

# CompTIA

## Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam



**NEW QUESTION 1**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 2**

An IT security analyst has received an email alert regarding a 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:**

The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.

CAN bus stands for Controller Area Network bus, which is a communication protocol that allows different devices and components in a vehicle to communicate and exchange data. The vulnerability within the new fleet of vehicles is most likely targeting the CAN bus, because it could allow an attacker to manipulate or disrupt the operation of the vehicle. SCADA, Modbus, and IoT are other terms related to communication protocols or systems, but they are not specific to vehicles.

Reference: <https://www.csoonline.com/article/3218104/what-is-a-can-bus-and-how-can-it-be-hacked.html>

**NEW QUESTION 3**

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 4**

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 5**

A company is aiming to test a new incident response plan. The management team has made it clear that the initial test should have no impact on the environment. The company has limited resources to support testing. Which of the following exercises would be the best approach?

- A. Tabletop scenarios
- B. Capture the flag
- C. Red team v
- D. blue team
- E. Unknown-environment penetration test

**Answer:** A

**Explanation:**

A tabletop scenario is an informal, discussion-based session in which a team discusses their roles and responses during an emergency, walking through one or more example scenarios. A tabletop scenario is the best approach for a company that wants to test a new incident response plan without impacting the environment or using many resources. A tabletop scenario can help the company identify strengths and weaknesses in their plan, clarify roles and responsibilities, and improve communication and coordination among team members. The other options are more intensive and disruptive exercises that involve simulating a real incident or attack. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 16; <https://www.linkedin.com/pulse/tabletop-exercises-explained-matt-lemon-phd>

**NEW QUESTION 6**

A company's threat team has been reviewing recent security incidents and looking for a common theme. The team discovered the incidents were caused by incorrect configurations on the impacted systems. The issues were reported to support teams, but no action was taken. Which of the following is the next step the company should take to ensure any future issues are remediated?

- A. Require support teams to develop a corrective control that ensures security failures are addressed once they are identified.
- B. Require support teams to develop a preventive control that ensures new systems are built with the required security configurations.
- C. Require support teams to develop a detective control that ensures they continuously assess systems for configuration errors.
- D. Require support teams to develop a managerial control that ensures systems have a documented configuration baseline.

**Answer:** A

**Explanation:**

Requiring support teams to develop a corrective control that ensures security failures are addressed once they are identified is the best step to prevent future issues from being remediated. Corrective controls are actions or mechanisms that are implemented after a security incident or failure has occurred to fix or restore the normal state of the system or network. Corrective controls can include patching, updating, repairing, restoring, or reconfiguring systems or components that were affected by the incident or failure .

**NEW QUESTION 7**

A company notices unknown devices connecting to the internal network and would like to implement a solution to block all non-corporate managed machines. Which of the following solutions would be best to accomplish this goal?

- A. WPA2 for W1F1 networks
- B. NAC with 802.1X implementation
- C. Extensible Authentication Protocol
- D. RADIUS with challenge/response

**Answer:** B

**Explanation:**

This solution is the best to accomplish the goal of blocking all non-corporate managed machines from connecting to the internal network. NAC stands for network access control, which is a method of enforcing policies and rules on network devices based on their identity, role, location, and other attributes. 802.1X is a standard for port-based network access control, which authenticates devices before granting them access to a network port or wireless access point.

**NEW QUESTION 8**

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 9**

A security operations manager wants some recommendations for improving security monitoring. The security team currently uses past events to create an IOC list for monitoring.

Which of the following is the best suggestion for improving monitoring capabilities?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 10**

An organization has the following risk mitigation policies

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

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

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 10**

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 12**

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

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

**Answer:** C

**Explanation:**

An independent third-party audit report can provide the highest assurance of compliance with the organization's policies by vendors, as it involves an objective



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

**NEW QUESTION 13**

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

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

**Answer: B**

**Explanation:**

Building the chain-of-custody document is the procedure that must be completed first for this type of evidence acquisition. The chain-of-custody document is a record that tracks the handling and custody of digital evidence from the time it is collected until it is presented in court. The chain-of-custody document should include information such as the media model, serial number, size, vendor, date, and time of acquisition, as well as the names and signatures of the persons who handled, transferred, or examined the evidence. The chain-of-custody document helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss<sup>1</sup>.

**NEW QUESTION 17**

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 18**

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 19**

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

- A. Ensure the certificate is applied to the certificate revocation list.
- B. Ensure the certificate key algorithm is SHA-1 compliant.
- C. Ensure the certificate is requested from a trusted CA.
- D. Ensure the developer has self-signed the certificate.
- E. Ensure the certificate key is less than 1028 bits long.

**Answer: C**

**Explanation:**

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

### NEW QUESTION 20

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 22

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

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

**Answer: C**

#### Explanation:

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

### NEW QUESTION 27

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 30**

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

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

**Answer: C**

**Explanation:**

The security analyst should review the IDS rule set first. The IDS (Intrusion Detection System) is a tool that monitors network traffic and alerts on any suspicious or malicious activity. The IDS rule set is a set of conditions or patterns that define what constitutes normal or abnormal behavior on the network. The IDS rule set can affect the number of security incidents being reported, as it determines what triggers an alert or not<sup>3</sup>. The security analyst should review the IDS rule set to check if it is up to date, accurate, and comprehensive. If the IDS rule set is outdated, inaccurate, or incomplete, it may miss some incidents or generate false positives or negatives.

