Vendor: CompTIA

Exam Code:CS0-001

Exam Name: CompTIA Cybersecurity Analyst

Version: Demo

QUESTION 1

An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

A. Log review

B. Service discovery

C. Packet capture

D. DNS harvesting

Correct Answer: C

QUESTION 2

A security analyst notices PII has been copied from the customer database to an anonymous FTP server in the DMZ. Firewall logs indicate the customer database has not been accessed from anonymous FTP server. Which of the following departments should make a decision about pursuing further investigation? (Choose two.)

A. Human resources

B. Public relations

C. Legal

D. Executive management

E. IT management

Correct Answer: D

QUESTION 3

Company A suspects an employee has been exfiltrating PII via a USB thumb drive. An analyst is tasked with attempting to locate the information on the drive. The PII in question includes the following:

comp@mail.com	564-23-4765
tia@mail.com	754-09-3276
puter@mail.com	143-32-2323
sam@mail.com	545-11-0192
jim@mail.com	093-45-3748

Which of the following would BEST accomplish the task assigned to the analyst?

A. 3 [0-9]\d-2[0-9]\d-4[0-9]\d

B. \d(3)-d(2)-\d(4)

C. ?[3]-?[2]-?[3]

D. \d[9] `XXX-XX-XX\\'

Correct Answer: B

QUESTION 4

A security analyst wants to confirm a finding from a penetration test report on the internal web server. To do so, the analyst logs into the web server using SSH to send the request locally. The report provides a link to https://hrserver.internal/../

../etc/passwd, and the server IP address is 10.10.10.15.

However, after several attempts, the analyst cannot get the file, despite attempting to get it using different ways, as shown below.

Request	Response
https://hrserver.internal/../../etc/passwd	Host not found
https://localhost/../../etc/passwd	File not found
https://10.10.10.15/../../etc/passwd	File not found

Which of the following would explain this problem? (Choose two.)

A. The web server uses SNI to check for a domain name

B. Requests can only be sent remotely to the web server

C. The password file is write protected

D. The web service has not started

Correct Answer: A

QUESTION 5

A cybersecurity analyst was hired to resolve a security issue within a company after it was reported that many employee account passwords had been compromised. Upon investigating the incident, the cybersecurity analyst found that a brute

force attack was launched against the company.

Which of the following remediation actions should the cybersecurity analyst recommend to senior management to address these security issues?

A. Prohibit password reuse using a GPO.

B. Deploy multifactor authentication.

C. Require security awareness training.

D. Implement DLP solution.

Correct Answer: B

QUESTION 6

After reading about data breaches at a competing company, senior leaders in an organization have grown increasingly concerned about social engineering attacks. They want to increase awareness among staff regarding this threat, but do not want to use traditional training methods because they regard these methods as ineffective. Which of the following approaches would BEST meet the requirements?

A. Classroom training on the dangers of social media followed by a test and gift certificates for any employee getting a perfect score.

B. Simulated phishing emails asking employees to reply to the email with their updated phone number and office location

C. A poster contest to raise awareness of PII and asking employees to provide examples of data breaches and consequences

D. USB drives randomly placed inside and outside the organization that contain a pop-up warning to any users who plug the drive into their computer

Correct Answer: A

QUESTION 7

A security analyst\\'s daily review of system logs and SIEM showed fluctuating patterns of latency. During the analysis, the analyst discovered recent attempts of intrusion related to malware that overwrites the MBR. The facilities manager informed the analyst that a nearby construction project damaged the primary power lines, impacting the analyst\\'s support systems. The electric company has temporarily restored power, but the area may experience temporary outages.

Which of the following issues the analyst focus on to continue operations?

A. Updating the ACL

B. Conducting backups

C. Virus scanning

D. Additional log analysis

Correct Answer: C

QUESTION 8

A software development company in the manufacturing sector has just completed the alpha version of its flagship application. The application has been under development for the past three years. The SOC has seen intrusion attempts

made by indicators associated with a particular APT. The company has a hot site location for COOP. Which of the following threats would most likely incur the BIGGEST economic impact for the company?

A. DDoS

B. ICS destruction

C. IP theft

D. IPS evasion

Correct Answer: A

QUESTION 9

An application development company released a new version of its software to the public. A few days after the release, the company is notified by end users that the application is notably slower, and older security bugs have reappeared in the new release. The development team has decided to include the security analyst during their next development cycle to help address the reported issues. Which of the following should the security analyst focus on to remedy the existing reported problems?

A. The security analyst should perform security regression testing during each application development cycle.

B. The security analyst should perform end user acceptance security testing during each application development cycle.

C. The security analyst should perform secure coding practices during each application development cycle.

D. The security analyst should perform application fuzzing to locate application vulnerabilities during each application development cycle.

Correct Answer: A

QUESTION 10

While conducting research on malicious domains, a threat intelligence analyst received a blue screen of death. The analyst rebooted and received a message stating that the computer had been locked and could only be opened by following the instructions on the screen. Which of the following combinations describes the MOST likely threat and the PRIMARY mitigation for the threat?

A. Ransomware and update antivirus

B. Account takeover and data backups

C. Ransomware and full disk encryption

D. Ransomware and data backups

Correct Answer: D

QUESTION 11

A security analyst received an email with the following key:

Xj3XJ3LLc

A second security analyst received an email with following key:

3XJ3xjcLLC

The security manager has informed the two analysts that the email they received is a key that allows access to the company\\'s financial segment for maintenance. This is an example of:

A. dual control

B. private key encryption

C. separation of duties

D. public key encryption

E. two-factor authentication

Correct Answer: A

QUESTION 12

Which of the following should be found within an organization\\'s acceptable use policy?

A. Passwords must be eight characters in length and contain at least one special character.

B. Customer data must be handled properly, stored on company servers, and encrypted when possible

C. Administrator accounts must be audited monthly, and inactive accounts should be removed.

D. Consequences of violating the policy could include discipline up to and including termination.

Correct Answer: D

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: