CS0-002$^{Q\&As}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

QUESTION 1

A security analyst has determined that the user interface on an embedded device is vulnerable to common SQL injections. The device is unable to be replaced, and the software cannot be upgraded. Which of the following should the security analyst recommend to add additional security to this device?

A. The security analyst should recommend this device be placed behind a WAF.

B. The security analyst should recommend an IDS be placed on the network segment.

C. The security analyst should recommend this device regularly export the web logs to a SIEM system.

D. The security analyst should recommend this device be included in regular vulnerability scans.

Correct Answer: A

QUESTION 2

Which of the following best practices is used to identify areas in the network that may be vulnerable to penetration testing from known external sources?

A. Blue team training exercises

B. Technical control reviews

C. White team training exercises

D. Operational control reviews

Correct Answer: A

QUESTION 3

A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?

A. Modify the IDS rules to have a signature for SQL injection.

B. Take the server offline to prevent continued SQL injection attacks.

C. Create a WAF rule In block mode for SQL injection

D. Ask the developers to implement parameterized SQL queries.

Correct Answer: A

QUESTION 4

A cybersecurity analyst has several log files to review. Instead of using grep and cat commands, the analyst decides to find a better approach to analyze the logs. Given a list of tools, which of the following would provide a more efficient way for the analyst to conduct a timeline analysis, do keyword searches, and output a report?

A. Kali

B. Splunk

C. Syslog

D. OSSIM

Correct Answer: B

QUESTION 5

SIMULATION

Part2: AppServ1

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:

1.

TLS 1.2 is the only version of TLS running.

2.

Apache 2.4.18 or greater should be used.

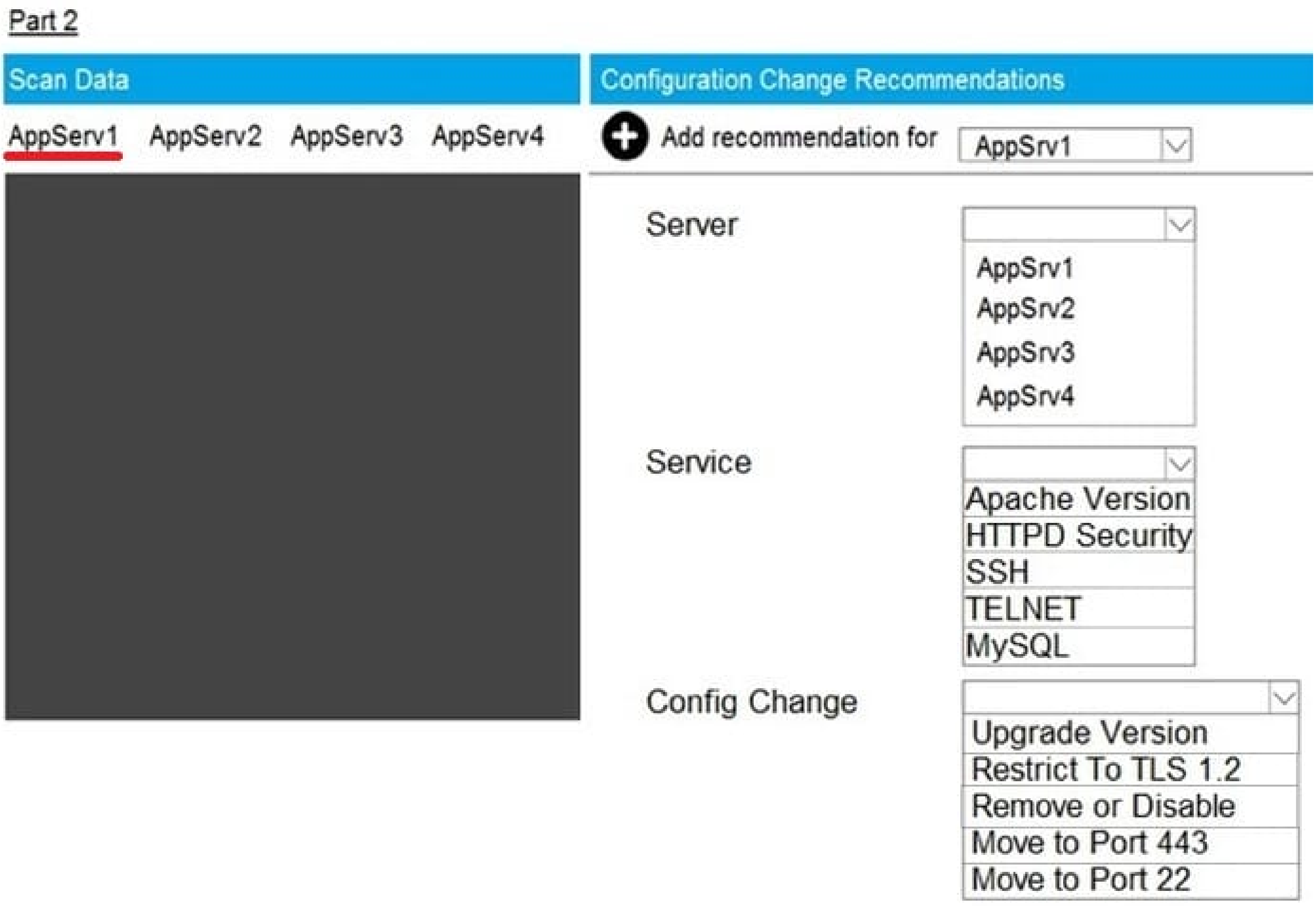
3.

