is $1,000. The exposure factor is the impact of the attack on the server’s capacity, which is 20%. Therefore, the SLE is $1,000 x 0.2 = $2001.

NEW QUESTION 43
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 47
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

A. Infrastructure
B. Capabilities
C. Adversary
D. Victims

Answer: A

Explanation:
The Diamond Model of Intrusion Analysis is a framework for analyzing and understanding malicious activity on a system or network. It defines the basic atomic element of any intrusion activity as the event, which
consists of four core features: adversary, infrastructure, capability, and victim. These features are connected by edges that represent their underlying relationships and arranged in the shape of a diamond1
The infrastructure feature refers to the physical or logical communication structures that are used by the adversary to deliver a capability or interact with a victim. Examples of infrastructure elements are IP addresses, domain names, email addresses, servers, routers, etc. The domain, IP address, email address, and software version that the analyst extracted from the artifacts are all examples of infrastructure elements that can be used to identify or track the adversary’s activity.

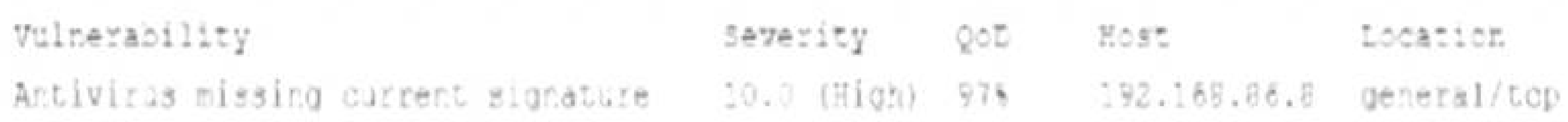
NEW QUESTION 50
A security analyst discovers the company's website is vulnerable to cross-site scripting. Which of the following solutions will best remedy the vulnerability?

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 54
A security is reviewing a vulnerability scan report and notes the following finding:



Vulnerability	Severity	QoD	Host	Location
Antivirus missing current signature	10.0 (High)	97%	192.168.86.8	general/tcp

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?

A. Patch or reimage the device to complete the recovery
B. Restart the antiviruses running processes
C. Isolate the host from the network to prevent exposure
D. Confirm the workstation's signatures against the most current signatures.

Answer: D

Explanation:
The vulnerability scan report shows that the workstation has a high-risk vulnerability (CVE-2019-0708) that affects Remote Desktop Services on Windows systems. This vulnerability allows remote code execution without authentication or user interaction, and can be exploited by sending specially crafted requests to the target system1
As part of the detection and analysis procedures, the analyst should confirm the workstation's signatures against the most current signatures. This can help verify if the workstation has been patched or updated to address the vulnerability, or if it is still vulnerable and needs remediation. The analyst can use tools such as Windows Update or Microsoft Baseline Security Analyzer to check the workstation's patch level and compare it with the latest available signatures.

NEW QUESTION 55
During an incident response procedure, a security analyst extracted a binary file from the disk of a compromised server. Which of the following is the best approach for analyzing the file without executing it?

A. Memory analysis
B. Hash signature check
C. Reverse engineering
D. Dynamic analysis

Answer: C

Explanation:
Reverse engineering is the process of analyzing a binary file without executing it, by using tools such as disassemblers, debuggers, and decompilers. Reverse engineering can help identify the functionality, behavior, and purpose of a binary file, as well as any malicious code or vulnerabilities it may contain.

NEW QUESTION 58
An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?

A. The human resources department
B. Customers
C. Company leadership
D. The legal team

Answer: C

Explanation:
Lessons learned is a critical stage of incident response that involves evaluating the effectiveness of the response, identifying gaps and areas for improvement, and updating the incident response plan accordingly1.
Company leadership should be involved in this process to ensure they are aware of the incident, its impact, and the actions taken to prevent or mitigate future incidents. Additionally, company leadership can provide support and guidance for implementing the recommendations from the lessons learned session2.

NEW QUESTION 60
An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the first steps to confirm and respond to the incident? (Select two).

A. Pause the virtual machine.

B. Shut down the virtual machine.
C. Take a snapshot of the virtual machine.
D. Remove the NIC from the virtual machine.
E. Review host hypervisor log of the virtual machine.
F. Execute a migration of the virtual machine.

Answer: AC

Explanation:
These steps are the best to confirm and respond to the incident because they preserve the state of the compromised server for further analysis and evidence collection. Pausing the virtual machine prevents any further changes or damage by the attacker, while taking a snapshot creates a copy of the virtual machine's memory and disk contents.

NEW QUESTION 64
A company is setting up a small, remote office to support five to ten employees. The company's home office is in a different city, where the company uses a cloud service provider for its business applications and a local server to host its data. To provide shared access from the remote office to the local server and the business applications, which of the following would be the easiest and most secure solution?

A. Use a VPC to host the company's data and keep the current solution for the business applications.
B. Use a new server for the remote office to host the data and keep the current solution for the business applications.
C. Use a VDI for the home office and keep the current solution for the business applications.
D. Use a VPN to access the company's data in the home office and keep the current solution for the business applications.

Answer: D

Explanation:
The correct answer is D. Use a VPN to access the company's data in the home office and keep the current solution for the business applications. A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN can allow users to access resources on a remote network, such as a server, as if they were on the same local network. A VPN can provide shared access from the remote office to the company's data in the home office, while maintaining security and privacy1.

NEW QUESTION 65
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 66
A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations Which of the following steps in the intelligence cycle is the security analyst performing?

A. Analysis and production
B. Processing and exploitation
C. Dissemination and evaluation
D. Data collection
E. Planning and direction

Answer: B

Explanation:
Processing and exploitation is the step in the intelligence cycle that involves converting raw data into a format that can be used for analysis and producing intelligence products that can be disseminated to consumers. The security analyst is performing this step by correlating, ranking, and enriching raw data into a report. Analysis and production, dissemination and evaluation, data collection, and planning and direction are other steps in the intelligence cycle, but they do not match the description of the security analyst's task. Reference:
https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-cycle.htm

NEW QUESTION 67
An analyst determines a security incident has occurred Which of the following is the most appropnate NEXT step in an incident response plan?

A. Consult the malware analysis process
B. Consult the disaster recovery plan
C. Consult the data classification process
D. Consult the communications plan

Answer: D

Explanation:
A communications plan is a document that outlines who should be notified and how during an incident response. It can also specify the roles and responsibilities of

the incident response team members, the escalation procedures, and the communication channels. Consulting the communications plan is the most appropriate next step in an incident response plan after determining a security incident has occurred. Consulting the malware analysis process, the disaster recovery plan, or the data classification process may be relevant at later stages of the incident response, but not as the next step. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 69
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.

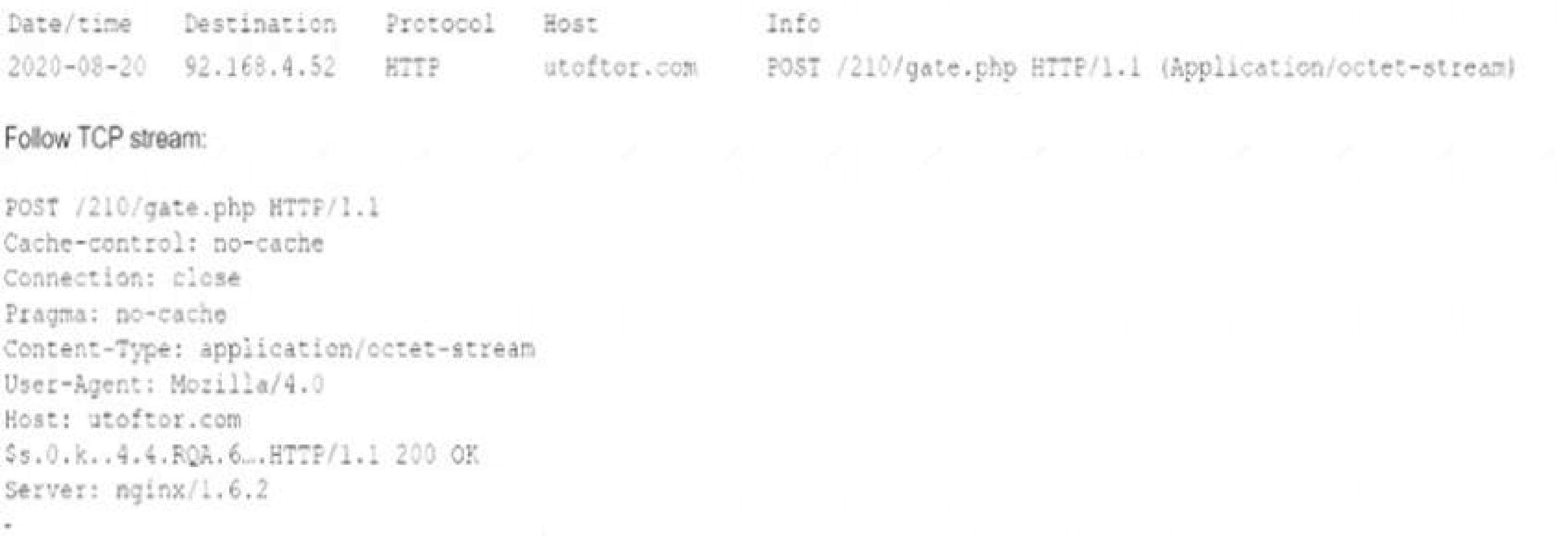
Answer: BD

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 74
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:



```
Date/time    Destination   Protocol   Host          Info
2020-08-20   92.168.4.52   HTTP       utoftor.com   POST /210/gate.php HTTP/1.1 (Application/octet-stream)
```

Follow TCP stream:

```
POST /210/gate.php HTTP/1.1
Cache-control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
$s.0.k..4.4.RQA.6….HTTP/1.1 200 OK
Server: nginx/1.6.2
-
```

Which of the following describes what has occurred?

A. The host attempted to download an application from utoftor.com.
B. The host downloaded an application from utoftor.com.
C. The host attempted to make a secure connection to utoftor.com.
D. The host rejected the connection from utoftor.com.

Answer: C

Explanation:
The packet capture shows that the host sent a Client Hello message to utoftor.com on port 443. This message is part of the TLS (Transport Layer Security) handshake protocol, which is used to establish a secure connection between a client and a server1. The Client Hello message contains information such as the supported TLS version, cipher suites, and extensions that the client can use for the secure connection. The server is expected to respond with a Server Hello message that selects the parameters for the secure connection. However, the packet capture does not show any response from the server, which means that the host only attempted to make a secure connection to utoftor.com, but did not succeed. The host did not download (B) or reject (D) any application from utoftor.com.

NEW QUESTION 79
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 84
An organization's internal department frequently uses a cloud provider to store large amounts of sensitive data. A threat actor has deployed a virtual machine to at the use of the cloud hosted hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability?

A. Sandbox the virtual machine.
B. Implement an MFA solution.
C. Update lo the secure hypervisor version.
D. Implement dedicated hardware for each customer.

Answer: C

Explanation:
MFA can be used to reduce the likelihood that the attacker gains access to the VM, however, the scenario specifically states that the attacker was able to escalate rights and the question asks what can be done to remediate the vulnerability. the vulnerability in this case would be the ability to escalate rights.
The best way to remediate the vulnerability is to update to the secure hypervisor version. A hypervisor is a software that creates and manages virtual machines on a physical server. A hypervisor can be vulnerable to various attacks, such as privilege escalation, code injection, or denial-of-service. Updating to the secure hypervisor version can help fix any known bugs or flaws in the hypervisor software and prevent attackers from exploiting them. Updating to the secure hypervisor version can also provide additional security features or enhancements that can improve the protection of the virtual machines and their data.

