

# CompTIA

## Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam



**NEW QUESTION 1**

A security analyst is deploying a new application in the environment. The application needs to be integrated with several existing applications that contain SPI. Prior to the deployment, the analyst should conduct:

- A. a tabletop exercise
- B. a business impact analysis
- C. a PCI assessment
- D. an application stress test.

**Answer: C**

**Explanation:**

A PCI assessment should be conducted prior to the deployment of a new application that contains SPI (Sensitive Personal Information). A PCI assessment is an evaluation of how well an organization complies with the Payment Card Industry Data Security Standard (PCI DSS), which is a set of requirements for protecting cardholder data. PCI DSS applies to any organization that stores, processes, or transmits cardholder data, such as credit card numbers, expiration dates, or security codes<sup>4</sup>. A PCI assessment can help identify and remediate any gaps or weaknesses in the security controls of an application that handles cardholder data.

**NEW QUESTION 2**

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 3**

As part of an Intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several domains 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 system<sup>2</sup>.

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 4**

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 features<sup>123</sup>. 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 5**

Due to a rise in cyberattacks 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 compromise<sup>2</sup>. PAM can help protect PHI from cyberattackers who may try to exploit privileged accounts to access or exfiltrate sensitive data.

**NEW QUESTION 6**

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

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

**Answer:** D

**Explanation:**

A VPN is a secure network connection that allows users to access their private corporate networks over the internet, while keeping the connection encrypted and secure. This makes it an ideal solution for providing the development team with secure connectivity from the corporate network to a three-tier cloud environment. <https://www.comptia.org/content/virtual-private-networks>

**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 operation<sup>1</sup>.
- 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 switch<sup>23</sup>.
- 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 alarm<sup>23</sup>.
- 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 system<sup>14</sup>. 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 communication<sup>56</sup>.
  - 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 methods<sup>56</sup>.
  - 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 communication<sup>24</sup>.
  - 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 detected<sup>24</sup>.

**NEW QUESTION 8**

A security analyst is reviewing the following log entries to identify anomalous activity:

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

Which of the following attack types is occurring?

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

**Answer:** A

**Explanation:**

A directory traversal attack is a type of web application attack that exploits insufficient input validation or improper configuration to access files or directories that are outside the intended scope of the web server. The log entries given in the question show several requests that contain “../” sequences in the URL, which indicate an attempt to move up one level in the directory structure. For example, the request “/images/../../../../etc/passwd” tries to access the /etc/passwd file, which contains user account information on Linux systems. If successful, this attack could allow an attacker to read, modify, or execute files on the web server that are not meant to be accessible.

**NEW QUESTION 9**

A security analyst reviews SIEM logs and discovers the following error event:

```
ERROR Event ID 4
The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server
DBASVRR4$. The target name used was GC/PDC1DC.Domain57/Administrator. This
indicates that the target server failed to decrypt the ticket provided by
the client. Check if there are identically named server accounts in these
two domains, or use the fully qualified name to identify the server.
```

Which of the following environments does the analyst need to examine to continue troubleshooting the event?

- A. Proxy server
- B. SQL server
- C. Windows domain controller
- D. WAF appliance
- E. DNS server

**Answer:** C

**Explanation:**

A Windows domain controller is a server that manages authentication and authorization for users and computers in a Windows domain. A Windows domain controller uses Active Directory Domain Services (AD DS) to store information about users, groups, computers, policies, and other objects in a domain. A Windows domain controller can generate event logs that record various activities and events related to security, system, application, etc. The event log shown in the question indicates that it was generated by a Windows domain controller with an IP address of 10.0.0.1 and a hostname of DC01.

**NEW QUESTION 10**

After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?

- A. Make a backup of the server and update the JBoss server that is running on it.
- B. Contact the vendor for the legacy application and request an updated version.
- C. Create a proper DMZ for outdated components and segregate the JBoss server.
- D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.

**Answer:** C

**Explanation:**

What is that application for? "The DMZ is a special network zone designed to house systems that receive connections from the outside world, such as web and email servers. Sound firewall designs place these systems on an isolated network where, if they become compromised, they pose little threat to the internal network because connections between the DMZ and the internal network must still pass through the firewall and are subject to its security policy" Creating a proper DMZ for outdated components and segregating the JBoss server is the best action to take first to prevent server compromise and business disruption at the same time. A DMZ (demilitarized zone) is a network segment that separates internal networks from external networks, such as the internet, and provides an additional layer of security<sup>3</sup>. Creating a proper DMZ for outdated components and segregating the JBoss server can isolate and protect the critical server from external attacks that may exploit its vulnerability.

**NEW QUESTION 10**

A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment Which of the following is the BEST recommendation?

- A. Require users to sign NDAs
- B. Create a data minimization plan.
- C. Add access control requirements
- D. Implement a data loss prevention solution

**Answer:** B

**Explanation:**

Creating a data minimization plan would be the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Data minimization is a principle that states that organizations should collect, store, process, and retain only the minimum amount of personal data that is necessary for their legitimate purposes. Data minimization can help reduce the risk of data breaches, data leaks, or data misuse by limiting the exposure and access to sensitive data. Data minimization can also help comply with data protection regulations, such as the General Data Protection Regulation (GDPR), that require organizations to justify their data collection and processing activities. Data minimization can be achieved by implementing various measures, such as deleting or anonymizing unnecessary data, applying retention policies, or using encryption or pseudonymization techniques.



#### NEW QUESTION 12

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 15

During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the next step the analyst should take?

