DUMPSHQ

Free Questions for CS0-002 by dumpshq

Shared by Hendricks on 05-09-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking

To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the .

Options:

A) email server that automatically deletes attached executables.

B) IDS to match the malware sample.

C) proxy to block all connections to <malwaresource>.

D) firewall to block connection attempts to dynamic DNS hosts.

Answer:

C

Question 2

Question Type: **MultipleChoice**

Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:

* File access auditing is turned off.

* When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.

* All processes running appear to be legitimate processes for this user and machine.

* Network traffic spikes when the space is cleared on the laptop.

* No browser is open.

Which of the following initial actions and tools would provide the BEST approach to determining what is happening?

Options:

A) Delete the temporary files, run an Nmap scan, and utilize Burp Suite.

B) Disable the network connection, check Sysinternals Process Explorer, and review netstat output.

C) Perform a hard power down of the laptop, take a dd image, and analyze with FTK.

D) Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

Answer:

B

Question 3

Question Type: **MultipleChoice**

An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:

* The source of the breach is linked to an IP located in a foreign country.

* The breach is isolated to the research and development servers.

* The hash values of the data before and after the breach are unchanged.

* The affected servers were regularly patched, and a recent scan showed no vulnerabilities.

Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

Options:

A) The confidentiality of the data is unaffected.

B) The threat is an APT.

C) The source IP of the threat has been spoofed.

D) The integrity of the data is unaffected.

E) The threat is an insider.

Answer:

B, D

Question 4

Question Type: **MultipleChoice**

SIMULATION

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:

* TLS 1.2 is the only version of TLS running.

* Apache 2.4.18 or greater should be used.

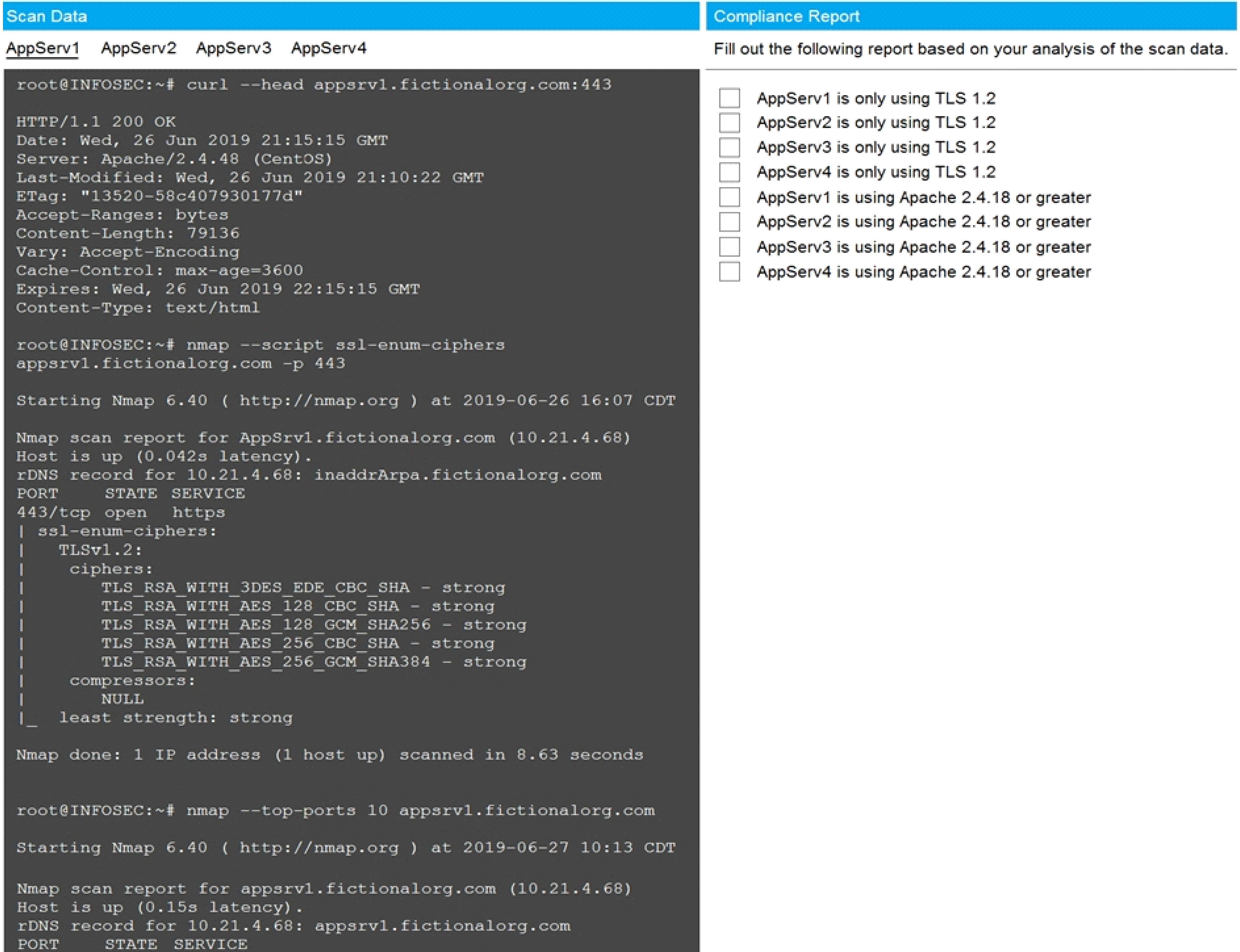
* Only default ports should be used.

