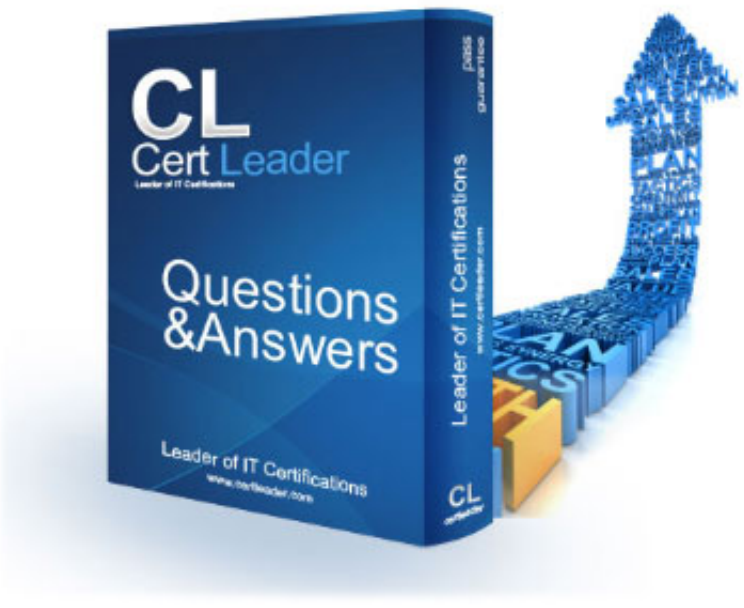
CS0-002 Dumps

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

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



NEW QUESTION 1
After running the cat file01.bin | hexdump -c command, a security analyst reviews the following output snippet:
00000000 ff d8 ft e0 00 10 4a 46 49 46 00 01 01 00 00 01 |.....JFIF.....|
Which of the following digital-forensics techniques is the analyst using?

A. Reviewing the file hash
B. Debugging the binary file
C. Implementing file carving
D. Verifying the file type
E. Utilizing reverse engineering

Answer: D

Explanation:
This is the digital-forensics technique that the analyst is using by running the cat file01.bin | hexdump -c command. This command displays the contents of the binary file in hexadecimal and ASCII format, which can help identify the file type based on its header or signature. In this case, the output snippet shows that the file type is JPEG, as indicated by the ff d8 ff e0 bytes at the beginning and the JFIF string in ASCII.

NEW QUESTION 2
An organization wants to collect IoCs from multiple geographic regions so it can sell the information to its customers. Which of the following should the organization deploy to accomplish this task?

A. A honeypot
B. A bastion host
C. A proxy server
D. A Jumpbox

Answer: A

Explanation:
A honeypot is a decoy system that is designed to attract and trap attackers, by mimicking a real system or network, but containing fake or harmless data. A honeypot can be used to collect IoCs from multiple geographic regions, by deploying it in different locations or networks, and monitoring the activities or attacks that target it. A honeypot can also provide valuable threat intelligence data that can be sold to customers.

NEW QUESTION 3
The management team has asked a senior security engineer to explore DLP security solutions for the company's growing use of cloud-based storage. Which of the following is an appropriate solution to control the sensitive data that is being stored in the cloud?

A. NAC
B. IPS
C. CASB
D. WAF

Answer: C

Explanation:
A cloud access security broker (CASB) is a security solution that monitors and controls the use of cloud-based services and applications. A CASB can provide data loss prevention (DLP) capabilities for sensitive data that is being stored in the cloud, such as encryption, masking, tokenization, or redaction. A CASB can also enforce policies and compliance requirements for cloud usage, such as authentication, authorization, auditing, and reporting. The other options are not appropriate solutions for controlling sensitive data in the cloud. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

NEW QUESTION 4
As part of an Intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several detrains and reputational information that suggest the company's employees may be targeted for a phishing campaign. Which of the following configuration changes would be the MOST appropriate for Mergence gathering?

A. Update the whitelist.
B. Develop a malware signature.
C. Sinkhole the domains
D. Update the Blacklist

Answer: D

Explanation:
A blacklist is a list of domains, IP addresses, email addresses, or other identifiers that are known or suspected to be malicious or harmful. A blacklist can be used to block or filter unwanted or dangerous traffic from reaching a network or system2
Updating the blacklist can help prevent phishing campaigns by adding the
domains or email addresses of the phishing sources to the list and preventing them from sending emails to the company’s employees.

NEW QUESTION 5
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 6
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 7
Which of the following is a vulnerability associated with the Modbus protocol?

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

Answer: D

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

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

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

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

NEW QUESTION 8
Which of the following is the most effective approach to minimize the occurrence of vulnerabilities introduced by unintentional misconfigurations in the cloud?

A. Requiring security training certification before granting access to staff
B. Migrating all resources to a private cloud deployment
C. Restricting changes to the deployment of validated laC templates
D. Reducing laaS deployments by fostering serverless architectures

Answer: C

Explanation:
IaC stands for infrastructure as code, which is a practice of using code or configuration files to automate the provisioning and management of cloud resources. IaC templates can help ensure consistency, repeatability, and scalability of cloud deployments, as well as reduce human errors and misconfigurations. However, IaC templates need to be validated and tested before deployment, and any changes to the templates should be controlled and monitored. This can help minimize the occurrence of vulnerabilities introduced by unintentional misconfigurations in the cloud

NEW QUESTION 9
A Chief Information Officer wants to implement a BYOD strategy for all company laptops and mobile phones. The Chief Information Security Officer is concerned with ensuring all devices are patched and running some sort of protection against malicious software. Which of the following existing technical controls should a security analyst recommend to best meet all the requirements?

A. EDR
B. Port security
C. NAC
D. Segmentation

Answer: A

Explanation:
EDR stands for endpoint detection and response, which is a type of security solution that monitors and protects all devices that are connected to a network, such as laptops and mobile phones. EDR can help to ensure that all devices are patched and running some sort of protection against malicious software by providing continuous visibility, threat detection, incident response, and remediation capabilities. EDR can also help to enforce security policies and compliance requirements across all devices .

NEW QUESTION 10
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).

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

Answer: CE

Explanation:
Documenting the respective chain of custody and performing a memory dump of the mobile device for analysis would help during the forensic analysis of the mobile device. The chain of custody is a record of who handled the evidence, when, where, how, and why. The chain of custody helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1. A memory dump is a process of capturing and storing the contents of the device's memory (RAM) for analysis. A memory dump can help to recover volatile data that may be lost when the device is powered off or rebooted, such as running processes, network connections, encryption keys, or malware traces2.

NEW QUESTION 10
A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?

A. Implement UEM on an systems and deploy security software.
B. Implement DLP on all workstations and block company data from being sent outside the company
C. Implement a CASB and prevent certain types of data from being downloaded to a workstation
D. Implement centralized monitoring and logging for an company systems.

Answer: C

Explanation:
A CASB, or Cloud Access Security Broker, is a software tool or service that acts as an intermediary between an organization's cloud services and its users. A CASB can provide various security functions, such as visibility, compliance, threat protection, and data security2
A CASB can help protect the company's data stored in the cloud by preventing certain types of data from being downloaded to a workstation, such as sensitive or confidential information. This can reduce the risk of data leakage, theft, or loss if a workstation is compromised or stolen.

NEW QUESTION 15
A security operations manager wants some recommendations for improving security monitoring. The security team currently uses past events to create an IOC list for monitoring.
Which of the following is the best suggestion for improving monitoring capabilities?

