CAS-004$^{\text{Q\&As}}$

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cas-004.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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

An employee\\'s device was missing for 96 hours before being reported. The employee called the help desk to ask for another device. Which of the following phases of the incident response cycle needs improvement?

A. Containment

B. Preparation

C. Resolution

D. Investigation

Correct Answer: B

QUESTION 2

An investigator is attempting to determine if recent data breaches may be due to issues with a company\\'s web server that offers news subscription services. The investigator has gathered the following data:

1.

Clients successfully establish TLS connections to web services provided by the server.

2.

After establishing the connections, most client connections are renegotiated.

3.

The renegotiated sessions use cipher suite TLS_RSA_WITH_NULL_SHA.

Which of the following is the MOST likely root cause?

A. The clients disallow the use of modem cipher suites.

B. The web server is misconfigured to support HTTP/1.1

C. A ransomware payload dropper has been installed.

D. An entity is performing downgrade attacks on path.

Correct Answer: D

QUESTION 3

A SaaS startup is maturing its DevSecOps program and wants to identify weaknesses earlier in the development process in order to reduce the average time to identify serverless application vulnerabilities and the costs associated with remediation. The startup began its early security testing efforts with DAST to cover public-facing application components and recently implemented a bug bounty program. Which of the following will BEST accomplish the company\\'s objectives?

A. RASP

B. SAST

C. WAF

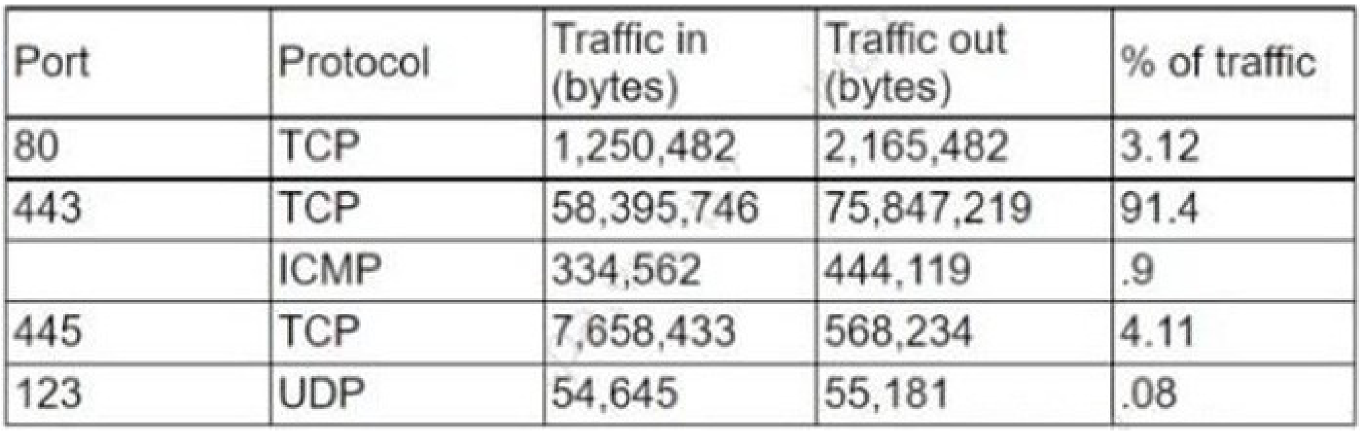
D. CMS

Correct Answer: B

to identify bug at the early stage of the SDLC

QUESTION 4

A firewall administrator needs to ensure all traffic across the company network is inspected. The administrator gathers data and finds the following information regarding the typical traffic in the network:



Port	Protocol	Traffic in (bytes)	Traffic out (bytes)	% of traffic
80	TCP	1,250,482	2,165,482	3.12
443	TCP	58,395,746	75,847,219	91.4
	ICMP	334,562	444,119	.9
445	TCP	7,658,433	568,234	4.11
123	UDP	54,645	55,181	.08

Which of the following is the BEST solution to ensure the administrator can complete the assigned task?

A. A full-tunnel VPN

B. Web content filtering

C. An endpoint DLP solution

D. SSL/TLS decryption

Correct Answer: D

QUESTION 5

An analyst is evaluating the security of a web application that does not hold sensitive or financial data. The application requires users to have a minimum password length of 12 characters. One of the characters must be capitalized, and one must be a number. To reset the password, the user is asked to provide the birthplace, birthdate, and mother\\'s maiden name. When all of these are entered correctly, a new password is emailed to the user. Which of the following should concern the analyst the MOST?

A. The security answers may be determined via online reconnaissance.

B. The password is too long, which may encourage users to write the password down.

C. The password should include a special character.

D. The minimum password length is too short.

Correct Answer: A

CAS-004 Study Guide CAS-004 Exam Questions CAS-004 Braindumps