DUMPSBOSS.

CompTIA CyberSecurity Analyst CySA+ Certification Exam

CompTIA CS0-003

Version Demo

Total Demo Questions: 10

Total Premium Questions: 149

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud:

Cobain: Yes
Grohl: No Novo: Yes Smear: Yes Channing: No

B. TSpirit:

Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No

C. ENameless: Cobain: Yes Grohl: No Novo: Yes Smear: No Channing: No

D. PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

ANSWER: B

Explanation:

The vulnerability that should be patched first, given the above third-party scoring system, is: TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No

This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

QUESTION NO: 2

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

A. SLA

B. LOI

C. MOU

D. KPI

ANSWER: A

Explanation:

SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its

key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

QUESTION NO: 3

An analyst is reviewing a vulnerability report for a server environment with the following entries:

Which of the following systems should be prioritized for patching first?

A. 10.101.27.98

B. 54.73.225.17

C. 54.74.110.26

D. 54.74.110.228

ANSWER: D

Explanation:

The system that should be prioritized for patching first is 54.74.110.228, as it has the highest number and severity of vulnerabilities among the four systems listed in the vulnerability report. According to the report, this system has 12 vulnerabilities, with 8 critical, 3 high, and 1 medium severity ratings. The critical vulnerabilities include CVE-2019-0708 (BlueKeep), CVE-2019-1182 (DejaBlue), CVE-2017-0144

(EternalBlue), and CVE-2017-0145 (EternalRomance), which are all remote code execution vulnerabilities that can allow an attacker to compromise the system without any user interaction or authentication. These vulnerabilities pose a high risk to the system and should be patched as soon as possible.

QUESTION NO: 4

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country.

Which of the following best describes what is happening? (Choose two.)

A. Beaconinq

B. Domain Name System hijacking

C. Social engineering attack

D. On-path attack

E. Obfuscated links

F. Address Resolution Protocol poisoning

ANSWER: C E

Explanation:

A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, an incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

QUESTION NO: 5

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

ANSWER: D

Explanation:

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 NO: 6

An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Select two).

A. Drop the tables on the database server to prevent data exfiltration.

B. Deploy EDR on the web server and the database server to reduce the adversaries capabilities.

C. Stop the httpd service on the web server so that the adversary can not use web exploits

D. use micro segmentation to restrict connectivity to/from the web and database servers.

E. Comment out the HTTP account in the / etc/passwd file of the web server

F. Move the database from the database server to the web server.

ANSWER: B D

Explanation:

Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them. Official

References:

https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.comptia.org/certifications/cybersecurity-analyst

https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

QUESTION NO: 7

Which of the following items should be included in a vulnerability scan report? (Choose two.)

A. Lessons learned

B. Service-level agreement

C. Playbook

D. Affected hosts

E. Risk score

F. Education plan

ANSWER: D E

Explanation:

A vulnerability scan report should include information about the affected hosts, such as their IP addresses, hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official

References:

https://www.first.org/cvss/

QUESTION NO: 8

A security audit for unsecured network services was conducted, and the following output was generated:

Which of the following services should the security team investigate further? (Select two).

A. 21

B. 22

C. 23

D. 636

E. 1723

F. 3389

ANSWER: C D

Explanation:

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices1

The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.

Among the six ports listed, two are particularly risky and should be investigated further by the security team:

port 23 and port 636.

Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host23

Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections.

Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 6362

QUESTION NO: 9

A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to https://offce365password.acme.co. The site's standard VPN logon page is

www.acme.com/logon. Which of the following is most likely true?

A. This is a normal password change URL.

B. The security operations center is performing a routine password audit.

C. A new VPN gateway has been deployed

D. A social engineering attack is underway

ANSWER: D

Explanation:

A social engineering attack is underway is the most likely explanation for the outbound traffic to a host IP that resolves to https://offce365password.acme.co, while the site's standard VPN logon page is www.acme.com/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (offce365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. Official

References:

https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.comptia.org/certifications/cybersecurity-analyst

https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

QUESTION NO: 10 - (SIMULATION)

You are a cybersecurity analyst tasked with interpreting scan data from Company As 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

• TLS 1 2 is the only version of TLS running.