**NEW QUESTION 34**

A new government regulation requires that organizations only retain the minimum amount of data on a person to perform the organization's necessary activities. Which of the following techniques would help an organization comply with this new regulation?

- A. Storing the highest-risk data in a separate and secured environment
- B. Limiting access to data on a need-to-know basis
- C. Deidentifying a data subject throughout the organization's applications
- D. Having a privacy expert peer review source code before deployment

**Answer: C**

**Explanation:**

Deidentifying a data subject means removing or obscuring any data that can be used to identify, locate, or contact an individual, such as names, addresses, phone numbers, email addresses, social security numbers, etc. Deidentifying a data subject throughout the organization's applications can help comply with the new regulation that requires only retaining the minimum amount of data on a person to perform the organization's necessary activities.

**NEW QUESTION 35**

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 36**

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 38**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 43**

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 46**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 51**

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

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

**Answer:** C

**Explanation:**



A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.

"Compensating controls are additional security measures that you take to address a vulnerability without remediating the underlying issue."

A compensating control is a control that reduces the risk of an existing or potential control weakness<sup>2</sup>

In this case, the lack of segregation of duties in the accounting department is a control weakness that increases the risk of fraud or error. The quarterly reviews by a different officer are a compensating control that reduces this risk by providing an independent verification of the transactions recorded by the controller.

#### NEW QUESTION 54

The following output is from a tcpdump at the edge of the corporate network:

```
12:47:22.179345 PPPoE [len 0x0122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 10.5.1.1 > 198.134.5.201: 196 (hlen 43, next-header: TCP (6) payload length: 32) 2001:67c:2158:a019::ace.53104 > 2001:0:5ef5:79fd:360c:1d57:a601:24fa.13788: Flags [S], cksum 0x58cf (correct), seq 1155375165, win 8192, options [max 1412,nop,wscale 2,nop,nop,sackOK], length 0

12:47:22.251065 PPPoE [len 0x0122] IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 198.134.5.201 > 10.5.1.1: 196 (hlen 127, next-header: TCP (6) payload length: 32) 2001:0:5ef5:79fd:360c:1d57:a601:24fa.13788 > 2001:67c:2158:a019::ace.53104: Flags [S.], cksum 0xd361 (correct), seq 2642471061, ack 1155375166, win 8192, options [max 1220,nop,wscale 6,nop,nop,sackOK], length 0
```

Which of the following best describes the potential security concern?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 57

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 58

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<sup>1</sup>.

**NEW QUESTION 63**

A development team recently released a new version of a public-facing website for testing prior to production. The development team is soliciting the help of various teams to validate the functionality of the website due to its high visibility. Which of the following activities best describes the process the development team is initiating?

- A. Static analysis
- B. Stress testing
- C. Code review
- D. User acceptance testing

**Answer: D**

**Explanation:**

User acceptance testing is a process of verifying that a software application meets the requirements and expectations of the end users before it is released to production. User acceptance testing can help to validate the functionality, usability, performance and compatibility of the software application with real-world scenarios and feedback. User acceptance testing can involve various teams, such as developers, testers, customers and stakeholders.

**NEW QUESTION 64**

An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by public users accessing the server. The results should be written to a text file and should include the date, time, and IP address associated with any spreadsheet downloads. The web server's log file is named webserver.log, and the report file name should be accessreport.txt. Following is a sample of the web server's log file:

```
2017-0-12 21:01:12 GET /index.html - @4..102.33.7 - return=200 1622
```

Which of the following commands should be run if an analyst only wants to include entries in which spreadsheet was successfully downloaded?

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

**Answer: C**

**Explanation:**

The grep command is a tool that searches for a pattern of characters in a file or input and prints the matching lines<sup>1</sup>

The egrep command is a variant of grep that supports extended regular expressions, which allow more complex and flexible pattern matching<sup>2</sup>

The more command is a filter that displays the contents of a file or input one screen at a time<sup>3</sup>

The pipe symbol (|) is used to redirect the output of one command to the input of another command. The redirection symbol (>) is used to redirect the output of a command to a file.

The command given in option C performs the following steps:

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

**NEW QUESTION 67**

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

- A. Message queuing telemetry transport does not support encryption.
- B. The devices may have weak or known passwords.
- C. The devices may cause a dramatic increase in wireless network traffic.
- D. The devices may utilize unsecure network protocols.
- E. Multiple devices may interface with the functions of other IoT devices.
- F. The devices are not compatible with TLS 1.2.

