CompTIA

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two
compromised devices.
Which of the following should be used to identify the traffic?

A. Carving
B. Disk imaging
C. Packet analysis
D. Memory dump
E. Hashing

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
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 3
- (Exam Topic 1)
An analyst is investigating an anomalous event reported by the SOC. After reviewing the system logs the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?

A. Patching logs
B. Threat feed
C. Backup logs
D. Change requests
E. Data classification matrix

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization $1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised.
Which of the following is the value of this risk?

A. $75.000
B. $300.000
C. $1.425 million
D. $1.5 million

Answer: A

NEW QUESTION 5
- (Exam Topic 1)
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 6
- (Exam Topic 1)
An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply.
Which of the following would BEST identify potential indicators of compromise?

A. Use Burp Suite to capture packets to the SCADA device's IP.
B. Use tcpdump to capture packets from the SCADA device IP.

C. Use Wireshark to capture packets between SCADA devices and the management system.
D. Use Nmap to capture packets from the management system to the SCADA devices.

Answer: C

NEW QUESTION 7
- (Exam Topic 1)
The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently added to the existing ones. The analyst runs the following command on the new server.

Given the output, which of the following should the security analyst check NEXT?

A. The DNS name of the new email server
B. The version of SPF that is being used
C. The IP address of the new email server
D. The DMARC policy

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
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 us
B. Provide PII training to all employees at the compan
C. Encrypt PII information.
D. Enforce encryption on all emails sent within the compan
E. Create a PII program and policy on how to handle dat
F. Train all human resources employees.
G. Train all employee
H. Encrypt data sent on the company networ
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 dat
K. Train company employees on how to handle PII dat
L. Outsource all PII to another compan
M. Send the human resourcesdirector to training for PII handling.

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
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: A

NEW QUESTION 10
- (Exam Topic 1)
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: A

NEW QUESTION 10
- (Exam Topic 1)
The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:
Reduce the number of potential findings by the auditors.
Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
Prevent the external-facing web infrastructure used by other teams from coming into scope.
Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.
Which of the following would be the MOST effective way for the security team to meet these objectives?

A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
B. Segment the servers and systems used by the business unit from the rest of the network.
C. Deploy patches to all servers and workstations across the entire organization.
D. Implement full-disk encryption on the laptops used by employees of the payment-processing team.

Answer: B

NEW QUESTION 11
- (Exam Topic 1)
As part of a review of modern response plans, which of the following is MOST important for an organization lo 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 14
- (Exam Topic 1)
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: D

NEW QUESTION 17
- (Exam Topic 1)
Which of the following attacks can be prevented by using output encoding?

A. Server-side request forgery
B. Cross-site scripting
C. SQL injection
D. Command injection
E. Cross-site request forgery
F. Directory traversal

Answer: B

NEW QUESTION 21
- (Exam Topic 1)
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

A. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
B. Examine the server logs for further indicators of compromise of a web application.
C. Run kill -9 1325 to bring the load average down so the server is usable again.
D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

Answer: B

NEW QUESTION 26
- (Exam Topic 1)
A security analyst has discovered suspicious traffic and determined a host is connecting to a known malicious website. The MOST appropriate action for the analyst to take would be lo implement a change request to:

A. update the antivirus software
B. configure the firewall to block traffic to the domain
C. add the domain to the blacklist
D. create an IPS signature for the domain

Answer: B

NEW QUESTION 27
- (Exam Topic 1)
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 30
- (Exam Topic 1)
A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentially 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 IX technology
D. Switch to the WPA2 protocol.

Answer: D

NEW QUESTION 32
- (Exam Topic 1)
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 35
- (Exam Topic 1)
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. tracert 10.79.95.173

Answer: B

NEW QUESTION 39
- (Exam Topic 1)
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 40
- (Exam Topic 1)
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: A

NEW QUESTION 42
- (Exam Topic 1)
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

Explanation:
Reference: https://www.pearsonitcertification.com/articles/article.aspx?p=2731933&seqNum=3

NEW QUESTION 46
- (Exam Topic 1)
During a cyber incident, which of the following is the BEST course of action?