- A. Validate the binaries' hashes from a trusted source.
- B. Use file integrity monitoring to validate the digital signature
- C. Run an antivirus against the binaries to check for malware.
- D. Only allow binaries on the approve list to execute.

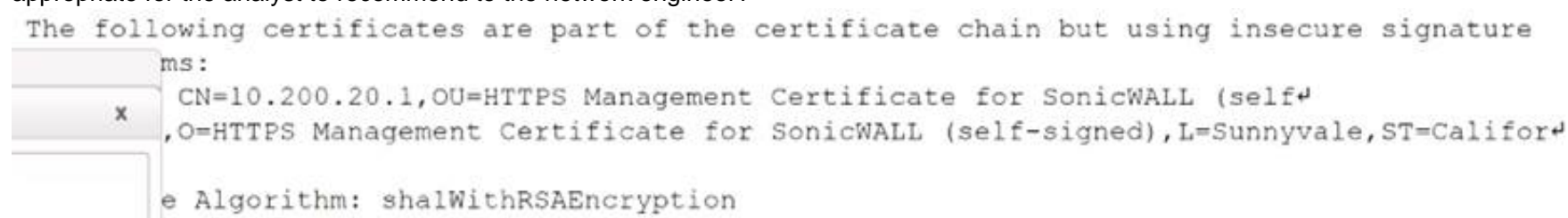
**Answer: A**

#### Explanation:

Validating the binaries' hashes from a trusted source is the next step the analyst should take after discovering some binaries that are exhibiting abnormal behaviors and finding unexpected content in their strings. A hash is a fixed-length value that uniquely represents the contents of a file or message. By comparing the hashes of the binaries on the compromised machine with the hashes of the original or legitimate binaries from a trusted source, such as the software vendor or repository, the analyst can determine whether the binaries have been modified or replaced by malicious code. If the hashes do not match, it indicates that the binaries have been tampered with and may contain malware.

#### NEW QUESTION 17

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



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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 20

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 21**

When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

```
Jun 25 10:40:34 localhost pkexec[19962]: comptia: Executing command [USER=root] [TTY=unknown] [CWD=/home/comptia] [COMMAND=/usr/libexec/gsd-backlight-helper --set-brightness 3484]
Jun 25 11:22:10 localhost gdm-password]: gkr-pam: unlocked login keyring
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): conversation failed
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): auth could not identify password for [comptia]
Jun 25 11:23:04 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:09 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:16 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=xoot ; COMMAND=/bin/bash
Jun 25 11:23:29 localhost sudo: comptia ; user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:24:13 localhost su: pam_unix(su-l:session): session opened for user root by comptia(uid=1000)
Jun 26 09:50:41 localhost gdm-password]: gkr-pam: unlocked login keyring
```

Which of the following can the analyst conclude from viewing the log file?

- A. The comptia user knows the sudo password.
- B. The comptia user executed the sudo su command.
- C. The comptia user knows the root password.
- D. The comptia user added himself or herself to the /etc/sudoers file.

**Answer: B**

**Explanation:**

The /var/log/secure log file is a file that records security-related events on a Linux system, such as authentication attempts or sudo commands. The log file shows that the comptia user executed the sudo su command, which allows the user to switch to the root account and gain superuser privileges. The log file does not show that the comptia user knows the sudo password, knows the root password, or added himself or herself to the /etc/sudoers file. Reference: <https://www.cyberciti.biz/faq/linux-log-files-location-and-how-do-i-view-logs-files/>

**NEW QUESTION 22**

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

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

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

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

**Answer: DF**

**Explanation:**

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

**NEW QUESTION 26**

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

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

**Answer: A**

**Explanation:**

A jump box is a secure computer that can be used to access a remote server or network. It acts as an intermediary between the user and the target system, and can limit access to specific IP addresses. A jump box can also provide logging and auditing of the user's actions on the remote system. A jump box is a common solution for accessing highly sensitive servers or networks<sup>1</sup>.

**NEW QUESTION 30**

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

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

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

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

**Answer: B**

**Explanation:**

[https://owasp.org/www-community/attacks/Password\\_Spraying\\_Attack](https://owasp.org/www-community/attacks/Password_Spraying_Attack)

A credential stuffing attack would be using the full credentials and most likely being used across many common platforms. A credential stuffing attack depends on the reuse of passwords. With so many people reusing their passwords for multiple accounts, just one set of credentials is enough to expose most or all of their accounts.

**NEW QUESTION 35**

While conducting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

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

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

- A. Delete CloudDev access key 1.
- B. Delete BusinessUsr access key 1.
- C. Delete access key 1.
- D. Delete access key 2.

**Answer: C**

**Explanation:**

Prowler is a tool that can scan AWS environments for security issues and compliance violations. The Prowler report shows that there are two access keys for CloudDev user: access key 1 and access key 2. Access key 1 has not been used in more than 90 days, which violates the AWS CIS benchmark 1.4 (Ensure access keys are rotated every 90 days or less). Therefore, the best recommendation is to delete access key 1 and use access key 2 instead. Deleting CloudDev access key 1, deleting BusinessUsr access key 1, or deleting access key 2 are not appropriate recommendations based on the Prowler report. Reference: <https://github.com/toniblyx/prowler>

**NEW QUESTION 36**

An IT security analyst has received an email alert regarding vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