• Apache 2.4.18 or greater should be used.

• 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.

Part 1: AppServ1:

AppServ1 AppServ2 AppServ3 AppServ4

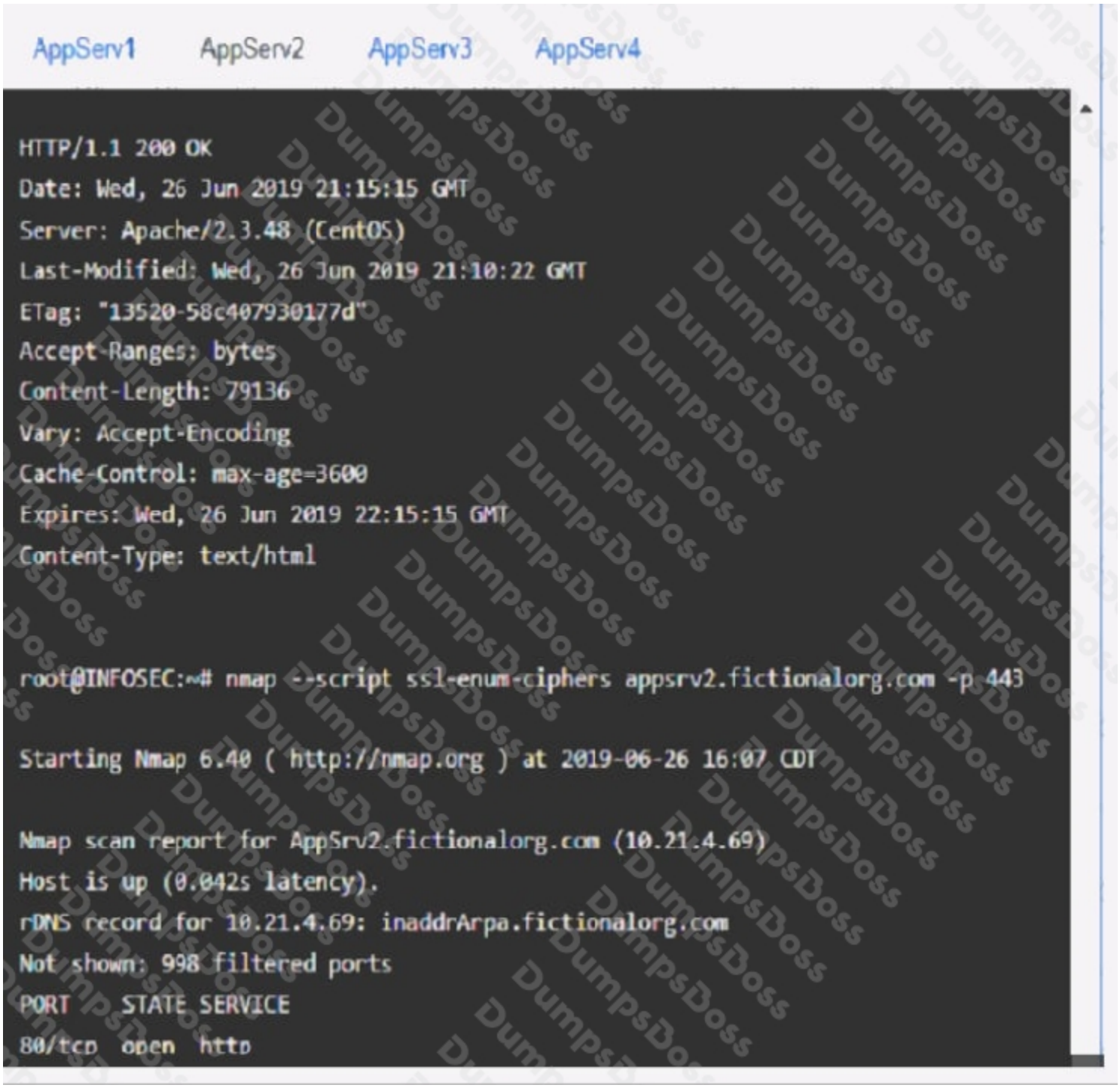
```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
```


```
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
```

```
Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
```

```
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
```