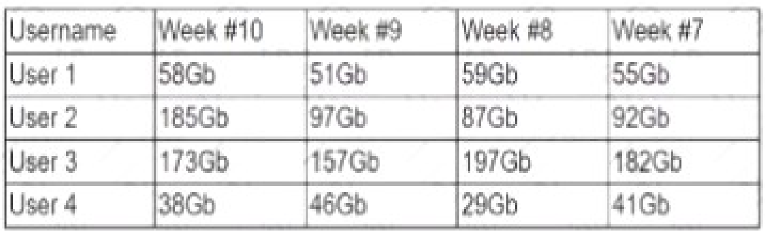
NEW QUESTION 85
An organization completed an internal assessment of its policies and procedures. The audit team identified a deficiency in the policies and procedures for PH. Which of the following should be the first step to secure the organization's Pll?

A. Complete Pll training within the organization.
B. Contact all Pll data owners within the organization.
C. Identify what type of Pll is on the network.
D. Formalize current Pll documentation.

Answer: C

Explanation:
Pll stands for Personally Identifiable Information, and it is any data that can be used to identify, locate, or contact an individual. Examples of Pll include names, addresses, phone numbers, email addresses, social security numbers, bank account numbers, etc. The first step to secure the organization’s Pll is to identify what type of Pll is on the network, where it is stored, who has access to it, and how it is transmitted. This can help determine the scope and impact of the deficiency in the policies and procedures for Pll.

NEW QUESTION 89
A security analyst is reviewing the following Internet usage trend report:



Username	Week #10	Week #9	Week #8	Week #7
User 1	58Gb	51Gb	59Gb	55Gb
User 2	185Gb	97Gb	87Gb	92Gb
User 3	173Gb	157Gb	197Gb	182Gb
User 4	38Gb	46Gb	29Gb	41Gb

Which of the following usernames should the security analyst investigate further?

A. User1
B. User 2
C. User 3
D. User 4

Answer: D

Explanation:
The Internet usage trend report shows that User 4 has an unusually high amount of data downloaded compared to other users. User 4 downloaded 2.5 GB of data in one day, while the average data downloaded by other users was around 0.2 GB. This could indicate that User 4 is engaged in some suspicious or malicious activity, such as downloading unauthorized or illegal content, exfiltrating sensitive data, or installing malware. Therefore, the security analyst should investigate User 4 further to determine the nature and source of the data downloaded.

NEW QUESTION 94
During an audit several customer order forms were found to contain inconsistencies between the actual price of an item and the amount charged to the customer

Further investigation narrowed the cause of the issue to manipulation of the public-facing web form used by customers to order products Which of the following would be the BEST way to locate this issue?

A. Reduce the session timeout threshold
B. Deploy MFA for access to the web server
C. Implement input validation
D. Run a static code scan

Answer: C

Explanation:
In this scenario, the issue is related to manipulation of the public-facing web form, indicating that attackers might be altering the prices before submitting the form. One of the best ways to prevent such attacks is to implement input validation, which can help ensure that the data submitted to the web form is correct, complete, and in the expected format. Input validation can also help prevent SQL injection and other types of web-based attacks.

NEW QUESTION 95
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 98
Ensuring that all areas of security have the proper controls is a primary reason why organizations use:

A. frameworks.
B. directors and officers.
C. incident response plans.
D. engineering rigor.

Answer: A

Explanation:
Ensuring that all areas of security have the proper controls is a primary reason why organizations use frameworks. Frameworks provide an organized structure for organizations to evaluate their security posture and implement the necessary security measures for their operations. Frameworks such as NIST, COBIT, and ISO 27001 provide guidance on how to develop, implement and monitor security policies, controls, and procedures for an organization. Additionally, frameworks provide a benchmark for organizations to measure their security posture against and create a roadmap for continued improvement.

NEW QUESTION 103
A security analyst discovers the accounting department is hosting an accounts receivable form on a public document service. Anyone with the link can access it. Which of the following threats applies to this situation?

A. Potential data loss to external users
B. Loss of public/private key management
C. Cloud-based authentication attack
D. Identification and authentication failures

Answer: A

Explanation:
Potential data loss to external users is a threat that applies to this situation, where the accounting department is hosting an accounts receivable form on a public document service. Anyone with the link can access it. Data loss is an event that results in the destruction, corruption, or unauthorized disclosure of sensitive or confidential data. Data loss can occur due to various reasons, such as human error, hardware failure, malware infection, or cyberattack. In this case, hosting an accounts receivable form on a public document service exposes the data to potential data loss to external users who may access it without authorization or maliciously modify or delete it .

NEW QUESTION 104
A security analyst needs to provide the development learn with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

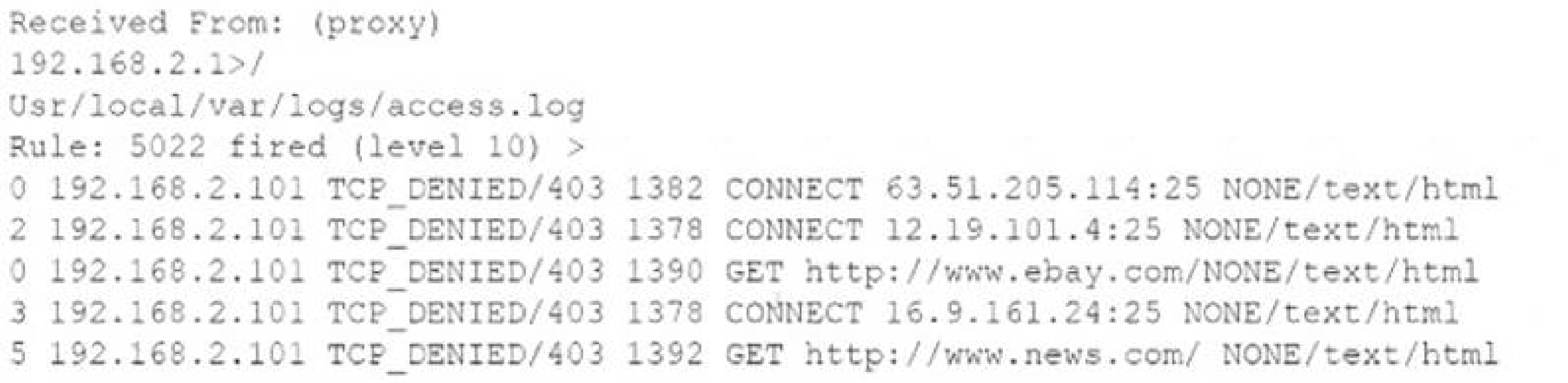
A. CASB
B. VPC
C. Federation
D. VPN

Answer: D

Explanation:

What is the difference between VPN and VPC?
Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.
VPN (Virtual Private Network) is a technology that provides secure connectivity from the corporate network to a cloud environment. VPN creates an encrypted tunnel between the two networks, allowing developers to access servers in all three tiers of the cloud environment without exposing their traffic to interception or tampering. VPN can also provide authentication and authorization mechanisms to verify the identity and permissions of the developers.

NEW QUESTION 106
A security analyst notices the following proxy log entries:



```
Received From: (proxy)
192.168.2.1>/
Usr/local/var/logs/access.log
Rule: 5022 fired (level 10) >
0 192.168.2.101 TCP_DENIED/403 1382 CONNECT 63.51.205.114:25 NONE/text/html
2 192.168.2.101 TCP_DENIED/403 1378 CONNECT 12.19.101.4:25 NONE/text/html
0 192.168.2.101 TCP_DENIED/403 1390 GET http://www.ebay.com/NONE/text/html
3 192.168.2.101 TCP_DENIED/403 1378 CONNECT 16.9.161.24:25 NONE/text/html
5 192.168.2.101 TCP_DENIED/403 1392 GET http://www.news.com/ NONE/text/html
```

Which of the following is the user attempting to do based on the log entries?

A. Use a DoS attack on external hosts.
B. Exfiltrate data.
C. Scan the network.
D. Relay email.

Answer: C

Explanation:
Scanning the network is what the user is attempting to do based on the log entries. The log entries show that the user is sending ping requests to various IP addresses on different ports using a proxy server. Ping requests are a common network diagnostic tool that can be used to test network connectivity and latency by sending packets of data and measuring their response time. However, ping requests can also be used by attackers to scan the network and discover active hosts, open ports, or potential vulnerabilities .

NEW QUESTION 110
A Chief Information Security Officer has requested a security measure be put in place to redirect certain traffic on the network. Which of the following would best resolve this issue?

A. Sinkholing
B. Blocklisting
C. Geoblocking
D. Sandboxing

Answer: A

Explanation:
Sinkholing is a technique for manipulating data flow in a network; you redirect traffic from its intended destination to a server of your choosing. It can be used maliciously, to steer legitimate traffic away from its intended recipient, but security professionals more commonly use sinkholing as a tool for research and reacting to attacks1.
For example, sinkholing can be used to redirect traffic from a botnet or a malware-infected host to a server under the control of the defender, where the traffic can be analyzed, blocked, or neutralized. This can help identify and isolate compromised devices, prevent command-and-control communication, and disrupt malicious activities2.
The other options are not the best solutions for the following reasons:

- Blocklisting is a technique for preventing access to or communication with certain IP addresses, domains, or applications that are known or suspected to be malicious. Blocklisting can be implemented using firewalls, routers, proxies, or software tools. Blocklisting can protect a network from unwanted or harmful traffic, but it does not redirect the traffic to a different destination.
- Geoblocking is a technique for restricting access to or communication with certain IP addresses, domains, or applications based on their geographic location. Geoblocking can be implemented using firewalls, routers, proxies, or software tools. Geoblocking can protect a network from unauthorized or undesirable traffic from specific regions or countries, but it does not redirect the traffic to a different destination.
- Sandboxing is a technique for isolating and executing potentially malicious code or applications in a separate and secure environment. Sandboxing can be implemented using virtual machines, containers, or software tools. Sandboxing can protect a network from malware infection or damage, but it does not redirect the network traffic to a different destination.

NEW QUESTION 115
Which of the following is a reason for correctly identifying APTs that might be targeting an organization?

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

Answer: B

Explanation:
APTs utilize methods and technologies differently than other threats. APTs stand for Advanced Persistent Threats, and they are sophisticated and stealthy attacks that target specific organizations or networks over a long period of time, often with political or financial motives. APTs utilize methods and technologies differently

than other threats, such as using custom-made malware, exploiting zero-day vulnerabilities, leveraging social engineering techniques, or employing multiple vectors of attack. APTs can also evade detection by existing security tools or controls, by using encryption, obfuscation, proxy servers, or other techniques to hide their activities or communications.

NEW QUESTION 116
A company's legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations. Which of the following will allow all data to be kept on the third-party network?

A. VDI
B. SaaS
C. CASB
D. FaaS

Answer: B

Explanation:
SaaS stands for Software as a Service, which is a cloud model that allows users to access software applications over the internet without installing or maintaining them on their own devices. SaaS will allow all data to be kept on the third-party network, because the software applications and the data they generate or process are stored on the cloud provider’s servers. VDI, CASB, and FaaS are other terms related to cloud computing or security, but they do not match the description of keeping all data on the third-party network. Reference: https://www.ibm.com/cloud/learn/software-as-a-service

NEW QUESTION 117
An organization wants to move non-essential services into a cloud computing environment. The management team has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work best to attain the desired outcome?

A. Duplicate all services in another instance and load balance between the instances.
B. Establish a hot site with active replication to another region within the same cloud provider.
C. Set up a warm disaster recovery site with the same cloud provider in a different region.
D. Configure the systems with a cold site at another cloud provider that can be used for failover.

Answer: C

Explanation:
Setting up a warm disaster recovery site with the same cloud provider in a different region can help to achieve a recovery time objective (RTO) of 12 hours while keeping the costs low. A warm disaster recovery site is a partially configured site that has some of the essential hardware and software components ready to be activated in case of a disaster. A warm site can provide faster recovery than a cold site, which has no preconfigured components, but lower costs than a hot site, which has fully configured and replicated components. Using the same cloud provider can help to simplify the migration and synchronization processes, while using a different region can help to avoid regional outages or disasters .