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



Scan Data

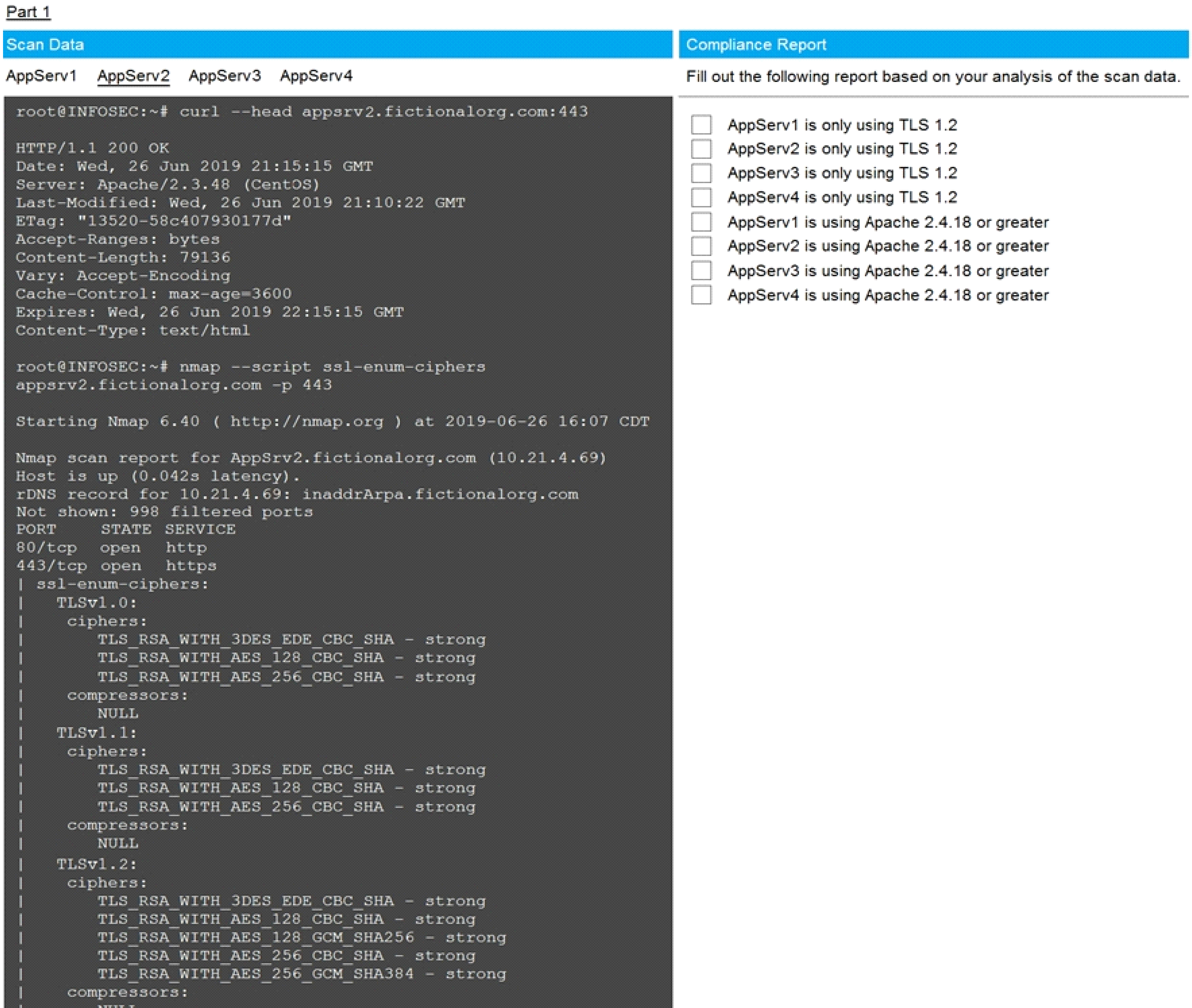
AppServ1 AppServ2 AppServ3 AppServ4

```
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
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       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
```