A. Switch to using a pre-approved, secure, third-party communication system.
B. Keep the entire company informed to ensure transparency and integrity during the incident.
C. Restrict customer communication until the severity of the breach is confirmed.
D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

Answer: D

NEW QUESTION 50
- (Exam Topic 1)
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 54
- (Exam Topic 1)
Which of the following MOST accurately describes an HSM?

A. An HSM is a low-cost solution for encryption.
B. An HSM can be networked based or a removable USB
C. An HSM is slower at encrypting than software
D. An HSM is explicitly used for MFA

Answer: B

NEW QUESTION 56
- (Exam Topic 1)
An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Which of the following should be the focus of the investigation?

A. webserver.org-dmz.org
B. sftp.org-dmz.org
C. 83hht23.org-int.org
D. ftps.bluemed.net

Answer: A

NEW QUESTION 59
- (Exam Topic 1)
A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach.
Which of the following is the BEST mitigation to prevent unauthorized access?

A. Single sign-on
B. Mandatory access control
C. Multifactor authentication
D. Federation
E. Privileged access management

Answer: C

NEW QUESTION 63
- (Exam Topic 1)
A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
B. Accept this risk for now because this is a “high” severity, but testing will require more than the four days available, and the system ATO needs to be competed.
C. Ignore i
D. This is false positive, and the organization needs to focus its efforts on other findings.
E. Ensure HTTP validation is enabled by rebooting the server.

Answer: A

NEW QUESTION 68
- (Exam Topic 1)
An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server.
Which of the following is MOST likely to be a false positive?

A. OpenSSH/OpenSSL Package Random Number Generator Weakness
B. Apache HTTP Server Byte Range DoS
C. GDI+ Remote Code Execution Vulnerability (MS08-052)
D. HTTP TRACE / TRACK Methods Allowed (002-1208)
E. SSL Certificate Expiry

Answer: C

NEW QUESTION 71
- (Exam Topic 1)
A security analyst is reviewing the following web server log:

Which of the following BEST describes the issue?

A. Directory traversal exploit
B. Cross-site scripting
C. SQL injection
D. Cross-site request forgery

Answer: A

NEW QUESTION 74
- (Exam Topic 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 79
- (Exam Topic 1)

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 84
- (Exam Topic 1)
A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet.
Which of the following solutions would meet this requirement?

A. Establish a hosted SSO.
B. Implement a CASB.
C. Virtualize the server.
D. Air gap the server.

Answer: D

NEW QUESTION 87
- (Exam Topic 1)

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. HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
D. HKEY_USERS\<user SID>\Software\Microsoft\Internet Explorer\Typed URLs
E. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub

Answer: E

NEW QUESTION 91
- (Exam Topic 1)
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: D

Explanation:
The DNS debug log provides extremely detailed data about all DNS information that is sent and received by the DNS server, similar to the data that can be gathered using packet capture tools such as network monitor.
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn80066

NEW QUESTION 95
- (Exam Topic 1)
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 99
- (Exam Topic 1)
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 104
- (Exam Topic 1)
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts
.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 109
- (Exam Topic 1)
A security analyst is providing a risk assessment for a medical device that will be installed on the corporate network. During the assessment, the analyst discovers the device has an embedded operating system that will be at the end of its life in two years. Due to the criticality of the device, the security committee makes a risk-based policy decision to review and enforce the vendor upgrade before the end of life is reached.
Which of the following risk actions has the security committee taken?

A. Risk exception
B. Risk avoidance

C. Risk tolerance
D. Risk acceptance

Answer: D

NEW QUESTION 113
- (Exam Topic 1)
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

Explanation:
Reference: https://blog.finjan.com/email-spoofing/

NEW QUESTION 115
- (Exam Topic 1)
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 120
- (Exam Topic 1)
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 123
- (Exam Topic 1)
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 125
- (Exam Topic 1)
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 127
- (Exam Topic 1)
A threat feed notes malicious actors have been infiltrating companies and exfiltration data to a specific set of domains Management at an organization wants to know if it is a victim Which of the following should the security analyst recommend to identity this behavior without alerting any potential malicious actors?