- A. SCADA
- B. CAN bus
- C. Modbus
- D. IoT

**Answer: B**

**Explanation:**

CAN bus (Controller Area Network) is a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer<sup>1</sup>. CAN bus is a message-based protocol, designed originally for multiplex electrical wiring within automobiles to save on copper, but it can also be used in many other contexts. CAN bus enables each device to send and receive data on a shared network, reducing the need for complex wiring and increasing reliability and performance. CAN bus is one of the five protocols used in the on-board diagnostics (OBD)-II vehicle diagnostics standard. A vulnerability within the new fleet of vehicles that the company recently purchased is most likely targeting CAN bus, as it is a common and critical communication system in modern vehicles. An attacker could exploit a vulnerability in CAN bus to compromise or manipulate various vehicle functions or systems, such as braking, steering, engine control, airbags, etc. SCADA (A) stands for Supervisory Control And Data Acquisition, which is a system that monitors and controls industrial processes or infrastructure<sup>2</sup>. SCADA is not a vehicle bus standard and is not likely to be targeted by a vulnerability within a fleet of vehicles. Modbus © is a serial communications protocol that connects industrial electronic devices<sup>3</sup>. Modbus is not a vehicle bus standard and is not likely to be targeted by a vulnerability within a fleet of vehicles. IoT (D) stands for Internet of Things, which is a network of physical objects that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. IoT is not a vehicle bus standard and is not likely to be targeted by a vulnerability within a fleet of vehicles.

References: 1: <https://www.techopedia.com/definition/24771/technical-controls> 2:



<https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl> 3: <https://www.techopedia.com/definition/31686/resource-exhaustion> :  
<https://www.techopedia.com/definition/13493/penetration-testing>

**NEW QUESTION 38**

A security team has begun updating the risk management plan, incident response plan, and system security plan to ensure compliance with security review guidelines. Which of the following can be executed by internal managers to simulate and validate the proposed changes?

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

**Answer: C**

**Explanation:**

According to the CompTIA CySA+ Certification Exam (CS0-002) study guide, a tabletop exercise can be executed by internal managers to simulate and validate changes to the risk management plan, incident response plan, and system security plan. In a tabletop exercise, participants discuss and work through a simulated scenario, usually in a classroom or conference room setting, to evaluate their readiness and understanding of the proposed changes. This type of exercise can help to identify any potential issues or gaps in the proposed changes and can provide valuable insights for refining and improving the plans.

**NEW QUESTION 39**

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 systems.

**NEW QUESTION 43**

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 48**

A company needs to expand its development group due to an influx of new feature requirements from 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**

Which of the following is MOST important when developing a threat hunting program?

- A. Understanding penetration testing techniques



- B. Understanding how to build correlation rules within a SIEM
- C. Understanding security software technologies
- D. Understanding assets and categories of assets

**Answer:** D

**Explanation:**

Understanding assets and categories of assets is most important when developing a threat hunting program. Assets are anything that have value to an organization, such as data, systems, networks, applications, devices, people, processes, or reputation. Categories of assets are groups of assets that share common characteristics or attributes, such as type, function, location, owner, or criticality. Understanding assets and categories of assets can help to identify and prioritize the potential targets and impact of threats in an organization. Understanding assets and categories of assets can also help to determine and apply appropriate security controls and measures for each asset or category. Understanding assets and categories of assets can also help to collect and analyze relevant data and indicators for each asset or category during threat hunting activities. Understanding penetration testing techniques (A) is not most important when developing a threat hunting program. Penetration testing techniques are methods or tools that are used to simulate attacks on a system or network to evaluate its security posture and identify vulnerabilities or weaknesses. Penetration testing techniques can help to validate and improve the security of an organization, but they are not directly related to threat hunting activities. Penetration testing techniques are reactive rather than proactive approaches to security. Understanding how to build correlation rules within a SIEM (B) is also not most important when developing a threat hunting program. Correlation rules are logic statements that define relationships or patterns between different events or data points in a system or network. A SIEM (Security Information and Event Management) is a software solution that collects, analyzes, and correlates data from various sources in an organization to provide security monitoring and alerting capabilities<sup>1</sup>. Correlation rules can help to detect and respond to known threats in an organization, but they are not sufficient for threat hunting activities. Correlation rules are based on predefined criteria rather than hypotheses or assumptions about unknown threats. Understanding security software technologies © is also not most important when developing a threat hunting program. Security software technologies are applications or programs that provide security functions or features for an organization, such as antivirus software, firewalls, encryption software, VPNs (Virtual Private Networks), etc<sup>2</sup>. Security software technologies can help to protect an organization from various threats, but they are not essential for threat hunting activities. Security software technologies are based on signatures or heuristics rather than indicators of compromise or behavioral analysis.

References: 1: <https://www.techopedia.com/definition/24771/technical-controls> 2: <https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl>

**NEW QUESTION 51**

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

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

**Answer:** C

**Explanation:**

The security team should perform postmortem data correlation next after receiving notification of the incident from the help desk technician. Postmortem data correlation is an activity that involves analyzing data from various sources (such as logs, alerts, reports, etc.) to identify root causes, impacts, indicators of compromise (IoCs), lessons learned, and recommendations for improvement after an incident<sup>3</sup>. Postmortem data correlation can help the security team to:

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

**NEW QUESTION 56**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 60**

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

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

Which of the following best represents the security concern?