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 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv2.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (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
appsrv2.fictionalorg.com -p 443

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

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
| ssl-enum-ciphers:
|   TLSv1.0:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|    compressors:
|       NULL
|   TLSv1.1:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|    compressors:
|       NULL
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
```

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

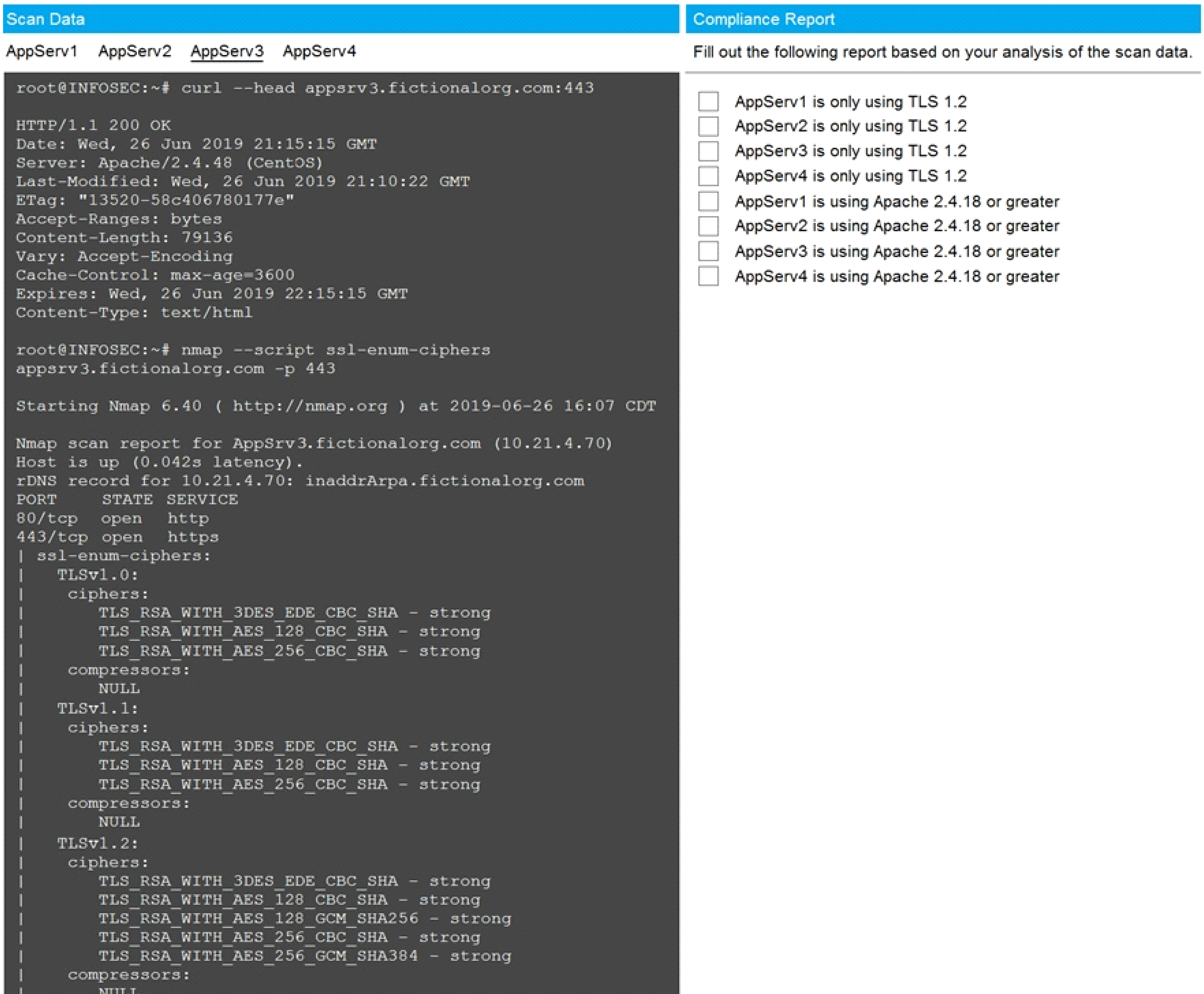
□ AppServ1 is using Apache 2.4.18 or greater

□ 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 1



Scan Data

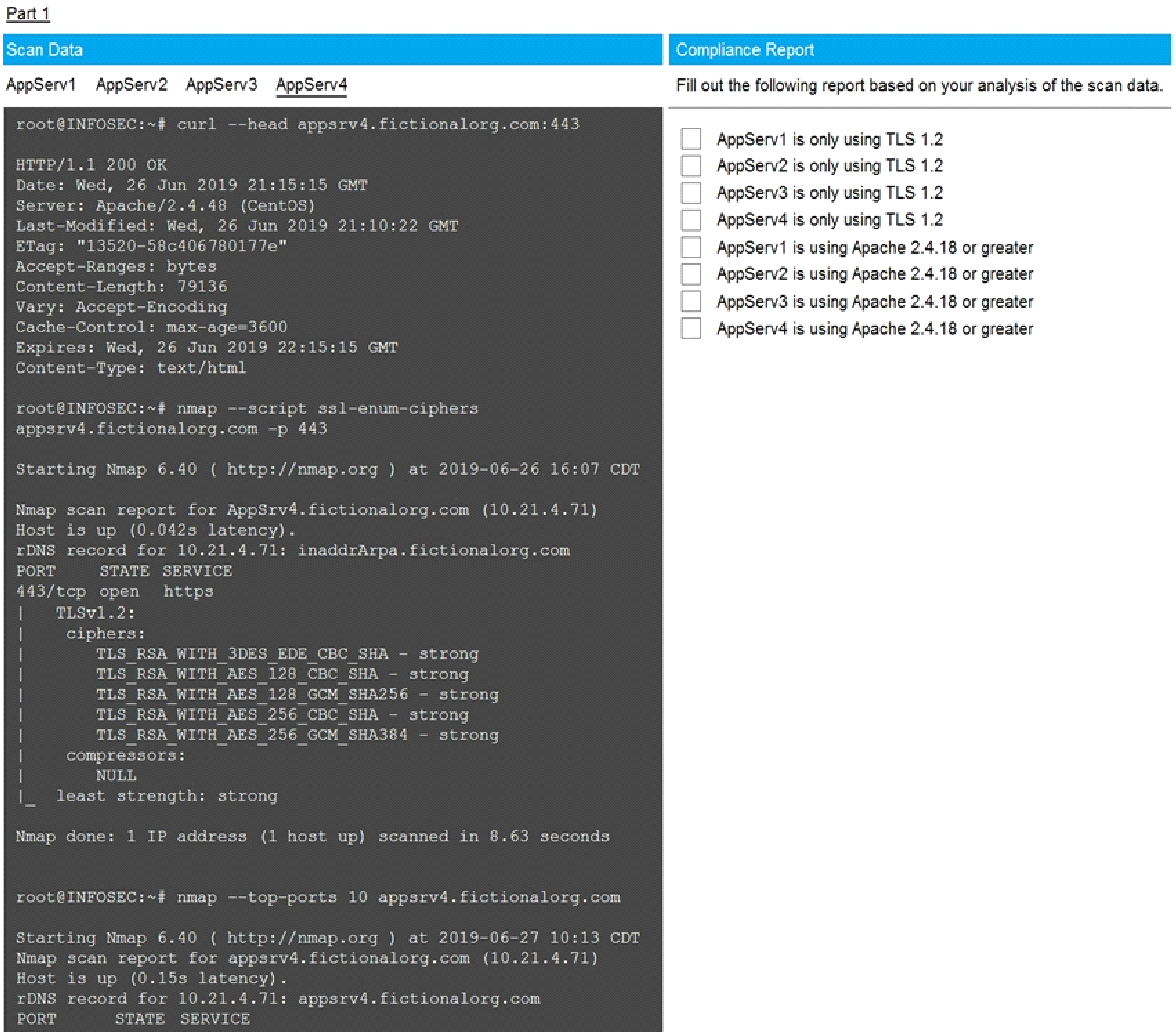
AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv3.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: "13520-58c406780177e"
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
| ssl-enum-ciphers:
|   TLSv1.0:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|    compressors:
|       NULL
|   TLSv1.1:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|    compressors:
|       NULL
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
```