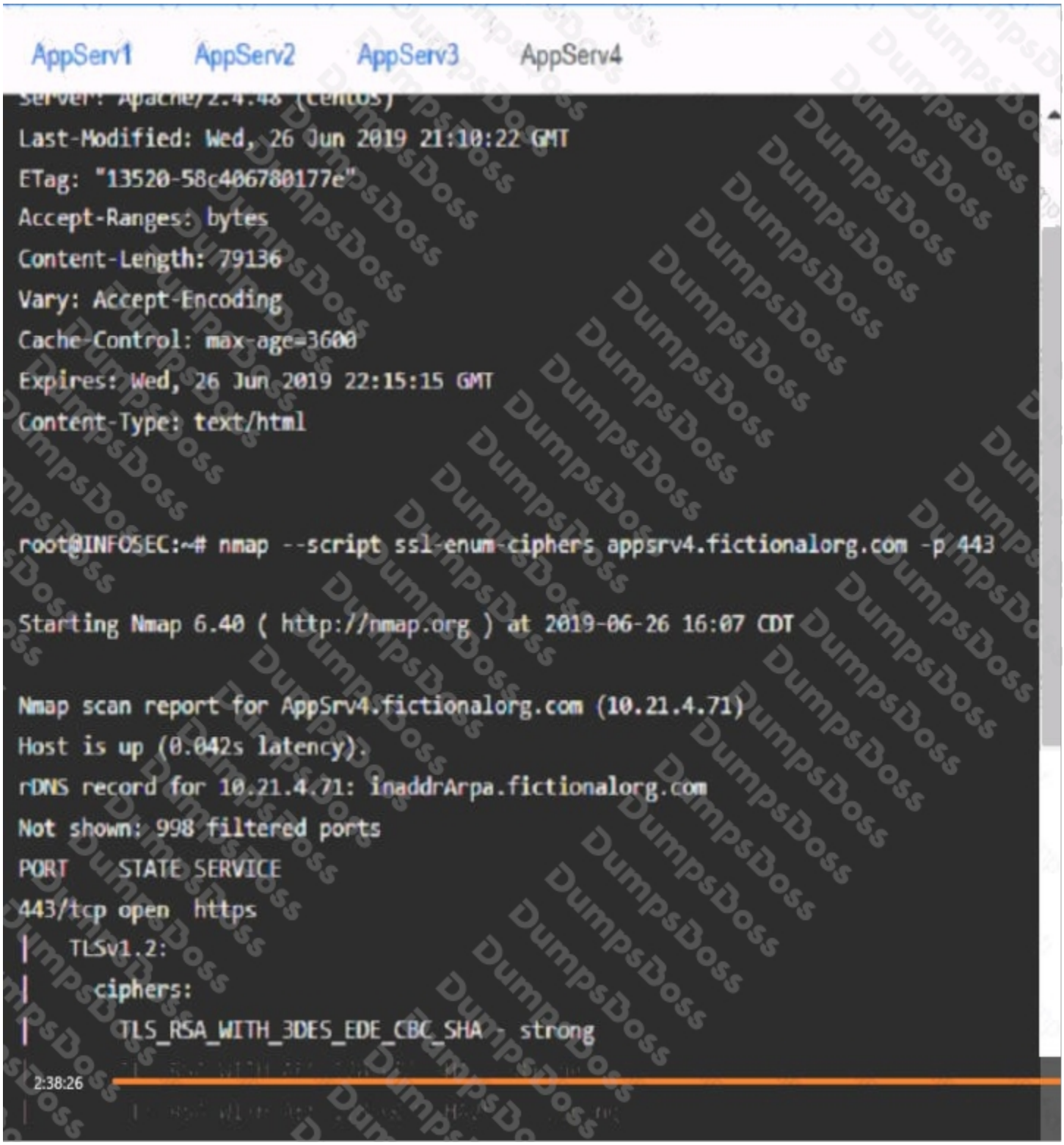
AppServ2:

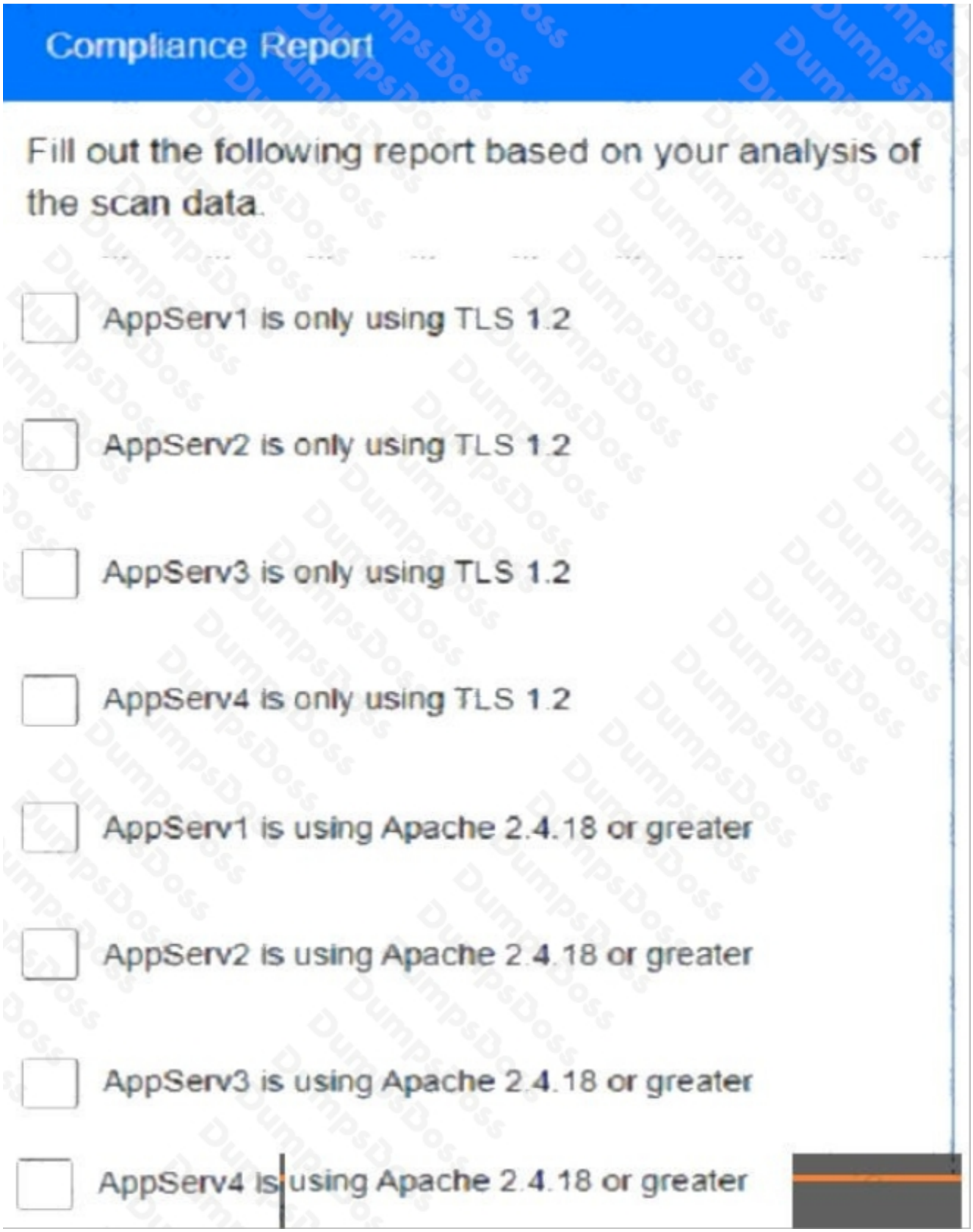


AppServ3:

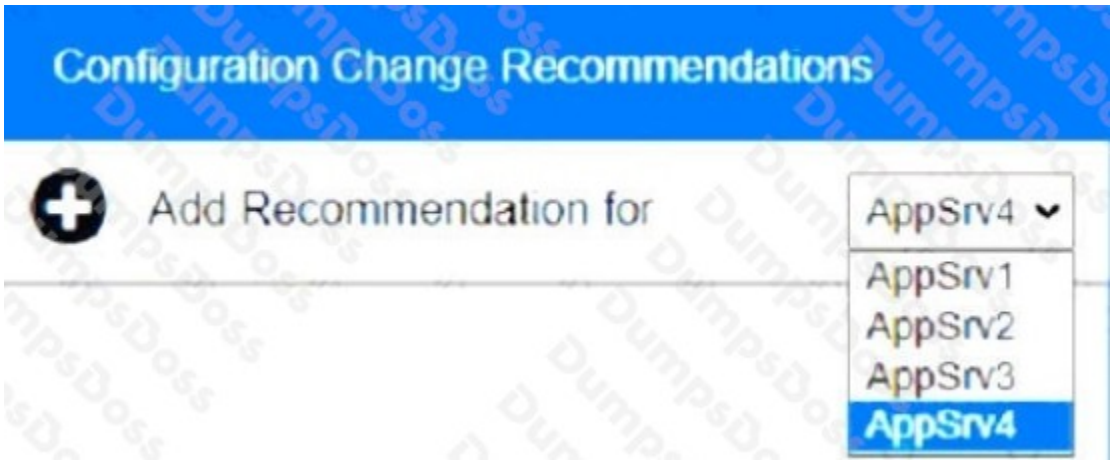

AppServ1
AppServ2
AppServ3
AppServ4
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv3.fictionalorg.com -p 443
Starting Nmap 6.40 (http://nmap.org) at 2019-06-26 16:07 CDT
Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT STATE SERVICE
80/tcp open http
443/tcp open https