A. Update the IPS and IDS with the latest rule sets from the provider.
B. Create an automated script to update the IPS and IDS rule sets.
C. Use an automated subscription to select threat feeds for IDS.
D. Implement an automated malware solution on the IPS.

Answer: C

Explanation:
Threat feeds are sources of information that provide timely and relevant data about current or emerging cyber threats, such as indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs), or threat actors. An IDS, or intrusion detection system, is a tool that monitors network traffic and detects malicious or anomalous activities based on predefined or custom rules. Using an automated subscription to select threat feeds for IDS can help to improve security monitoring capabilities by providing the security team with up-to-date and actionable intelligence that can enhance the detection and response to cyberattacks

NEW QUESTION 19
During the onboarding process for a new vendor, a security analyst obtains a copy of the vendor's latest penetration test summary:

Severity	Finding count
Critical	2
High	5
Medium	3
Low	2
Informational	4

Performed by: Vendor Red Team Last performed: 14 days ago
Which of the following recommendations should the analyst make first?

A. Perform a more recent penetration test.
B. Continue vendor onboarding.
C. Disclose details regarding the findings.
D. Have a neutral third party perform a penetration test.

Answer: C

Explanation:
The analyst should disclose details regarding the findings of the vendor’s latest penetration test summary as the first recommendation, as this can help assess the vendor’s security posture and identify any potential risks or issues that may affect the organization. The analyst should review the findings and ask for more information about the scope, methodology, and remediation actions of the penetration test, as well as any evidence or artifacts that support the findings.

NEW QUESTION 23
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 28
An analyst is reviewing the following output as part of an incident:

```
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=10 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=10 ABCDEFGHIJ
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=15 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=15 ABCDEFGHIJ[]8fd
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=20 ABCDEFGHIJ1234567890
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=20 ABCDEFGHIJ1234567890
```

Which of the Wowing is MOST likely happening?

A. The hosts are part of a reflective denial -of -service attack.
B. Information is leaking from the memory of host 10.20 30.40
C. Sensitive data is being exfilltrated by host 192.168.1.10.
D. Host 291.168.1.10 is performing firewall port knocking.

Answer: A

Explanation:
The hosts are most likely part of a reflective denial-of-service attack. A reflective denial-of-service attack is a technique that allows attackers to both magnify the amount of malicious traffic they can generate and obscure the sources of the attack traffic. This type of distributed denial-of-service (DDoS) attack overwhelms the target, causing disruption or outage of systems and services. A reflective denial-of-service attack works by spoofing the target’s IP address and sending requests to vulnerable servers that will respond to the target. The servers act as reflectors that bounce back the responses to the target, amplifying the attack volume and hiding the attacker’s identity1. The output shows that host 10.20.30.40 is sending requests with a spoofed source IP address of 192.168.1.10 to host 203.0.113.15 on port 123, which is used by the Network Time Protocol (NTP). NTP is a common protocol used for reflection/amplification attacks, as it can generate large responses to small requests2.

NEW QUESTION 33
Some hard disks need to be taken as evidence for further analysis during an incident response. Which of the following procedures must be completed FIRST for this type of evidence acquisition?

A. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from nonauthorized access.
B. Build the chain-of-custody document, noting the media model, serial number, size, vendor, date, and time of acquisition.
C. Perform a disk sanitization using the command #dd if=/dev/zero of=/dev/sdc bs=1M over the media that will receive a copy of the collected data.
D. Execute the command #dd if-/dev/sda of=/dev/sdc bs=512 to clone the evidence data to external media to prevent any further change.

Answer: B

Explanation:
Building the chain-of-custody document is the procedure that must be completed first for this type of evidence acquisition. The chain-of-custody document is a record that tracks the handling and custody of digital evidence from the time it is collected until it is presented in court. The chain-of-custody document should include information such as the media model, serial number, size, vendor, date, and time of acquisition, as well as the names and signatures of the persons who handled, transferred, or examined the evidence. The chain-of-custody document helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1.

NEW QUESTION 37
A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse
non-business-related websites?

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

Answer: A

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

NEW QUESTION 40
A SIEM analyst receives an alert containing the following URL:
http://companywebsite.com/displayPicture?filename=../../../etc/passwd
Which of the following BEST describes the attack?

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

Answer: D

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

NEW QUESTION 43
Which of the following should a database administrator for an analytics firm implement to best protect PII from an insider threat?

A. Data deidentification
B. Data encryption
C. Data auditing
D. Data minimization

Answer: C

Explanation:
Data auditing is the most essential and effective method to protect PII from an insider threat. Data auditing is the process of monitoring and recording the activities and events related to data access and usage. Data
auditing can help detect and prevent any suspicious or anomalous behavior by an insider threat who tries to
access or manipulate PII.
Data auditing can provide several benefits for data protection, such as:

- It can provide accountability and transparency for data access and usage, which can deter potential insider threats from abusing their privileges or violating policies.
- It can provide evidence and traceability for data incidents, which can help investigate and respond to data breaches or leaks by insider threats.
- It can provide feedback and insights for data security improvement, which can help identify and address any gaps or weaknesses in data protection measures.

Data auditing can be done by using tools such as logs, alerts, reports, or dashboards. These tools can help security analysts track and analyze data activity and identify any patterns or anomalies that indicate a possible insider threat.

NEW QUESTION 46
A company needs to expand Its development group due to an influx of new feature requirements (rom Its customers. To do so quickly, the company is using Junior-level developers to fill in as needed. The company has found a number of vulnerabilities that have a direct correlation to the code contributed by the junior-level developers. Which of the following controls would best help to reduce the number of software vulnerabilities Introduced by this situation?

A. Requiring senior-level developers to review code written by junior-level developers
B. Hiring senior-level developers only
C. Allowing only senior-level developers to write code for new features
D. Using authorized source code repositories only

Answer: A

Explanation:
This control would best help to reduce the number of software vulnerabilities introduced by this situation because it ensures that code quality and security standards are met before deploying to production.
Senior-level developers can provide feedback, guidance, and corrections to junior-level developers and catch any errors or flaws in their code.

NEW QUESTION 50
A security analyst is monitoring a company's network traffic and finds ping requests going to accounting and human resources servers from a SQL server. Upon investigation, the analyst discovers a technician responded to potential network connectivity issues. Which of the following is the best way for the security analyst to respond?

A. Report this activity as a false positive, as the activity is legitimate.
B. Isolate the system and begin a forensic investigation to determine what was compromised.
C. Recommend network segmentation to the management team as a way to secure the various environments.
D. Implement host-based firewalls on all systems to prevent ping sweeps in the future.

Answer: A

Explanation:
Reporting this activity as a false positive, as the activity is legitimate, is the best way for the security analyst to respond. A false positive is a condition in which harmless traffic is classified as a potential network attack by a security monitoring tool. Ping requests are a common network diagnostic tool that can be used to test network connectivity issues. The technician who responded to potential network connectivity issues was performing a legitimate task and did not pose any threat to the accounting and human resources servers .

NEW QUESTION 51
During a review of SIEM alerts, a securrty analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring toot about files from a newly deployed application that should not change. Which of the following steps should the analyst complete FIRST to respond to the issue7

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

Answer: C

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

NEW QUESTION 54
A security analyst is concerned about sensitive data living on company file servers following a zero-day attack that nearly resulted in a breach of millions of customer records. The after action report indicates a lack of controls around the file servers that contain sensitive data. Which of the following DLP considerations would best help the analyst to classify and address the sensitive data on the file servers?