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 1

Scan Data

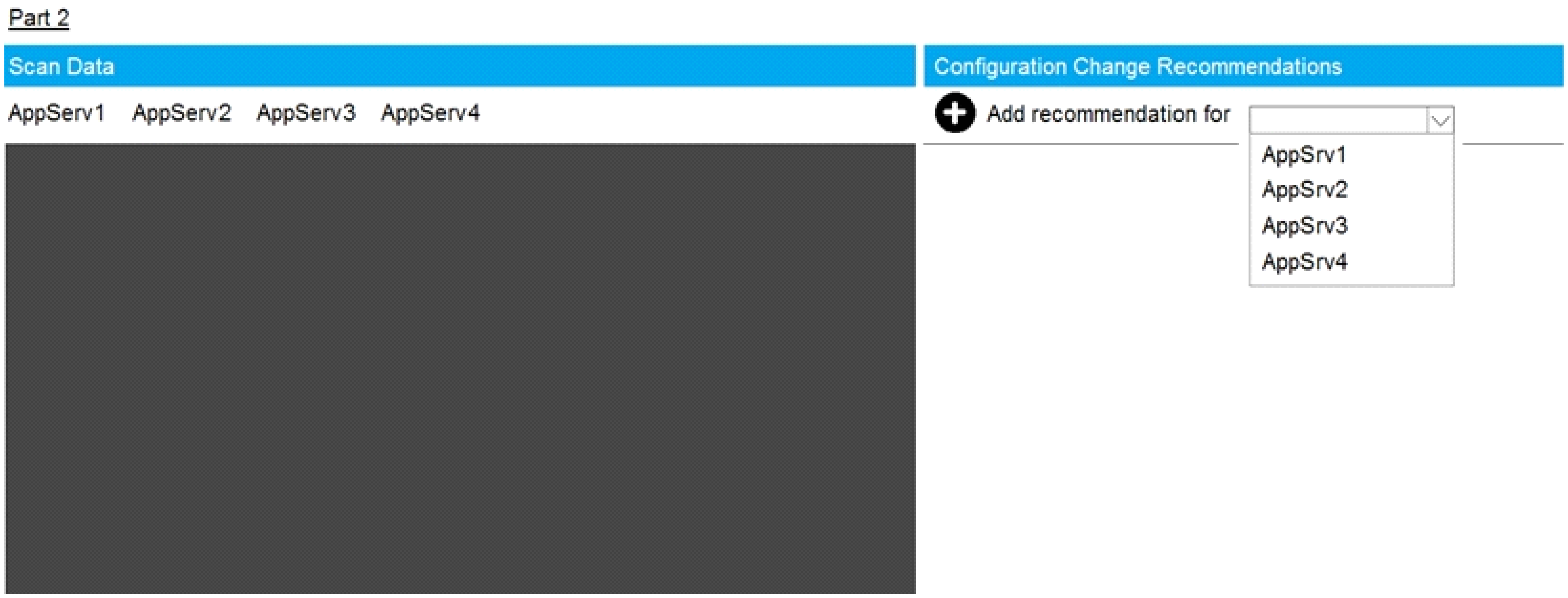
AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv4.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: "13520-58c406780177e"
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
PORT    STATE SERVICE
443/tcp open  https
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       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 appsrv4.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71)
Host is up (0.15s latency).
rDNS record for 10.21.4.71: appsrv4.fictionalorg.com
PORT      STATE  SERVICE
```

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



Options:

A) Part 1 Answer:

Check on the following:

AppServ1 is only using TLS.1.2

AppServ4 is only using TLS.1.2

AppServ1 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 answer:

Recommendation:

Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48

B) Part 1 Answer:
Check on the following:
AppServ1 is only using TLS.1.2
AppServ4 is only using TLS.1.2
AppServ1 is using Apache 2.4.18 or greater
Part 2 answer:
Recommendation:
Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48

Answer:

A

Question 5

Question Type: MultipleChoice

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer dat

a. Developers use personal workstations, giving the company little to no visibility into the development activities.

Which of the following would be BEST to implement to alleviate the CISO's concern?

Options:

A) DLP

B) Encryption

C) Test data

D) NDA

Answer:

D

Question 6

Question Type: **MultipleChoice**

It is important to parameterize queries to prevent .

Options:

A) the execution of unauthorized actions against a database.

B) a memory overflow that executes code with elevated privileges.

C) the establishment of a web shell that would allow unauthorized access.

D) the queries from using an outdated library with security vulnerabilities.

Answer:

A

Explanation:

https://stackoverflow.com/QUESTION NO:s/4712037/what-is-parameterized-query

Question 7

Question Type: MultipleChoice

Clients are unable to access a company's API to obtain pricing dat

Options:

A) An analyst discovers sources other than
clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?

A) IP whitelisting

B) Certificate-based authentication

C) Virtual private network

D) Web application firewall

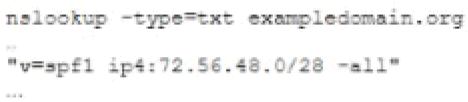
Answer:

D

Question 8

Question Type: **MultipleChoice**

The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently to the existing ones. The analyst runs the following command on the new server.