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

**Answer: C**

**Explanation:**

The correct answer is C. Microsoft RDP is accepting connections on TCP. Microsoft RDP stands for Microsoft Remote Desktop Protocol, and it is a protocol that allows users to remotely access and control a Windows computer or server. RDP uses TCP port 3389 by default, and this port is open on the host according to the results. This indicates that the host is allowing RDP connections from anyone on the internet, which poses a security concern. An attacker could exploit vulnerabilities in RDP or use brute force attacks to gain unauthorized access to the host and compromise its data or resources<sup>1</sup>.

\* A. A remote communications port is exposed is not correct. A remote communications port is a generic term for any port that allows remote access or communication with a host. There are many types of remote communications ports, such as SSH, Telnet, FTP, or RDP, and each one has its own security implications. The results do not specify which remote communications port is exposed, so this answer is too vague and inaccurate.

\* B. The FTP port should be using TCP only is not correct. FTP stands for File Transfer Protocol, and it is a protocol that allows users to transfer files between hosts. FTP uses TCP ports 20 and 21 by default, and these ports are closed on the host according to the results. However, FTP can also use UDP ports 20 and 21 for data transfer in some cases, such as when using passive mode or extended passive mode<sup>2</sup>. Therefore, it is not true that FTP should be using TCP only, and this answer does not represent a security concern.

\* D. The company's DNS server is exposed to everyone is not correct. DNS stands for Domain Name System, and it is a system that translates domain names into IP addresses. DNS uses UDP port 53 by default, and this port is open on the host according to the results. This indicates that the host is providing DNS services to anyone on the internet, which may or may not be a security concern depending on the configuration and purpose of the host. For example, if the host is a public DNS server that is intended to serve DNS queries from anyone, then this answer does not represent a security concern. However, if the host is a private DNS server that is meant to serve DNS queries only from authorized users or devices, then this answer could represent a security concern.

\* 1: What Is Remote Desktop Protocol (RDP)? 2: FTP - File Transfer Protocol : [What Is Domain Name S (DNS)?]

**NEW QUESTION 62**

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 applied<sup>1</sup>.

**NEW QUESTION 63**

A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

```
nresp = packet_get_inf();
if (nresp > 0) {
    response = xmalloc(nresp*sizeof(char));
    for (i = 0; i < nresp; i++)
        response[i] = packet_get_string(NULL);
}
```

Which of the following controls must be in place to prevent this vulnerability?

- A. Convert all integer numbers in strings to handle the memory buffer correctly.
- B. Implement float numbers instead of integers to prevent integer overflows.
- C. Use built-in functions from libraries to check and handle long numbers properly.
- D. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.

**Answer:** C

**Explanation:**

The security analyst should implement a control that uses built-in functions from libraries to check and handle long numbers properly. This will help prevent integer overflow vulnerabilities, which occur when a value is moved into a variable type too small to hold it. For example, if an integer variable can only store values up to 255, and a value of 256 is assigned to it, the variable will overflow and wrap around to 0. This can cause unexpected program behavior or lead to buffer overflow vulnerabilities if the overflowed value is used as an index or size for memory allocation<sup>1</sup>. Built-in functions from libraries can help avoid integer overflow by performing checks on the input values and the resulting values, and throwing exceptions or errors if they exceed the limits of the variable type<sup>2</sup>.

**NEW QUESTION 64**

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 65**

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 regarding disclosures.
- 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 in 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 69**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 70**

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



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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 74**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 78**

An analyst receives an alert from the continuous-monitoring solution about unauthorized changes to the firmware versions on several field devices. The asset owners confirm that no firmware version updates were performed by authorized technicians, and customers have not reported any performance issues or outages. Which Of the following actions would be BEST for the analyst to recommend to the asset owners to secure the devices from further exploitation?

- A. Change the passwords on the devices.
- B. Implement BIOS passwords.
- C. Remove the assets from the production network for analysis.
- D. Report the findings to the threat intel community.

**Answer:** C

**Explanation:**

If were referring to other devices, yes - Implement BIOS passwords before they are compromised. But the ones that were already compromised, they need to be removed from the system to avoid further exploitation. Plus, if you put a password on there, the attacker may now have your password. Remove the assets from the production network for analysis. If the analyst receives an alert about unauthorized changes to the firmware versions on several field devices, the best action to recommend to the asset owners is to remove the assets from the production network for analysis. This would prevent further exploitation of the devices by isolating them from potential attackers and allow the analyst to investigate the source and nature of the unauthorized changes. Changing the passwords on the devices, implementing BIOS passwords, or reporting the findings to the threat intel community are other possible actions, but they are not as effective or urgent as removing the assets from the production network for analysis. Reference: <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

**NEW QUESTION 79**

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 80**

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-repudiation
- 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 84**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 87**

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 92**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 95**

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

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

Which of the following is the GREATEST security concern?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 99**

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

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

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 100**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 102**

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

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

**Answer:** B

**Explanation:**

Supervised and unsupervised machine-learning algorithms are two types of machine-learning methods that are used in cybersecurity applications. Machine learning is a branch of artificial intelligence that enables systems to learn from data and improve their performance without explicit programming. Supervised machine-learning algorithms are trained on labeled data, which means that each data point has a known outcome or class. Supervised algorithms learn to map input data to output data by finding patterns or rules from the training data. Supervised algorithms require security analyst feedback to provide labels

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

**NEW QUESTION 104**

A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results, the manager requests information regarding the possible exploitation of vulnerabilities. Which of the following information data points would be MOST useful for the analyst to provide to the security manager, who would then communicate the risk factors to the senior management team? (Select TWO).