**Answer: BD**

**Explanation:**

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

- The devices may have weak or known passwords: Many consumer IoT devices come with default or hardcoded passwords that are easy to guess or find online. Some devices may not allow users to change their passwords or enforce strong password policies. This can make them vulnerable to brute-force attacks or unauthorized access by attackers.
- The devices may utilize unsecure network protocols: Many consumer IoT devices use unsecure network protocols to communicate with other devices or servers, such as HTTP, FTP, Telnet, etc. These protocols do not encrypt or authenticate the data they transmit or receive, which can expose them to interception, modification, or spoofing by attackers.

**NEW QUESTION 70**

Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

- A. vulnerability scanning.
- B. threat hunting.
- C. red learning.

D. penetration testing.

**Answer:** B

**Explanation:**

Threat hunting is a proactive process of searching for signs of malicious activity or compromise within a system or network, by using hypotheses, indicators of compromise, and analytical tools. Threat hunting can help improve detection capabilities by identifying unknown threats, uncovering gaps in security controls, and providing insights for remediation and prevention. Vulnerability scanning (A) is a reactive process of scanning systems or networks for known vulnerabilities or weaknesses that can be exploited by attackers. It can help identify and prioritize vulnerabilities, but not proactively hunt for threats. Red teaming © is a simulated attack on a system or network by a group of ethical hackers who act as adversaries and try to breach security controls. It can help test the effectiveness of security defenses and response capabilities, but not proactively hunt for threats. Penetration testing (D) is similar to red teaming, but with a more defined scope and objective. It can help evaluate the security of a system or network by simulating real-world attacks and exploiting vulnerabilities, but not proactively hunt for threats. References: : <https://www.techopedia.com/definition/33297/threat-hunting> : <https://www.techopedia.com/definition/4160/web-application-security-scanner-was> : <https://www.techopedia.com/definition/32694/red-teaming> : <https://www.techopedia.com/definition/13493/penetration-testing>

**NEW QUESTION 72**

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

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

**Answer:** C

**Explanation:**

The correct answer is C. eFUSE. An eFUSE is a type of electronic fuse that can be programmed to permanently alter the functionality or configuration of a chipset. An eFUSE can be used to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset, by locking the firmware to a specific version or preventing unauthorized modifications. An eFUSE can also provide other benefits, such as anti-tampering, anti-counterfeiting, and device authentication<sup>1</sup>.

\* A. UEFI is not correct. UEFI stands for Unified Extensible Firmware Interface, and it is a standard that defines the software interface between an operating system and a platform firmware. UEFI can provide security features, such as secure boot, which verifies the integrity of the boot loader and prevents unauthorized code execution during the boot process. However, UEFI does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset<sup>2</sup>.

\* B. A hardware security module is not correct. A hardware security module (HSM) is a physical device that provides secure storage and processing of cryptographic keys and operations. An HSM can protect sensitive data and transactions, such as encryption, decryption, signing, or verification, from unauthorized access or tampering. However, an HSM does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset<sup>3</sup>.

\* D. Certificate signed updates are not correct. Certificate signed updates are a method of ensuring the authenticity and integrity of firmware updates by using digital certificates and signatures. Certificate signed updates can prevent malicious or corrupted firmware updates from being installed on the chipset, but they do not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. 1: What Is an eFUSE? 2: What Is UEFI? 3: What Is a Hardware Security Module (HSM)?

**NEW QUESTION 75**

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

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

**Answer:** C

**Explanation:**

MFA can be used to reduce the likelihood that the attacker gains access to the VM, however, the scenario specifically states that the attacker was able to escalate rights and the question asks what can be done to remediate the vulnerability. the vulnerability in this case would be the ability to escalate rights.

The best way to remediate the vulnerability is to update to the secure hypervisor version. A hypervisor is a software that creates and manages virtual machines on a physical server. A hypervisor can be vulnerable to various attacks, such as privilege escalation, code injection, or denial-of-service. Updating to the secure hypervisor version can help fix any known bugs or flaws in the hypervisor software and prevent attackers from exploiting them. Updating to the secure hypervisor version can also provide additional security features or enhancements that can improve the protection of the virtual machines and their data.

**NEW QUESTION 78**

A security analyst at exampte.com receives a SIEM alert for an IDS signature and reviews the associated packet capture and TCP stream:

Packet capture:

Source	Destination	Protocol	Length	Info
203.0.113.15	192.168.100.56	TCP	1016	60100 > 80 [PSH, ACK] Seq=1 Ack=1 Win=229 Len=946 TSval=419499016 TSecr=668384771 [TCP segment of a reassembled PDU]



TCP stream:

```
GET /admin/auth/Register.do HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
connection: close
content-type: <[<test='multipart/form-data'>(<dm=>ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(<_memberAccess?(<_memberAccess=>dm):
(<(<container=>context['com.opensymphony.xwork2.ActionContext.container']).(<ognlUtil=>container.getInstance(<com.opensymphony.xwork2.ognl.OgnlUtil@class>).
(<ognlUtil.getExcludedPackageNames().clear()).(<ognlUtil.getExcludedClasses().clear()).(<context.setMemberAccess(<dm>)).(<ros=
(<org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(<ros.println(31337*31337)).(<ros.flush())
host: connect.example.local
iv-user: Unauthenticated
user-agent: Security Operations Center: X-SOC-Scan (soc@example.com);
via: HTTP/1.1 revproxy.dmr.example.local:443
iv_server_name: connect-webseald-revproxy.dmr.example.local
X-
```

Winch of the following actions should the security analyst lake NEXT?