NEW QUESTION 122
A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?

A. The extended support mitigates any risk associated with the software.
B. The extended support contract changes this vulnerability finding to a false positive.
C. The company is transferring the risk for the vulnerability to the software vendor.
D. The company is accepting the inherent risk of the vulnerability.

Answer: C

Explanation:
The company is transferring the risk for the vulnerability to the software vendor. Risk transfer is a risk treatment strategy that involves shifting the potential loss or impact of a risk to a third party, such as an insurance company or a vendor. Risk transfer does not eliminate the risk, but it reduces the organization’s exposure or liability for the risk1. In this scenario, the company is transferring the risk for the vulnerability in the out-of-support database software to the software vendor by signing an extended support contract. The extended support contract means that the software vendor will continue to provide security patches and updates for the software until the company can complete the software update. This reduces the likelihood and impact of a potential exploit of the vulnerability.

NEW QUESTION 123
A Chief Information Security Officer has asked for a list of hosts that have critical and high-severity findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?

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

Answer: A

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

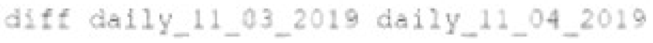
NEW QUESTION 124

An organization is experiencing security incidents in which a systems administrator is creating unauthorized user accounts A security analyst has created a script to snapshot the system configuration each day. Following iss one of the scripts:

```
cat /etc/passwd > daily_$(date +"%m_%d_%Y")
```

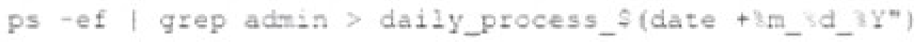
This script has been running successfully every day. Which of the following commands would provide the analyst with additional useful information relevant to the above script?

A)



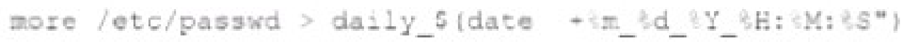
```
diff daily_11_03_2019 daily_11_04_2019
```

B)



```
ps -ef | grep admin > daily_process_$(date +%m_%d_%Y")
```

C)



```
more /etc/passwd > daily_$(date  +%m_%d_%Y_%H:%M:%S")
```

D)

```
la -lai /usr/sbin > daily_applications
```

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

Answer: D

Explanation:
Option D would provide the analyst with additional useful information relevant to the above script. Option D is a command that compares two files and shows the differences between them. In this case, the command compares the current snapshot of the system configuration (sysconfig.txt) with the previous snapshot (sysconfig.txt.old). This can help the analyst to identify any changes or anomalies in the system configuration that may indicate unauthorized or malicious activity. Option A is a command that copies a file from one location to another. In this case, the command copies the current snapshot of the system configuration (sysconfig.txt) to a backup location (/backup/sysconfig.txt). This can help the analyst to preserve evidence or restore the system configuration if needed, but it does not provide any additional information relevant to the above script. Option B is a command that prints a file to standard output. In this case, the command prints the current snapshot of the system configuration (sysconfig.txt) to the screen. This can help the analyst to review or analyze the system configuration, but it does not provide any additional information relevant to the above script. Option C is a command that moves a file from one location to another. In this case, the command moves the current snapshot of the system configuration (sysconfig.txt) to another location (/old/sysconfig.txt). This can help the analyst to organize or archive the system configuration files, but it does not provide any additional information relevant to the above script.

NEW QUESTION 129
An incident response team is responding to a breach of multiple systems that contain Pll and PHI Disclosure of the incident to external entities should be based on:

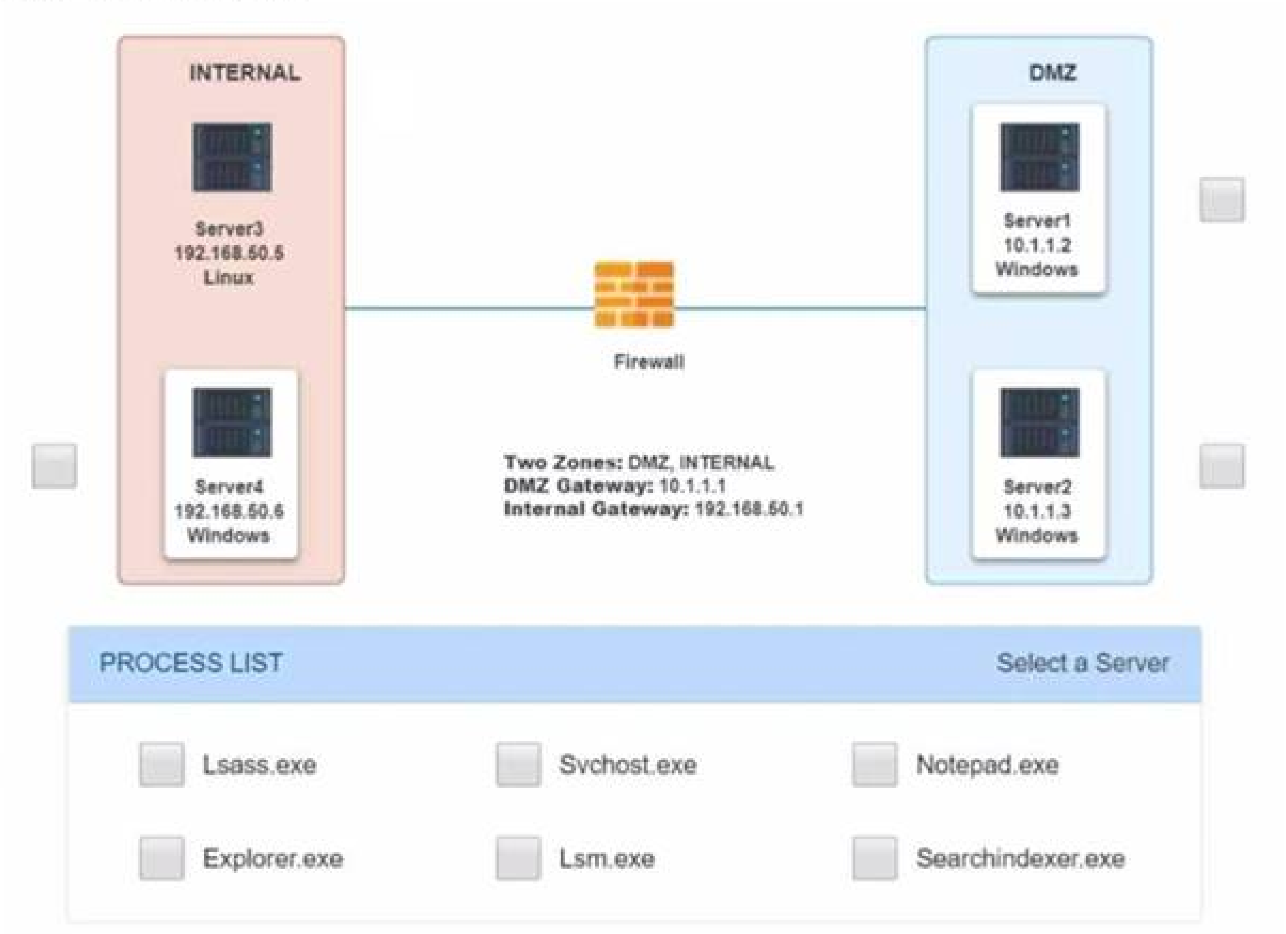
A. the responder's discretion.
B. the public relations policy.
C. the communication plan.
D. the senior management team's guidance.

Answer: C

Explanation:
The communication plan is an important part of incident response, as it outlines how and when information about the incident should be shared with external entities.
A communication plan is a set of procedures and protocols that define how an organization should communicate with external entities during times of emergency or security incident. The plan typically outlines how and when information about the incident should be shared, and ensures that any relevant stakeholders are informed of the incident in a timely manner. It also serves as a guide for determining what information to share with outside parties. Here is a link to an article from CompTIA's website about the importance of a communication plan for incident response for your reference:
https://www.comptia.org/content/incident-response-communication-plan

NEW QUESTION 132
Malware is suspected on a server in the environment.
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one Of the servers may be malware.
INSTRUCTIONS
Servers 1 , 2, and 4 are clickable. Select the Server and the process that host the malware.