- A. Probability
- B. Adversary capability
- C. Attack vector
- D. Impact
- E. Classification
- F. Indicators of compromise

**Answer:** BD

**Explanation:**

According to the CompTIA CySA+ (CS0-002) best practices, the most useful information data points to provide to the security manager for communicating the risk factors to senior management are the impact and adversary capability. The impact refers to the potential consequences of a successful attack or exploitation of a vulnerability, such as data loss or system compromise. The adversary capability refers to the ability of an attacker to exploit a vulnerability, including their technical expertise and resources. Together, these data points help to provide a complete picture of the risk associated with a vulnerability, and allow senior management to make informed decisions regarding risk mitigation and remediation. The other data points, such as probability, attack vector, classification, and indicators of compromise, can also be valuable, but the impact and adversary capability are considered the most critical for prioritizing risk mitigation efforts.

**NEW QUESTION 107**

A security analyst is researching ways to improve the security of a company's email system to mitigate emails that are impersonating company executives. Which of the following would be BEST for the analyst to configure to achieve this objective?

- A. A TXT record on the name server for SPF
- B. DNSSEC keys to secure replication
- C. Domain Keys identified Mail
- D. A sandbox to check incoming mail

**Answer:** C

**Explanation:**

Domain Keys Identified Mail (DKIM) is an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a domain<sup>1</sup>

DKIM helps prevent phishing emails that spoof or impersonate other domains by verifying the identity and integrity of the sender. DKIM works by adding a DKIM signature header to each outgoing email message, which contains a hash value of selected parts of the message and the domain name of the sender. The sender's domain also publishes a public key in its DNS records, which can be used by the receiver to decrypt the DKIM signature and compare it with its own hash value of the message. If they match, it means that the message was not altered in transit and that it came from the claimed domain.

**NEW QUESTION 112**

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 114**

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 117**

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. Log4j 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 119**

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 123**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 125**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 128**

A threat hunting team received a new IoC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

- A. The whitelist
- B. The DNS



- C. The blocklist
- D. The IDS signature

**Answer:** D

**Explanation:**

The IDS signature should be updated next after receiving a new IoC (Indicator of Compromise) from an ISAC (Information Sharing and Analysis Center) that follows a threat actor's profile and activities. An IoC is a piece of evidence or artifact that suggests a system or network has been compromised or attacked by a threat actor<sup>4</sup>. An IoC can be an IP address, domain name, URL, file hash, email address, registry key, etc. An ISAC is a nonprofit organization that collects, analyzes, and shares threat intelligence and best practices among its members within a specific sector or industry<sup>5</sup>. An ISAC can help to improve the security awareness and preparedness of its members by providing timely and relevant information about emerging threats and incidents.

**NEW QUESTION 132**

Which of the following SCAP standards provides standardization for measuring and describing the severity 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 133**

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

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

**Answer:** DF

**Explanation:**

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

- Maximum downtime before impact is unacceptable: This metric defines the maximum amount of time that a business process or function can be disrupted without causing significant or irreversible damage to the organization's reputation, operations, finances, or legal obligations. This metric is also known as the maximum tolerable downtime (MTD) or maximum tolerable period of disruption (MTPD). It helps to determine the recovery time objective (RTO), which is the target time for restoring the process or function to an acceptable level of service after a disruption<sup>1</sup>.
- Total time accepted for business process outage: This metric defines the total amount of time that a business process or function can be out of service within a given period, such as a day, a week, or a month. This metric is also known as the recovery point objective (RPO), which is the maximum amount of data loss or corruption that can be tolerated after a disruption<sup>1</sup>. It helps to determine the backup frequency and retention policy for the data and systems that support the process or function.
- Time required to inform stakeholders about outage: This metric defines the time frame for communicating with the internal and external stakeholders who are affected by or involved in the disruption and recovery of a business process or function. This metric helps to establish the crisis communication plan and protocol, which specifies who, what, when, where, why, and how to communicate during and after a disruption<sup>2</sup>. It also helps to manage the expectations and perceptions of the stakeholders and to maintain their trust and confidence in the organization.
- Time to reimage the server: This metric defines the time needed to restore a server to its original or desired state after a disruption. This metric helps to estimate the resources and efforts required for recovering the server and its applications. It also helps to evaluate the feasibility and effectiveness of different recovery strategies, such as restoring from backup, rebuilding from scratch, or replacing with a spare<sup>3</sup>.
- Minimum data backup volume: This metric defines the minimum amount of data that needs to be backed up regularly to ensure the continuity and integrity of a business process or function. This metric helps to optimize the backup process and reduce the storage costs and bandwidth consumption. It also helps to identify the critical data elements and sources that are essential for the process or function<sup>4</sup>.

**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 for IP addresses from outside the country.
- C. Implement strong authentication controls for all contractors.
- D. Implement user behavior analytics for key staff members.

**Answer:** A

**Explanation:**

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 disasters<sup>1</sup>. 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 139**

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 140**

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

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

**Answer: D**

**Explanation:**

What is the difference between VPN and VPC?

Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.

VPN (Virtual Private Network) is a technology that provides secure connectivity from the corporate network to a cloud environment. VPN creates an encrypted tunnel between the two networks, allowing developers to access servers in all three tiers of the cloud environment without exposing their traffic to interception or tampering. VPN can also provide authentication and authorization mechanisms to verify the identity and permissions of the developers.

**NEW QUESTION 145**

A security analyst notices the following proxy log entries:

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

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

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

**Answer: C**

**Explanation:**

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

hosts, open ports, or potential vulnerabilities .