A. Implement a CASB device and connect the SaaS applications.
B. Deploy network DLP appliances pointed to all file servers.
C. Use data-at-rest scans to locate and identify sensitive data.
D. Install endpoint DLP agents on all computing resources.

Answer: C

Explanation:
Use data-at-rest scans to locate and identify sensitive data. This option is the best DLP consideration for addressing the sensitive data on the file servers. Data-at-rest scans are performed on data that is stored on a device or a network, such as file servers, and can help identify and classify sensitive data based on predefined policies or rules. The other options are not relevant for this scenario, as they either deal with data in transit (network DLP appliances), data in use (endpoint DLP agents), or cloud-based data (CASB device).

NEW QUESTION 59
A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?

A. Ask for external scans from industry peers, look at the open ports, and compare Information with the client.
B. Discuss potential tools the client can purchase lo reduce the livelihood of an attack.
C. Look at attacks against similar industry peers and assess the probability of the same attacks happening.
D. Meet with the senior management team to determine if funding is available for recommended solutions.

Answer: C

Explanation:
A good approach for modeling the client’s attack surface is to look at attacks against similar industry peers and assess the probability of the same attacks happening. This can help the consultant to identify the most relevant and likely threats for the client based on their industry sector, size, location, and other factors. This can also help the consultant to prioritize the most critical risks and recommend appropriate mitigation strategies. Asking for external scans from industry peers (A) may not be feasible or reliable, as industry peers may not share their scan results or have different security configurations and vulnerabilities than the client. Discussing potential tools the client can purchase (B) may not be effective, as tools alone cannot reduce the likelihood of an attack without proper implementation and management. Meeting with senior management team (D) may not be helpful, as funding is not directly related to modeling the attack surface and may depend on other factors such as budget constraints and risk appetite.

NEW QUESTION 64
An organization wants to implement controls for protecting private information at rest. Which of the following would meet the organization's need?

A. Non-disclosure agreements
B. Retention policies
C. Data minimization
D. Encryption

Answer: D

Explanation:
The correct answer is D. Encryption. Encryption is a technical control that transforms data into an unreadable format using a secret key or algorithm. Encryption can protect data at rest by preventing unauthorized access, modification, or exfiltration of the data. Encryption can also protect data in transit and in use, depending on the type and level of encryption applied1.

NEW QUESTION 68
While reviewing system logs, a network administrator discovers the following entry:

```
psexec \\10.1.11.2 -u Administrator -p testpw cmd.exe
```

Which of the following occurred?

A. An attempt was made to access a remote workstation.
B. The PsExec services failed to execute.
C. A remote shell failed to open.
D. A user was trying to download a password file from a remote system.

Answer: D

Explanation:
The output shows an entry from a system log that indicates a user was trying to download a password file from a remote system using PsExec. PsExec is a command-line tool that allows users to execute processes on remote systems. The entry shows that the user “administrator” tried to run PsExec with the following parameters: \192.168.1.100 -u administrator -p P@ssw0rd -c cmd.exe /c type c:\windows\system32\config\SAM > \192.168.1.101\c$\temp\sam.txt This means that the user tried to connect to the remote system with IP address 192.168.1.100 using the username “administrator” and password “P@ssw0rd”, copy cmd.exe to the remote system, and execute it with the command “type c:\windows\system32\config\SAM > \192.168.1.101\c$\temp\sam.txt”. This command attempts to read the SAM file, which contains hashed passwords of local users, and write it to a file on another system with IP address 192.168.1.101. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

NEW QUESTION 72
A security analyst is reviewing a new Internet portal that will be used for corporate employees to obtain their pay statements. Corporate policy classifies pay statement information as confidential, and it must be protected by MFA. Which of the following would best fulfill the MFA requirement while keeping the portal accessible from the internet?

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

Answer: B

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

NEW QUESTION 74
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

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

Answer: B

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

NEW QUESTION 76
Which of the following factors would determine the regulations placed on data under data sovereignty laws?

A. What the company intends to do with the data it owns
B. The company's data security policy
C. The type of data the company stores
D. The data laws of the country in which the company is located

Answer: D

Explanation:
The data laws of the country in which the company is located would determine the regulations placed on data under data sovereignty laws. Data sovereignty laws are laws that govern how data is collected, stored, processed, and transferred within a country's jurisdiction. Data sovereignty laws can vary from country to country, depending on their legal system, political system, culture, and values. Data sovereignty laws can affect how companies handle their data, especially when they operate across borders or use cloud services. For example, some countries may have strict data protection or privacy laws that require companies to obtain consent from data subjects before collecting or processing their data. Some countries may also have data localization or data residency laws that require companies to store their data within the country's borders or limit cross-border data transfers.

NEW QUESTION 79
A security analyst needs to recommend a solution that will allow users at a company to access cloud-based SaaS services but also prevent them from uploading and exfiltrating data. Which of the following solutions should the security analyst recommend?

A. CASB
B. MFA
C. VPN
D. VPS
E. DLP

Answer: A

Explanation:
A cloud access security broker (CASB) is a solution that acts as a gatekeeper between users and cloud-based SaaS services. A CASB can enforce security policies, such as data loss prevention (DLP), encryption, authentication, or access control, to protect sensitive data from unauthorized access, upload, or exfiltration. A CASB can also provide visibility and monitoring of cloud usage and activity1.

NEW QUESTION 82
A security analyst is reviewing the following server statistics:

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

Which of the following is MOST likely occurring?

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

Answer: C

Explanation:
Resource exhaustion is most likely occurring on the server. Resource exhaustion is a condition where a system runs out of resources, such as CPU, memory, disk space, or network bandwidth, due to excessive demand or consumption by one or more processes. Resource exhaustion can cause performance degradation, system instability, or denial-of-service. The server statistics show that the CPU usage is 100%, the memory usage is 99%, and the disk usage is 98%. These indicate that the server is under heavy load and has little or no resources available to handle incoming requests or perform other tasks.

NEW QUESTION 87
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 89
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 94
An organization wants to consolidate a number of security technologies throughout the organization and standardize a workflow for identifying security issues prioritizing the severity and automating a response Which of the following would best meet the organization's needs'?

A. MaaS
B. SIEM
C. SOAR
D. CI/CD

Answer: C

Explanation:
A security orchestration, automation, and response (SOAR) system is a solution that combines various security technologies and workflows to identify security issues, prioritize their severity, and automate a response. A SOAR system can help an organization consolidate its security tools and processes and standardize its workflow for incident response. The other options are not relevant or comprehensive for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15; https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-and-response-s

NEW QUESTION 95
An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?

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

Answer: B

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

NEW QUESTION 97
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 102
A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

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

Answer: C

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

NEW QUESTION 103
The following output is from a tcpdump al the edge of the corporate network:

```
12:47:22.179345 PPPoE  [ses 0x8122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 10.5.1.1 > 198.134.5.201: IP6 (hlim 63, next-header
TCP (6) payload length: 32) 2001:67c:2158:a019::ace.53104 > 2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788: Flags [S], cksum 0x58cf (correct), seq 1155375165, win 8192,
options [mss 1412,nop,wscale 2,nop,nop,sackOK], length 0

12:47:22.251065 PPPoE  [ses 0x8122] IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 198.134.5.201 > 10.5.1.1: IP6 (hlim 127, next-
header TCP (6) payload length: 32) 2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788 > 2001:67c:2158:a019::ace.53104: Flags [S.], cksum 0xd361 (correct), seq 2642471061,
ack 1155375166, win 8192, options [mss 1220,nop,wscale 6,nop,nop,sackOK], length 0
```

Which of the following best describes the potential security concern?

