

CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam



NEW QUESTION 1

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

- A. Human resources
- B. Public relations
- C. Marketing
- D. Internal network operations center

Answer: B

NEW QUESTION 2

A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities. The type of vulnerability that should be disseminated FIRST is one that:

- A. enables remote code execution that is being exploited in the wild.
- B. enables data leakage but is not known to be in the environment
- C. enables lateral movement and was reported as a proof of concept
- D. affected the organization in the past but was probably contained and eradicated

Answer: C

NEW QUESTION 3

After receiving reports of latency, a security analyst performs an Nmap scan and observes the following output:

Which of the following suggests the system that produced output was compromised?

- A. Secure shell is operating on this system.
- B. There are no indicators of compromise on this system.
- C. MySQL services are identified on a standard PostgreSQL port.
- D. Standard HTTP is open on the system and should be closed.

Answer: B

NEW QUESTION 4

A security analyst needs to reduce the overall attack surface.

Which of the following infrastructure changes should the analyst recommend?

- A. Implement a honeypot.
- B. Air gap sensitive systems.
- C. Increase the network segmentation.
- D. Implement a cloud-based architecture.

Answer: C

NEW QUESTION 5

Which of the following should be found within an organization's acceptable use policy?

- A. Passwords must be eight characters in length and contain at least one special character.
- B. Customer data must be handled properly, stored on company servers, and encrypted when possible.
- C. Administrator accounts must be audited monthly, and inactive accounts should be removed.
- D. Consequences of violating the policy could include discipline up to and including termination.

Answer: D

NEW QUESTION 6

An organization is moving its infrastructure to the cloud in an effort to meet the budget and reduce staffing requirements. The organization has three environments: development, testing, and production. These environments have interdependencies but must remain relatively segmented.

Which of the following methods would BEST secure the company's infrastructure and be the simplest to manage and maintain?

- A. Create three separate cloud accounts for each environment
- B. Configure account peering and security rules to allow access to and from each environment.
- C. Create one cloud account with one VPC for all environments
- D. Purchase a virtual firewall and create granular security rules.
- E. Create one cloud account and three separate VPCs for each environment
- F. Create security rules to allow access to and from each environment.
- G. Create three separate cloud accounts for each environment and a single core account for network service
- H. Route all traffic through the core account.

Answer: C

NEW QUESTION 7

A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

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

Answer: B

NEW QUESTION 8

A security analyst has been alerted to several emails that show evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

- A. the public relations department
- B. senior leadership
- C. law enforcement
- D. the human resources department

Answer: D

NEW QUESTION 9

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

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

Answer: AD

NEW QUESTION 10

A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future. Which of the following would be the BEST solution to recommend to the director?

- A. Install a data loss prevention system, and train human resources employees on its use
- B. Provide PII training to all employees at the company
- C. Encrypt PII information.
- D. Enforce encryption on all emails sent within the company
- E. Create a PII program and policy on how to handle data
- F. Train all human resources employees.

- G. Train all employee
- H. Encrypt data sent on the company network
- I. Bring in privacy personnel to present a plan on how PII should be handled.
- J. Install specific equipment to create a human resources policy that protects PII data
- K. Train company employees on how to handle PII data
- L. Outsource all PII to another company
- M. Send the human resources director to training for PII handling.

Answer: A

NEW QUESTION 10

A web developer wants to create a new web part within the company website that aggregates sales from individual team sites. A cybersecurity analyst wants to ensure security measurements are implemented during this process. Which of the following remediation actions should the analyst take to implement a vulnerability management process?

- A. Personnel training
- B. Vulnerability scan
- C. Change management
- D. Sandboxing

Answer: C

NEW QUESTION 14

A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance software as identified from the firewall logs but the destination IP is blocked and not captured. Which of the following should the analyst do?

- A. Shut down the computer
- B. Capture live data using Wireshark
- C. Take a snapshot
- D. Determine if DNS logging is enabled.
- E. Review the network logs.

Answer: A

NEW QUESTION 15

A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT. Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?