**NEW QUESTION 146**

A customer notifies a security analyst that a web application is vulnerable to information disclosure. The analyst needs to indicate the severity of the vulnerability based on its CVSS score, which the analyst needs to calculate. When analyzing the vulnerability, the analyst realizes that for 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 149**

The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?

- A. A Linux-based system and mandatory training on Linux for all BYOD users
- B. A firewalled environment for client devices and a secure VDI for BYOD users
- C. A standardized anti-malware platform and a unified operating system vendor
- D. 802.1X to enforce company policy on BYOD user hardware

**Answer: B**

**Explanation:**

VDI means virtual desktop interface. Using VDI, you can maintain a standard image and remove the threat of an infected machine plugging into your network. A firewalled environment for client devices and a secure VDI (Virtual Desktop Infrastructure) for BYOD users would be the most likely recommendation for securing the proposed solution. A firewalled environment can help isolate and protect the client devices from unauthorized network access or attacks. A secure VDI can provide a virtualized desktop environment for BYOD users that can be centrally managed and controlled by the organization. A VDI can also prevent data leakage or malware infection from BYOD devices, as the data and applications are stored on the server side rather than on the device itself.

**NEW QUESTION 150**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 154**

A security analyst responds to a series of events surrounding sporadic bandwidth consumption from an endpoint device. The security analyst then identifies the following additional details:

- Bursts of network utilization occur approximately every seven days.
- The content being transferred appears to be encrypted or obfuscated.
- A separate but persistent outbound TCP connection from the host to infrastructure in a third-party cloud is in place.
- The HDD utilization on the device grows by 10GB to 12GB over the course of every seven days.
- Single file sizes are 10GB.

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

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

**Answer: C**

**Explanation:**

data exfiltration is the unauthorized transfer of data from an organization's network to an external destination, usually for malicious purposes such as espionage, sabotage, or theft. The details given in the question suggest that data exfiltration is occurring from an endpoint device. The bursts of network utilization every seven days indicate periodic data transfers. The content being transferred appears to be encrypted or obfuscated to avoid detection or analysis. The persistent



outbound TCP connection from the host to infrastructure in a third-party cloud indicates a possible command and control channel for an attacker. The HDD utilization on the device grows by 10GB to 12GB over the course of every seven days, and single file sizes are 10GB, indicating that large amounts of data are being collected and compressed before being exfiltrated.

**NEW QUESTION 159**

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 160**

During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideration. Which of the following are part of a known threat modeling method?

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

**Answer: C**

**Explanation:**

Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege are part of a known threat modeling method called STRIDE. STRIDE is a mnemonic that stands for six categories of threats that can affect the security of a system or application. STRIDE was developed by Microsoft in 1999 and has been widely adopted as a threat modeling method by many organizations. STRIDE can help identify and prioritize potential threats based on their impact and likelihood<sup>1</sup>.

**NEW QUESTION 165**

An organization has a policy that requires dedicated user accounts to run programs that need elevated privileges. Users must be part of a group that allows elevated permissions. While reviewing security logs, an analyst sees the following:

PRI	TIME	HOST	MESSAGE
34	Oct 22 10:01:33	lincoln	'su root' failed for ldavis on /dev/pts/8
38	Oct 22 11:01:45	ford	'sudo apache.bin' failed for ldavis on /dev/sda
34	Oct 22 13:32:18	gremlin	'sudo more /etc/passwd' failed for ldavis on /dev/hda
30	Oct 22 15:27:19	pacar	'more /etc/passwd' failed for ldavis on /dev/hda

Which of the following hosts violates the organizational policies?

- A. pacar
- B. ford
- C. gremlin
- D. lincoln

**Answer: D**

**Explanation:**

The host "lincoln" violates the organizational policies that require dedicated user accounts to run programs that need elevated privileges. The log file shows that the user "ldavis" tried to run programs such as "su root", "sudo apache.bin", and "sudo grep" on the host "lincoln", which indicate attempts to gain elevated privileges or access sensitive files. The other hosts do not show any evidence of policy violation.

**NEW QUESTION 170**

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

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

**Answer: C**

**Explanation:**

Setting up a warm disaster recovery site with the same cloud provider in a different region can help to achieve a recovery time objective (RTO) of 12 hours while keeping the costs low. A warm disaster recovery site is a partially configured site that has some of the essential hardware and software components ready to be



activated in case of a disaster. A warm site can provide faster recovery than a cold site, which has no preconfigured components, but lower costs than a hot site, which has fully configured and replicated components. Using the same cloud provider can help to simplify the migration and synchronization processes, while using a different region can help to avoid regional outages or disasters .

**NEW QUESTION 174**

A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is compatia.org. The testing is successful, and the security technician is prepared to fully implement the solution. Which of the following actions should the technician take to accomplish this task?

- A. Add TXT @ "v=spf1 mx include:\_spf.compti
- B. org -all" to the DNS record.
- C. Add : XT @ "v=spf1 mx include:\_spf.comptia.org -all" to the email server.
- D. Add TXT @ "v=spf1 mx include:\_spf.comptia.org +all" to the domain controller.
- E. AddTXT @ "v=apfl mx Include:\_spf .comptia.org +a 11" to the web server.