- A. Review the known Apache vulnerabilities to determine if a compromise actually occurred
- B. Contact the application owner for connect example local tor additional information
- C. Mark the alert as a false positive scan coming from an approved source.
- D. Raise a request to the firewall team to block 203.0.113.15.

**Answer: A**

**Explanation:**

The security analyst should review the known Apache vulnerabilities to determine if a compromise actually occurred. The SIEM alert indicates that an IDS signature detected an attempt to exploit a vulnerability in Apache Struts 2 (CVE-2017-5638), which allows remote code execution via a crafted Content-Type header<sup>4</sup>. The packet capture and TCP stream show that the attacker sent a malicious request with a Content-Type header containing an OGNL expression that executes the command “whoami” on the target server. However, this does not necessarily mean that the attack was successful, as it depends on whether the target server was running a vulnerable version of Apache Struts 2 or not. Therefore, the security analyst should review the known Apache vulnerabilities and compare them with the version of Apache Struts 2 running on the server to confirm if a compromise actually occurred or not.

**NEW QUESTION 81**

A threat hurting 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 85**

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 BYOO users
- C. A standardized anti-malware platform and a unified operating system vendor
- D. 802.1X lo 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<sup>5</sup>.

**NEW QUESTION 86**

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 87**

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 88**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 93**

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 94**

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

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

**Answer:** C

**Explanation:**

This command would most likely indicate if the email attachment is malicious, as it would display any JavaScript code embedded in the PDF file. JavaScript code can be used by attackers to execute malicious commands or scripts on the victim's system when the PDF file is opened<sup>1</sup>. The strings command extracts the printable characters from a binary file, such as a PDF file, and the grep -i "<script" option searches for the presence of JavaScript code in a case-insensitive manner<sup>2</sup>.

**NEW QUESTION 95**

Which of following allows Secure Boot to be enabled?

- A. eFuse
- B. UEFI
- C. MSM
- D. PAM

**Answer:** B

**Explanation:**

UEFI, or Unified Extensible Firmware Interface, is a specification that defines the software interface between an operating system and platform firmware. UEFI replaces the legacy BIOS (Basic Input/Output System) interface that was used to boot and configure computers. UEFI provides several advantages over BIOS, such as faster boot times, better security features, larger disk support, graphical user interface, etc. One of the security features that UEFI supports is Secure Boot, which is a mechanism that ensures that only authorized software can run during the boot process. Secure Boot prevents unauthorized or malicious code from loading or executing before the operating system starts. Secure Boot works by verifying the digital signature of each piece of boot software against a database of trusted keys stored in UEFI firmware. If the signature is valid, the software is allowed to run; otherwise, it is blocked or rejected.

**NEW QUESTION 100**

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

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

**Answer:** D

**Explanation:**

Fuzzing is a technique that involves sending random, malformed, or unexpected inputs to an application to trigger errors, crashes, or vulnerabilities. Fuzzing can be used to test the robustness and security of software, especially when the source code is not available or the input format is complex<sup>1</sup>. Fuzzing can also simulate abnormal user behavior, such as entering invalid data, clicking on random buttons, or sending malicious requests<sup>2</sup>.

Fuzzing tools are software programs that automate the process of generating and sending inputs to the application under test. There are different types of fuzzing tools, such as black-box fuzzers, white-box fuzzers, and grey-box fuzzers, depending on the level of information and feedback they have about the application<sup>1</sup>. Some examples of fuzzing tools are AFL, Peach, and [Sulley].

Polymorphic methods are techniques that allow fuzzing tools to modify or mutate the inputs in different ways, such as changing the length, value, type, or structure of the data. Polymorphic methods can increase the diversity and effectiveness of the inputs and help discover more bugs or vulnerabilities in the application .

Therefore, using fuzzing tools with polymorphic methods would be the best approach to test a new application that simulates abnormal user behavior to find software bugs. This approach would generate a large number of inputs that cover various scenarios and edge cases and expose any flaws or weaknesses in the application's functionality or security.

**NEW QUESTION 105**

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

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

**Answer:** B

**Explanation:**

User access logging (UAL) is a feature on Windows Server operating systems that records the details of remote access and management activities performed by users on the server. UAL can provide information such as the user name, the source IP address, the destination host name, the protocol used, and the time and duration of the connection<sup>1</sup>. Enabling user access logging on the VPN server can help the security analyst to obtain the best information to identify and investigate the inbound connection originating from an unknown IP address.

**NEW QUESTION 107**

A current, validated DLP solution is now in place because of a previous data breach. However, a new data breach has taken place. The following symptoms were

observed shortly after a recent sales meeting:

- \* Sensitive corporate documents appeared on the dark web.
- \* Unusually large packets of data were being sent out.

Which of the following is most likely occurring?

- A. Documents are not tagged properly to restrict sharing.
- B. An insider threat is exfiltration data.
- C. The DLP solution is not configured for unsecured web traffic
- D. File audits are not enabled on CASB.

**Answer: B**

**Explanation:**

This is most likely occurring based on the symptoms observed after a recent sales meeting. An insider threat is a person who has legitimate access to an organization's network or data and uses it for malicious purposes, such as stealing, leaking, or sabotaging information. The symptoms suggest that someone from the sales team or someone who attended the meeting has copied sensitive corporate documents and uploaded them to the dark web using large data packets.

**NEW QUESTION 111**

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

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

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 112**

A security analyst is supporting an embedded software team. Which of the following is the best recommendation to ensure proper error handling at runtime?

- A. Perform static code analysis.
- B. Require application fuzzing.
- C. Enforce input validation.
- D. Perform a code review.

**Answer: D**

**Explanation:**

Performing a code review is the best recommendation to ensure proper error handling at runtime for an embedded software team. A code review is a process of examining and evaluating source code by one or more developers other than the original author. A code review can help to identify and fix any errors, bugs, vulnerabilities, or inefficiencies in the code before it is deployed or executed. A code review can also help to ensure that the code follows the best practices, standards, and guidelines for error handling at runtime .

**NEW QUESTION 117**

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

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

**Answer: B**

**Explanation:**

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

<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

**NEW QUESTION 122**

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 124**

Industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacker was able to gain access to the SCADA by logging in to an account with weak credentials. Which of the following identity and access management solutions would help to mitigate this risk?

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

**Answer: D**

**Explanation:**

RBAC helps organizations manage access to critical infrastructure networks by assigning access based on roles. This allows organizations to control who can access specific resources and helps eliminate weak credentials that attackers could exploit. Manual reviews and endpoint detection and response can also help to mitigate risk, but role based access control is the best solution for this scenario.

**NEW QUESTION 126**

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 131**

A security analyst is reviewing the following DNS logs as part of security-monitoring activities:

```
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www.company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfchfaerwfj.co 32.56.32.122
FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53
FROM 192.168.1.93 ARAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www.comptia.org 122.10.31.87
```

Which of the following most likely occurred?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 132**

Which of the following is the best method to review and assess the security of the cloud service models used by a company on multiple CSPs?



- A. Unifying and migrating all services in a single CSP
- B. Executing an API hardening process on the CSPs' endpoints
- C. Integrating the security benchmarks of the CSPs with a CASB
- D. Deploying cloud instances using Nikto and OpenVAS

**Answer: C**

**Explanation:**

This is the best method to review and assess the security of the cloud service models used by a company on multiple CSPs. CSP stands for cloud service provider, which is a company that offers cloud-based services such as infrastructure, platform, or software. CASB stands for cloud access security broker, which is a software or service that acts as a gateway between the company and the CSPs, and provides visibility, control, compliance, and threat protection for the cloud services.

Integrating the security benchmarks of the CSPs with a CASB means that the company can use a common set of standards and metrics to measure and compare the security posture and performance of different cloud service models, such as IaaS, PaaS, or SaaS. Security benchmarks are predefined criteria or best practices that define the minimum level of security required for a cloud service model. For example, some security benchmarks may include encryption, authentication, logging, auditing, patching, backup, etc. By integrating these benchmarks with a CASB, the company can monitor and enforce them across multiple CSPs, and identify any gaps or risks in their cloud security.

**NEW QUESTION 137**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 140**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 143**

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 145**

A security analyst performs a weekly vulnerability scan on a network that has 240 devices and receives a report with 2,450 pages. Which of the following would most likely decrease the number of false positives?

- A. Manual validation
- B. Penetration testing
- C. A known-environment assessment
- D. Credentialed scanning

**Answer:** D

**Explanation:**

Credentialed scanning is a method of vulnerability scanning that uses valid user credentials to access the target systems and perform a more thorough and accurate assessment of their security posture. Credentialed scanning can help to reduce the number of false positives by allowing the scanner to access more information and resources on the systems, such as configuration files, registry keys, installed software, patches, and permissions .

**NEW QUESTION 150**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 152**

An organization supports a large number of remote users. Which of the following is the best option to protect the data on the remote users' laptops?

- A. Require the use of VPNs.
- B. Require employees to sign an NDA.
- C. Implement a DLP solution.
- D. Use whole disk encryption.

**Answer:** D

**Explanation:**

Using whole disk encryption is the best option to protect the data on the remote users' laptops. Whole disk encryption is a technique that encrypts all data on a hard disk drive, including the operating system, applications and files. Whole disk encryption can prevent unauthorized access to the data if the laptop is lost, stolen or compromised. Whole disk encryption can also protect the data from physical attacks, such as removing the hard disk and connecting it to another device .

