CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A development team is preparing to roll out a beta version of a web application and wants to quickly test for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. Which of the following tools would the security team most likely recommend to perform this test?

A. Has heat

B. OpenVAS

C. OWASP ZAP

D. Nmap

Correct Answer: C

OWASP ZAP (Zed Attack Proxy) is a tool recommended for quickly testing web applications for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. It is an open-source web application security scanner that helps identify security issues in web applications during the development and testing phases.

QUESTION 2

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

Correct Answer: A

QUESTION 3

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.

Correct Answer: D

QUESTION 4

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. Weaporization

Correct Answer: B

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

QUESTION 5

A security analyst is reviewing existing email protection mechanisms to generate a report. The analysis finds the following DNS records:

Record 1

v=spf1 ip4:192:168.0.0/16 include:_spf.marketing.com include: thirdpartyprovider.com ~all

Record 2

"v=DKIM1\ k=rsa\;
p=MIGfMA0GCSqh7d8hyh78Gdg87gd98hag86ga98dhay8gd7ashdca7yg79auhudig7df9ah8g76ag98dhay87ga9"

Record 3

_dmarc.comptia.com TXT v=DMARC1\; p=reject\; pct=100; rua=mailto:dmarc-reports@comptia.com

Which of the following options provides accurate information to be included in the report?

A. Record 3 serves as a reference of the security features configured at Record 1 and 2.

B. Record 1 is used as a blocklist mechanism to filter unauthorized senders.

C. Record 2 is used as a key to encrypt all outbound messages sent.

D. The three records contain private information that should not be disclosed.

Correct Answer: A

The DMARC record is what tells us to do with messages that don\\'t properly align to SPF / DKIM.

WRONG ANSWERS

?B ?this SPF record, as configured, is a softfail. That means it functions as less of a blocklist and more as a quarantine list.

?C ?the DKIM key is used to sign, not encrypt, outbound messages.

?D ?all 3 records must be in public DNS or e-mail servers outside the organization would be unable to reference them and use them.

QUESTION 6

An incident response analyst is taking over an investigation from another analyst. The investigation has been going on for the past few days. Which of the following steps is most important during the transition between the two analysts?

A. Identify and discuss the lessons learned with the prior analyst.

B. Accept all findings and continue to investigate the next item target.

C. Review the steps that the previous analyst followed.

D. Validate the root cause from the prior analyst.

Correct Answer: C

QUESTION 7

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

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

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

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

A. An output of characters > and " as the parameters used m the attempt

B. The vulnerable parameter ID hccp://l72.31.15.2.php?id-2 and unfiltered characters returned

C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe

D. The vulnerable parameter and characters > and " with a reflected XSS attempt

Correct Answer: D

A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back t" case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL http:/.31.15.2.php?id=2.

QUESTION 8

Which of the following describes the difference between intentional and unintentional insider threats\\'?

A. Their access levels will be different

B. The risk factor will be the same

C. Their behavior will be different

D. The rate of occurrence will be the same

Correct Answer: C

The difference between intentional and unintentional insider threats is their behavior. Intentional insider threats are malicious actors who deliberately misuse their access to harm the organization or its assets. Unintentional insider threats are

careless or negligent users who accidentally compromise the security of the organization or its assets. Their access levels, risk factors, and rates of occurrence may vary depending on various factors, but their behavior is the main distinction.

Reference:

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 12;

https://www.cisa.gov/sites/default/files/publications/Insider_Threat_Mitigation_Guide_508.pdf

QUESTION 9

An employee downloads a freeware program to change the desktop to the classic look of legacy Windows. Shortly after the employee installs the program, a high volume of random DNS queries begin to originate from the system. An investigation on the system reveals the following:

Add-MpPreference -ExclusionPath \\'%Program Filest\ksysconfig\\'

Which of the following is possibly occurring?

A. Persistence

B. Privilege escalation

C. Credential harvesting

D. Defense evasion

Correct Answer: D

Defense evasion is the technique of avoiding detection or prevention by security tools or mechanisms. In this case, the freeware program is likely a malware that generates random DNS queries to communicate with a command and control server or exfiltrate data. The command Add-MpPreference -ExclusionPath \\'%Program Filest\ksysconfig\\' is used to add an exclusion path to Windows Defender, which is a built-in antivirus software, to prevent it from scanning the malware folder. References: CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 5, page 204; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 212. pr

QUESTION 10

A security analyst who works in the SOC receives a new requirement to monitor for indicators of compromise. Which of the following is the first action the analyst should take in this situation?

A. Develop a dashboard to track the indicators of compromise.

B. Develop a query to search for the indicators of compromise.

C. Develop a new signature to alert on the indicators of compromise.

D. Develop a new signature to block the indicators of compromise.

Correct Answer: B

Developing a query to search for the indicators of compromise is the first action the analyst should take in this situation. Indicators of compromise (IOCs) are pieces of information that suggest a system or network has been compromised by

an attacker. IOCs can include IP addresses, domain names, file hashes, URLs, or other artifacts that are associated with malicious activity. Developing a query to search for IOCs can help to identify any potential incidents or threats in the

environment and initiate further investigation or response .

https://www.crowdstrike.com/cybersecurity-101/incident-response/indicators-ofcompromise/

QUESTION 11

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

Correct Answer: A

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 and 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]

QUESTION 12

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

Correct Answer: A

MITRE ATTandCK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATTandCK 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 ATTandCK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities

QUESTION 13

A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device\\'s operating system. Which of the following best meets this requirement?

A. SIEM

B. CASB

C. SOAR

D. EDR

Correct Answer: D

EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device\\'s operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objective

https://www.comptia.org/certifications/cybersecurity-analyst https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered https://resources.infosecinstitute.com/certification/cysa-plus-ia-levels/

QUESTION 14

A development team recently released a new version of a public-facing website for testing prior to production. The development team is soliciting the help of various teams to validate the functionality of the website due to its high visibility. Which of the following activities best describes the process the development team is initiating?

A. Static analysis

B. Stress testing

C. Code review

D. User acceptance testing

Correct Answer: D

User acceptance testing is a process of verifying that a software application meets the requirements and expectations of the end users before it is released to production. User acceptance testing can help to validate the functionality, usability, performance and compatibility of the software application with real-world scenarios and feedback . User acceptance testing can involve various teams, such as developers, testers, customers and stakeholders. https://www.techopedia.com/ definition7/user-acceptance-testing-uat

QUESTION 15

During an incident in which a user machine was compromised, an analyst recovered a binary file that potentially caused the exploitation. Which of the following techniques could be used for further analysis?

A. Fuzzing

B. Static analysis

C. Sandboxing

D. Packet capture

Correct Answer: B