**Answer: A**

**Explanation:**

Adding TXT @ "v=spf1 mx include:\_spf.comptia. org -all" to the DNS record can help to prevent outside entities from spoofing the company's email domain, which is comptia.org. This is an example of a Sender Policy Framework (SPF) record, which is a type of DNS record that specifies which mail servers are authorized to send email on behalf of a domain. SPF records can help to prevent spoofing by allowing the recipient mail servers to check the validity of the sender's domain against the SPF record. The "-all" at the end of the SPF record indicates that any mail server that is not listed in the SPF record is not authorized to send email for comptia.org .

**NEW QUESTION 175**

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

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

**Answer: C**

**Explanation:**

The company is transferring the risk for the vulnerability to the software vendor. Risk transfer is a risk treatment strategy that involves shifting the potential loss or impact of a risk to a third party, such as an insurance company or a vendor. Risk transfer does not eliminate the risk, but it reduces the organization's exposure or liability for the risk<sup>1</sup>. In this scenario, the company is transferring the risk for the vulnerability in the out-of-support database software to the software vendor by signing an extended support contract. The extended support contract means that the software vendor will continue to provide security patches and updates for the software until the company can complete the software update. This reduces the likelihood and impact of a potential exploit of the vulnerability.

**NEW QUESTION 176**

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)

```
ls -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 178**

An incident response team is responding to a breach of multiple systems that contain PII 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 182**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 187**

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 191**

An organization is concerned about the proper handling of data and wants to implement measures to help safeguard customer data and the organization's proprietary information from exposure. Which of the following is the first step to improve awareness of overall privacy and protection?

- A. Perform user acceptance testing.
- B. Implement corporate policies.
- C. Conduct biannual training.
- D. Review data classification processes.

**Answer: D**

**Explanation:**

Data classification is the process of categorizing data based on its level of sensitivity, value, and risk. Data classification can help determine the appropriate level of protection and access control for each type of data.

Data classification processes should be reviewed regularly to ensure that they are aligned with the organization's goals, policies, and standards. Data classification processes should also reflect the changing nature and value of data, as well as the evolving threats and regulations in the data environment.

Reviewing data classification processes can help improve awareness of overall privacy and protection by: ➤ Educating data owners and users about their roles and responsibilities in handling data.

- Establishing clear and consistent criteria for labeling and handling data.
- Identifying and prioritizing the most critical and sensitive data assets.
- Applying the appropriate security measures and controls for each data category.
- Reducing the risk of data loss, theft, or misuse.

**NEW QUESTION 193**

A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

- A. Implement a mobile device wiping solution for use if a device is lost or stolen.
- B. Install a DLP solution to track data now
- C. Install an encryption solution on all mobile devices.
- D. Train employees to report a lost or stolen laptop to the security department immediately

**Answer: A**

**Explanation:**

A mobile device wiping solution is a security feature that allows an organization to remotely erase or delete all data on a mobile device if it is lost or stolen. A mobile device wiping solution can help protect the privacy of the data on a device and prevent unauthorized access or disclosure of sensitive information. A mobile device wiping solution can be implemented using built-in features of some mobile operating systems, third-party applications, or mobile device management (MDM) software.

**NEW QUESTION 195**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 199**

Given the Nmap request below:

```
Scanner# nmap -p 22,113,139,1433 www.scannable.org -d --packet-trace
Starting Nmap(http://nmap.org)
Nmap scan report for www.scannable.org
SENT(0.0149s) ICMP SCANNER > SCANNABLE
echo request (type=8/code=0) TTL=52 ID=1929
SENT(0.0112s) TCP SCANNER:63541 > SCANNABLE:80 iplen=40 seq=99850910
RCVC(0.0179s) ICMP SCANNABLE > SCANNER echo reply(type=0/code=0 iplen=28 seq=99850910
we got a ping back for SCANNABLE: ID=48822 seq=713 checksum=16000
massping done: num_host:1 num_response:1
Initiating SYN Stealth Scan against www.scannable.org (SCANNABLE) 3 ports at 00:47
SENT(0.0134s) TCP SCANNER:63517 > SCANNABLE:113 iplen=40 seq=1048634
SENT(0.0148s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
SENT(0.0092s) TCP SCANNER:63517 > SCANNABLE:22 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:113 > SCANNER:63517 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:22 > SCANNER:63517 iplen=40 seq=1048634
SENT(0.0097s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
The SYN Stealth Scan took 1.25s to scan 3 total ports
Nmap Report for www.scannable.org (SCANNABLE)