A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested

B. Add the domains to a DNS sinkhole and create an alert m the SIEM toot when the domains are queried
C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443
D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information

Answer: D

NEW QUESTION 129
- (Exam Topic 1)
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 130
- (Exam Topic 1)
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 133
- (Exam Topic 1)
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 136
- (Exam Topic 2)
While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from beinq successful?

A. Implement MFA on the email portal using out-of-band code delivery.
B. Create a new rule in the IDS that triggers an alert on repeated login attempts
C. Leverage password filters to prevent weak passwords on employee accounts from being exploited.
D. Alter the lockout policy to ensure users are permanently locked out after five attempts.
E. Configure a WAF with brute force protection rules in block mode

Answer: A

NEW QUESTION 137
- (Exam Topic 2)
A company's security officer needs to implement geographical IP blocks for nation-state actors from a foreign country On which of the following should the blocks be implemented'?

A. Web content filter
B. Access control list
C. Network access control
D. Data loss prevention

Answer: B

NEW QUESTION 139

- (Exam Topic 2)
Malware is suspected on a server in the environment.
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.
INSTRUCTIONS
Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.
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:
Server 4 192.168.50.6 Windows, svchost.exe

NEW QUESTION 144
- (Exam Topic 2)
A remote code-execution vulnerability was discovered in the RDP for the servers running a key-hosted application. While there is no automated check for this vulnerability from the vulnerability assessment vendor, the in-house technicians were able to evaluate manually whether this vulnerability was present through the use of custom scripts. This evaluation determined that all the hosts are vulnerable. A technician then tested the patch for this vulnerability and found that it can cause stability issues in the key-hosted application. The application is accessed through RDP to a jump host that does not run the application directly. To mitigate this vulnerability, the security operations team needs to provide remediation steps that will mitigate the vulnerability temporarily until the compatibility issues with the patch are resolved. Which of the following will BEST allow systems to continue to operate and mitigate the vulnerability in the short term?

A. Implement IPSec rules on the application servers through a GPO that limits RDP access from only the jump hos
B. Patch the jump hos
C. Since it does not run the application natively, it will not affect the software's operation and functionalit
D. Do not patch the application servers until the compatibility issue is resolved.
E. Implement IPSec rules on the jump host server through a GPO that limits RDP access from only the other application server
F. Do not patch the jump hos
G. Since it does not run the application natively, it is at less risk of being compromise
H. Patch the application servers to secure them.
I. Implement IPSec rules on the application servers through a GPO that limits RDP access to only other application server
J. Do not patch the jump hos
K. Since it does not run the application natively, it is at less risk of being compromise
L. Patch the application servers to secure them.
M. Implement firewall rules on the application servers through a GPO that limits RDP access to only other application server
N. Manually check the jump host to see if it has been compromise
O. Patch the application servers to secure them.

Answer: A

NEW QUESTION 148
- (Exam Topic 2)
The management team assigned the following values to an inadvertent breach of privacy regulations during the original risk assessment:
Probability = 25%
Magnitude = $1,015 per record Total records = 10,000
Two breaches occurred during the fiscal year. The first compromised 35 records, and the second compromised 65 records. Which of the following is the value of the records that were compromised?

A. $10,150
B. $25,375
C. $101,500
D. $2,537,500

Answer: A

NEW QUESTION 151
- (Exam Topic 2)
An organization's network administrator uncovered a rogue device on the network that is emulating the charactenstics of a switch. The device is trunking protocols and inserting tagging va the flow of traffic at the data link layer
Which of the following BEST describes this attack?