- A. Attack vectors
- B. Adversary capability
- C. Diamond Model of Intrusion Analysis
- D. Kill chain
- E. Total attack surface

Answer: B

NEW QUESTION 19

It is important to parameterize queries to prevent:

- A. the execution of unauthorized actions against a database.
- B. a memory overflow that executes code with elevated privileges.
- C. the establishment of a web shell that would allow unauthorized access.
- D. the queries from using an outdated library with security vulnerabilities.

Answer: A

NEW QUESTION 24

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.

The company's hardening guidelines indicate the following:

- TLS 1.2 is the only version of TLS running.
- Apache 2.4.18 or greater should be used.
- Only default ports should be used. INSTRUCTIONS

Using the supplied data, record the status of compliance with the company's guidelines for each server.

The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Part 1 Answer

Check on the following:

AppServ1 is only using TLS.1.2

AppServ4 is only using TLS.1.2

AppServ1 is using Apache 2.4.18 or greater

AppServ3 is using Apache 2.4.18 or greater

AppServ4 is using Apache 2.4.18 or greater

Part 2 Answer

Recommendation:

Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48

NEW QUESTION 25

A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?

- A. Motion detection
- B. Perimeter fencing
- C. Monitored security cameras
- D. Badged entry

Answer: A

NEW QUESTION 27

A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server.

Which of the following should be done to correct the cause of the vulnerability?

- A. Deploy a WAF in front of the application.
- B. Implement a software repository management tool.
- C. Install a HIPS on the server.
- D. Instruct the developers to use input validation in the code.

Answer: B

NEW QUESTION 32

A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named Webserverlist.Xml. The host list is provided in a file named webserverlist.txt. Which of the following Nmap commands would BEST accomplish this goal?

- A)
- B)
- C)
- D)

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

Answer: A

NEW QUESTION 33

A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:

In which of the following phases is this APT MOST likely to leave discoverable artifacts?

- A. Data collection/exfiltration
- B. Defensive evasion
- C. Lateral movement
- D. Reconnaissance

Answer: A

NEW QUESTION 38

A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.

Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

- A. Development of a hypothesis as part of threat hunting
- B. Log correlation, monitoring, and automated reporting through a SIEM platform
- C. Continuous compliance monitoring using SCAP dashboards
- D. Quarterly vulnerability scanning using credentialed scans

Answer: A

NEW QUESTION 40

A web-based front end for a business intelligence application uses pass-through authentication to authenticate users. The application then uses a service account, to perform queries and look up data in a database. A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

- A. Change the security model to force the users to access the database as themselves
- B. Parameterize queries to prevent unauthorized SQL queries against the database
- C. Configure database security logging using syslog or a SIEM
- D. Enforce unique session IDs so users do not get a reused session ID

Answer: B

NEW QUESTION 44

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer data. Developers use personal workstations, giving the company little to no visibility into the development activities.

Which of the following would be BEST to implement to alleviate the CISO's concern?

- A. DLP
- B. Encryption
- C. Test data
- D. NDA

Answer: D

NEW QUESTION 46

Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

- A. Self-encrypting drive
- B. Bus encryption
- C. TPM
- D. HSM

Answer: A

NEW QUESTION 48

A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database. Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

- A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.
- B. Remove the servers reported to have high and medium vulnerabilities.
- C. Tag the computers with critical findings as a business risk acceptance.
- D. Manually patch the computers on the network, as recommended on the CVE website.
- E. Harden the hosts on the network, as recommended by the NIST framework.
- F. Resolve the monthly job issues and test them before applying them to the production network.

Answer: CE

NEW QUESTION 49

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

Which of the following attack types is occurring?

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

Answer: A

NEW QUESTION 53

A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:

Which of the following can the analyst conclude?

- A. Malware is attempting to beacon to 128.50.100.3.
- B. The system is running a DoS attack against ajgidwle.com.
- C. The system is scanning ajgidwle.com for PII.
- D. Data is being exfiltrated over DNS.

Answer: D

NEW QUESTION 57

A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

- A. PC1
- B. PC2
- C. Server1
- D. Server2
- E. Firewall

Answer: B

NEW QUESTION 58

An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds. Which of the following can be inferred from this activity?

