Vendor: CompTIA

Exam Code:CS0-003

Exam Name: CompTIA Cybersecurity Analyst (CySA+)

Version: Demo

QUESTION 1

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

A. Develop a call tree to inform impacted users

B. Schedule a review with all teams to discuss what occurred

C. Create an executive summary to update company leadership

D. Review regulatory compliance with public relations for official notification

Correct Answer: B

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

QUESTION 2

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.

Correct Answer: A

QUESTION 3

A security team conducts a lessons-learned meeting after struggling to determine who should conduct the next steps following a security event. Which of the following should the team create to address this issue?

A. Service-level agreement

B. Change management plan

C. Incident response plan

D. Memorandum of understanding

Correct Answer: C

An incident response plan outlines the procedures, roles, and responsibilities for responding to security incidents within an organization. It provides clear guidance on how to handle different types of incidents, including who is responsible for

what actions during and after an incident.

QUESTION 4

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

A. Uncredentialed scan

B. Discovery scan

C. Vulnerability scan

D. Credentialed scan

Correct Answer: B

A discovery scan is typically used to identify the scope of a web application and understand where the scan will go. This type of scan is often the first step in assessing a web application\\'s security and helps the analyst determine which areas

should be further examined or tested in-depth.

Reference: https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/scans/scanning_basics.htm

---

QUESTION 5

A security analyst is reviewing the following log entries to identify anomalous activity:

```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/..%5c../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

A. Directory traversal

B. SQL injection

C. Buffer overflow

D. Cross-site scripting

Correct Answer: A

A directory traversal attack is a type of web application attack that exploits insufficient input validation or improper configuration to access files or directories that are outside the intended scope of the web server. The log entries given in the question show s" sequences in the URL, which indicate an attempt to move up one level in the directory structure. For "" tries to access the /etc/passwd file, which contains user account information on Linux systems. If successful, this attack could allow an attacker to read, modify, or execute files on the web server that are not meant to be accessible.

QUESTION 6

A security analyst is evaluating the following support ticket:

Issue: Marketing campaigns are being filtered by the customer\\'s email servers.

Description: Our marketing partner cannot send emails using our email address. The following log messages were collected from multiple customers:

1.

The SPF result is PermError.

2.

The SPF result is SoftFail or Fail.

3.

The 550 SPF check failed.

Which of the following should the analyst do next?

A. Ask the marketing partner\\'s ISP to disable the DKIM setting.

B. Request approval to disable DMARC on the company\\'s ISP.

C. Ask the customers to disable SPF validation.

D. Request a configuration change on the company\\'s public DNS.

Correct Answer: D

QUESTION 7

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

A. Deploy a CASB and enable policy enforcement

B. Configure MFA with strict access

C. Deploy an API gateway

D. Enable SSO to the cloud applications

Correct Answer: A

A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

QUESTION 8

Which of the following tools would work best to prevent the exposure of PII outside of an organization?

A. PAM

B. IDS

C. PKI

D. DLP

Correct Answer: D

Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

QUESTION 9

During the log analysis phase, the following suspicious command is detected

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

Which of the following is being attempted?

A. Buffer overflow

B. RCE

C. ICMP tunneling

D. Smurf attack

Correct Answer: B

RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory

locations and corrupting the program\\'s execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified References: What Is Buffer Overflow? Attacks, Types and Vulnerabilities - Fortinet1, What Is a Smurf Attack? Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of …3

QUESTION 10

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

A. To satisfy regulatory requirements for incident reporting

B. To hold other departments accountable

C. To identify areas of improvement in the incident response process

D. To highlight the notable practices of the organization\\'s incident response team

Correct Answer: C

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

QUESTION 11

A web application team notifies a SOC analyst that there are thousands of HTTP/404 events on the public-facing web server. Which of the following is the next step for the analyst to take?

A. Instruct the firewall engineer that a rule needs to be added to block this external server

B. Escalate the event to an incident and notify the SOC manager of the activity

C. Notify the incident response team that there is a DDoS attack occurring

D. Identify the IP/hostname for the requests and look at the related activity

Correct Answer: D

Identifying the IP/hostname for the requests and looking at the related activity is the first step in understanding the nature of the issue. This step is crucial for making informed decisions about how to respond to the situation. Once the analyst has gathered more information, they can then decide whether further escalation or actions are necessary, such as alerting the incident response team or notifying higher management.

QUESTION 12

Given the output below:

#nmap 7.70 scan initiated Tues, Feb 8 12:34:56 2022 as: nmap -v -Pn -p 80,8000,443 --script http-* -oA server.out 192.168.220.42

Which of the following is being performed?

A. Cross-site scripting

B. Local file inclusion attack

C. Log4] check

D. Web server enumeration

Correct Answer: D

Web server enumeration is the process of identifying information about a web server, such as its software version, operating system, configuration, services, and vulnerabilities. This can be done using tools like Nmap, which can scan ports and run scripts to gather information. In this question, the Nmap command is using the -p option to scan ports 80, 8000, and 443, which are commonly used for web services. It is also using the --script option to run scripts that start with http-*, which are related to web server enumeration. The output file name server.out also suggests that the purpose of the scan is to enumerate web servers. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://partners.comptia.org/docs/defaultsource/ resources/comptia-cysa-cs0-002-exam-objectives