A. Payload lengths may be used to overflow buffers enabling code execution.
B. Encapsulated traffic may evade security monitoring and defenses
C. This traffic exhibits a reconnaissance technique to create network footprints.
D. The content of the traffic payload may permit VLAN hopping.

Answer: B

Explanation:
Encapsulated traffic may evade security monitoring and defenses by hiding or obfuscating the actual content or source of the traffic. Encapsulation is a technique that wraps data packets with additional headers or protocols to enable communication across different network types or layers. Encapsulation can be used for legitimate purposes, such as tunneling, VPNs, or NAT, but it can also be used by attackers to bypass security controls or detection mechanisms that are not able to inspect or analyze the encapsulated traffic .

NEW QUESTION 104
A security analyst needs to automate the incident response process for malware infections. When the following logs are generated, an alert email should automatically be sent within 30 minutes:

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

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

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

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

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

Answer: D

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

NEW QUESTION 108
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 113
A security analyst is reviewing WAF alerts and sees the following request:

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

Which of the following BEST describes the attack?

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

Answer: A

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

NEW QUESTION 116
A security analyst observes a large amount of scanning activity coming from an IP address outside the organization's environment. Which of the following should the analyst do to block this activity?

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

Answer: C

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

NEW QUESTION 118
An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by pubic users accessing the server. The results should be written to a text file and should induce the date. time, and IP address associated with any spreadsheet downloads. The web server's log file Is named webserver log, and the report We name should be accessreport.txt. Following is a sample of the web servefs.log file:
2017-0-12 21:01:12 GET /index.htlm - @4..102.33.7 - return=200 1622
Which of the following commands should be run if an analyst only wants to include entries in which spreadsheet was successfully downloaded?

A. more webserver.log | grep * xIs > accessreport.txt
B. more webserver.log > grep "xIs > egrep -E 'success' > accessreport.txt
C. more webserver.log | grep ' -E "return=200 | accessreport.txt
D. more webserver.log | grep -A *.xIs < accessreport.txt

Answer: C

Explanation:
The grep command is a tool that searches for a pattern of characters in a file or input and prints the matching lines1
The egrep command is a variant of grep that supports extended regular expressions, which allow more
complex and flexible pattern matching2
The more command is a filter that displays the contents of a file or
input one screen at a time3
The pipe symbol (|) is used to redirect the output of one command to the input of
another command. The redirection symbol (>) is used to redirect the output of a command to a file.
The command given in option C performs the following steps:

- It uses the more command to display the contents of the webserver.log file.
- It pipes the output of the more command to the grep command, which searches for lines that contain '*.xls', which is a pattern that matches any file name ending with .xls (a spreadsheet file extension).
- It pipes the output of the grep command to the egrep command, which searches for lines that contain 'return=200', which is a pattern that matches any HTTP status code of 200 (which indicates a successful request).
- It redirects the output of the egrep command to a file named accessreport.txt, which contains the date, time, and IP address associated with any spreadsheet downloads.

NEW QUESTION 120
A security analyst identified one server that was compromised and used as a data making machine, and a few of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?

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

Answer: A

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

NEW QUESTION 121
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 124
Given the output below:
#nmap 7.70 scan initiated Tues, Feb 8 12:34:56 2022 as: nmap -v -Pn -p 80,8000,443 --script http-* -oA server.out 192.168.220.42
Which of the following is being performed?

A. Cross-site scripting
B. Local file inclusion attack
C. Log4] check
D. Web server enumeration

Answer: D

Explanation:
Web server enumeration is the process of identifying information about a web server, such as its software version, operating system, configuration, services, and vulnerabilities. This can be done using tools like Nmap, which can scan ports and run scripts to gather information. In this question, the Nmap command is using the -p option to scan ports 80, 8000, and 443, which are commonly used for web services. It is also using the --script option to run scripts that start with http-*, which are related to web server enumeration. The output file name server.out also suggests that the purpose of the scan is to enumerate web servers. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

NEW QUESTION 129
Which of the following SCAP standards provides standardization tor measuring and describing the seventy of security-related software flaws?

A. OVAL
B. CVSS
C. CVE
D. CCE

Answer: B

Explanation:
CVSS stands for Common Vulnerability Scoring System, and it is a standard for measuring and describing the severity of security-related software flaws. CVSS provides a numerical score and a vector string that represent the characteristics and impact of a vulnerability. CVSS can help prioritize remediation efforts and communicate risk levels to stakeholders.

NEW QUESTION 134
Which of the following is a difference between SOAR and SCAP?

A. SOAR can be executed taster and with fewer false positives than SCAP because of advanced heunstics
B. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope
C. SOAR is less expensive because process and vulnerability remediation is more automated than what SCAP does
D. SOAR eliminates the need for people to perform remediation, while SCAP relies heavily on security analysts

Answer: B

Explanation:
SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope. SOAR (Security Orchestration, Automation and Response) is a technology that helps coordinate, execute and automate tasks between various people and tools within a single platform. SOAR can help improve the efficiency and effectiveness of security operations by reducing manual effort, enhancing
collaboration, and accelerating incident response1. SCAP (Security Content Automation Protocol) is a standard that enables automated vulnerability management, measurement and policy compliance evaluation of systems deployed in an organization2. SCAP can help assess the security posture and compliance status of systems by using predefined specifications and checklists. However, SCAP does not provide orchestration or automation capabilities beyond vulnerability scanning and reporting.

NEW QUESTION 136
A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

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

Answer: A

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

NEW QUESTION 137
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 138
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 143
A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified Which of the following values should the security analyst choose when evaluating the CVSS score?

A. Network
B. Physical
C. Adjacent
D. Local

Answer: C

Explanation:
The Common Vulnerability Scoring System (CVSS) is a standard for measuring the severity of vulnerabilities in software systems. One of the factors that affects the CVSS score is the attack vector, which describes how the vulnerability can be exploited. The possible values for the attack vector are network, adjacent network, local, or physical. In this case, the analyst should choose local as the value for the attack vector, because the Tomcat configuration file must be modified for the attack to be successful, which implies that the attacker needs local access to the system. Network, adjacent network, or physical are not appropriate values for the attack vector in this scenario. Reference:
https://www.first.org/cvss/v3.1/specification-document#Vector-String

NEW QUESTION 146
An organization is required to be able to consume multiple threat feeds simultaneously and to provide actionable intelligence to various teams. The organization would also like to be able to leverage the intelligence to enrich security event data. Which of the following functions would most likely help the security analyst meet the organization's requirements?