- A. 10.200.2.0/24 is infected with ransomware.
- B. 10.200.2.0/24 is not routable address space.
- C. 10.200.2.5 is a rogue endpoint.
- D. 10.200.2.5 is exfiltrating data.

Answer: D

NEW QUESTION 61

A large software company wants to move «s source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

- A. Establish an alternate site with active replication to other regions
- B. Configure a duplicate environment in the same region and load balance between both instances
- C. Set up every cloud component with duplicated copies and auto scaling turned on
- D. Create a duplicate copy on premises that can be used for failover in a disaster situation

Answer: A

NEW QUESTION 62

As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

- A. Critical asset list
- B. Threat vector
- C. Attack profile
- D. Hypothesis

Answer: A

NEW QUESTION 67

Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?

- A. Unauthorized, unintentional, benign
- B. Unauthorized, intentional, malicious
- C. Authorized, intentional, malicious
- D. Authorized, unintentional, benign

Answer: C

NEW QUESTION 70

A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization.

Which of the following BEST describes the security analyst's goal?

- A. To create a system baseline
- B. To reduce the attack surface
- C. To optimize system performance
- D. To improve malware detection

Answer: B

NEW QUESTION 75

An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?

- A. Tokenization of sensitive data
- B. Establishment o' data classifications
- C. Reporting on data retention and purging activities
- D. Formal identification of data ownership
- E. Execution of NDAs

Answer: A

NEW QUESTION 76

A company just chose a global software company based in Europe to implement a new supply chain management solution. Which of the following would be the MAIN concern of the company?

- A. Violating national security policy
- B. Packet injection
- C. Loss of intellectual property
- D. International labor laws

Answer: A

NEW QUESTION 77

Which of the following are components of the intelligence cycle? (Select TWO.)

- A. Collection

- B. Normalization
- C. Response
- D. Analysis
- E. Correction
- F. Dissension

Answer: BE

NEW QUESTION 81

A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.

Which of the following will remediate this software vulnerability?

- A. Enforce unique session IDs for the application.
- B. Deploy a WAF in front of the web application.
- C. Check for and enforce the proper domain for the redirect.
- D. Use a parameterized query to check the credentials.
- E. Implement email filtering with anti-phishing protection.

Answer: D

NEW QUESTION 86

The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:

- A. web servers on private networks
- B. HVAC control systems
- C. smartphones
- D. firewalls and UTM devices

Answer: D

NEW QUESTION 89

An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company. Which of the following technical controls would BEST accomplish this goal?

- A. DLP
- B. Encryption
- C. Data masking
- D. SPF

Answer: A

NEW QUESTION 90

The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

- A. Post of the company blog
- B. Corporate-hosted encrypted email
- C. VoIP phone call
- D. Summary sent by certified mail
- E. Externally hosted instant message

Answer: C

NEW QUESTION 93

A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a timely manner when an employee leaves the organization. To BEST resolve the issue, the organization should implement

- A. federated authentication
- B. role-based access control.
- C. manual account reviews
- D. multifactor authentication.

Answer: A

NEW QUESTION 96

As part of a review of modern response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?

- A. Organizational policies
- B. Vendor requirements and contracts
- C. Service-level agreements
- D. Legal requirements

Answer: D

NEW QUESTION 97

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

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

Answer: C

NEW QUESTION 102

An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment One of the primary concerns is exfiltration of data by malicious insiders Which of the following controls is the MOST appropriate to mitigate risks?

- A. Data deduplication
- B. OS fingerprinting
- C. Digital watermarking
- D. Data loss prevention

Answer: D

NEW QUESTION 106

Which of the following will allow different cloud instances to share various types of data with a minimal amount of complexity?

- A. Reverse engineering
- B. Application log collectors
- C. Workflow orchestration
- D. API integration
- E. Scripting

Answer: D

NEW QUESTION 111

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

The analyst runs the following command next:

Which of the following would explain the difference in results?