A. VLAN hopping
B. Injection attack

C. Spoofing
D. DNS pharming

Answer: A

NEW QUESTION 154
- (Exam Topic 2)
Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?

A. Input validation
B. Output encoding
C. Parameterized queries
D. Tokenization

Answer: D

NEW QUESTION 159
- (Exam Topic 2)
A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?

A. Modify the IDS rules to have a signature for SQL injection.
B. Take the server offline to prevent continued SQL injection attacks.
C. Create a WAF rule In block mode for SQL injection
D. Ask the developers to implement parameterized SQL queries.

Answer: A

NEW QUESTION 161
- (Exam Topic 2)
Which of the following technologies can be used to store digital certificates and is typically used in highsecurity implementations where integrity is paramount?

A. HSM
B. eFuse
C. UEFI
D. Self-encrypting drive

Answer: A

NEW QUESTION 165
- (Exam Topic 2)
A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:

A. proprietary and timely
B. proprietary and accurate
C. relevant and deep
D. relevant and accurate

Answer: D

NEW QUESTION 169
- (Exam Topic 2)
A security analyst receives a CVE bulletin, which lists several products that are used in the enterprise. The analyst immediately deploys a critical security patch. Which of the following BEST describes the reason for the analyst's immediate action?

A. A known exploit was discovered.
B. There is an insider threat.
C. Nation-state hackers are targeting the region.
D. A new zero-day threat needs to be addressed.
E. A new vulnerability was discovered by a vendor.

Answer: E

NEW QUESTION 171
- (Exam Topic 2)
While reviewing a cyber-risk assessment, an analyst notes there are concerns related to FPGA usage. Which of the following statements would BEST convince the analyst's supervisor to use additional controls?

A. FPGAs are vulnerable to malware installation and require additional protections for their codebase.
B. FPGAs are expensive to produc
C. Anti-counterierting safeguards are needed.
D. FPGAs are expensive and can only be programmed onc
E. Code deployment safeguards are needed.
F. FPGAs have an inflexible architectur
G. Additional training for developers is needed

Answer: B

Explanation:
Ethernet switches are mass-produced and offered at discounts on not so widely-used chips with massive economies of scale. While in case of FPGAs,they are used as Ethernet switches and hence cost more since the expense of development and infrastructure are distributed among fewer clients.

NEW QUESTION 172
- (Exam Topic 2)
An organization that uses SPF has been notified emails sent via its authorized third-party partner are getting rejected A security analyst reviews the DNS entry and sees the following:
v=spf1 ip4:180.10.6.5 ip4:180.10.6.10 include:robustmail.com –all
The organization's primary mail server IP is 180.10 6.6, and the secondary mail server IP is 180.10.6.5. The organization's third-party mail provider is "Robust Mail" with the domain name robustmail.com.
Which of the following is the MOST likely reason for the rejected emails?

A. The wrong domain name is in the SPF record.
B. The primary and secondary email server IP addresses are out of sequence.
C. SPF version 1 does not support third-party providers
D. An incorrect IP version is being used.

Answer: A

NEW QUESTION 176
- (Exam Topic 2)
Which of the following should a database administrator implement to BEST protect data from an untrusted server administrator?

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

Answer: A

NEW QUESTION 179
- (Exam Topic 2)
A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur They have asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the BEST way to achieve this goal?

A. Focus on incidents that may require law enforcement support.
B. Focus on common attack vectors first.
C. Focus on incidents that have a high chance of reputation harm.
D. Focus on incidents that affect critical systems.

Answer: D

NEW QUESTION 180
- (Exam Topic 2)
A cybersecurity analyst is investigating a potential incident affecting multiple systems on a company's internal network. Although there is a negligible impact to performance, the following symptom present on each of the affected systems:
- Existence of a new and unexpected svchost exe process
- Persistent, outbound TCP/IP connections to an unknown external host with routine keep-alives transferred
- DNS query logs showing successful name resolution for an Internet-resident dynamic DNS domain If this situation remains unresolved, which of the following will MOST likely occur?