Network Diagram for Company A

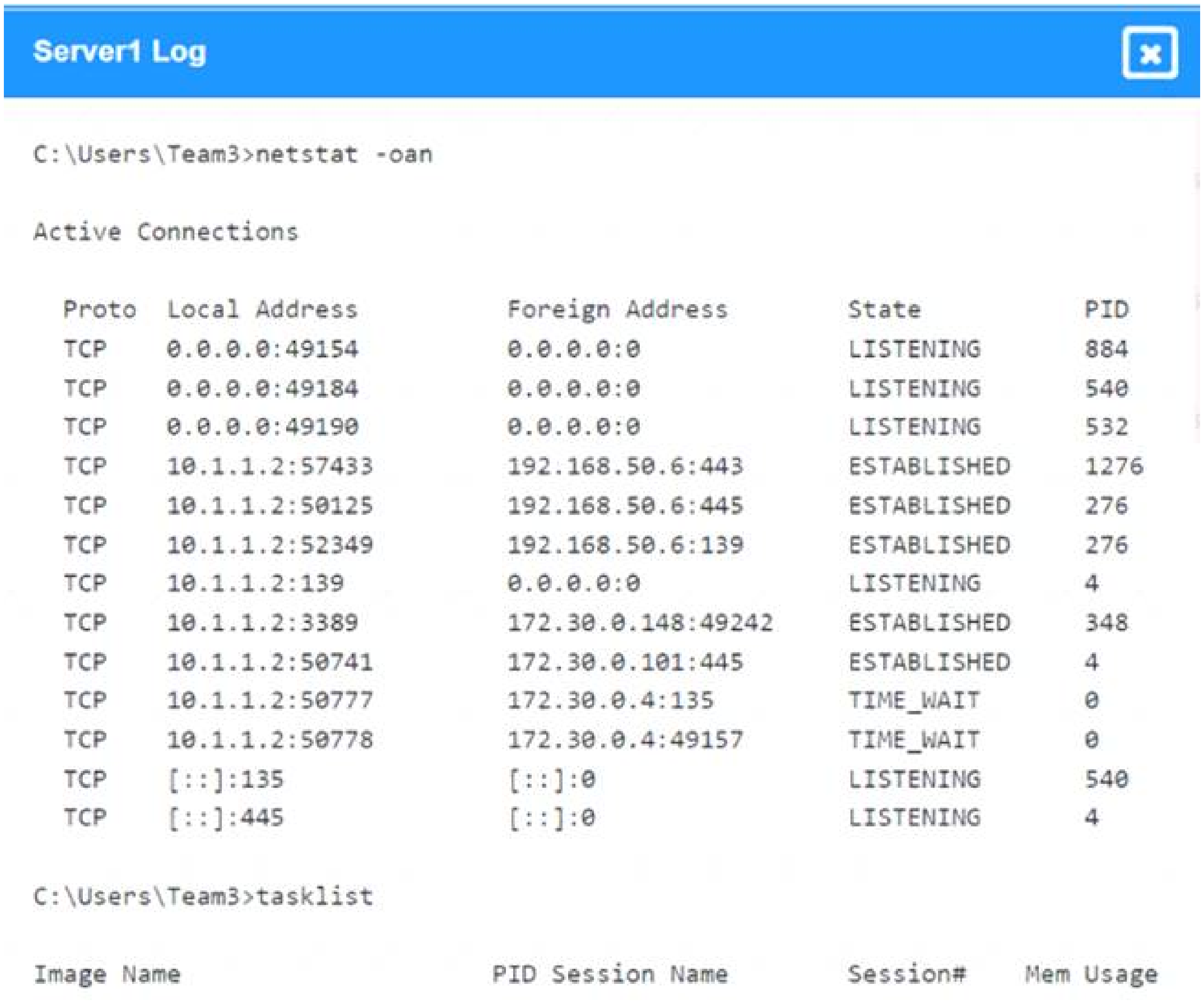


Two Zones: DMZ, INTERNAL
DMZ Gateway: 10.1.1.1
Internal Gateway: 192.168.50.1

PROCESS LIST — Select a Server

□ Lsass.exe □ Svchost.exe □ Notepad.exe

□ Explorer.exe □ Lsm.exe □ Searchindexer.exe



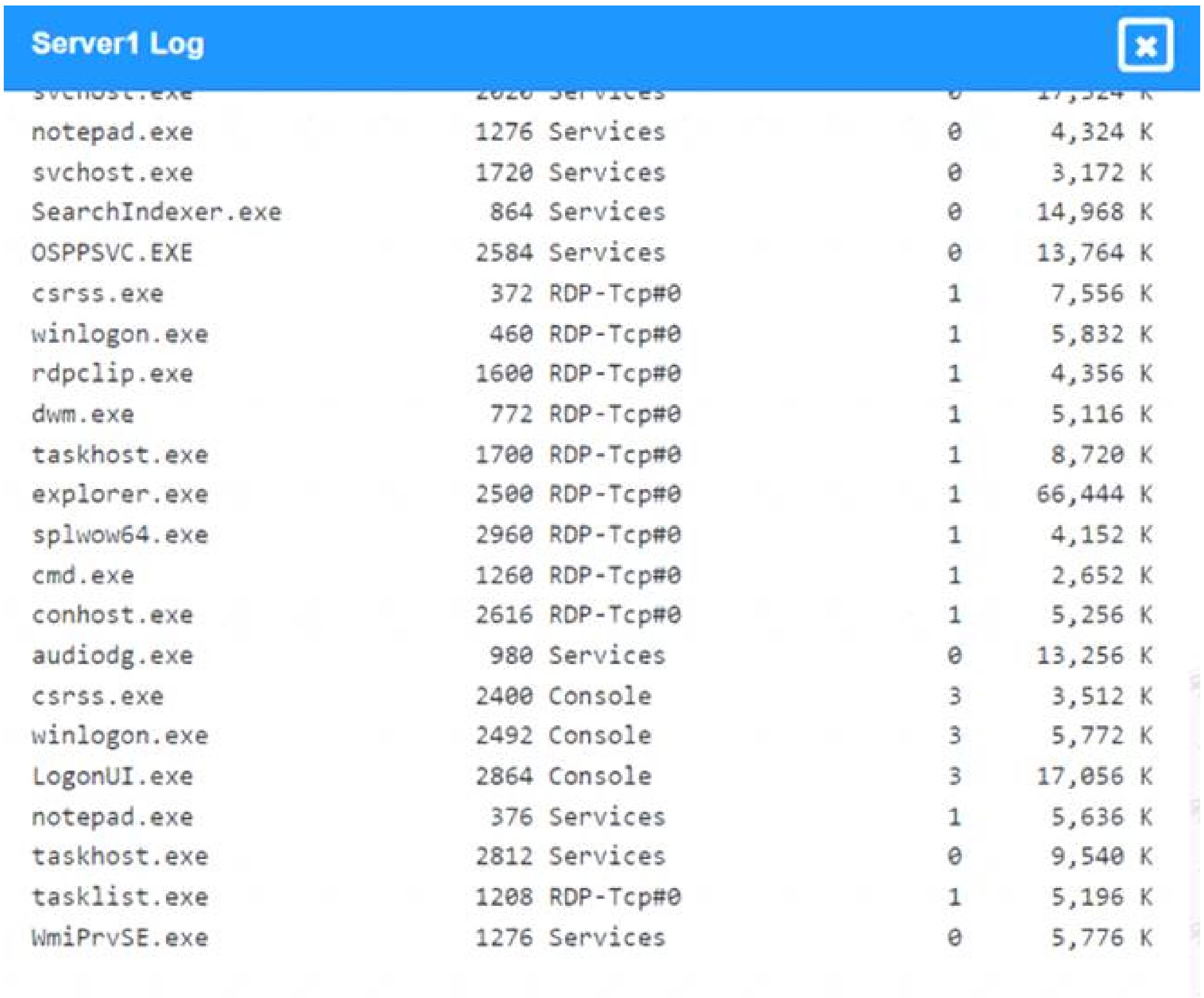
```
C:\Users\Team3>netstat -oan

Active Connections

  Proto  Local Address          Foreign Address        State          PID
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING      884
  TCP    0.0.0.0:49184          0.0.0.0:0              LISTENING      540
  TCP    0.0.0.0:49190          0.0.0.0:0              LISTENING      532
  TCP    10.1.1.2:57433         192.168.50.6:443       ESTABLISHED    1276
  TCP    10.1.1.2:50125         192.168.50.6:445       ESTABLISHED    276
  TCP    10.1.1.2:52349         192.168.50.6:139       ESTABLISHED    276
  TCP    10.1.1.2:139           0.0.0.0:0              LISTENING      4
  TCP    10.1.1.2:3389          172.30.0.148:49242     ESTABLISHED    348
  TCP    10.1.1.2:50741         172.30.0.101:445       ESTABLISHED    4
  TCP    10.1.1.2:50777         172.30.0.4:135         TIME_WAIT      0
  TCP    10.1.1.2:50778         172.30.0.4:49157       TIME_WAIT      0
  TCP    [::]:135               [::]:0                 LISTENING      540
  TCP    [::]:445               [::]:0                 LISTENING      4

C:\Users\Team3>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
```



Server1 Log

```
svchost.exe                2020 Services          0    17,324 K
notepad.exe                1276 Services          0     4,324 K
svchost.exe                1720 Services          0     3,172 K
SearchIndexer.exe           864 Services          0    14,968 K
OSPPSVC.EXE                2584 Services          0    13,764 K
csrss.exe                   372 RDP-Tcp#0         1     7,556 K
winlogon.exe                460 RDP-Tcp#0         1     5,832 K
rdpclip.exe                1600 RDP-Tcp#0         1     4,356 K
dwm.exe                     772 RDP-Tcp#0         1     5,116 K
taskhost.exe               1700 RDP-Tcp#0         1     8,720 K
explorer.exe               2500 RDP-Tcp#0         1    66,444 K
splwow64.exe               2960 RDP-Tcp#0         1     4,152 K
cmd.exe                    1260 RDP-Tcp#0         1     2,652 K
conhost.exe                2616 RDP-Tcp#0         1     5,256 K
audiodg.exe                 980 Services          0    13,256 K
csrss.exe                  2400 Console           3     3,512 K
winlogon.exe               2492 Console           3     5,772 K
LogonUI.exe                2864 Console           3    17,056 K
notepad.exe                 376 Services          1     5,636 K
taskhost.exe               2812 Services          0     9,540 K
tasklist.exe               1208 RDP-Tcp#0         1     5,196 K
WmiPrvSE.exe               1276 Services          0     5,776 K
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Server1 and svchost.exe

NEW QUESTION 135
A security analyst is reviewing malware files without running them. Which of the following analysis types is the security analyst using?

A. Dynamic
B. Sandbox
C. Static
D. Heuristic

Answer: C

Explanation:
Static analysis is the process of reviewing malware files without running them, by using tools such as hex editors, strings, and signature scanners. Static analysis can help extract basic information from malware files, such as file type, size, checksum, metadata, imports, exports, etc. Static analysis can also help identify known malware samples based on their signatures or hashes.

NEW QUESTION 137
A security analyst needs to determine the best method for securing access to a top-secret datacenter Along with an access card and PIN code, which of the following additional authentication methods would be BEST to enhance the datacenter's security?

A. Physical key
B. Retinal scan
C. Passphrase
D. Fingerprint

Answer: B

Explanation:
A retinal scan is a biometric authentication method that uses the unique pattern of blood vessels in the retina to verify a person’s identity. It is considered a strong and reliable authentication method that would enhance the datacenter’s security. A physical key, a passphrase, or a fingerprint are other authentication methods, but they are not as secure or reliable as a retinal scan. Reference:
https://www.techopedia.com/definition/2586/retinal-scan

NEW QUESTION 139
An intrusion detection analyst reported an inbound connection originating from an unknown IP address recorded on the VPN server for multiple internal hosts. During an investigation, a security analyst determines there were no identifiers associated with the hosts. Which of the following should the security analyst enforce to obtain the best information?

A. Update the organization's IP table.
B. Enable user access logging.
C. Shut down all VPN connections.
D. Create rules for the Active Directory.

Answer: B

Explanation:
User access logging (UAL) is a feature on Windows Server operating systems that records the details of
remote access and management activities performed by users on the server. UAL can provide information such as the user name, the source IP address, the destination host name, the protocol used, and the time and duration of the connection1. Enabling user access logging on the VPN server can help the security analyst to obtain the best information to identify and investigate the inbound connection originating from an unknown IP address.

NEW QUESTION 140
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 .

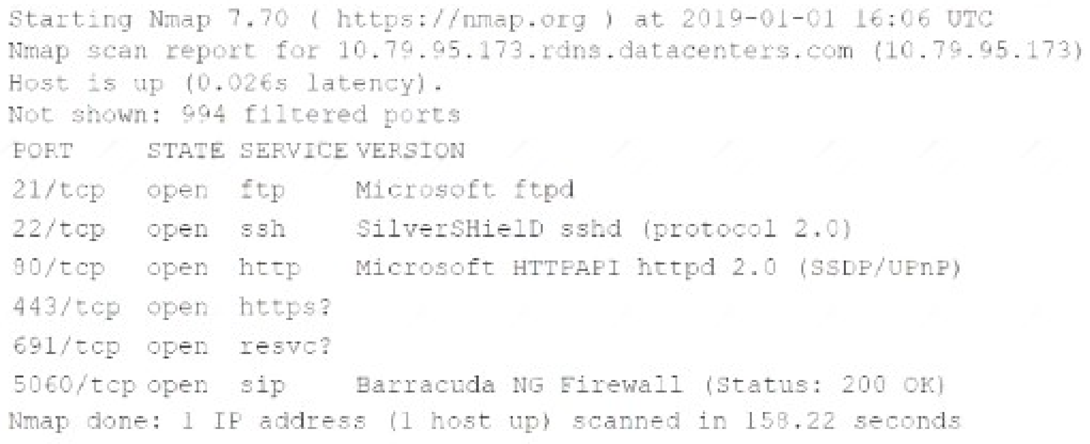
NEW QUESTION 142
A company wants to run a leaner team and needs to deploy a threat management system with minimal human Interaction. Which of the following is the server component of the threat management system that can accomplish this goal?

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

Answer: D

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

NEW QUESTION 144
An information security analyst is compiling data from a recent penetration test and reviews the following output:



```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 16:06 UTC
Nmap scan report for 10.79.95.173.rdns.datacenters.com (10.79.95.173)
Host is up (0.026s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Microsoft ftpd
22/tcp   open  ssh     SilverSHielD sshd (protocol 2.0)
80/tcp   open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp  open  https?
691/tcp  open  resvc?
5060/tcp open  sip     Barracuda NG Firewall (Status: 200 OK)
Nmap done: 1 IP address (1 host up) scanned in 158.22 seconds
```

The analyst wants to obtain more information about the web-based services that are running on the target. Which of the following commands would most likely provide the needed information?

A. ping -t 10.79.95.173,rdns.datacenter.com
B. telnet 10.79.95.17.17 443
C. ftpd 10.79.95.173.rdns.datacenters.com 443
D. tracert 10.79,,95,173

Answer: B

Explanation:
Telnet is a command-line tool that can be used to connect to a remote host on a specified port, and to send or receive data over that connection. Telnet can be used to obtain more information about the web-based services that are running on the target, by interacting with them or observing their responses. For example, telnet 10.79.95.173 443 would connect to the target on port 443, which is commonly used for HTTPS or SSL/TLS encrypted web traffic.

NEW QUESTION 146
A security analyst discovers suspicious activity going to a high-value corporate asset. After reviewing the traffic, the security analyst identifies that

malware was successfully installed on a machine. Which of the following should be completed first?

A. Create an IDS signature of the malware file.
B. Create an IPS signature of the malware file.
C. Remove the malware from the host.
D. Contact the systems administrator.

Answer: C

Explanation:
According to the CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives1, one of the skills required for the exam is to “apply incident response procedures and analyze potential indicators of
compromise (IOCs)”. The document also states that “the first step in incident response is to contain the incident and prevent further damage” (page 14).
Based on this information, the best answer to your question is C. Remove the malware from the host. This would prevent the malware from spreading to other machines or exfiltrating data from the infected host.

NEW QUESTION 151
An organization is focused on restructuring its data governance programs and an analyst has been Tasked with surveying sensitive data within the organization. Which of the following is the MOST accurate method for the security analyst to complete this assignment?

A. Perform an enterprise-wide discovery scan.
B. Consult with an internal data custodian.
C. Review enterprise-wide asset Inventory.
D. Create a survey and distribute it to data owners.

Answer: A

Explanation:
A data governance program is a collection of practices, policies, and procedures that manage, leverage, and protect the data assets of an organization1. It requires changing the workplace culture and adding some software1. To survey sensitive data within the organization, the most accurate method is to perform an enterprise-wide discovery scan that can identify and classify data from various sources and systems2. This way, the analyst can have a comprehensive view of the data landscape and its quality, security, accessibility, and usage. Consulting with an internal data custodian (B) or reviewing enterprise-wide asset inventory © may provide some insights, but not as accurate or complete as a discovery scan. Creating a survey and distributing it to data owners (D) may be time-consuming and unreliable, as data owners may not have the full knowledge or awareness of their data.
References: 1: https://www.analytics8.com/blog/8-steps-to-start-your-data-governance-program/ 2: https://solutionsreview.com/data-management/the-best-data-governance-tools-and-software/

NEW QUESTION 155
Which of the following activities is designed to handle a control failure that leads to a breach?

A. Risk assessment
B. Incident management
C. Root cause analysis
D. Vulnerability management

Answer: B

Explanation:
Incident management is a process that aims to handle a control failure that leads to a breach by restoring normal operations as quickly as possible and minimizing the impact and damage of the incident. Incident management involves activities such as identifying, analyzing, containing, eradicating, recovering, and learning from security incidents. Risk assessment, root cause analysis, and vulnerability management are other processes related to security management, but they are not designed to handle a control failure that leads to a breach. Reference:
https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 159
A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The Organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?

A. Make sure the scan is credentialed, covers at hosts in the patch management system, and is scheduled during business hours so it can be terminated if it affects business operations.
B. Make sure the scan is uncredentialed, covers at hosts in the patch management system, and Is scheduled during of business hours so it has the least impact on operations.
C. Make sure the scan is credentialed, has the latest software and signature versions, covers all external hosts in the patch management system and is scheduled during off-business hours so it has the least impact on operations.
D. Make sure the scan is credentialed, uses a ironed plug-in set, scans all host IP addresses in the enterprise, and is scheduled during off-business hours so it has the least impact on operations.

Answer: D

Explanation:
A vulnerability scan is a process of identifying and assessing known vulnerabilities in a system or network
using automated tools or software1
A vulnerability scan can help improve the security posture of a vulnerability management program by detecting and prioritizing potential weaknesses that could be exploited by attackers. To increase the security posture of a vulnerability scan, the following actions can be taken:
➢ Expand the ports being scanned to include all ports: This means scanning all possible ports on a system or network, not just the well-known or commonly used ones. This can help discover more vulnerabilities that may be hidden or overlooked on less frequently used ports.
➢ Increase the scan interval to a number the business will accept without causing service interruption: This means scanning more frequently or regularly, but not so often that it causes performance issues or downtime for the system or network. This can help keep up with new vulnerabilities that may emerge over time and reduce the window of opportunity for attackers.

> Enable authentication and perform credentialed scans: This means using login credentials or SSH keys on an asset to get deeper access to its data, processes, configurations, and vulnerabilities2
This can help discover more vulnerabilities that cannot be seen from the network, such as insecure versions of software or poor security permissions.

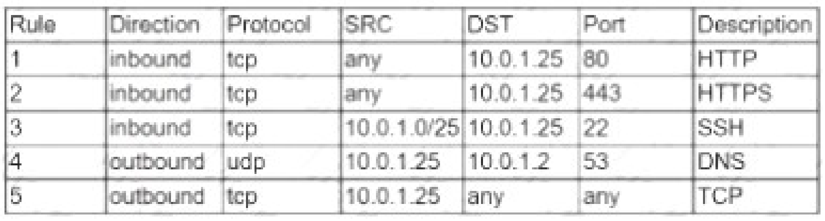
NEW QUESTION 163
An analyst is responding 10 an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the held. Maiware was loaded on the device via the installation of a third-party software package The analyst has baselined the device Which of the following should the analyst do to BEST mitigate future attacks?

A. Implement MDM
B. Update the maiware catalog
C. Patch the mobile device's OS
D. Block third-party applications

Answer: D

Explanation:
Blocking third-party applications would be the best way to mitigate future attacks on company-owned mobile devices that are used by employees to collect data from clients in the field. Third-party applications are applications that are not developed or authorized by the device manufacturer or operating system provider1. Third-party applications can pose a security risk for mobile devices, as they may contain malware, spyware, or other malicious code that can compromise the device or its data2. Blocking third-party applications can help prevent employees from installing unauthorized or untrusted applications on company-owned mobile devices and reduce the attack surface.

NEW QUESTION 166
A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0 1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.
The network rules for the instance are the following:



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

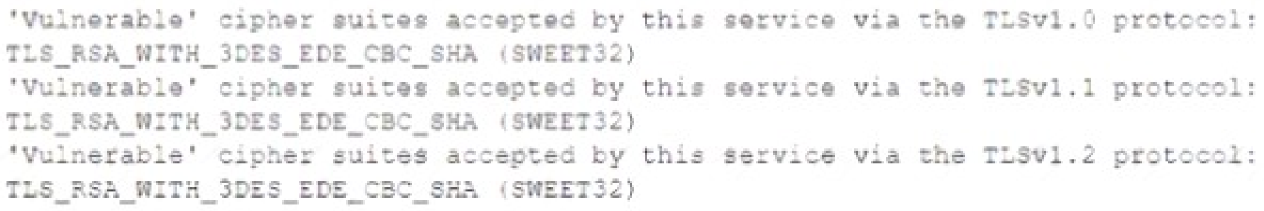
Which of the following is the BEST way to isolate and triage the host?

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

Answer: C

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

NEW QUESTION 169
During a review of the vulnerability scan results on a server, an information security analyst notices the following:



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

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

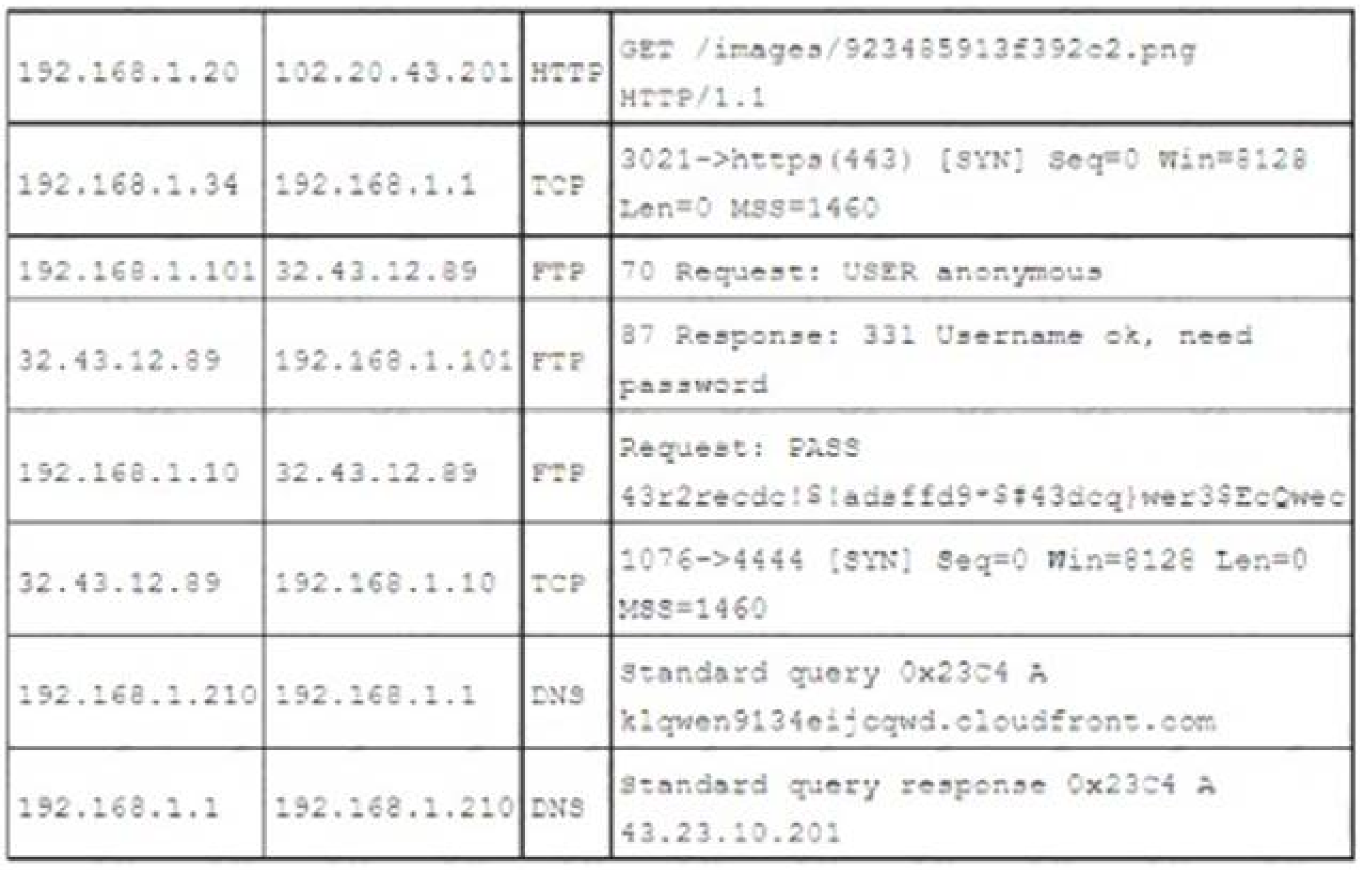
A. It only accepts TLSvl 2
B. It only accepts cipher suites using AES and SHA
C. It no longer accepts the vulnerable cipher suites
D. SSL/TLS is offloaded to a WAF and load balancer

Answer: C

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

NEW QUESTION 172

A security analyst reviews the following post-incident information to determine the origin and cause of a breach:



192.168.1.20	102.20.43.201	HTTP	GET /images/923485913f392c2.png HTTP/1.1
192.168.1.34	192.168.1.1	TCP	3021->https(443) [SYN] Seq=0 Win=8128 Len=0 MSS=1460
192.168.1.101	32.43.12.89	FTP	70 Request: USER anonymous
32.43.12.89	192.168.1.101	FTP	87 Response: 331 Username ok, need password
192.168.1.10	32.43.12.89	FTP	Request: PASS 43r2recdc!$!adsffd9*$#43dcq}wer3$EcQwec
32.43.12.89	192.168.1.10	TCP	1076->4444 [SYN] Seq=0 Win=8128 Len=0 MSS=1460
192.168.1.210	192.168.1.1	DNS	Standard query 0x23C4 A klqwen9134eijcqwd.cloudfront.com
192.168.1.1	192.168.1.210	DNS	Standard query response 0x23C4 A 43.23.10.201

Based on this information, which of the following should the analyst record in the incident report related to the breach? (Select two).

A. Forensic analysis Should be performed on 192.168, 1.10.
B. An on-path attack is impersonating the gateway.
C. IP address 43.23.10.201 should be blocked at the firewall.
D. Host 192.168.1.210 should be disconnected from the network.
E. The /images folder should be scanned with anti-malware.
F. A reverse shell was used.

Answer: CF

Explanation:
> F. A reverse shell was used: A reverse shell is a technique that allows a remote attacker to execute commands on a compromised system by opening a connection from the target to the attacker's machine. The image shows that the attacker used the netcat tool to create a reverse shell on host 192.168.1.210, which is running a web server on port 80. The attacker then used the reverse shell to access the /images folder and download a file named secret.jpg.
> C. IP address 43.23.10.201 should be blocked at the firewall: IP address 43.23.10.201 is the source of the attack, as shown by the netstat command output in the image. The attacker used this IP address to connect to host 192.168.1.210 on port 80 and exploit a vulnerability in the web server software. Blocking this IP address at the firewall would prevent further attacks from this source.

NEW QUESTION 174
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.

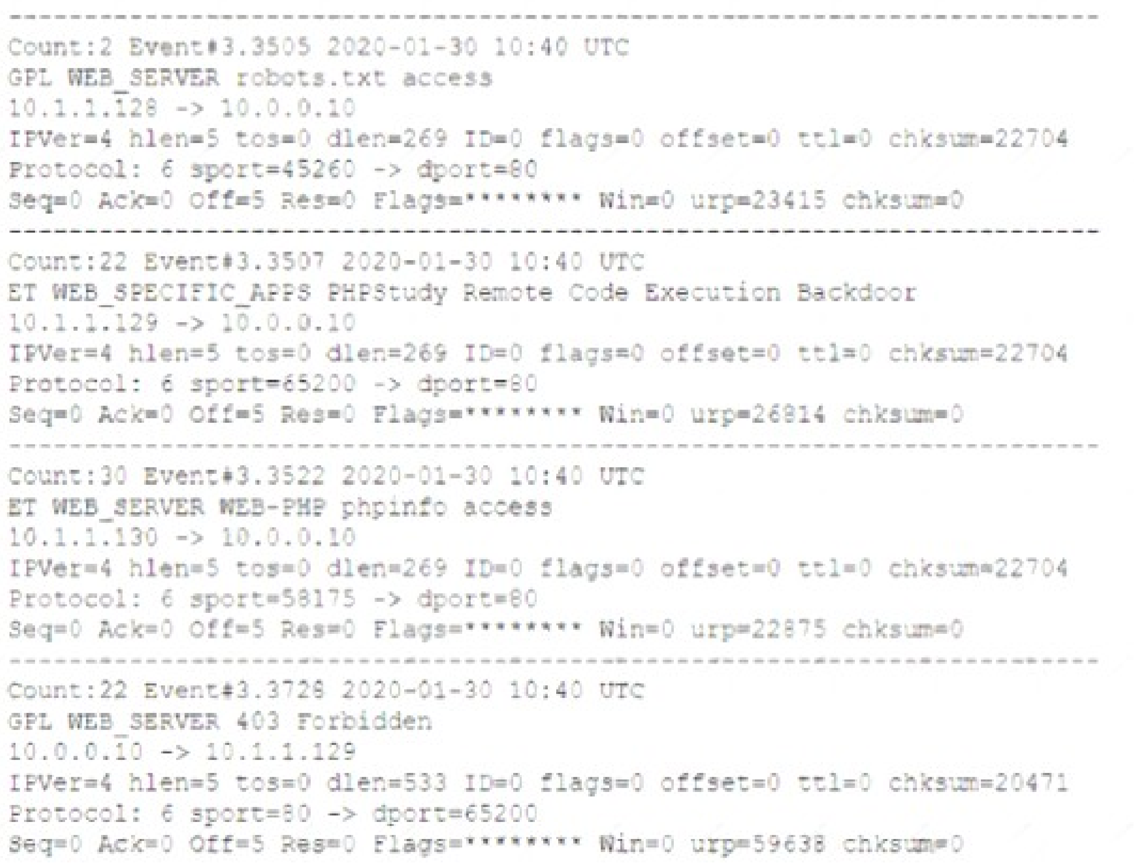
NEW QUESTION 178
industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration and access management solutions would help to mitigate this risk?

A. Multifactor authentication
B. Manual access reviews
C. Endpoint detection and response
D. Role-based access control

Answer: D

Explanation:
Role-based access control (RBAC) is a method of restricting access to resources based on the roles of users within an organization. RBAC assigns permissions and privileges to roles, rather than individual users, and grants access based on the principle of least privilege3
RBAC can help mitigate the risk of privilege escalation attacks on SCADA devices by ensuring that only authorized users have access to SCADA administration and management functions, and that they have the minimum level of access required to perform their tasks.

NEW QUESTION 182
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
```