A. Vulnerability management
B. Risk management
C. Detection and monitoring
D. Incident response

Answer: C

Explanation:
The correct answer is C. Detection and monitoring. Detection and monitoring is a function that involves collecting, analyzing, and correlating data from various sources, such as threat feeds, logs, alerts, or events, to identify and respond to potential or ongoing threats. Detection and monitoring can help the organization to consume multiple threat feeds simultaneously and to provide actionable intelligence to various teams, such as security operations center (SOC) analysts, incident responders, or threat hunters. Detection and monitoring can also help the organization to leverage the intelligence to enrich security event data, such as adding context, severity, or priority to the events1.
* A. Vulnerability management is not correct. Vulnerability management is a function that involves identifying, assessing, and mitigating the weaknesses or flaws in systems, applications, or networks that could be exploited by attackers. Vulnerability management can help the organization to reduce its attack surface and prevent potential breaches, but it does not directly involve consuming multiple threat feeds simultaneously or providing actionable intelligence to various teams.
* B. Risk management is not correct. Risk management is a function that involves identifying, analyzing, and evaluating the risks that could affect the organization’s assets, operations, or objectives. Risk management can help the organization to prioritize and implement appropriate controls or mitigation strategies to reduce the likelihood or impact of the risks, but it does not directly involve consuming multiple threat feeds simultaneously or providing actionable intelligence to various teams.
* D. Incident response is not correct. Incident response is a function that involves preparing for, detecting, containing, analyzing, and recovering from security incidents that compromise the confidentiality, integrity, or availability of the organization’s assets or operations. Incident response can help the organization to minimize the damage and restore normal operations as quickly as possible, but it does not directly involve consuming multiple threat feeds simultaneously or providing actionable intelligence to various teams.
1: Cybersecurity Analyst+ - CompTIA

NEW QUESTION 151
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 153

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 156
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 157
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

Server1 Log

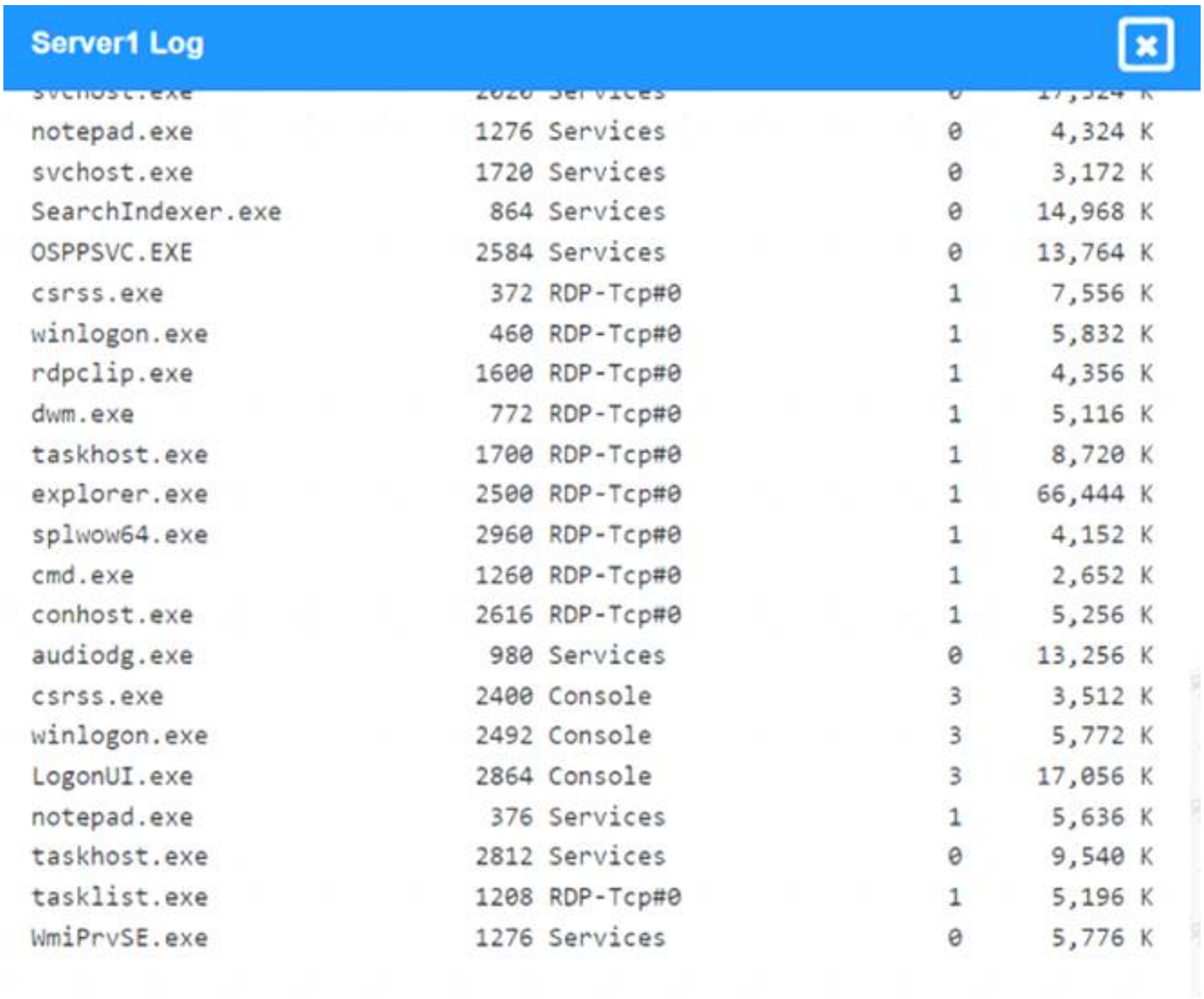
```
C:\Users\Team3>netstat -oan

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
```



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Server1 and svchost.exe

NEW QUESTION 159
A security engineer is reviewing security products that identify malicious actions by users as part of a company's insider threat program. Which of the following is the most appropriate product category for this purpose?

A. SCAP
B. SOAR
C. UEBA
D. WAF

Answer: C

Explanation:
UEBA stands for User and Entity Behavior Analytics, which is a category of security products that use machine learning and statistical analysis to identify malicious actions by users or entities on a network. UEBA products can detect anomalous or suspicious behaviors that deviate from normal patterns or baselines, such as data exfiltration, privilege escalation, unauthorized access, insider threats, or compromised accounts. UEBA products can also provide alerts, reports, or recommendations for response actions based on the detected behaviors.

NEW QUESTION 161
An employee observes degraded system performance on a Windows workstation. While attempting to access documents, the employee notices the file icons appear abnormal and the file extensions have been changed. The employee instantly shuts down the machine and alerts a supervisor.
Which of the following forensic evidence will be lost as a result of these actions?

A. All user actions prior to shutting down the machine
B. All information stored in the machine's local database
C. All cached items that are queued to be written to the registry
D. Volatile artifacts in the system's memory

Answer: D

Explanation:
Volatile artifacts are data that is stored in a computer’s volatile memory while it is running, such as open network connections, running processes, encryption keys, and internet history. Volatile artifacts can provide
valuable evidence for forensic investigations, especially for detecting and analyzing malware or malicious activities that do not leave traces on the hard drive. However, volatile artifacts are wiped off the system’s memory once the power is turned off, so they cannot be recovered later

NEW QUESTION 162

A security analyst needs to recommend the best approach to test a new application that simulates abnormal user behavior to find software bugs. Which of the following would best accomplish this task?

A. A static analysis to find libraries with flaws handling user inputs
B. A dynamic analysis using a dictionary to simulate user inputs
C. Reverse engineering to circumvent software protections
D. Fuzzing tools with polymorphic methods

Answer: D

Explanation:
Fuzzing is a technique that involves sending random, malformed, or unexpected inputs to an application to trigger errors, crashes, or vulnerabilities. Fuzzing can be used to test the robustness and security of software, especially when the source code is not available or the input format is complex1. Fuzzing can also simulate abnormal user behavior, such as entering invalid data, clicking on random buttons, or sending malicious requests2.
Fuzzing tools are software programs that automate the process of generating and sending inputs to the application under test. There are different types of fuzzing tools, such as black-box fuzzers, white-box fuzzers, and grey-box fuzzers, depending on the level of information and feedback they have about the application1. Some examples of fuzzing tools are AFL, Peach, and [Sulley].
Polymorphic methods are techniques that allow fuzzing tools to modify or mutate the inputs in different ways, such as changing the length, value, type, or structure of the data. Polymorphic methods can increase the diversity and effectiveness of the inputs and help discover more bugs or vulnerabilities in the application .
Therefore, using fuzzing tools with polymorphic methods would be the best approach to test a new application that simulates abnormal user behavior to find software bugs. This approach would generate a large number of inputs that cover various scenarios and edge cases and expose any flaws or weaknesses in the application's functionality or security.