A. The affected hosts may participate in a coordinated DDoS attack upon command
B. An adversary may leverage the affected hosts to reconfigure the company's router ACLs.
C. Key files on the affected hosts may become encrypted and require ransom payment for unlock.
D. The adversary may attempt to perform a man-in-the-middle attack.

Answer: C

NEW QUESTION 182
- (Exam Topic 2)
A custom script currently monitors real-time logs of a SAMIL authentication server to mitigate brute-force attacks. Which of the following is a concern when moving authentication to a cloud service?

A. Logs may contain incorrect information.
B. SAML logging is not supported for cloud-based authentication.
C. Access to logs may be delayed for some time.
D. Log data may be visible to other customers.

Answer: C

Explanation:
Threats & Vulnerabilities Associated with the Cloud, Subsection "Logging and Monitoring"
"Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse."
CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158).

NEW QUESTION 184
- (Exam Topic 2)
A company recently experienced multiple DNS DDoS attacks, and the information security analyst must provide a DDoS solution to deploy in the company's datacenter Which of the following would BEST prevent future attacks?

A. Configure a sinkhole on the router.
B. Buy a UTM to block the number of requests.
C. Route the queries on the DNS server to 127.0.0.1.
D. Call the Internet service provider to block the attack.

Answer: A

NEW QUESTION 189
- (Exam Topic 2)
An employee was found to have performed fraudulent activities. The employee was dismissed, and the employee's laptop was sent to the IT service desk to undergo a data sanitization procedure. However, the security analyst responsible for the investigation wants to avoid data sanitization. Which of the following can the security analyst use to justify the request?

A. Data retention
B. Evidence retention
C. GDPR
D. Data correlation procedure

Answer: A

NEW QUESTION 190
- (Exam Topic 2)
An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal. Which of the following commands will allow the security analyst to confirm the incident?

A. cat log xxd -r -p | egrep ' [0-9] {16}
B. egrep '(3(0-9)) (16) ' log
C. cat log | xxd -r -p egrep '(0-9) (16)'
D. egrep ' (0-9) (16) ' log | xxdc

Answer: C

NEW QUESTION 193
- (Exam Topic 2)
A security analyst is reviewing the following requirements (or new time clocks that will be installed in a shipping warehouse:
• The clocks must be configured so they do not respond to ARP broadcasts.
• The server must be configured with static ARP entries for each clock.
Which of the following types of attacks will this configuration mitigate?

A. Spoofing
B. Overflows
C. Rootkits
D. Sniffing

Answer: A

NEW QUESTION 198
- (Exam Topic 3)
Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)

A. Kitten
B. Panda
C. Tiger
D. Jackal
E. Bear
F. Spider

Answer: CD

NEW QUESTION 202
- (Exam Topic 3)
An analyst is responding 10 an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the held. Maiware was loaded on the device via the installation of a third-party software package The analyst has baselined the device Which of the following should the analyst do to BEST mitigate future attacks?

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

Answer: A

NEW QUESTION 203
- (Exam Topic 3)
A vulnerability assessment solution is hosted in the cloud This solution will be used as an accurate inventory data source for both the configuration management database and the governance nsk and compliance tool An analyst has been asked to automate the data acquisition Which of the following would be the BEST way to acqutre the data'

A. CSV export
B. SOAR
C. API
D. Machine learning

Answer: C

Explanation:
An example of API is google weather app, using the weather channel's API to collect accurate weather data and broadcast it on goggle weather app, so google doesn't have to do it their selves

NEW QUESTION 205
- (Exam Topic 3)
While conoXicting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

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

A. Delete Cloud Dev access key 1
B. Delete BusinessUsr access key 1.
C. Delete access key 1.
D. Delete access key 2.

Answer: D

NEW QUESTION 210
- (Exam Topic 3)
During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

A. strings
B. head
C. fsstat
D. dd

Answer: A

NEW QUESTION 215
- (Exam Topic 3)
A company's application development has been outsourced to a third-party development team. Based on the SLA. The development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

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

Answer: C

Explanation:
Fuzzing or fuzz testing is a dynamic application security testing technique for negative testing. Fuzzing aims to detect known, unknown, and zero-day vulnerabilities
https://brightsec.com/blog/fuzzing/

NEW QUESTION 218
- (Exam Topic 3)
A security analyst is reviewing the following server statistics:

Which of the following Is MOST likely occurring?