**NEW QUESTION 156**

A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

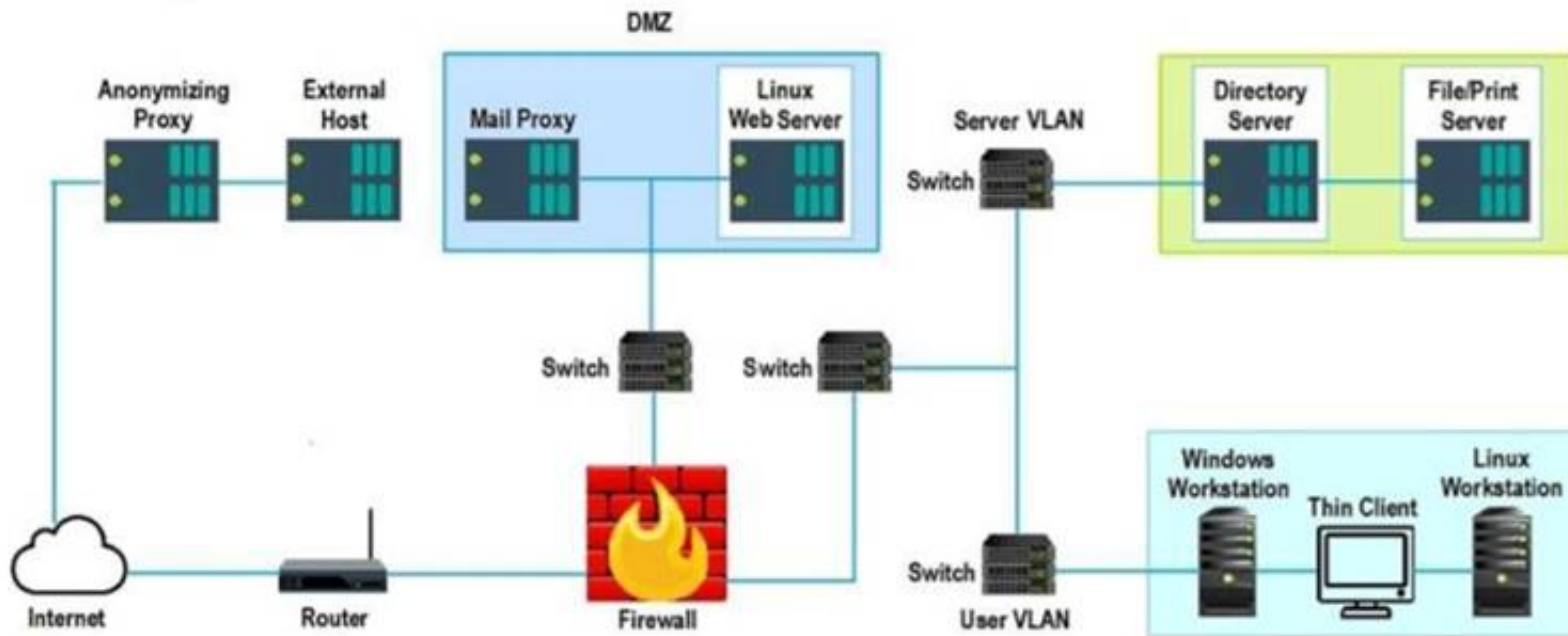
Instructions:

Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan. For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.

If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Network Diagram



### Hot Area:

False Positive	Findings Listing	Results Generated
<input type="radio"/>	<b>Findings Listing 1</b> Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	Credentialed Non-Credentialed Compliance
<input type="radio"/>	<b>Findings Listing 2</b> Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035) Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)	Credentialed Non-Credentialed Compliance
<input type="radio"/>	<b>Findings Listing 3</b> WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves	Credentialed Non-Credentialed Compliance

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

### Hot Area:

False Positive	Findings Listing	Results Generated
<input type="radio"/>	<b>Findings Listing 1</b> Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	Credentialed Non-Credentialed Compliance
<input type="radio"/>	<b>Findings Listing 2</b> Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035) Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)	Credentialed Non-Credentialed Compliance
<input type="radio"/>	<b>Findings Listing 3</b> WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves	Credentialed Non-Credentialed Compliance



**NEW QUESTION 161**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 163**

Which of the following are important reasons for performing proactive threat-hunting activities? (Select two).

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

**Answer: CE**

**Explanation:**

Proactive threat-hunting is the process of actively searching for unknown threats in the network, rather than waiting for alerts or indicators of compromise. Some of the important reasons for performing proactive threat-hunting activities are:

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

**NEW QUESTION 165**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 170**

At which of the following phases of the SDLC should security FIRST be involved?

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

**Answer: E**

**Explanation:**

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

**NEW QUESTION 174**

During routine monitoring a security analyst identified the following enterprise network traffic: Packet capture output:



No.	Source	Destination	Protocol	Info
105	66.187.224.210	192.168.12.21	DNS	Standard query response A 209.132.177.50
106	192.168.12.21	209.132.177.50	TCP	48890 > http [SYN] Seq=0 len=0 MSS=1460 TSV=1535
107	209.132.177.50	192.168.12.21	TCP	http > 48890 [SYN, ACK] Seq=0 Ack=1 Win=5792 len=0
108	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq=1 Ack=1 len=0
109	192.168.12.21	209.132.177.50	HTTP	GET / HTTP/1.1

Which of the following BEST describes what the security analyst observed?