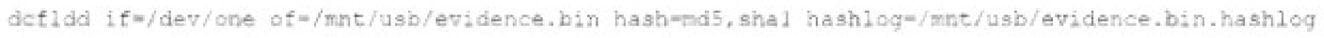
Which of the following is the analyst most likely observing? (Select two).

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

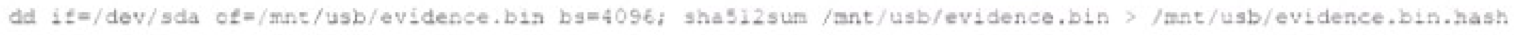
Explanation:
A security analyst is reviewing the network security monitoring logs listed below and is most likely observing that 10.1.1.129 sent potential malicious requests to the web server and that 10.1.1.130 can potentially obtain information about the PHP version. The logs show that 10.1.1.129 sent 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 186
A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?
A)



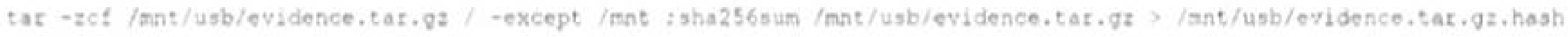
```
dcfldd if=/dev/one of=/mnt/usb/evidence.bin hash=md5,sha1 hashlog=/mnt/usb/evidence.bin.hashlog
```

B)



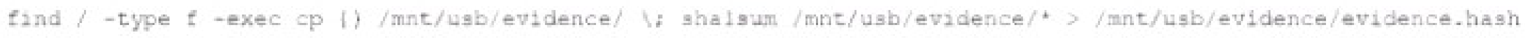
```
dd if=/dev/sda of=/mnt/usb/evidence.bin bs=4096; sha512sum /mnt/usb/evidence.bin > /mnt/usb/evidence.bin.hash
```

C)



```
tar -zcf /mnt/usb/evidence.tar.gz / -except /mnt :sha256sum /mnt/usb/evidence.tar.gz > /mnt/usb/evidence.tar.gz.hash
```

D)



```
find / -type f -exec cp {} /mnt/usb/evidence/ \; sha1sum /mnt/usb/evidence/* > /mnt/usb/evidence/evidence.hash
```

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

Answer: C

Explanation:
Option C shows a device that can perform a forensic copy of a hard drive. A forensic copy, also known as a forensic image or a bit-stream image, is an exact, unaltered digital copy of a piece of digital evidence. A forensic copy captures everything on the hard drive, including active and latent data, and preserves the integrity of the original evidence. A forensic copy can be used for forensic analysis without risking any changes to the original drive1. Option C shows a device that can connect to two hard drives and create a
forensic copy from one drive to another using a write-blocker. A write-blocker is a tool that prevents any data from being written to the destination drive, ensuring that only a read-only copy is made2.

NEW QUESTION 190
A cyber-security analyst is implementing a new network configuration on an existing network access layer to prevent possible physical attacks. Which of the following BEST describes a solution that would apply and cause fewer issues during the deployment phase?

A. Implement port security with one MAC address per network port of the switch.
B. Deploy network address protection with DHCP and dynamic VLANs.
C. Configure 802.1X and EAPOL across the network
D. Implement software-defined networking and security groups for isolation

Answer: A

Explanation:
The security analyst should implement port security with one MAC address per network port of the switch. This will help prevent possible physical attacks on the network access layer, such as MAC flooding or MAC spoofing. Port security is a feature that allows a switch to limit the number of MAC addresses that can be learned on a specific port. By setting the limit to one MAC address per port, the switch will only allow traffic from the device that is connected to that port, and drop any traffic from other devices that try to use that
port. This will prevent attackers from connecting unauthorized devices to the network or impersonating
legitimate devices by changing their MAC addresses3.

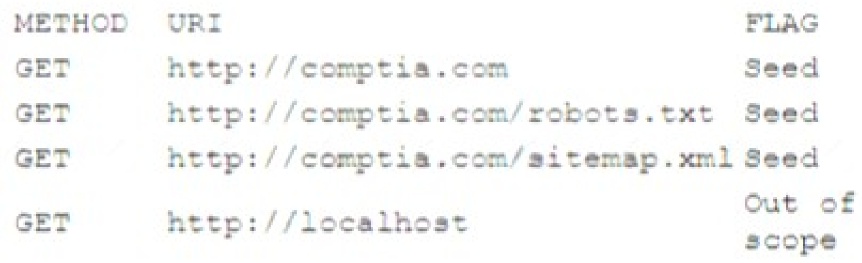
NEW QUESTION 194
During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

A. strings
B. head
C. fsstat
D. dd

Answer: A

Explanation:
The strings command is a Linux utility that can extract human-readable content from any file or partition3. It can be used to analyze a Linux swap partition by finding text strings that may indicate malicious activity or compromise4. The head command (B) can only display the first few lines of a file or partition, which may not contain any useful information. The fsstat command © can only display file system statistics such as size, type, and layout, which may not reveal any human-readable content. The dd command (D) can only copy or convert a file or partition, which may not extract any human-readable content.
References: 3: https://linux.die.net/man/1/strings 4: https://www.linuxjournal.com/content/using-strings-command

NEW QUESTION 199
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
                                         Out of
GET     http://localhost                 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/