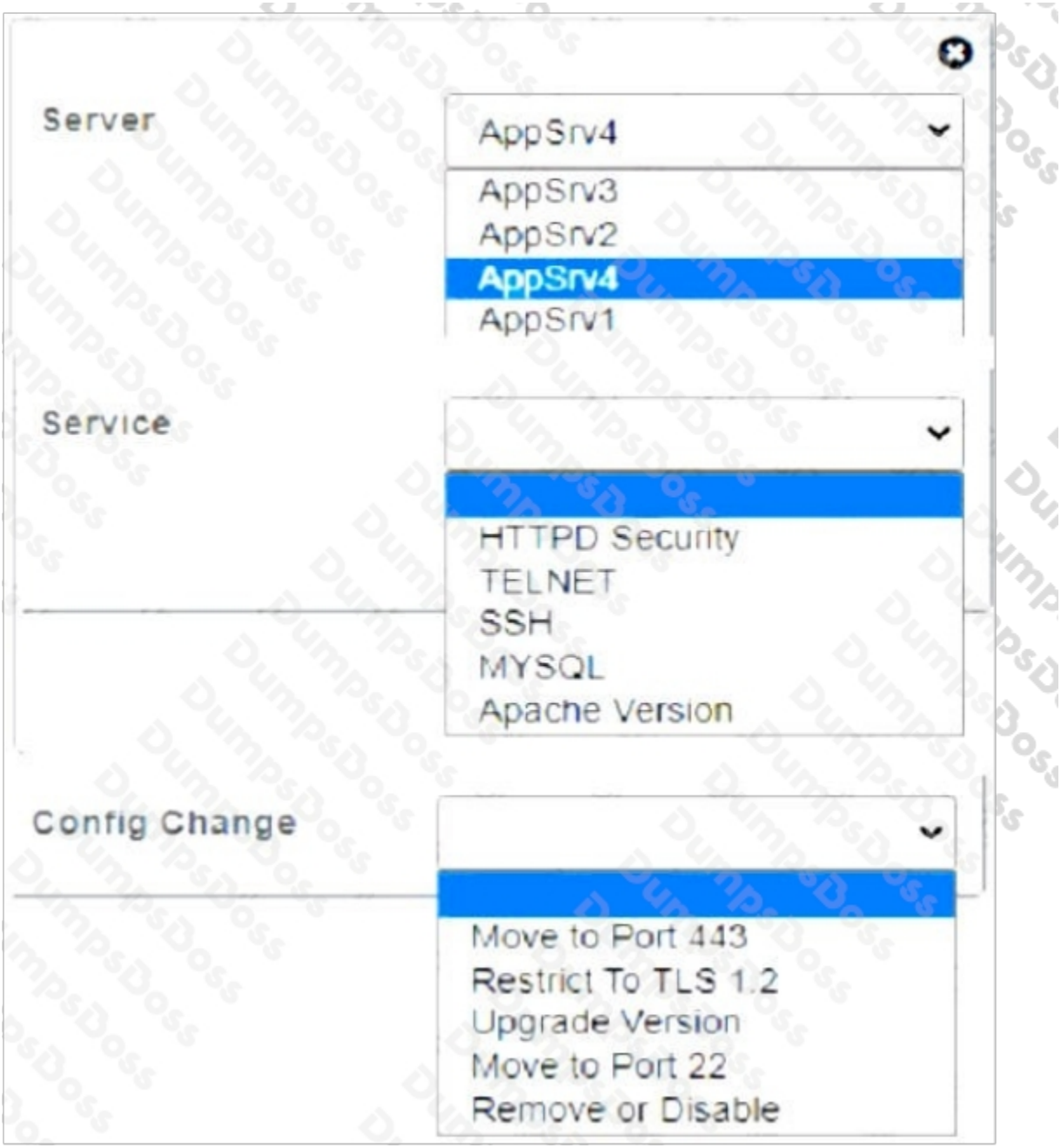
AppServ4:


AppServ1
AppServ2
AppServ3
AppServ4
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443
Starting Nmap 6.40 (http://nmap.org) at 2019-06-26 16:07 CDT
Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT STATE SERVICE
443/tcp open https
| TLSv1.2:
| ciphers:
| TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
2:38:26


Compliance Report
Fill out the following report based on your analysis of the scan data.
AppServ1 is only using TLS 1.2
AppServ2 is only using TLS 1.2
AppServ3 is only using TLS 1.2
AppServ4 is only using TLS 1.2
AppServ1 is using Apache 2.4.18 or greater
AppServ2 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater

Part 2:

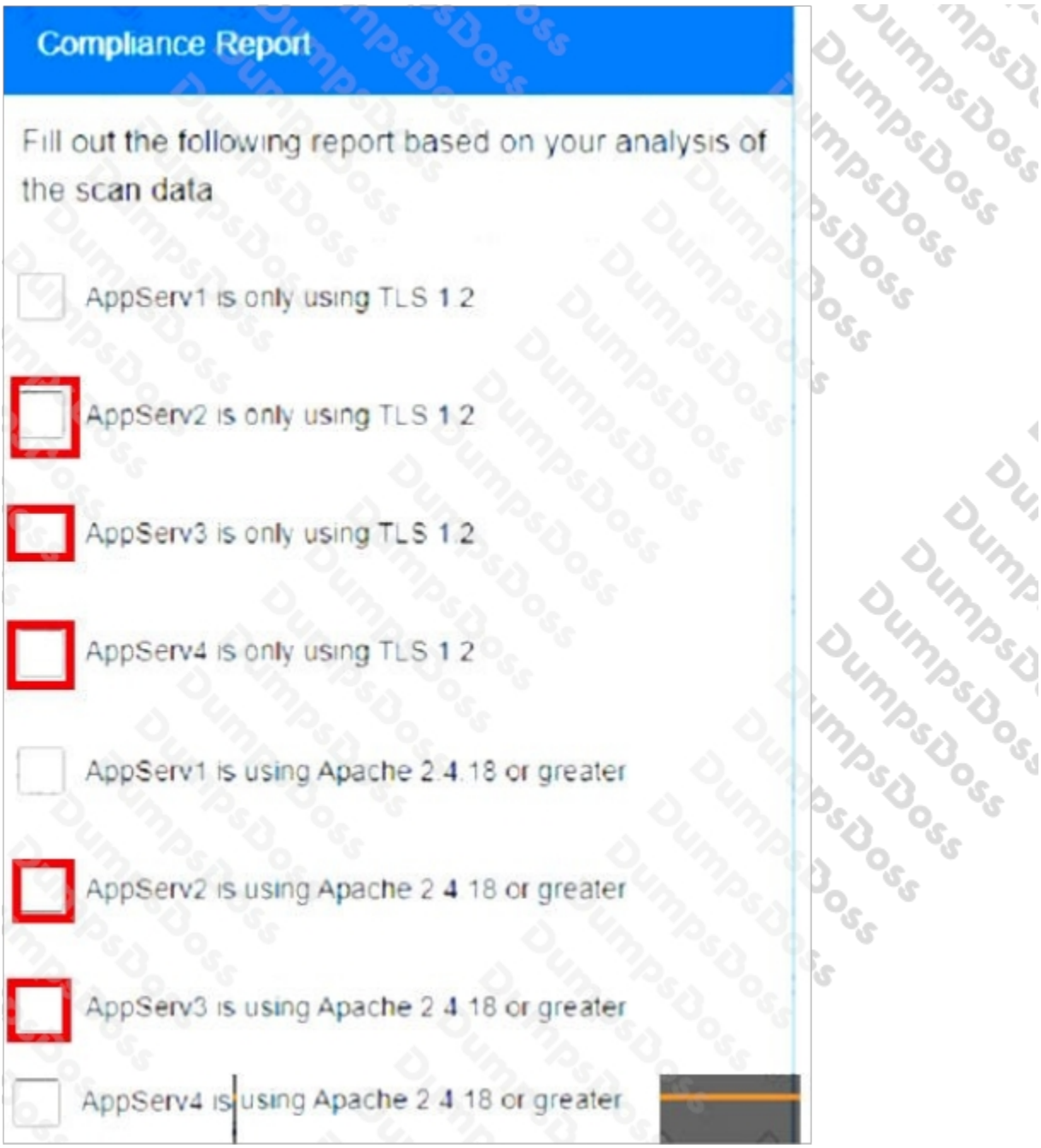

Configuration Change Recommendations
Add Recommendation for
AppSrv4
AppSrv1
AppSrv2
AppSrv3
AppSrv4



check the explanation part below for the solution:

Explanation:

Part 1:



Part 2:

Based on the compliance report, I recommend the following changes for each server: AppServ1: No changes are needed for this server.

AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.