- A. 66.187.224.210 set up a DNS hijack with 192.168.12.21.
- B. 192.168.12.21 made a TCP connection to 66 187 224 210
- C. 192.168.12.21 made a TCP connection to 209 132 177 50
- D. 209.132.177.50 set up a TCP reset attack to 192 168 12 21

**Answer: C**

**Explanation:**

The security analyst observed that 192.168.12.21 made a TCP connection to 209.132.177.50. This can be inferred from the packet capture output, which shows the following sequence of packets:

- Packet 1: A SYN packet from 192.168.12.21 to 209.132.177.50 on port 80 (HTTP). This is the first step of the TCP three-way handshake, where the source initiates a connection request to the destination.
- Packet 2: A SYN-ACK packet from 209.132.177.50 to 192.168.12.21 on port 80 (HTTP). This is the second step of the TCP three-way handshake, where the destination acknowledges and accepts the connection request from the source.
- Packet 3: An ACK packet from 192.168.12.21 to 209.132.177.50 on port 80 (HTTP). This is the third and final step of the TCP three-way handshake, where the source confirms and completes the connection establishment with the destination.

These packets indicate that a TCP connection was successfully established between 192.168.12.21 and 209.132.177.50 on port 80.

**NEW QUESTION 175**

During a company's most recent incident, a vulnerability in custom software was exploited on an externally facing server by an APT. The lessons-learned report noted the following:

- The development team used a new software language that was not supported by the security team's automated assessment tools.
- During the deployment, the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. Therefore, the vulnerability was not detected.
- The current IPS did not have effective signatures and policies in place to detect and prevent runtime attacks on the new application.

To allow this new technology to be deployed securely going forward, which of the following will BEST address these findings? (Choose two.)

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

**Answer: AB**

**Explanation:**

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

**NEW QUESTION 177**

A security analyst is reviewing port scan data that was collected over the course of several months. The following data represents the trends:

	Number of devices with open ports					
Port	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
445	8	8	8	8	8	8
8443	7	9	10	13	16	19
22	6	6	7	6	8	6

Which of the following is the BEST action for the security analyst to take after analyzing the trends?

- A. Review the system configurations to determine if port 445 needs to be open.
- B. Assume there are new instances of Apache in the environment.
- C. Investigate why the number of open SSH ports varied during the six months.
- D. Raise a concern to a supervisor regarding possible malicious use Of port 8443.

**Answer: C**

**Explanation:**

According to the CompTIA CySA+ Certification Exam Study guide, the best action for the security analyst to take after analyzing the trends is to investigate why

the number of open SSH ports varied during the six months. This could indicate that malicious actors are attempting to gain access to the system, and it would be important to find out the root cause of this activity in order to prevent further intrusions. Additionally, raising a concern to a supervisor regarding possible malicious use of port 8443 would also be a prudent step, as this port is often used by attackers. As stated in the study guide, "Monitoring network ports and traffic can provide insight into suspicious activity and may be necessary to identify malicious activities". Additionally, "Ports can be used to gain unauthorized access to a system, so it is important to monitor the ports and to take steps to ensure that only necessary ports are open".

**NEW QUESTION 181**

Which of the following BEST explains the function of a managerial control?

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

**Answer:** A

**Explanation:**

A managerial control is a function of management that involves setting performance standards, measuring performance, and taking corrective actions when necessary. A managerial control helps to regulate the organizational activities and ensure that they are aligned with the organizational goals and objectives<sup>1</sup>. One of the functions of a managerial control is to help design and implement the security planning, program development, and maintenance of the security life cycle. The security life cycle is a process that defines the phases of security activities from initiation to disposal<sup>2</sup>. A managerial control can help to establish the security policies, procedures, roles, and responsibilities for each phase of the security life cycle. A managerial control can also help to monitor and evaluate the security performance and effectiveness of each phase and take corrective actions if needed.

**NEW QUESTION 186**

A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application. Which of the following is a security concern when using a PaaS solution?

- A. The use of infrastructure-as-code capabilities leads to an increased attack surface.
- B. Patching the underlying application server becomes the responsibility of the client.
- C. The application is unable to use encryption at the database level.
- D. Insecure application programming interfaces can lead to data compromise.

**Answer:** D

**Explanation:**

Insecure application programming interfaces (APIs) can lead to data compromise when using a PaaS solution. APIs are interfaces that allow applications to communicate with each other and with the underlying platform. APIs can expose sensitive data or functionality to unauthorized or malicious users if they are not properly designed, implemented, or secured. Insecure APIs can result in data breaches, denial of service, unauthorized access, or code injection .

