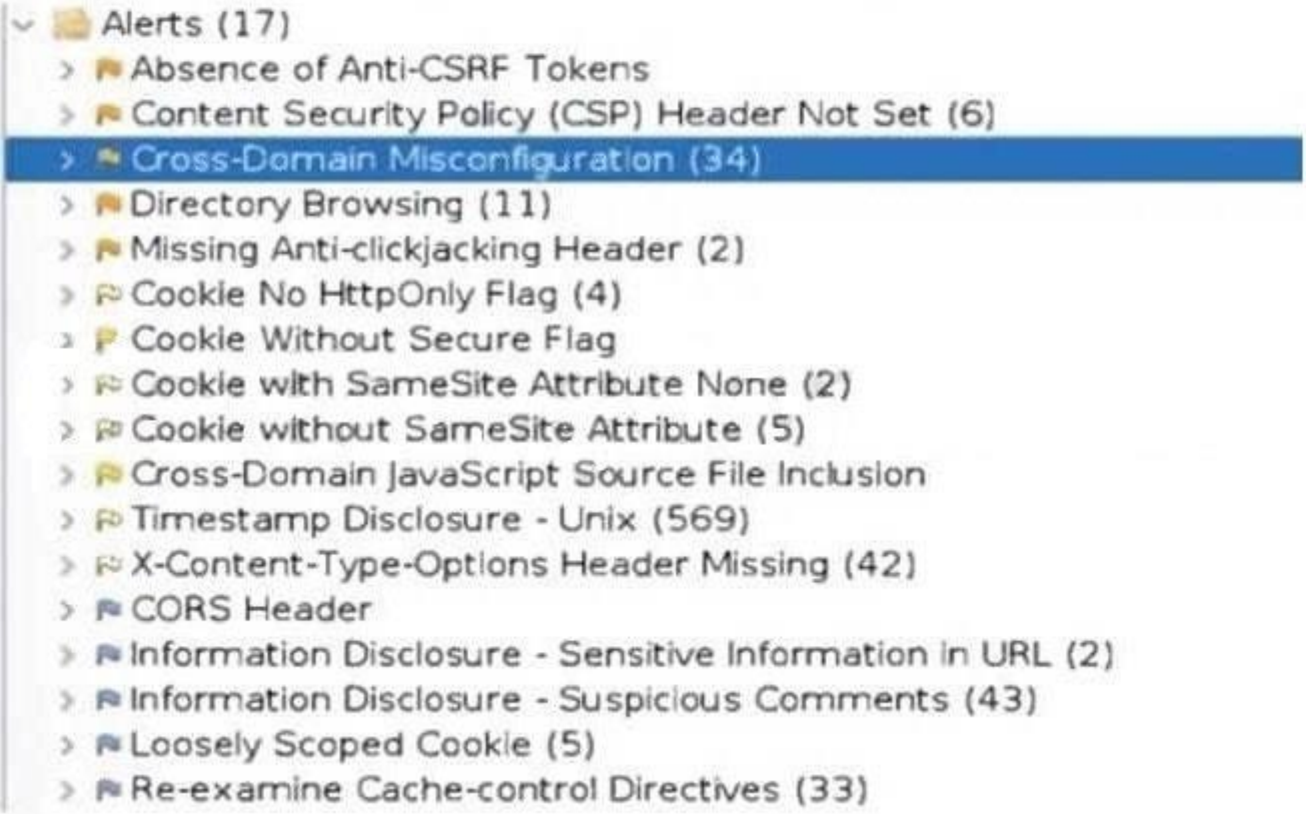
https://www.leads4pass.com/cs0-003.html

Vendor: CompTIA
Exam Code: CS0-003
Exam Name: CompTIA Cybersecurity Analyst (CySA+)
Certification: CompTIA Certifications
Total Questions: 567 Q&A (View Details)
Updated on: Feb 28, 2026

Question 1:

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Alerts (17)
- Absence of Anti-CSRF Tokens
- Content Security Policy (CSP) Header Not Set (6)
- Cross-Domain Misconfiguration (34)
- Directory Browsing (11)
- Missing Anti-clickjacking Header (2)
- Cookie No HttpOnly Flag (4)
- Cookie Without Secure Flag
- Cookie with SameSite Attribute None (2)
- Cookie without SameSite Attribute (5)
- Cross-Domain JavaScript Source File Inclusion
- Timestamp Disclosure - Unix (569)
- X-Content-Type-Options Header Missing (42)
- CORS Header
- Information Disclosure - Sensitive Information in URL (2)
- Information Disclosure - Suspicious Comments (43)
- Loosely Scoped Cookie (5)
- Re-examine Cache-control Directives (33)

Which of the following tuning recommendations should the security analyst share?