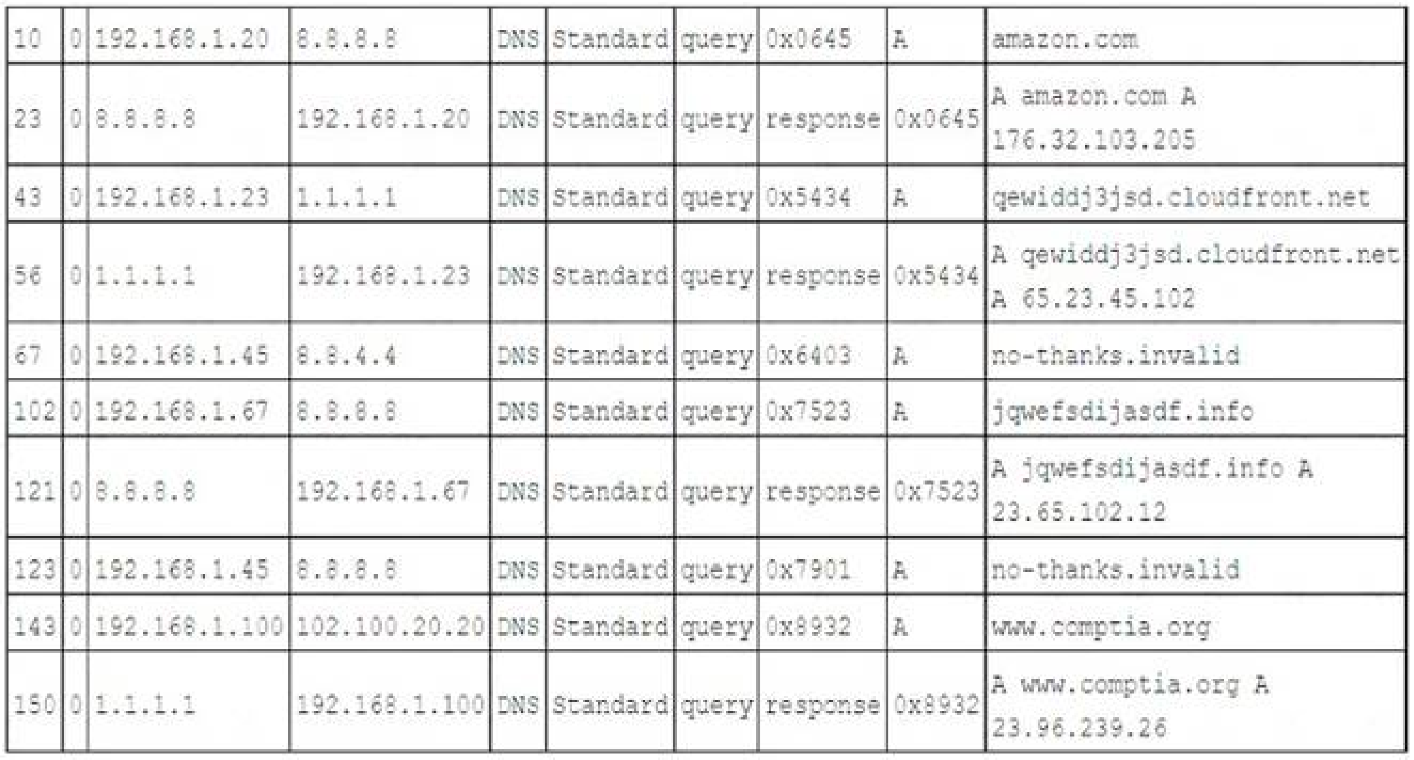
NEW QUESTION 201
Members of the sales team are using email to send sensitive client lists with contact information to their personal accounts The company's AUP and code of conduct prohibits this practice. Which of the following configuration changes would improve security and help prevent this from occurring?

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

Answer: A

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

NEW QUESTION 205
A cybersecurity analyst inspects DNS logs on a regular basis to identify possible IOCs that are not triggered by known signatures. The analyst reviews the following log snippet:



10	0	192.168.1.20	8.8.8.8	DNS	Standard	query	0x0645	A	amazon.com
23	0	8.8.8.8	192.168.1.20	DNS	Standard	query	response	0x0645	A amazon.com A 176.32.103.205
43	0	192.168.1.23	1.1.1.1	DNS	Standard	query	0x5434	A	qewiddj3jsd.cloudfront.net
56	0	1.1.1.1	192.168.1.23	DNS	Standard	query	response	0x5434	A qewiddj3jsd.cloudfront.net A 65.23.45.102
67	0	192.168.1.45	8.8.4.4	DNS	Standard	query	0x6403	A	no-thanks.invalid
102	0	192.168.1.67	8.8.8.8	DNS	Standard	query	0x7523	A	jqwefsdijasdf.info
121	0	8.8.8.8	192.168.1.67	DNS	Standard	query	response	0x7523	A jqwefsdijasdf.info A 23.65.102.12
123	0	192.168.1.45	8.8.8.8	DNS	Standard	query	0x7901	A	no-thanks.invalid
143	0	192.168.1.100	102.100.20.20	DNS	Standard	query	0x8932	A	www.comptia.org
150	0	1.1.1.1	192.168.1.100	DNS	Standard	query	response	0x8932	A www.comptia.org A 23.96.239.26

Which of the following should the analyst do next based on the information reviewed?

A. The analyst should disable DNS recursion.
B. The analyst should block requests to no—thank
C. invalid.
D. The analyst should disconnect host 192.168.1.67.
E. The analyst should sinkhole 102.100.20.20.
F. The analyst should disallow queries to the 8.8.8.8 resolver.

Answer: B

Explanation:
The correct answer is B. The analyst should block requests to no-thanks.invalid. The log snippet shows a DNS query from host 192.168.1.67 to the public resolver 8.8.8.8 for the domain name no-thanks.invalid, which is resolved to the IP address 102.100.20.20. This is a possible indicator of compromise (IOC), as no-thanks.invalid is a known malicious domain that is used by attackers to exfiltrate data or execute
commands on compromised hosts1. The analyst should block requests to this domain to prevent further communication with the attacker's server and investigate the host 192.168.1.67 for signs of infection.
* A. The analyst should disable DNS recursion is not correct. DNS recursion is a process where a DNS server queries other DNS servers on behalf of a client until it finds the authoritative answer for a domain name2.
Disabling DNS recursion would prevent the DNS server from resolving any domain names that are not in its cache or zone files, which would affect the normal functionality of the network and the internet access of the clients.
* C. The analyst should disconnect host 192.168.1.67 is not correct. Disconnecting host 192.168.1.67 would stop the communication with the malicious domain, but it would also disrupt the legitimate activities of the host and its user. Moreover, disconnecting the host would not remove the malware or root cause of the compromise, and it would not prevent the host from reconnecting to the malicious domain once it is online again.
* D. The analyst should sinkhole 102.100.20.20 is not correct. Sinkholing is a technique that redirects malicious or unwanted traffic to a controlled destination, such as a fake or isolated server3. Sinkholing 102.100.20.20 would prevent the communication with the malicious domain, but it would also require access and control over the public resolver 8.8.8.8, which is not owned or managed by the analyst or the company.
* E. The analyst should disallow queries to the 8.8.8.8 resolver is not correct. Disallowing queries to the 8.8.8.8 resolver would prevent the communication with the malicious domain, but it would also affect the resolution of other legitimate domain names that are not in the local DNS server's cache or zone files.
* 1: DNS Tunneling: how DNS can be (ab)used by malicious actors 2: What Is DNS Recursion? 3: What Sinkhole Attack?

NEW QUESTION 210
Which of the following is the most important reason to involve the human resources department in incident response?

A. To better Inform recruiters during hiring so they can include incident response Interview questions
B. To ensure the incident response process captures evidence needed in case of disciplinary actions
C. To validate that the incident response process meets the organization's best practices
D. To prevent Incident responders from Interacting directly with any users

Answer: B

Explanation:
The human resources department should be involved in incident response, to ensure that the incident response process captures evidence needed in case of disciplinary actions against any employees who may have caused or contributed to the incident, either intentionally or unintentionally. The human resources department can also help with enforcing policies and procedures, communicating with employees, and providing legal or ethical guidance.

NEW QUESTION 213
Which of the following is the best reason why organizations need operational security controls?

A. To supplement areas that other controls cannot address
B. To limit physical access to areas that contain sensitive data
C. To assess compliance automatically against a secure baseline
D. To prevent disclosure by potential insider threats

Answer: A

Explanation:
Operational security controls are security measures that are implemented and executed by people rather than by systems. Operational security controls are needed to supplement areas that other controls, such as technical or physical controls, cannot address. For example, operational security controls can include policies, procedures, training, awareness, audits, reviews, testing, etc. These controls can help ensure that employees follow best practices, comply with regulations, detect and report incidents, and respond to emergencies. The other options are not specific to operational security controls or are too narrow in scope.
References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/operational-security-controls

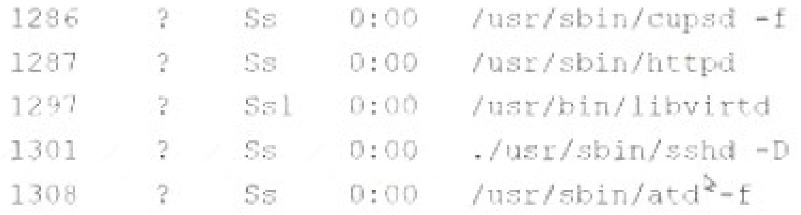
NEW QUESTION 218
A company is building a new fabrication plant and designing its production lines based on the products it manufactures and the networks to support them. The security engineer has the following requirements:
- Each production line must be secured using a single posture.
- Each production line must only communicate with the other lines in a least privilege method.
- Access to each production line from the rest of the network must be strictly controlled. To best provide the protection that meets these requirements, each product line should be:

A. logically segmented and firewalled to control inbound and outbound connectivity.
B. air gapped and firewalled to manage connectivity.
C. air gapped but connected to one another by data diodes.
D. logically segmented and then air gapped to specifically limit traffic.

Answer: A

Explanation:
Logical segmentation is a technique that divides a network into smaller, isolated segments based on logical criteria, such as function, role, or application. Logical segmentation can be implemented using various technologies, such as VLANs, subnets, virtual firewalls, or software-defined networking (SDN). Logical segmentation can enhance the security of a network by reducing the attack surface, limiting the lateral movement of threats, enforcing the principle of least privilege, and facilitating the monitoring and auditing of network traffic12.
Firewall is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules or policies. Firewall can be deployed at the network perimeter or within the network to create internal zones or segments. Firewall can protect a network from unauthorized access, malicious attacks, or data exfiltration by allowing or blocking traffic based on the source, destination, port, protocol, or application3 .
To best provide the protection that meets the requirements of the security engineer, each product line should be logically segmented and firewalled to control inbound and outbound connectivity. This way, each product line can be secured using a single posture that is consistent and manageable. Each product line can also communicate with the other lines in a least privilege method by allowing only the necessary traffic and blocking the rest. Access to each product line from the rest of the network can be strictly controlled by applying firewall rules that restrict or limit the traffic based on the business needs.

NEW QUESTION 222
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 .

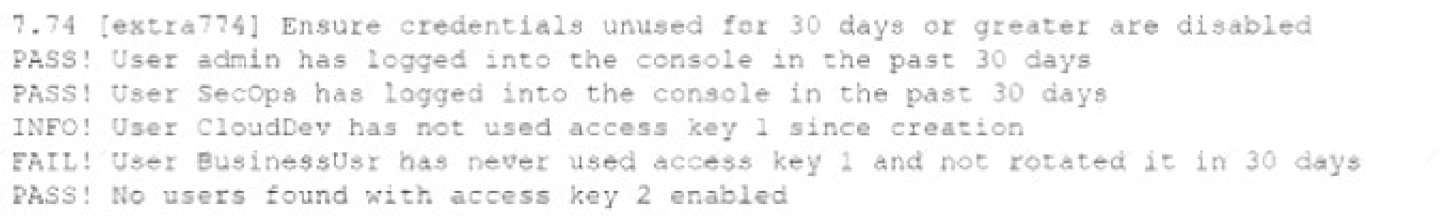
NEW QUESTION 223
While observing several host machines, a security analyst notices a program is overwriting data to a buffer. Which of the following controls will best mitigate this issue?

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

Answer: A

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

NEW QUESTION 228
While conoXicting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:



```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS! User admin has logged into the console in the past 30 days
PASS! User SecOps has logged into the console in the past 30 days
INFO! User CloudDev has not used access key 1 since creation
FAIL! User BusinessUsr has never used access key 1 and not rotated it in 30 days
PASS! No users found with access key 2 enabled
```

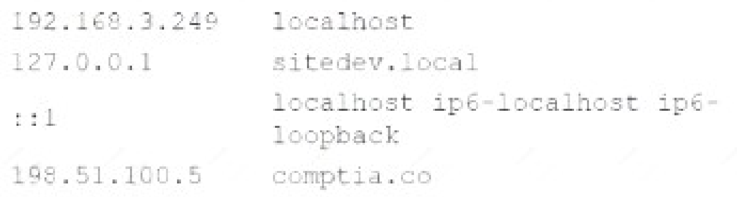
Based on the Prowler report, which of the following is the BEST recommendation?

