



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

After receiving reports 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 of compromise on this system.
- B. There are no indicators of compromise on this system.
- C. MySQL services is identified on a standard PostgreSQL port.
- D. Standard HTP is open on the system and should be closed.

Answer: B

NEW QUESTION 3

A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentiality protection. Which of the following is the BEST technical security control to mitigate this risk?

- A. Switch to RADIUS technology
- B. Switch to TACACS+ technology.
- C. Switch to 802.1X technology
- D. Switch to the WPA2 protocol.

Answer: B

NEW QUESTION 4

During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and.

- A. DST 138.10.2.5.
- B. DST 138.10.25.5.
- C. DST 172.10.3.5.
- D. DST 172.10.45.5.
- E. DST 175.35.20.5.

Answer: A

NEW QUESTION 5

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 6

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 7

A security analyst received an email with the following key: Xj3XJ3LLc

A second security analyst received an email with following key: 3XJ3xjcLLC

The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance. This is an example of:

- A. dual control
- B. private key encryption
- C. separation of duties
- D. public key encryption
- E. two-factor authentication

Answer: A

NEW QUESTION 8

A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

- A. Begin blocking all IP addresses within that subnet.
- B. Determine the attack vector and total attack surface.
- C. Begin a kill chain analysis to determine the impact.
- D. Conduct threat research on the IP addresses

Answer: D

NEW QUESTION 9

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 10

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 10

A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running. Sending some sample traffic to the external host, the administrator obtains the following packet capture:

Based on the output, which of the following services should be further tested for vulnerabilities?

- A. SSH
- B. HTTP
- C. SMB
- D. HTTPS

Answer: C

NEW QUESTION 14

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 15

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 17

A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server. Which of the following is the FIRST step the analyst should take?

- A. Create a full disk image of the server's hard drive to look for the file containing the malware.
- B. Run a manual antivirus scan on the machine to look for known malicious software.
- C. Take a memory snapshot of the machine to capture volatile information stored in memory.
- D. Start packet capturing to look for traffic that could be indicative of command and control from the miner.

Answer: D

NEW QUESTION 21

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 24

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 26

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 27

A security team wants to make SaaS solutions accessible from only the corporate campus.

Which of the following would BEST accomplish this goal?

- A. Geofencing
- B. IP restrictions
- C. Reverse proxy
- D. Single sign-on

Answer: A

NEW QUESTION 32

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 37

An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested in a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?

- A. TPM
- B. eFuse
- C. FPGA
- D. HSM
- E. UEFI

Answer: D

NEW QUESTION 42

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 47

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 51

A large software company wants to move its 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 54

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 56

Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:

File access auditing is turned off.

When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.

All processes running appear to be legitimate processes for this user and machine.

Network traffic spikes when the space is cleared on the laptop.

No browser is open.

Which of the following initial actions and tools would provide the BEST approach to determining what is happening?

- A. Delete the temporary files, run an Nmap scan, and utilize Burp Suite.
- B. Disable the network connection, check Sysinternals Process Explorer, and review netstat output.

- C. Perform a hard power down of the laptop, take a dd image, and analyze with FTK.
- D. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

Answer: B

NEW QUESTION 59

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 64

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 68

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 72

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 73

An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more 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 76

A development team is testing a new application release. The team needs to import existing client PHI data records from the production environment to the test environment to test accuracy and functionality.

Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?

- A. Deidentification
- B. Encoding
- C. Encryption
- D. Watermarking

Answer: A

NEW QUESTION 80

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 85

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>kmL4krG2CwwWBan5BRReGv5Djb7syxXTNKcWfUjSjd</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 88

Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue. INSTRUCTIONS
 Click on me ticket to see the ticket details Additional content is available on tabs within the ticket
 First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu
 If at any time you would like to bring back the initial state of the simulation, please click the Reset All button

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 91

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 94

A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO) asking the employee to perform a wife transfer. Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

- A. Implementing a sandboxing solution for viewing emails and attachments
- B. Limiting email from the finance department to recipients on a pre-approved whitelist
- C. Configuring email client settings to display all messages in plaintext when read
- D. Adding a banner to incoming messages that identifies the messages as external

Answer: D

NEW QUESTION 97

Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient. Which of the following controls would have MOST likely prevented this incident?

- A. SSO
- B. DLP
- C. WAF
- D. VDI

Answer: B

NEW QUESTION 102

A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment. Which of the following is the BEST solution?

- A. Virtualize the system and decommission the physical machine.
- B. Remove it from the network and require air gapping.
- C. Only allow access to the system via a jumpbox
- D. Implement MFA on the specific system.

Answer: A

NEW QUESTION 107

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

- A. It automatically performs remedial configuration changes to enterprise security services
- B. It enables standard checklist and vulnerability analysis expressions for automation
- 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 110

A security analyst is responding to an incident on a web server on the company network that is making a large number of outbound requests over DNS Which of the following is the FIRST step the analyst should take to evaluate this potential indicator of compromise'?

- A. Run an anti-malware scan on the system to detect and eradicate the current threat
- B. Start a network capture on the system to look into the DNS requests to validate command and control traffic.
- C. Shut down the system to prevent further degradation of the company network
- D. Reimage the machine to remove the threat completely and get back to a normal running state.
- E. Isolate the system on the network to ensure it cannot access other systems while evaluation is underway.

Answer: A

NEW QUESTION 113

A company's modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

- A. Quarantine the web server
- B. Deploy virtual firewalls
- C. Capture a forensic image of the memory and disk
- D. Enable web server containerization

Answer: B

NEW QUESTION 118

A developer wrote a script to make names and other PII data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?

- A. Data encoding
- B. Data masking
- C. Data loss prevention
- D. Data classification

Answer: C

NEW QUESTION 122

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. Aircrak-ng
- C. Nessus
- D. tcpdump

Answer: A

NEW QUESTION 127

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 130

A security analyst has discovered that developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

- A. Create a security rule that blocks Internet access in the development VPC
- B. Place a jumpbox in between the developers' workstations and the development VPC
- C. Remove the administrator profile from the developer user group in identity and access management
- D. Create an alert that is triggered when a developer installs an application on a server

Answer: A

NEW QUESTION 133

A security analyst has observed several incidents within an organization that are affecting one specific piece of hardware on the network. Further investigation reveals the equipment vendor previously released a patch.

Which of the following is the MOST appropriate threat classification for these incidents?

- A. Known threat
- B. Zero day
- C. Unknown threat
- D. Advanced persistent threat

Answer: B

NEW QUESTION 138

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 139

Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

- A. Code of conduct policy
- B. Account management policy
- C. Password policy
- D. Acceptable use policy

Answer: D

NEW QUESTION 143

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 144

The help desk provided a security analyst with a screenshot of a user's desktop:

For which of the following is aircrack-ng being used?

- A. Wireless access point discovery
- B. Rainbow attack
- C. Brute-force attack
- D. PCAP data collection

Answer: B

NEW QUESTION 149

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 150

A new on-premises application server was recently installed on the network. Remote access to the server was enabled for vendor support on required ports, but recent security reports show large amounts of data are being sent to various unauthorized networks through those ports. Which of the following configuration changes must be implemented to resolve this security issue while still allowing remote vendor access?

- A. Apply a firewall application server rule.
- B. Whitelist the application server.
- C. Sandbox the application server.
- D. Enable port security.
- E. Block the unauthorized networks.

Answer: B

NEW QUESTION 152

An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems.

As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

- A. Copies of prior audits that did not identify the servers as an issue
- B. Project plans relating to the replacement of the servers that were approved by management
- C. Minutes from meetings in which risk assessment activities addressing the servers were discussed
- D. ACLs from perimeter firewalls showing blocked access to the servers
- E. Copies of change orders relating to the vulnerable servers

Answer: C

NEW QUESTION 155

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints. Which of the following should the analyst do FIRST?

- A. Write detection logic.
- B. Establish a hypothesis.
- C. Profile the threat actors and activities.
- D. Perform a process analysis.

Answer: C

NEW QUESTION 156

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 160

When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

- A. `nmap -sA -O <system> -noping`
- B. `nmap -sT -O <system> -P0`
- C. `nmap -sS -O <system> -P0`
- D. `nmap -sQ -O <system> -P0`

Answer: C

NEW QUESTION 163

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 166

An employee in the billing department accidentally sent a spreadsheet containing payment card data to a recipient outside the organization. The employee intended to send the spreadsheet to an internal staff member with a similar name and was unaware of the mistake until the recipient replied to the message. In addition to retraining the employee, which of the following would prevent this from happening in the future?

- A. Implement outgoing filter rules to quarantine messages that contain card data
- B. Configure the outgoing mail filter to allow attachments only to addresses on the whitelist
- C. Remove all external recipients from the employee's address book
- D. Set the outgoing mail filter to strip spreadsheet attachments from all messages.

Answer: B

NEW QUESTION 168

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 171

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 176

A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.

Which of the following is the main concern a security analyst should have with this arrangement?

- A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
- B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
- C. Development phases occurring at multiple sites may produce change management issues.
- D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Answer: B

NEW QUESTION 177

A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-in-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 179

A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system. After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources. Which of the following BEST describes this attack?

- A. Injection attack
- B. Memory corruption
- C. Denial of service
- D. Array attack

Answer: B

NEW QUESTION 184

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.

```
Sudo nc -l -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. Honey pot

Answer: A

NEW QUESTION 189

An organization has several systems 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 190

.....

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 FirstTry
- * CS0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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