NEW QUESTION 165
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 166
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 167
A forensic examiner is investigating possible malware compromise on an active endpoint device. Which of the following steps should the examiner perform first?

A. Verify the hash value of the image with the value of the copy.
B. Use a write blocker to create an image of the hard drive.
C. Create a memory dump from RAM.
D. Download and apply the latest AV signature.
E. Reimage the hard drive and apply the latest updates.

Answer: C

Explanation:
A memory dump is a snapshot of the contents of the random access memory (RAM) of a system at a given
point in time. A memory dump can provide valuable information for a forensic examiner who is investigating possible malware compromise on an active endpoint device, such as running processes, open files, network connections, encryption keys, or malware artifacts. Creating a memory dump from RAM should be the first step that the examiner performs, as it preserves the volatile data that could be lost or altered if the system is powered off or rebooted1.

NEW QUESTION 170
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 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 175
An organization is performing a risk assessment to prioritize resources for mitigation and remediation based on impact. Which of the following metrics, in addition to the CVSS for each CVE, would best enable the organization to prioritize its efforts?

A. OS type
B. OS or application versions
C. Patch availability
D. System architecture
E. Mission criticality

Answer: C

Explanation:
A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect an organization's assets, operations, or objectives. A risk assessment matrix is a tool that can help prioritize the risks based on their likelihood and impact1.
The CVSS (Common Vulnerability Scoring System) is a standard framework for rating the severity of vulnerabilities in software systems. The CVSS provides a numerical score from 0 to 10, as well as a qualitative rating from Low to Critical, based on the characteristics and consequences of the vulnerability2.
However, the CVSS score alone may not be sufficient to determine the priority of mitigation and remediation actions for each vulnerability. Other factors that may influence the decision include:

- Patch availability: This metric indicates whether there is a fix or update available for the vulnerability from the vendor or developer. Patch availability can affect the urgency and feasibility of remediation, as well as the risk exposure and potential damage of exploitation. For example, a vulnerability with a high CVSS score but with a readily available patch may be less critical than a vulnerability with a lower CVSS score but with no patch available3.
- Mission criticality: This metric reflects the importance and value of the asset or system affected by the vulnerability to the organization's mission, goals, or functions. Mission criticality can affect the impact and priority of remediation, as well as the risk tolerance and acceptance level of the organization. For example, a vulnerability with a high CVSS score but affecting a non-essential system may be less critical than a vulnerability with a lower CVSS score but affecting a core system4.
- OS type: This metric indicates the operating system (OS) of the asset or system affected by the vulnerability. OS type can affect the likelihood and complexity of exploitation, as well as the availability and compatibility of patches or mitigations. For example, a vulnerability with a high CVSS score but affecting an uncommon or unsupported OS may be less critical than a vulnerability with a lower CVSS score but affecting a widely used or supported OS3.
- OS or application versions: This metric indicates the specific version of the OS or application affected by the vulnerability. OS or application versions can affect the applicability and relevance of the vulnerability, as well as the availability and compatibility of patches or mitigations. For example, a vulnerability with a high CVSS score but affecting an outdated or obsolete version may be less critical than a vulnerability with a lower CVSS score but affecting a current or popular version3.
- System architecture: This metric indicates the design and configuration of the asset or system affected by the vulnerability. System architecture can affect the exposure and accessibility of the vulnerability, as well as the effectiveness and efficiency of patches or mitigations. For example, a vulnerability with a high CVSS score but affecting an isolated or segmented system may be less critical than a vulnerability with a lower CVSS score but affecting an interconnected or integrated system3.

Therefore, to best enable the organization to prioritize its efforts based on impact, patch availability is one of the most important metrics to consider in addition to the CVSS score for each CVE (Common Vulnerabilities and Exposures). Patch availability can directly influence the risk level and remediation strategy for each vulnerability.

NEW QUESTION 180
A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verify that a user's data is not altered without the user's consent. Which of the following would be an appropriate course of action?

A. Automate the use of a hashing algorithm after verified users make changes to their data.
B. Use encryption first and then hash the data at regular, defined times.
C. Use a DLP product to monitor the data sets for unauthorized edits and changes.
D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

Answer: A

Explanation:
Automating the use of a hashing algorithm after verified users make changes to their data is an appropriate course of action to verify that a user's data is not altered without the user's consent. Hashing is a technique that produces a unique and fixed-length value for a given input, such as a file or a message. Hashing can help to verify the data integrity by comparing the hash values of the original and modified data. If the hash values match, then the data has not been altered without the user's consent. If the hash values differ, then the data may have been tampered with or corrupted .

NEW QUESTION 185
To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

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

Answer: A

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

NEW QUESTION 186
A company's application development has been outsourced to a third-party development team. Based on the SLA. The development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

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

Answer: B

Explanation:

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

NEW QUESTION 188
A security analyst is reviewing the following DNS logs as part of security-monitoring activities:
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www.company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfchfaerwfj.co 32.56.32.122
FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53
FROM 192.168.1.93 ARAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www.comptia.org 122.10.31.87
Which of the following most likely occurred?

A. The attack used an algorithm to generate command and control information dynamically.
B. The attack attempted to contact www.google.com to verify internet connectivity.
C. The attack used encryption to obfuscate the payload and bypass detection by an IDS.
D. The attack caused an internal host to connect to a command and control server.

Answer: A

Explanation:
This is a technique that is commonly used by malware to evade detection and blocking by security tools. The malware generates random domain names that are used to communicate with the command and control server, which can change its IP address frequently. The domain names are usually long and nonsensical, such as www.uewiryfajfchfaerwfj.co in the log. The malware uses a predefined algorithm or a seed value to generate the same domain names as the server, so that they can find each other on the internet12.

NEW QUESTION 192
A security analyst is reviewing the following server statistics:

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

Which of the following Is MOST likely occurring?

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

Answer: C

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

NEW QUESTION 195
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 197
A security analyst performed a targeted system vulnerability scan to obtain critical information. After the output result, the analyst used the OVAL XML language to review and calculate the discovered risk. Which of the following types of scans did the security analyst perform?

A. Active
B. Network map
C. Passive
D. External

Answer: A

Explanation:
An active scan is a type of system vulnerability scan that involves sending probes or packets to the target system, and analyzing the responses or behaviors of the system. An active scan can help obtain critical information about the system, such as open ports, running services, operating system, software versions, etc. An active scan can also use OVAL XML language to review and calculate the discovered risk. OVAL stands for Open Vulnerability and Assessment Language, and it is a standard for describing and exchanging information about system vulnerabilities and configurations.

NEW QUESTION 198
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 201
A developer is working on a program to convert user-generated input in a web form before it is displayed by the browser. This technique is referred to as:

A. output encoding.
B. data protection.
C. query parameterization.
D. input validation.

Answer: A

Explanation:
Output encoding is a technique that converts user-generated input in a web form before it is displayed by the browser. Output encoding is a form of data sanitization that prevents cross-site scripting (XSS) attacks, which occur when malicious scripts are injected into web pages and executed by unsuspecting users4.
Output encoding works by replacing special characters in user input, such as <, >, ", ', &, etc., with their
HTML-encoded equivalents, such as <, >, ", ', &, etc. This prevents the browser from interpreting the user input as HTML or JavaScript code and executing it.