```
nslookup -type=txt exampledomain.org
..
"v=spf1 ip4:72.56.48.0/28 -all"
...
```

Given the output, which of the following should the security analyst check NEXT?

Options:

A) The DNS name of the new email server

B) The version of SPF that is being used

C) The IP address of the new email server

D) The DMARC policy

Answer:

B

Question 9

Question Type: **MultipleChoice**

An organization has several system that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

Options:

A) Use SSO across all applications

B) Perform a manual privilege review

C) Adjust the current monitoring and logging rules

D) Implement multifactor authentication

Answer:

B

Question 10

Question Type: **MultipleChoice**

SIMULATION

Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

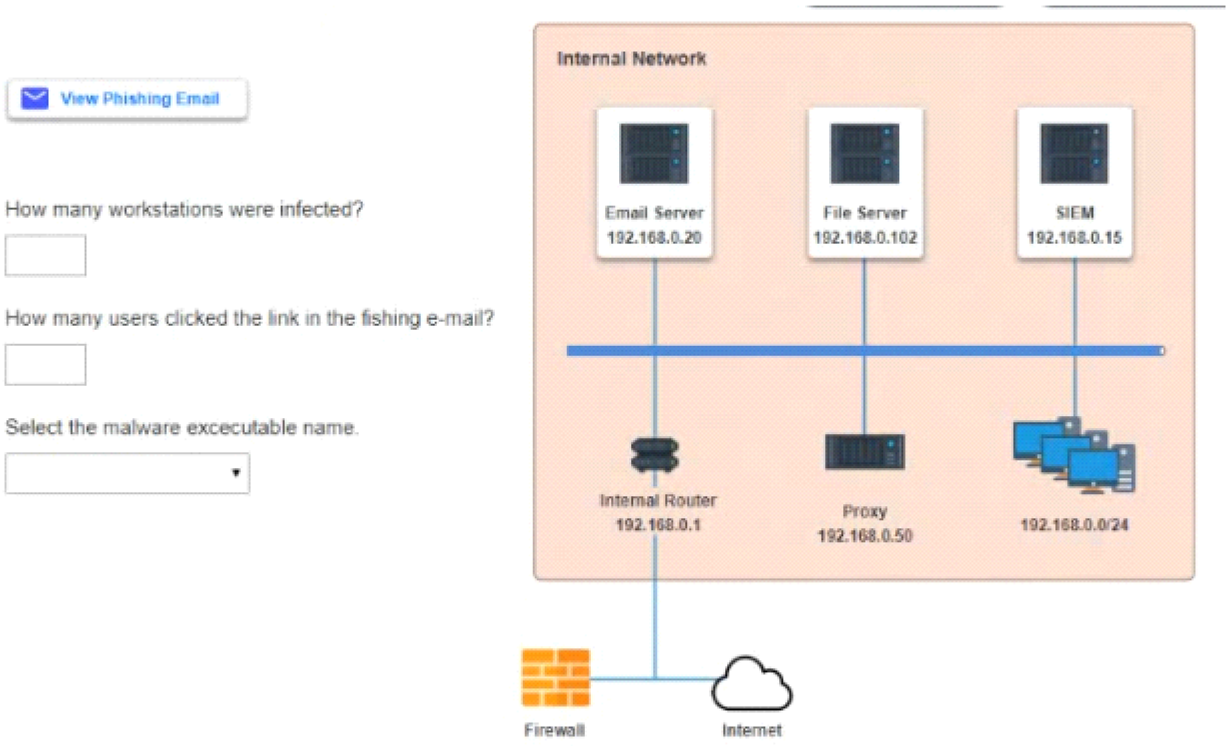
INSTRUCTIONS

Review the information provided and determine the following:

1. How many employees clicked on the link in the phishing email?

2. On how many workstations was the malware installed?

3. What is the executable file name or the malware?



View Phishing Email

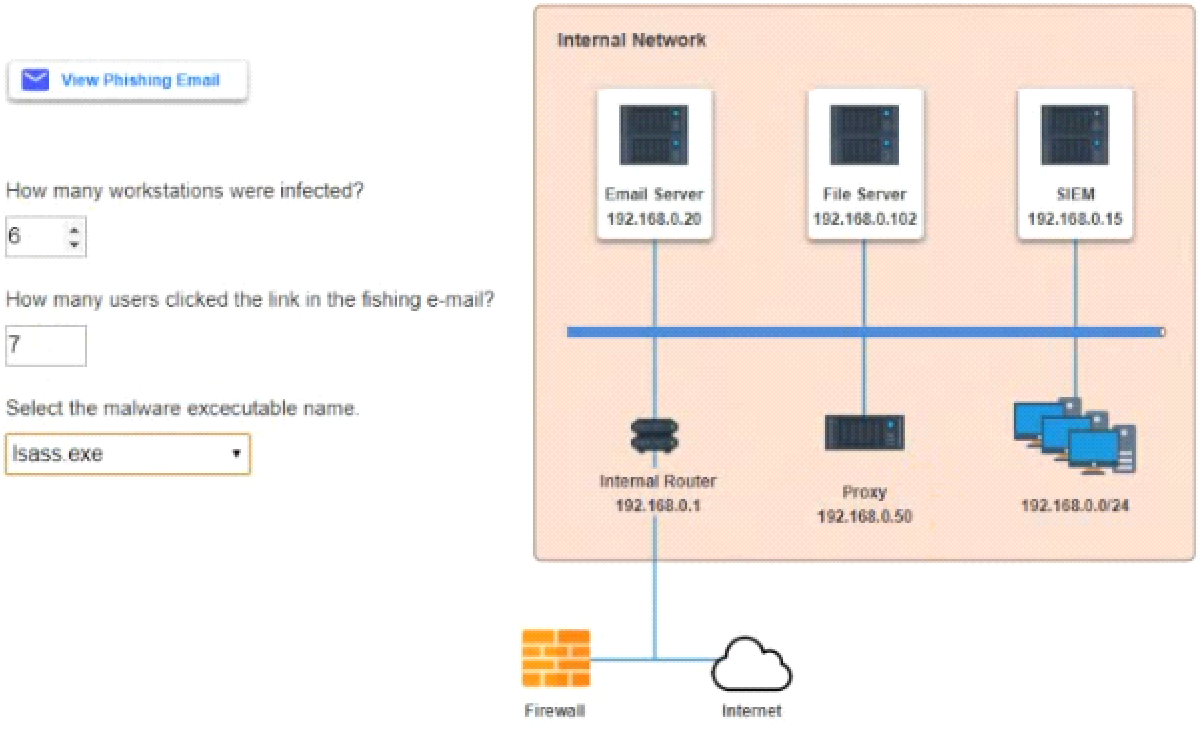
How many workstations were infected?

How many users clicked the link in the fishing e-mail?

Select the malware excecutable name.

Options:

A) Select the following answer as per diagram below:



How many workstations were infected?

6

How many users clicked the link in the fishing e-mail?

7

Select the malware excecutable name.

lsass.exe

Answer:

A

20%
DISCOUNT