- A. ICMP is being blocked by a firewall.
- B. The routing tables for ping and hping3 were different.
- C. The original ping command needed root permission to execute.
- D. hping3 is returning a false positive.

Answer: A

NEW QUESTION 116

Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:

```
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/ "><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance "></s:Body></s:Envelope> 192.168.1.22 - -
api.somesite.com 200 0 1006 1001 0 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com 192.168.5.66 - - api.somesite.com 200 0 11558
1712 2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body>< 192.168.1.22 - - api.somesite.com 200 0 1003 1011
307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="
http://www.w3.org/2001/XMLSchema-instance"><a:Authentication>
<a:ApiToken>kmL4krG2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:ImpersonateUserId>0
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authe 192.168.5.66 - - api.somesite.com 200 0 1378 1209
48 192.168.4.89
```

Which of the following MOST likely explains how the clients' accounts were compromised?

- A. The clients' authentication tokens were impersonated and replayed.
- B. The clients' usernames and passwords were transmitted in cleartext.
- C. An XSS scripting attack was carried out on the server.
- D. A SQL injection attack was carried out on the server.

Answer: A

NEW QUESTION 121

A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:

Which of the following commands would work BEST to achieve the desired result?

- A. `grep -v chatter14 chat.log`
- B. `grep -i pythonfun chat.log`
- C. `grep -i javashark chat.log`
- D. `grep -v javashark chat.log`
- E. `grep -v pythonfun chat.log`
- F. `grep -i chatter14 chat.log`

Answer: D

NEW QUESTION 123

An executive assistant wants to onboard a new cloud based product to help with business analytics and dashboarding. When of the following would be the BEST integration option for the service?

- A. Manually log in to the service and upload data files on a regular basis.
- B. Have the internal development team script connectivity and file translate to the new service.
- C. Create a dedicated SFTP sue and schedule transfers to ensue file transport security
- D. Utilize the cloud products API for supported and ongoing integrations

Answer: A

NEW QUESTION 124

A security analyst wants to identify which vulnerabilities a potential attacker might initially exploit if the network is compromised Which of the following would provide the BEST results?

- A. Baseline configuration assessment
- B. Uncredentialed scan
- C. Network ping sweep
- D. External penetration test

Answer: D

NEW QUESTION 125

A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN administrator moved a power plug when testing the SAN's fault notification features.

Which of the following should be done to prevent this issue from reoccurring?

- A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.
- B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.
- C. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.
- D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

Answer: A

NEW QUESTION 130

After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

Which of the following IP addresses does the analyst need to investigate further?

- A. 192.168.1.1
- B. 192.168.1.10
- C. 192.168.1.12
- D. 192.168.1.193

Answer: C

NEW QUESTION 132

A cybersecurity analyst is responding to an incident. The company's leadership team wants to attribute the incident to an attack group. Which of the following models would BEST apply to the situation?

- A. Intelligence cycle
- B. Diamond Model of Intrusion Analysis
- C. Kill chain
- D. MITRE ATT&CK

Answer: B

NEW QUESTION 135

An organization has not had an incident for several month. The Chief information Security Officer (CISO) wants to move to proactive stance for security investigations. Which of the following would BEST meet that goal?

- A. Root-cause analysis
- B. Active response
- C. Advanced antivirus
- D. Information-sharing community
- E. Threat hunting

Answer: E

NEW QUESTION 140

Which of me following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

- A. It automatically performs remedial configuration changes lo enterprise security services
- B. It enables standard checklist and vulnerability analysis expressions for automaton
- C. It establishes a continuous integration environment for software development operations
- D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 144

A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-payments .c onf file The output of the diff command against the

known-good backup reads as follows

Which of the following MOST likely occurred?

- A. The file was altered to accept payments without charging the cards
- B. The file was altered to avoid logging credit card information
- C. The file was altered to verify the card numbers are valid.
- D. The file was altered to harvest credit card numbers

Answer: A

NEW QUESTION 147

A user receives a potentially malicious email 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/file.pdf`
- B. `file ~/Desktop/file.pdf`
- C. `strings ~/Desktop/file.pdf | grep "<script"`
- D. `cat < ~/Desktop/file.pdf | grep -i .exe`

Answer: A

NEW QUESTION 150

A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:

Which of the following should the analyst review to find out how the data was exfiltrated?