**NEW QUESTION 187**

After a remote command execution incident occurred on a web server, a security analyst found the following piece of code in an XML file:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow"> ]>
<userInfo>
```

Which of the following is the BEST solution to mitigate this type of attack?

- A. Implement a better level of user input filters and content sanitization.
- B. Properly configure XML handlers so they do not process sent parameters coming from user inputs.
- C. Use parameterized Queries to avoid user inputs from being processed by the server.
- D. Escape user inputs using character encoding conjoined with whitelisting

**Answer:** A

**Explanation:**

The piece of code in the XML file is an example of a command injection attack, which is a type of attack that exploits insufficient input validation or output encoding to execute arbitrary commands on a server or system<sup>2</sup>

The attacker can inject malicious commands into an XML element that is processed by an XML handler on the server, and cause the server to execute those commands. The best solution to mitigate this type of attack is to implement a better level of user input filters and content sanitization, which means checking and validating any user input before processing it, and removing or encoding any potentially harmful characters or commands.

**NEW QUESTION 190**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 191**

An organization has the following policies:

\*Services must run on standard ports.

\*Unneeded services must be disabled.

The organization has the following servers:

\*192.168.10.1 - web server

\*192.168.10.2 - database server

A security analyst runs a scan on the servers and sees the following output:

```
Host 192.168.10.1
PORT      STATE    SERVICE
22/tcp    open    ssh
80/tcp    open    http
443/tcp   open    https
1027/tcp  open    IIS
```

```
Host 192.168.10.2
PORT      STATE    SERVICE
22/tcp    open    ssh
53/tcp    open    dns
1434/tcp  open    mssql
```

Which of the following actions should the analyst take?

- A. Disable HTTPS on 192.168.10.1.
- B. Disable IIS on 192.168.10.1.
- C. Disable DNS on 192.168.10.2.
- D. Disable MSSQL on 192.168.10.2.
- E. Disable SSH on both servers.

**Answer: E**

**Explanation:**

SSH stands for Secure Shell, which is a protocol that allows remote access and administration of a server. If the organization has a policy that services must run on standard ports and unneeded services must be disabled, then SSH should be disabled on both servers, because it runs on port 22, which is not a standard port for a web server or a database server, and it is not needed for those servers to function properly. Disabling HTTPS on 192.168.10.1, disabling IIS on 192.168.10.1, disabling DNS on 192.168.10.1, or disabling MSSQL on 192.168.10.2 are not appropriate actions, because they would affect the functionality of the web server or the database server and violate the organization's policy of running services on standard ports. Reference: <https://www.ssh.com/ssh/port>

**NEW QUESTION 193**

A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely performed to validate the code prior to pushing it to production?

- A. Web-application vulnerability scan
- B. Static analysis
- C. Packet inspection
- D. Penetration test

**Answer: B**

**Explanation:**

Static analysis is a method of analyzing software code without executing it, by using tools or techniques that check for syntax errors, logic errors, vulnerabilities, coding standards, and other quality issues. Static analysis can help software developers to correct the error-handling capabilities of an application before pushing it to production, as it can detect potential errors and bugs at an early stage of development. A web-application vulnerability scan (A) is a method of testing web applications for security flaws by simulating attacks and analyzing responses. It can be useful for finding vulnerabilities in web applications, but not for validating the error-handling capabilities of an application. A packet inspection (C) is a method of monitoring network traffic by examining the data packets that are sent and received over a network. It can be useful for detecting malicious or unauthorized activity on a network, but not for validating the error-handling capabilities of an application. A penetration test (D) is a method of evaluating the security of a system or network by simulating real-world attacks and exploiting vulnerabilities. It can be useful for assessing the overall security posture of a system or network, but not for validating the error-handling capabilities of an application.

References: : <https://www.techopedia.com/definition/14436/static-analysis> : <https://www.techopedia.com/definition/4160/web-application-security-scanner-was> : <https://www.techopedia.com/definition/4010/packet-inspection> : <https://www.techopedia.com/definition/13493/penetration-testing>

**NEW QUESTION 197**

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

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

**Answer: C**

**Explanation:**

<https://www.techtarget.com/searchsecurity/definition/data-masking>

Masking is a technique that involves replacing or hiding some parts of sensitive information with symbols or characters, such as asterisks (\*) or Xs. Masking can help safeguard the confidentiality of sensitive information while allowing limited access to authorized individuals, because it obscures the original data without altering its format or structure. For example, masking can be used to hide some digits of a credit card number or a social security number. Deidentification, hashing, or salting are other techniques that involve transforming or modifying sensitive information, but they do not allow limited access to authorized individuals.

Reference: <https://www.ibm.com/docs/en/ims/14.1?topic=masking-data>

#### NEW QUESTION 202

During a review of recent network traffic, an analyst realizes the team has seen this same traffic multiple times in the past three weeks, and it resulted in confirmed malware activity. The analyst also notes there is no other alert in place for this traffic. After resolving the security incident, which of the following would be the BEST action for the analyst to take to increase the chance of detecting this traffic in the future?

- A. Share details of the security incident with the organization's human resources management team
- B. Note the security incident so other analysts are aware the traffic is malicious
- C. Communicate the security incident to the threat team for further review and analysis
- D. Report the security incident to a manager for inclusion in the daily report

**Answer: C**

#### Explanation:

Communicate the security incident to the threat team for further review and analysis. This would allow the threat team to investigate the source and nature of the malicious traffic and create appropriate alerts or signatures to detect it in the future. Sharing details with human resources, noting the incident, or reporting it to a manager would not increase the chance of detection.

#### NEW QUESTION 206

.....



## 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](#)**