Only default ports should be used.

INSTRUCTIONS

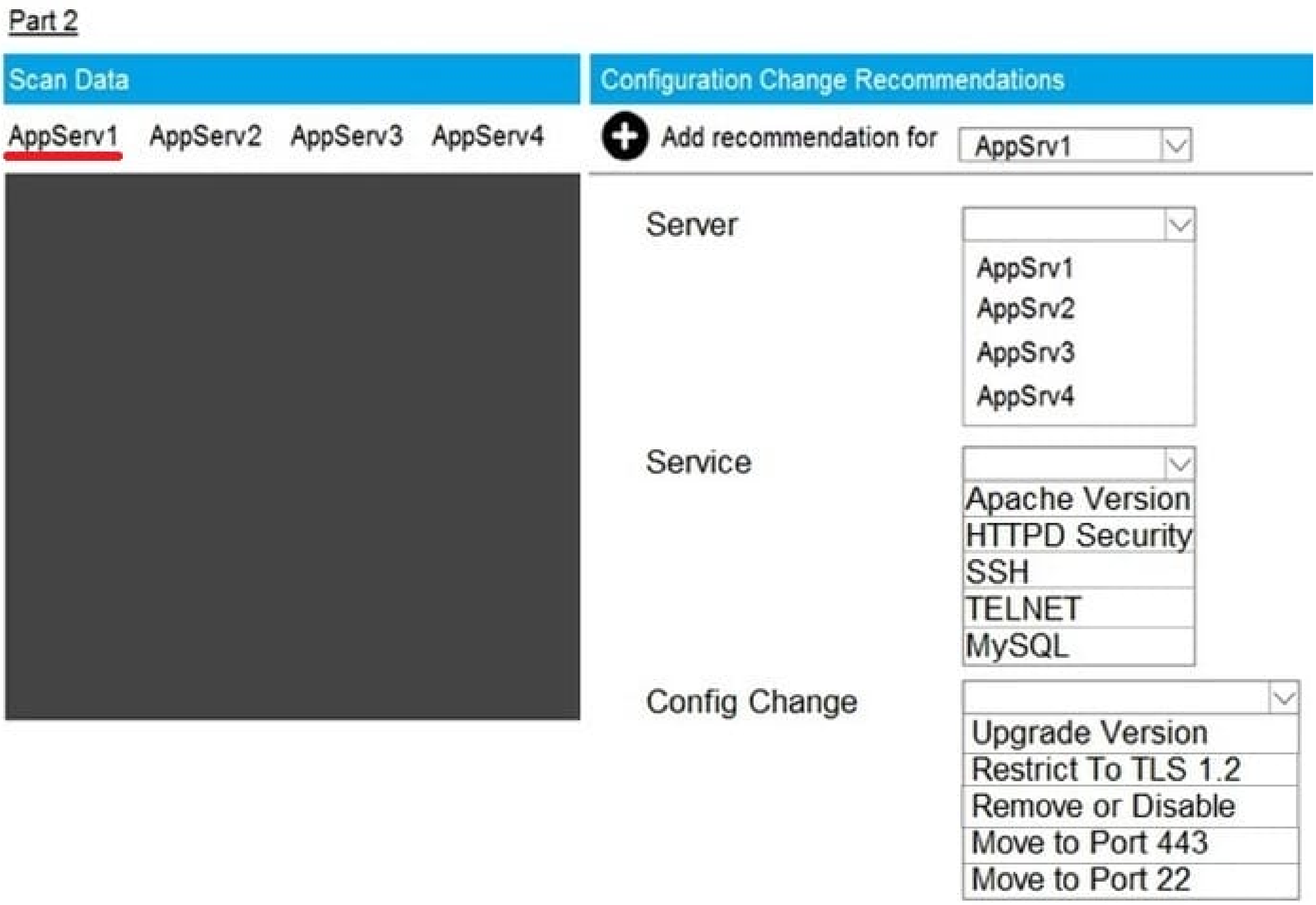
Using the supplied data, record the status of compliance with the company\\'s guidelines for each server. The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

Hot Area:



Part 2

Correct Answer:



AppServ1 - Nothing to do here

[CS0-002 PDF Dumps] [CS0-002 Practice Test] [CS0-002 Exam Questions]