NEW QUESTION 205
A security analyst is analyzing the following output from the Spider tab of OWASP ZAP after a vulnerability scan was completed:

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

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

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

Answer: D

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

NEW QUESTION 207
During an incident investigation, a security analyst discovers the web server is generating an unusually high volume of logs The analyst observes the following response codes:
• 20% of the logs are 403
• 20% of the logs are 404
• 50% of the logs are 200
• 10% of the logs are other codes
The server generates 2MB of logs on a daily basis, and the current day log is over 200MB. Which of the following commands should the analyst use to identify the source of the activity?

A. cat access_log Igrep " 403 "
B. cat access_log Igrep " 200 "
C. cat access_log Igrep " 100 "
D. cat access_log Igrep " 4 04 "
E. cat access_log Igrep " 204 "

Answer: B

Explanation:
Requests sent from the same IP address using different user agents are likely to be malicious or suspicious, as they indicate that an attacker is trying to evade detection or bypass security controls by changing their browser or device identification. These requests may indicate that an attacker is using automated tools or scripts to scan or attack the web server.
Requests identified by a threat intelligence service with a bad reputation are also likely to be malicious or suspicious, but they are not the source of the activity, as they originate from different IP addresses. These requests may indicate that an attacker is trying to exploit a vulnerability or perform reconnaissance on the web server.
Requests blocked by the web server per the input sanitization are not likely to be the source of the activity, as they indicate that the web server has successfully prevented an attack by validating and filtering any malicious input from the requests. These requests may indicate that an attacker is trying to inject malicious code or commands into the web server.
Failed log-in attempts against the web application are not likely to be the source of the activity, as they indicate that the web application has successfully prevented unauthorized access by verifying and rejecting any invalid credentials from the requests. These requests may indicate that an attacker is trying to guess or brute-force passwords or usernames for the web application.
Requests sent by NICs with outdated firmware are not likely to be the source of the activity, as they indicate that some devices on the network have not been updated with the latest security patches or features for their network interface cards (NICs). These requests may indicate that some devices are vulnerable to network attacks or have performance issues.
Existence of HTTP/501 status codes generated to the same IP address are not likely to be the source of the activity, as they indicate that the web server has encountered an error or does not support a request method from the client. These requests may indicate that an attacker is trying to use an invalid or unsupported method to access the web server.

NEW QUESTION 212
A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further in investigation?

A. Data carving
B. Timeline construction
C. File cloning
D. Reverse engineering

Answer: D

Explanation:
Reverse engineering is a process of analyzing a system or a component to understand how it works and how it was made. Reverse engineering can be used to examine malicious processes captured from memory and determine their functionality, origin, and purpose. Reverse engineering can help identify the type of malware, its infection vector, its capabilities, its communication methods, and its indicators of compromise2

NEW QUESTION 214
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 218
Which of the following is the primary reason financial institutions may share up-to-date threat intelligence information on a secure feed that is dedicated to their sector?

A. To augment information about common malicious actors and indicators of compromise
B. To prevent malicious actors from knowing they can defend against malicious attacks
C. To keep other industries from accessing information meant for financial institutions
D. To focus on attacks specifically targeted at their customers' mobile applications

Answer: A

Explanation:
This is the primary reason why financial institutions may share up-to-date threat intelligence information on a secure feed that is dedicated to their sector. Threat intelligence is the collection, analysis, and dissemination of information about current or potential threats to an organization's assets, operations, or reputation. By sharing threat intelligence information, financial institutions can benefit from the collective knowledge, experience, and capabilities of their peers and partners, and enhance their situational awareness, threat detection, and incident response. Sharing threat intelligence information can also help financial institutions identify common attack patterns, trends, and techniques, as well as the malicious actors and indicators of compromise (IOCs) associated with them. IOCs are pieces of forensic data that can be used to identify potentially malicious activities or intrusions on a network or system, such as IP addresses, domains, URLs, file hashes, or email addresses

NEW QUESTION 223
Which of the following software assessment methods world peak times?

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

E. User acceptance testing

Answer: B

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

NEW QUESTION 225
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 227
An organization has specific technical nsk mitigation configurations that must be implemented before a new server can be approved for production Several critical servers were recently deployed with the antivirus missing unnecessary ports disabled and insufficient password complexity Which of the following should the analyst recommend to prevent a recurrence of this risk exposure?

A. Perform password-cracking attempts on all devices going into production
B. Perform an Nmap scan on all devices before they are released to production
C. Perform antivirus scans on all devices before they are approved for production
D. Perform automated security controls testing of expected configurations pnor to production

Answer: D

Explanation:
Automated security controls testing is a method that uses tools or scripts to verify that the security controls of a system or device are configured correctly and comply with the organization’s policies and standards. Performing automated security controls testing of expected configurations prior to production would help prevent a recurrence of the risk exposure caused by missing antivirus, unnecessary ports enabled, and insufficient password complexity. Performing password-cracking attempts, Nmap scans, or antivirus scans on all devices before they are released to production are other methods that can help detect some security issues, but they are not as comprehensive or efficient as automated security controls testing. Reference:
https://www.nist.gov/system/files/documents/2017/04/28/sp800-115.pdf

NEW QUESTION 228
In response to an audit finding, a company's Chief information Officer (CIO) instructed the security department to Increase the security posture of the vulnerability management program. Currency, the company's vulnerability management program has the following attributes:
Which of the following would BEST Increase the security posture of the vulnerably management program?

A. Expand the ports Being scanned lo Include al ports increase the scan interval to a number the business win accept without causing service interruptio
B. Enable authentication and perform credentialed scans
C. Expand the ports being scanned to Include all port
D. Keep the scan interval at its current level Enable authentication and perform credentialed scans.
E. Expand the ports being scanned to Include at ports increase the scan interval to a number the business will accept without causing service Interruptio
F. Continue unauthenticated scans.
G. Continue scanning the well-known ports increase the scan interval to a number the business will accept without causing service Interruptio
H. Enable authentication and perform credentialed scans.

Answer: A

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 233
A company's security team recently discovered a number of workstations that are at the end of life. The workstation vendor informs the team that the product is no longer supported and patches are no longer available The company is not prepared to cease its use of these workstations Which of the following would be the

BEST method to protect these workstations from threats?

A. Deploy whitelisting to the identified workstations to limit the attack surface
B. Determine the system process centrality and document it
C. Isolate the workstations and air gap them when it is feasible
D. Increase security monitoring on the workstations

Answer: A

Explanation:
Deploying whitelisting to the identified workstations would be the best method to protect these workstations from threats. Whitelisting is a technique that allows only authorized applications, processes, or users to run or access a system or resource. Whitelisting can help limit the attack surface and prevent malware or unauthorized software from running on a system3. Deploying whitelisting to the workstations that are at the end of life can help mitigate the risk of exploitation due to lack of patches or support from the vendor.

NEW QUESTION 234
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 239
You are a penetration tester who is reviewing the system hardening guidelines for a company. Hardening guidelines indicate the following.

- There must be one primary server or service per device.
- Only default port should be used
- Non- secure protocols should be disabled.
- The corporate internet presence should be placed in a protected subnet Instructions :
- Using the available tools, discover devices on the corporate network and the services running on these devices.