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

Answer: C

NEW QUESTION 221
- (Exam Topic 3)
A threat hurting team received a new loC 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

NEW QUESTION 222
- (Exam Topic 3)
A routine vulnerability scan detected a known vulnerability in a critical enterprise web application. Which of the following would be the BEST next step?

A. Submit a change request to have the system patched
B. Evaluate the risk and criticality to determine it further action is necessary
C. Notify a manager of the breach and initiate emergency procedures.
D. Remove the application from production and Inform the users.

Answer: A

NEW QUESTION 225
- (Exam Topic 3)
Which of the following is the software development process by which function, usability, and scenarios are tested against a known set of base requirements?

A. Security regression testing
B. Code review
C. User acceptance testing
D. Stress testing

Answer: C

Explanation:
"User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications." https://www.plutora.com/blog/uat-user-acceptance-testing

NEW QUESTION 226
- (Exam Topic 3)
A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with acKvare. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

A. Blacklist the hash in the next-generation antivirus system.
B. Manually delete the file from each of the workstations.
C. Remove administrative rights from all developer workstations.
D. Block the download of the fie via the web proxy

Answer: A

NEW QUESTION 227
- (Exam Topic 3)
A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?

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

Answer: C

NEW QUESTION 231
- (Exam Topic 3)
A SIEM analyst receives an alert containing the following URL:

Which of the following BEST describes the attack?

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

Answer: D

NEW QUESTION 235
- (Exam Topic 3)
A company wants to configure the environment to allow passive network monitonng. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?

A. Port bridging
B. Tunnel all mode

C. Full-duplex mode
D. Port mirroring
E. Promiscuous mode

Answer: D

NEW QUESTION 239
- (Exam Topic 3)
An email analysis system notifies a security analyst that the following message was quarantined and requires further review.

Which of the following actions should the security analyst take?

A. Release the email for delivery due to its importance.
B. Immediately contact a purchasing agent to expedite.
C. Delete the email and block the sender.
D. Purchase the gift cards and submit an expense report.

Answer: C

NEW QUESTION 242
- (Exam Topic 3)
An organization has a strict policy that if elevated permissions are needed, users should always run commands under their own account, with temporary administrator privileges if necessary. A security analyst is reviewing syslog entries and sees the following:

Which of the following entries should cause the analyst the MOST concern?

A. <100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM ' su vi httpd.conf' failed for joe
B. <100>2 2020-01-10T20:36:36.0010z financeserver su 201 32001 = BOM ' sudo vi users.txt success
C. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi syslog.conf failed for jos
D. <100> 2020-01-10T19:34..002z financeserver su 201 32001 = BOM ' su vi success
E. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi httpd.conf' success

Answer: A

NEW QUESTION 245
- (Exam Topic 3)
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 lo 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.

NEW QUESTION 246
- (Exam Topic 3)
The help desk is having difficulty keeping up with all onboarding and offboarding requests. Managers often submit, requests for new users at the last minute. causing the help desk to scramble to create accounts across many different Interconnected systems. Which of the following solutions would work BEST to assist the help desk with the onboarding and offboarding process while protecting the company's assets?

A. MFA
B. CASB
C. SSO
D. RBAC

Answer: B

NEW QUESTION 251
- (Exam Topic 3)
A security learn implemented a SCM as part for its security-monitoring program there is a requirement to integrate a number of sources Into the SIEM to provide better context relative to the events being processed. Which of the following B€ST describes the result the security learn hopes to accomplish by adding these sources?