A. Delete Cloud Dev access key 1
B. Delete BusinessUsr access key 1.
C. Delete access key 1.
D. Delete access key 2.

Answer: A

Explanation:
The best recommendation based on the Prowler report is to delete Cloud Dev access key 1. This is because the report shows that this access key has not been used for more than 90 days, which violates the AWS security best practice of rotating access keys every 90 days or less. Deleting unused or inactive access keys can reduce the risk of unauthorized access or compromise of AWS resources.

NEW QUESTION 229
An analyst Is reviewing a web developer's workstation for potential compromise. While examining the workstation's hosts file, the analyst observes the following:



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

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

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

Answer: D

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

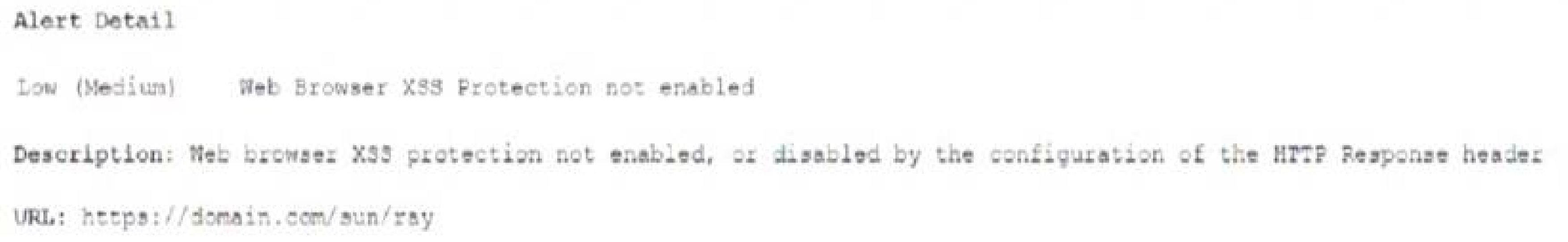
NEW QUESTION 230
At which of the following phases of the SDLC shoukJ security FIRST be involved?

A. Design
B. Maintenance
C. Implementation
D. Analysis
E. Planning
F. Testing

Answer: E

Explanation:
The software development life cycle (SDLC) is a process that consists of several phases that guide the development of software applications or systems. Security should be involved in every phase of the SDLC, but especially in the planning phase, which is the first phase where the scope, objectives, requirements, and resources of the project are defined. By involving security in the planning phase, potential risks and threats can be identified and mitigated early in the process, which can save time, money, and effort later on. Design, maintenance, implementation, analysis, and testing are other phases of the SDLC, but they are not the first phase where security should be involved. Reference:
https://www.bmc.com/blogs/software-development-life-cycle-phases/

NEW QUESTION 231
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 236
A company's blocklist has outgrown the current technologies in place. The ACLs are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures. Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

A. Implement a host-file-based solution that will use a list of all domains to deny for all machines on the network.
B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed
C. Review the current blocklist and prioritize it based on the level of threat severit
D. Add the domains with the highest severity to the blocklist.
E. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs

Answer: D

Explanation:
This is the most effective way to improve performance, as it allows you to reduce the amount of domains in the blocklist and reduce the size of the ACLs. By reviewing the blocklist and removing domains that are no longer active or no longer pose a threat, the blocklist can be reduced and the ACLs updated accordingly. This will reduce the amount of traffic and processing power required to manage the blocklist, and can help improve overall performance.

NEW QUESTION 238
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 242
A cybersecurity analyst needs to Implement controls that will reduce the attack surface of a web server. Which of the following is the best proactive control?

A. Disabling unused modules
B. Installing a host-based IDS
C. Sending logs to a remote server
D. Performing vulnerability scans

Answer: A

Explanation:
Disabling unused modules is a proactive control that can reduce the attack surface of a web server, by minimizing the number of potential entry points or vulnerabilities that an attacker can exploit. Disabling unused modules can also improve the performance and stability of the web server, by freeing up resources and reducing complexity.

NEW QUESTION 245
A security analyst is attempting to resolve an incident in which highly confidential company pricing information was sent to clients. It appears this information was unintentionally sent by an employee who attached it to public marketing material. Which of the following configuration changes would work BEST to limit the risk of this incident being repeated?

A. Add client addresses to the blocklist.
B. Update the DLP rules and metadata.
C. Sanitize the marketing material.
D. Update the insider threat procedures.

Answer: B

Explanation:
Data Loss Prevention (DLP) is a security technology designed to detect, prevent, and respond to the unauthorized disclosure of confidential data. By updating the DLP rules and metadata, it is possible to better define what types of confidential information can be shared and limit access to any sensitive documents.
DLP rules and metadata can help to identify, classify and label sensitive data based on its content and context. DLP rules and metadata can also help to enforce actions or policies on sensitive data, such as blocking, encrypting or alerting .

NEW QUESTION 250
During a company's most recent incident, a vulnerability in custom software was exploited on an externally facing server by an APT. The lessons-learned report noted the following:
• The development team used a new software language that was not supported by the security team's automated assessment tools.
• During the deployment, the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. Therefore, the vulnerability was not detected.
• The current IPS did not have effective signatures and policies in place to detect and prevent runtime attacks on the new application.
To allow this new technology to be deployed securely going forward, which of the following will BEST address these findings? (Choose two.)

A. Train the security assessment team to evaluate the new language and verify that best practices for secure coding have been followed
B. Work with the automated assessment-tool vendor to add support for the new language so these vulnerabilities are discovered automatically
C. Contact the human resources department to hire new security team members who are already familiar with the new language
D. Run the software on isolated systems so when they are compromised, the attacker cannot pivot to adjacent systems
E. Instruct only the development team to document the remediation steps for this vulnerability
F. Outsource development and hosting of the applications in the new language to a third-party vendor so the risk is transferred to that provider

Answer: AB

Explanation:
The solution will address the findings that the development team used a new software language that was not supported by the security team's automated assessment tools and the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. The training of the security assessment team and working with the automated assessment-tool vendor to add support for the new language will ensure that future deployments of the new technology are secure and the vulnerabilities are detected and prevented.

NEW QUESTION 252
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 257
Data sovereignty - Wikipedi2a What Is Data Sovereignty? Everything You Need to Know - What is data sovereignty?
Which of the following is the BEST way to gather patch information on a specific server?

A. Event Viewer
B. Custom script
C. SCAP software
D. CI/CD

Answer: B

Explanation:
A custom script is a piece of code that can be written to perform a specific task or automate a process. A custom script can be used to gather patch information on a specific server by querying the server's operating system, registry, or patch management software and retrieving the relevant data. A custom script can be more flexible and efficient than other methods, such as Event Viewer, SCAP software, or CI/CD, which may not provide the exact information needed or may require additional steps or tools.

NEW QUESTION 259
A company wants to ensure confidential data from its storage media files is sanitized so the drives cannot oe reused. Which of the following is the BEST approach?

A. Degaussing
B. Shredding
C. Formatting
D. Encrypting

Answer: B

Explanation:
https://legalshred.com/degaussing-vs-hard-drive-shredding/
The best and most secure method of rendering hard drive information completely unusable is to completely destroy it through hard drive shredding
Shredding is a method of physically destroying storage media files by cutting them into small pieces using a machine called a shredder. Shredding can ensure that confidential data from storage media files is sanitized so the drives cannot be reused, as it makes it impossible to recover any data from the shredded pieces.

NEW QUESTION 264
A vulnerability assessment solution is hosted in the cloud This solution will be used as an accurate inventory data source for both the configuration management

database and the governance nsk and compliance tool An analyst has been asked to automate the data acquisition Which of the following would be the BEST way to acqutre the data'

A. CSV export
B. SOAR
C. API
D. Machine learning

Answer: C

Explanation:
An example of API is google weather app, using the weather channel's API to collect accurate weather data and broadcast it on goggle weather app, so google doesn't have to do it their selves
API stands for application programming interface, which is a set of rules and protocols that allows different software applications or components to communicate and exchange data. Using an API would be the best way to acquire data from a cloud-based vulnerability assessment solution for both the configuration management database and the governance risk and compliance tool, because it would allow automated and standardized data transfer between different systems. CSV export, SOAR, or machine learning are not methods of data acquisition, but rather formats or tools that can be used for data analysis or processing.
Reference: https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces

NEW QUESTION 267
A company wants to configure the environment to allow passive network monitonng. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?

A. Port bridging
B. Tunnel all mode
C. Full-duplex mode
D. Port mirroring
E. Promiscuous mode

Answer: E

Explanation:
Promiscuous mode is the mode that must be supported by the scanner’s NIC to assist with the company’s request of passive network monitoring. Promiscuous mode is a mode of operation for a network interface controller (NIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is specifically programmed to receive. This mode is normally used for packet sniffing, the practice of collecting and logging packets that pass through the network for further analysis, such as the analysis of traffic or bandwidth usage1. Promiscuous mode makes sure all transmitted data packets are received and read by network adapters.

NEW QUESTION 270
The incident response team is working with a third-party forensic specialist to investigate the root cause of a recent intrusion An analyst was asked to submit sensitive network design details for review The forensic specialist recommended electronic delivery for efficiency but email was not an approved communication channel to send network details Which of the following BEST explains the importance of using a secure method of communication during incident response?

A. To prevent adversaries from intercepting response and recovery details
B. To ensure intellectual property remains on company servers
C. To have a backup plan in case email access is disabled
D. To ensure the management team has access to all the details that are being exchanged

Answer: A

Explanation:
To prevent adversaries from intercepting response and recovery details. Using a secure method of communication during incident response is important to prevent adversaries from intercepting response and recovery details that could reveal the incident response team’s actions, strategies, or findings. If the adversaries can intercept the communication, they could use it to evade detection, escalate their privileges, or launch further attacks. To ensure intellectual property remains on company servers, to have a backup plan in case email access is disabled, or to ensure the management team has access to all the details that are being exchanged are other possible reasons to use a secure method of communication, but they are not as important as preventing adversaries from intercepting response and recovery details. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 272
Which of the following BEST explains the function of a managerial control?

A. To help design and implement the security planning, program development, and maintenance of the security life cycle
B. To guide the development of training, education, security awareness programs, and system maintenance
C. To create data classification, risk assessments, security control reviews, and contingency planning
D. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of audit trails

Answer: A

Explanation:
A managerial control is a function of management that involves setting performance standards, measuring performance, and taking corrective actions when necessary. A managerial control helps to regulate the organizational activities and ensure that they are aligned with the organizational goals and objectives1. One of the functions of a managerial control is to help design and implement the security planning, program development, and maintenance of the security life cycle. The security life cycle is a process that defines the phases of security activities from initiation to disposal2. A managerial control can help to establish the security policies, procedures, roles, and responsibilities for each phase of the security life cycle. A managerial control can also help to monitor and evaluate the security performance and effectiveness of each phase and take corrective actions if needed.

NEW QUESTION 277
After examine 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:
Three common types of file carving methods are as follows: Header- and footer-based carving, which focuses on headers like those found in JPEG files. For example, JPEGs can be found by looking for \xFF\xD8 in the header and \xFF\xD9 in the footer. Content-based carving techniques look for information about the content of a file such as character counts and text recognition. File structure-based carving techniques that use information about the structure of files.
File carving is a technique for recovering files from raw data bytes by scanning and rebuilding them based on their file headers and footers. File headers and footers are sequences of bytes that indicate the beginning and end of a file format, such as JPEG, PDF, ZIP, etc. File carving can be used to reconstruct files that are deleted, corrupted, fragmented, or encrypted by bypassing the file system structure and looking for recognizable patterns in the data3
The analyst used file carving to reconstruct files from a hard disk by scanning the raw
data bytes and rebuilding them based on their file headers and footers.

NEW QUESTION 278
......