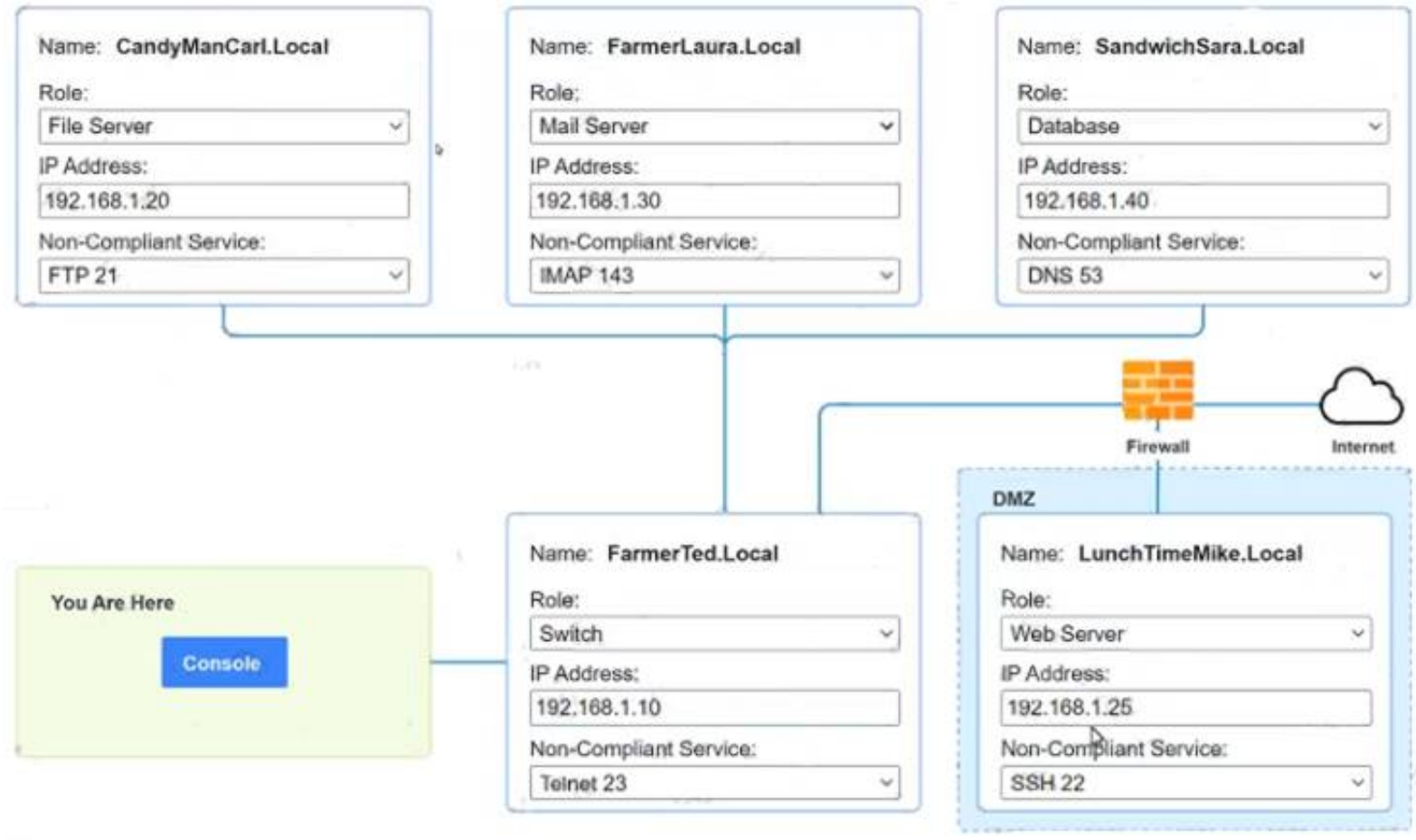
You must determine

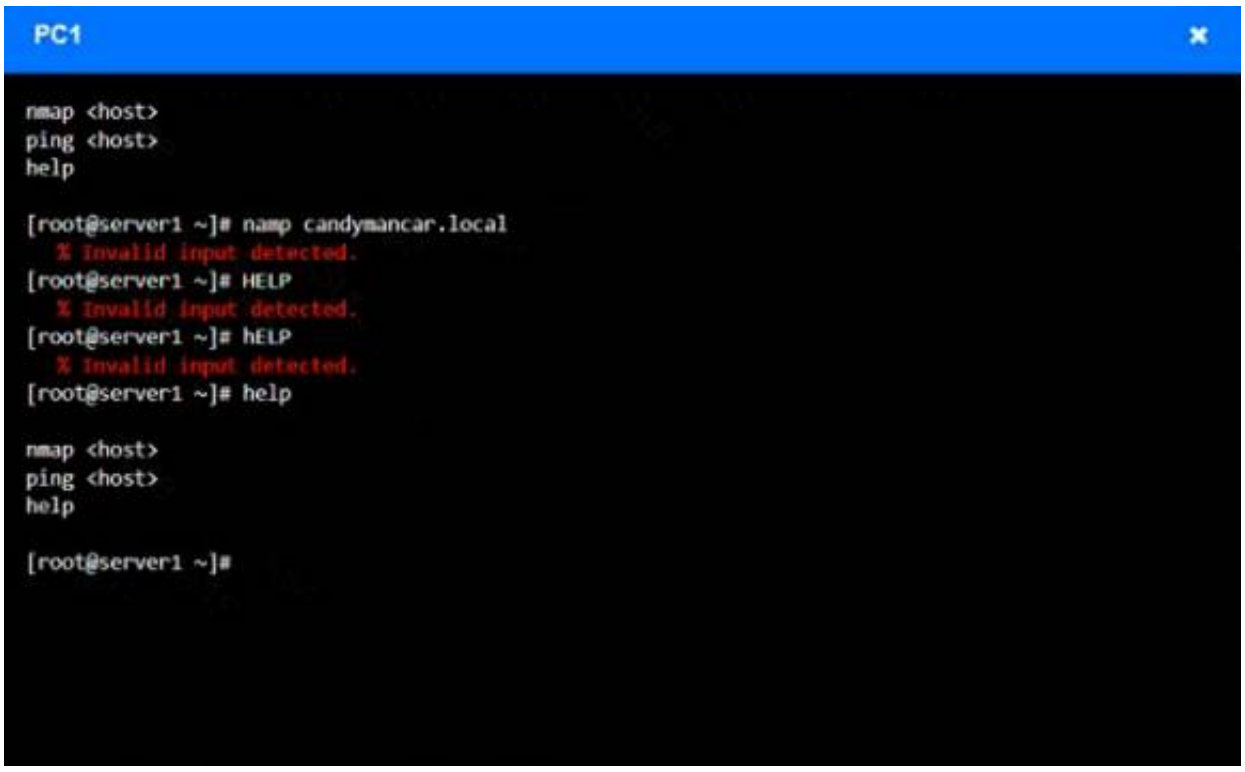
- ip address of each device
- The primary server or service each device
- The protocols that should be disabled based on the hardening guidelines

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer below images





NEW QUESTION 244
A user reports a malware alert to the help desk. A technician verities the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access. The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do next?

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

Answer: C

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

NEW QUESTION 247
A company employee downloads an application from the internet. After the installation, the employee begins experiencing noticeable performance issues, and files are appearing on the desktop.

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

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

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

Answer: D

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

NEW QUESTION 248
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 249

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CS0-002 Exam with Our Prep Materials Via below:

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