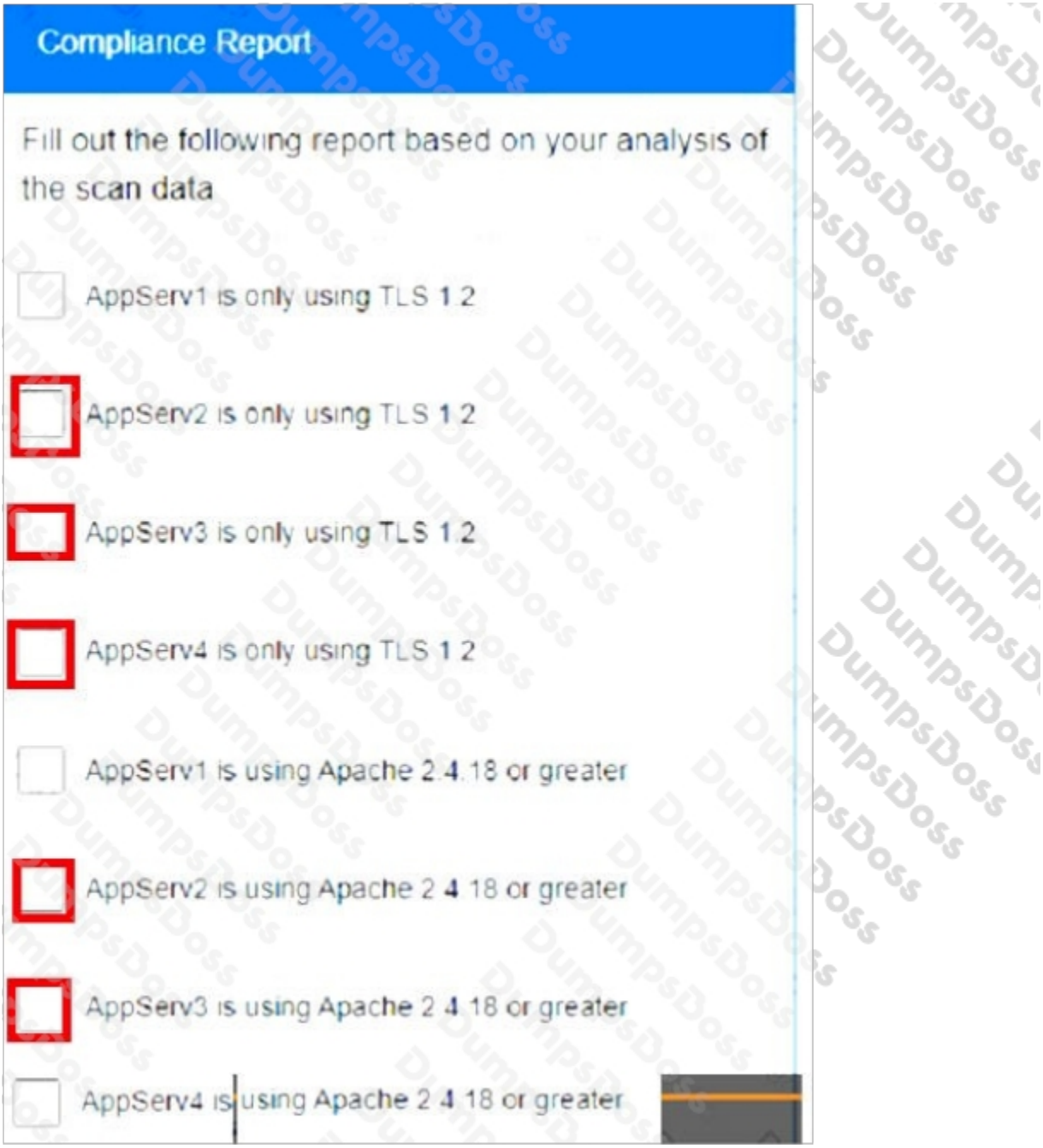
AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

ANSWER:

Explanation:

Part 1:



Part 2:

Based on the compliance report, I recommend the following changes for each server: AppServ1: No changes are needed for this server.

AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.

AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.