PORT      STATE      SERVICE
22/tcp    open       ssh
113/tcp   closed     auth
139/tcp   filtered  netbios-ssh
1433/tcp  closed     ms-sql
```

Which of the following actions will an attacker be able to initiate directly against this host?

- A. Password sniffing
- B. ARP spoofing
- C. A brute-force attack
- D. An SQL injection

**Answer: C**

**Explanation:**

The Nmap command given in the question performs a TCP SYN scan (-sS), a service version detection scan (-sV), an OS detection scan (-O), and a port scan for ports 1-1024 (-p 1-1024) on the host 192.168.1.1. This command will reveal information about the host's operating system, open ports, and running services, which can be used by an attacker to launch a brute-force attack against the host. A brute-force attack is a method of guessing passwords or encryption keys by trying many possible combinations until finding the correct one. An attacker can use the information from the Nmap scan to target specific services or protocols



that may have weak or default credentials, such as FTP, SSH, Telnet, or HTTP.

**NEW QUESTION 201**

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

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

**Answer:** A

**Explanation:**

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

References: 1: <https://www.analytics8.com/blog/8-steps-to-start-your-data-governance-program/> 2: <https://solutionsreview.com/data-management/the-best-data-governance-tools-and-software/>

**NEW QUESTION 205**

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

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

**Answer:** CE

**Explanation:**

Documenting the chain of custody is an important step in the forensic analysis of any device, as it helps to ensure that all evidence is collected and preserved correctly. A memory dump is also essential, as it can provide information about the state of the device when the attack occurred and can be used for further analysis.

Documenting the respective chain of custody can help to preserve the integrity and admissibility of the evidence collected from the mobile device during the forensic analysis. Chain of custody is a record of who handled, accessed or modified the evidence, when, where, how and why . Performing a memory dump of the mobile device for analysis can help to extract volatile data from the mobile device that may contain valuable information about the ransomware attack, such as processes, network connections or encryption keys. Memory dump is a process of copying the contents of the memory (RAM) to a file or storage device .

References: <https://www.techopedia.com/definition/23371/chain-of-custody> <https://www.techopedia.com/definition/10339/memory-dump>

**NEW QUESTION 207**

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

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

**Answer:** D

**Explanation:**

Blocking third-party applications would be the best way to mitigate future attacks on company-owned mobile devices that are used by employees to collect data from clients in the field. Third-party applications are applications that are not developed or authorized by the device manufacturer or operating system provider<sup>1</sup>. Third-party applications can pose a security risk for mobile devices, as they may contain malware, spyware, or other malicious code that can compromise the device or its data<sup>2</sup>. Blocking third-party applications can help prevent employees from installing unauthorized or untrusted applications on company-owned mobile devices and reduce the attack surface.

**NEW QUESTION 212**

A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Which of the following is the BEST recommendation?

- A. Require users to sign NDAs
- B. Create a data minimization plan.
- C. Add access control requirements.
- D. Implement a data loss prevention solution.

**Answer:** B

**Explanation:**

A data minimization plan is a strategy that aims to reduce the amount and type of data that an organization collects, stores, and processes. It can help improve data privacy and protection by limiting the exposure and impact of a data breach or loss. Creating a data minimization plan is the best recommendation for a



security officer who needs to find the most cost-effective solution to the current data privacy and protection gap. Requiring users to sign NDAs, adding access control requirements, or implementing a data loss prevention solution are other possible solutions, but they are not as cost-effective as creating a data minimization plan. Reference:  
<https://www.csoonline.com/article/3603898/data-minimization-what-is-it-and-how-to-implement-it.html>

**NEW QUESTION 214**

A security administrator needs to provide access from partners to an Isolated laboratory network inside an organization that meets the following requirements:

- The partners' PCs must not connect directly to the laboratory network.
- The tools the partners need to access while on the laboratory network must be available to all partners
- The partners must be able to run analyses on the laboratory network, which may take hours to complete Which of the following capabilities will MOST likely meet the security objectives of the request?

- A. Deployment of a jump box to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis
- B. Deployment of a firewall to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools tor analysis
- C. Deployment of a firewall to allow access to the laboratory network and use of VDI In persistent mode to provide the necessary tools for analysis
- D. Deployment of a jump box to allow access to the Laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis

**Answer: D**

**Explanation:**

A jump box is a system that is connected to two networks and acts as a gateway or intermediary between them 1. A jump box can help to isolate and secure a network by limiting the direct access to it from other networks.

A jump box can also help to monitor and audit the traffic and activity on the network. A VDI (Virtual Desktop Infrastructure) is a technology that allows users to access virtual desktops that are hosted on a server2. A VDI can help to provide users with the necessary tools and applications for analysis without installing them on their own PCs. A VDI can also help to reduce the maintenance and management costs of the desktops. A VDI can operate in two modes: persistent and non-persistent. In persistent mode, each user has a dedicated virtual desktop that retains its settings and data across sessions. In non-persistent mode, each user has a temporary virtual desktop that is deleted or reset after each session3. In this scenario, deploying a jump box to allow access to the laboratory network and using VDI in non-persistent mode can meet the security objectives of the request. The jump box can prevent the partners' PCs from connecting directly to the laboratory network and reduce the risk of unauthorized access or compromise. The VDI in non-persistent mode can provide the necessary tools for analysis without storing any data on the partners' PCs or the virtual desktops. The VDI in non-persistent mode can also allow the partners to run long analyses without losing their progress or results. Deploying a firewall (B) may not be sufficient or effective, as a firewall only filters or blocks traffic based on rules and does not provide access or tools for analysis. Using VDI in persistent mode (A) © may not be secure or efficient, as persistent mode stores data on the virtual desktops that may be sensitive or confidential.

References: 1: <https://www.techrepublic.com/article/jump-boxes-vs-firewalls/> 2:

<https://www.techopedia.com/definition/26139/virtual-desktop-infrastructure-vdi> 3: <https://www.techopedia.com/definition/31686/resource-exhaustion>

**NEW QUESTION 218**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 222**

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 227**

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 229**

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

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

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

- A. It only accepts TLSv1.2
- B. It only accepts cipher suites using AES and SHA
- C. It no longer accepts the vulnerable cipher suites
- D. SSL/TLS is offloaded to a WAF and load balancer

**Answer: C**

**Explanation:**

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

**NEW QUESTION 233**

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!S!adaffd9-S#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 klqwen9134eijcgwd.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 238**

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 243**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### CS0-002 Practice Exam Features:

- \* CS0-002 Questions and Answers Updated Frequently
- \* CS0-002 Practice Questions Verified by Expert Senior Certified Staff
- \* CS0-002 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* CS0-002 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CS0-002 Practice Test Here](#)**