- A. Monday's logs
- B. Tuesday's logs
- C. Wednesday's logs
- D. Thursday's logs

Answer: D

NEW QUESTION 155

A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?

- A. Nikto
- B. Aircrack-ng
- C. Nessus
- D. tcpdump

Answer: A

NEW QUESTION 159

Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?

- A. Data custodian
- B. Data owner
- C. Data processor
- D. Senior management

Answer: B

NEW QUESTION 163

Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

INSTRUCTIONS

Review the information provided and determine the following:

- * 1. How many employees clicked on the link in the phishing email?
- * 2. On how many workstations was the malware installed?
- * 3. What is the executable file name or the malware?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Select the following answer as per diagram below:

NEW QUESTION 168

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: B

NEW QUESTION 169

A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability. Company policy prohibits using portable media or mobile storage. The security analyst is trying to determine which user caused the malware to get onto the system. Which of the following registry keys would MOST likely have this information?

- A)
- B)
- C)
- D)

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

Answer: C

NEW QUESTION 171

While analyzing logs from a WAF, a cybersecurity analyst finds the following:

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

- A. This is an encrypted GET HTTP request
- B. A packet is being used to bypass the WAF
- C. This is an encrypted packet
- D. This is an encoded WAF bypass

Answer: D

NEW QUESTION 174

A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

Antivirus is installed on the remote host:

Installation path: C:\Program Files\AVProduct\Win32\ Product Engine: 14.12.101

Engine Version: 3.5.71

Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.

The engine version is out of date. The oldest supported version from the vendor is 4.2.11. The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

- A. This is a false positive, and the scanning plugin needs to be updated by the vendor.
- B. This is a true negative, and the new computers have the correct version of the software.
- C. This is a true positive, and the new computers were imaged with an old version of the software.
- D. This is a false negative, and the new computers need to be updated by the desktop team.

Answer: C

NEW QUESTION 177

A cybersecurity analyst is supporting an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

- A. Requirements analysis and collection planning
- B. Containment and eradication
- C. Recovery and post-incident review
- D. Indicator enrichment and research pivoting

Answer: A

NEW QUESTION 182

Which of the following technologies can be used to house the entropy keys for task encryption on desktops and laptops?

- A. Self-encrypting drive
- B. Bus encryption
- C. TPM
- D. HSM

Answer: A

NEW QUESTION 185

Bootloader malware was recently discovered on several company workstations. All the workstations run Windows and are current models with UEFI capability. Which of the following UEFI settings is the MOST likely cause of the infections?

- A. Compatibility mode
- B. Secure boot mode
- C. Native mode
- D. Fast boot mode

Answer: A

NEW QUESTION 190

A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:

Which of the following is MOST likely a false positive?

- A. ICMP timestamp request remote date disclosure
- B. Windows SMB service enumeration via \srvsvc
- C. Anonymous FTP enabled
- D. Unsupported web server detection

Answer: B

NEW QUESTION 191

An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability. Which of the following would be the MOST appropriate to remediate the controller?

- A. Segment the network to constrain access to administrative interfaces.
- B. Replace the equipment that has third-party support.
- C. Remove the legacy hardware from the network.
- D. Install an IDS on the network between the switch and the legacy equipment.

Answer: A

NEW QUESTION 194

A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in the situation?

- A. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
- B. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs
- C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
- D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains

Answer: C

NEW QUESTION 196

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

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.datacenters.com
- B. telnet 10.79.95.173 443
- C. ftpd 10.79.95.173.rdns.datacenters.com 443
- D. tracer 10.79.95.173

Answer: B

NEW QUESTION 200

During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect. Which of the following is the BEST place to acquire evidence to perform data carving?

- A. The system memory
- B. The hard drive
- C. Network packets
- D. The Windows Registry

Answer: A

NEW QUESTION 202

During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.

Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

- A. An IPS signature modification for the specific IP addresses
- B. An IDS signature modification for the specific IP addresses
- C. A firewall rule that will block port 80 traffic
- D. A firewall rule that will block traffic from the specific IP addresses

Answer: D

NEW QUESTION 203

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

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

- A. strace /proc/1301
- B. rpm -V openash-server
- C. /bin/ls -l /proc/1301/exe
- D. kill -9 1301

Answer: A

NEW QUESTION 207

An incident responder successfully acquired application binaries off a mobile device for later forensic analysis. Which of the following should the analyst do NEXT?

- A. Decompile each binary to derive the source code.
- B. Perform a factory reset on the affected mobile device.
- C. Compute SHA-256 hashes for each binary.
- D. Encrypt the binaries using an authenticated AES-256 mode of operation.
- E. Inspect the permissions manifests within each application.

Answer: C

NEW QUESTION 210

An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets.

Which of the following should be considered FIRST prior to disposing of the electronic data?

- A. Sanitization policy
- B. Data sovereignty
- C. Encryption policy
- D. Retention standards

Answer: D

NEW QUESTION 212

During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation . Which of the following would cause the analyst to further review the incident?

- A)
- B)
- C)
- D)
- E)

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

Answer: D

NEW QUESTION 215

As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:

- A. qualitative probabilities.
- B. quantitative probabilities.
- C. qualitative magnitude.
- D. quantitative magnitude.

Answer: D

NEW QUESTION 220

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

- A. Add TXT @ "v=spf1 mx include:_spf.comptia.org all" to the DNS record.
- B. Add TXT @ "v=spf1 mx include:_spf.comptia.org all" to the email server.
- C. Add TXT @ "v=spf1 mx include:_spf.comptia.org +all" to the domain controller.
- D. Add TXT @ "v=spf1 mx include:_spf.comptia.org +all" to the web server.

Answer: A

NEW QUESTION 225

An analyst performs a routine scan of a host using Nmap and receives the following output:

Which of the following should the analyst investigate FIRST?

- A. Port 21
- B. Port 22
- C. Port 23
- D. Port 80

Answer: C

NEW QUESTION 228

A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?

- A. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
- B. Incorporate prioritization levels into the remediation process and address critical findings first.
- C. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
- D. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities found.

Answer: B

NEW QUESTION 231

A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-m-the-middle attack .The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?

- A. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network,
- B. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router.
- C. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network
- D. Conduct a wireless survey to determine if the wireless strength needs to be reduced.

Answer: A

NEW QUESTION 235

Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

- A. Use a UEFI boot password.
- B. Implement a self-encrypted disk.
- C. Configure filesystem encryption
- D. Enable Secure Boot using TPM

Answer: A

NEW QUESTION 240

A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?

- A. Client-side whitelisting
- B. Server-side whitelisting
- C. Server-side blacklisting
- D. Client-side blacklisting

Answer: B

NEW QUESTION 244

A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame. Which of the following is the MOST likely cause of this issue?

- A. A password-spraying attack was performed against the organization.
- B. A DDoS attack was performed against the organization.
- C. This was normal shift work activity; the SIEM's AI is learning.
- D. A credentialed external vulnerability scan was performed.

Answer: A

NEW QUESTION 245

A security analyst implemented a solution that would analyze the attacks that the organization's firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command.

```
S sudo nc -1 -v -c maildemon . py 25 caplog, txt
```

Which of the following solutions did the analyst implement?

- A. Log collector
- B. Crontab mail script
- C. Snikhole
- D. Honeypot

Answer: A

NEW QUESTION 247

An organization has several system that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

- A. Use SSO across all applications
- B. Perform a manual privilege review
- C. Adjust the current monitoring and logging rules
- D. Implement multifactor authentication

Answer: B

NEW QUESTION 249

A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.

To BEST mitigate this risk, the analyst should use.

- A. an 802.11ac wireless bridge to create an air gap.
- B. a managed switch to segment the lab into a separate VLAN.
- C. a firewall to isolate the lab network from all other networks.
- D. an unmanaged switch to segment the environments from one another.

Answer: C

NEW QUESTION 253

.....

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](#)