A. Data enrichment
B. Continuous integration
C. Machine learning
D. Workflow orchestration

Answer: A

NEW QUESTION 253
- (Exam Topic 3)
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 poor to pushing it to production?

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

Answer: B

NEW QUESTION 255
- (Exam Topic 3)
During a review of SIEM alerts, a securrty analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring toot about files from a newly deployed application that should not change. Which of the following steps should the analyst complete FIRST to respond to the issue7

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

Answer: A

NEW QUESTION 260
- (Exam Topic 3)
A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

A. detection and prevention capabilities to improve.
B. which systems were exploited more frequently.
C. possible evidence that is missing during forensic analysis.
D. which analysts require more training.
E. the time spent by analysts on each of the incidents.

Answer: A

NEW QUESTION 261
- (Exam Topic 3)
A security analyst is investigating a reported phishing attempt that was received by many users throughout the company The text of one of the emails is shown below:

Office 365 User.
It looks like you account has been locked out Please click this <a href=Tittp7/accountfix-office356 com/login php">link</a> and follow the pfompts to restore access
Regards. Security Team
Due to the size of the company and the high storage requirements, the company does not log DNS requests or perform packet captures of network traffic, but rt does log network flow data Which of the following commands will the analyst most likely execute NEXT?

A. telnet office365.com 25
B. tracert 122.167.40.119
C. curl http:// accountfix-office365.com/logi
D. php
E. nslookup accountfix-office365.com

Answer: D

NEW QUESTION 262
- (Exam Topic 3)
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;

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

NEW QUESTION 263
- (Exam Topic 3)
White reviewing incident reports from the previous night, a security analyst notices the corporate websites were defaced with po mcai propaganda. Which of the following BEST Describes this type of actor?

A. Hacktivist

B. Nation-state
C. insider threat
D. Organized crime

Answer: A

NEW QUESTION 266
- (Exam Topic 3)
A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified Which of the following values should the security analyst choose when evaluating the CVSS score?

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

Answer: A

NEW QUESTION 267
- (Exam Topic 3)
Which of the following is the BEST way to gather patch information on a specific server?

A. Event Viewer
B. Custom script
C. SCAP software
D. CI/CD

Answer: C

NEW QUESTION 272
- (Exam Topic 3)
The IT department is concerned about the possibility of a guest device infecting machines on the corporate network or taking down the company's singe internet connection. Which of the following should a security analyst recommend to BEST meet the requirements outlined by the IT Department?

A. Require the guest machines to install the corporate-owned EDR solution.
B. Configure NAC to only allow machines on the network that are patched and have active antivirus.
C. Place a firewall In between the corporate network and the guest network
D. Configure the IPS with rules that will detect common malware signatures traveling from the guest network.

Answer: B

NEW QUESTION 275
- (Exam Topic 3)
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

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

Answer: B

NEW QUESTION 278
- (Exam Topic 3)
A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:

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

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

Answer: BD

NEW QUESTION 283
- (Exam Topic 3)
Which of the following are the MOST likely reasons lo include reporting processes when updating an incident response plan after a breach? (Select TWO).

A. To establish a clear chain of command
B. To meet regulatory requirements for timely reporting

C. To limit reputation damage caused by the breach
D. To remediate vulnerabilities that led to the breach
E. To isolate potential insider threats
F. To provide secure network design changes

Answer: BF

NEW QUESTION 288
- (Exam Topic 3)
A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network Customers are not authorized to alter the configuration The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation Which of the following processes is the company using to ensure the appliance is not altered from its ongmal configured state?

A. CI/CD
B. Software assurance
C. Anti-tamper
D. Change management

Answer: D

Explanation:
change management - process through which changes to the configuration of information systems are monitored and controlled. Each individual component should have a separate document or database record that describes its initial state and subsequent changes

NEW QUESTION 293
......

Relate Links

100% Pass Your CS0-003 Exam with Exambible Prep Materials

https://www.exambible.com/CS0-003-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/