A. Set an HttpOnlvflaq to force communication by HTTPS

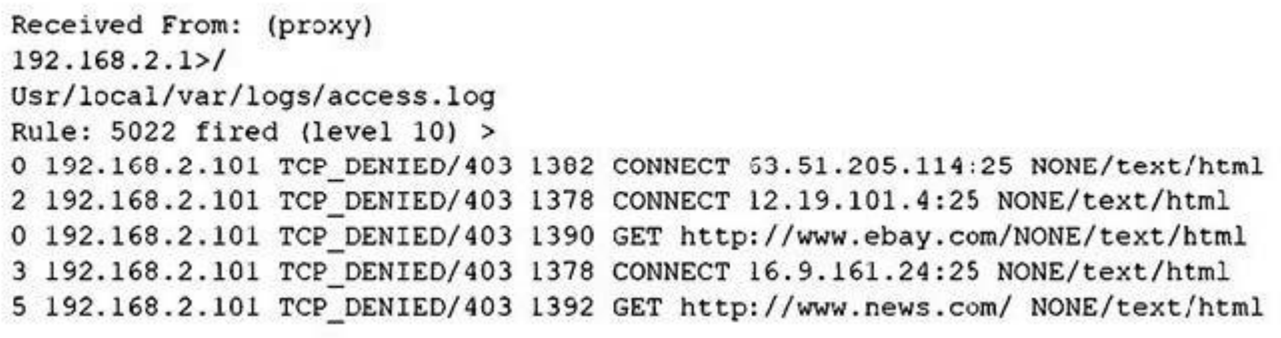
B. Block requests without an X-Frame-Options header

C. Configure an Access-Control-Allow-Origin header to authorized domains

D. Disable the cross-origin resource sharing header

Correct Answer: C

Question 2:
A security analyst notices the following proxy log entries:



```
Received From: (proxy)
192.168.2.1>/
Usr/local/var/logs/access.log
Rule: 5022 fired (level 10) >
0 192.168.2.101 TCP_DENIED/403 1382 CONNECT 63.51.205.114:25 NONE/text/html
2 192.168.2.101 TCP_DENIED/403 1378 CONNECT 12.19.101.4:25 NONE/text/html
0 192.168.2.101 TCP_DENIED/403 1390 GET http://www.ebay.com/NONE/text/html
3 192.168.2.101 TCP_DENIED/403 1378 CONNECT 16.9.161.24:25 NONE/text/html
5 192.168.2.101 TCP_DENIED/403 1392 GET http://www.news.com/ NONE/text/html
```

Which of the following is the user attempting to do based on the log entries?

A. Use a DoS attack on external hosts.

B. Exfiltrate data.

C. Scan the network.

D. Relay email.

Correct Answer: D

Based on the provided log entries, the user is attempting to relay email. This can be inferred from the log entries that show attempts to establish connections to external IP addresses on port 25, which is the default port for SMTP (Simple Mail Transfer Protocol) used for email transmission.

Question 3:
An organization wants to consolidate a number of security technologies throughout the organization and standardize a workflow for identifying security issues prioritizing the severity and automating a response Which of the following would best meet the organization\'s needs\'?

A. MaaS

B. SIEM

C. SOAR

D. CI/CD

Correct Answer: C

A security orchestration, automation, and response (SOAR) system is a solution that combines various security technologies and workflows to identify security issues, prioritize their severity, and automate a response. A SOAR system can help an organization consolidate its security tools and processes and standardize its workflow for incident response. The other options are not relevant or comprehensive for this purpose. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15; https://www.gartner.com/en/informationtechnology/glossary/security-orchestration-automation-and-response-soar

---

Question 4:
Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

A. Mean time to detect

B. Number of exploits by tactic

C. Alert volume

D. Quantity of intrusion attempts

Correct Answer: A

Mean time to detect (MTTD) is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system. MTTD is a metric that measures how long it takes to detect a security incident or threat from the time it occurs. MTTD can be improved by using tools and processes that can collect, correlate, analyze, and alert on security data from various sources. SIEM, SOAR, and ticketing systems are examples of such tools and processes that can help reduce MTTD and enhance security operations.
Official
https://www.eccouncil.org/cybersecurityexchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack

---

Question 5:
Which of the following best explains the importance of communicating with staff regarding the official public communication plan related to incidents impacting the organization?

A. To establish what information is allowed to be released by designated employees

B. To designate an external public relations firm to represent the organization

C. To ensure that all news media outlets are informed at the same time

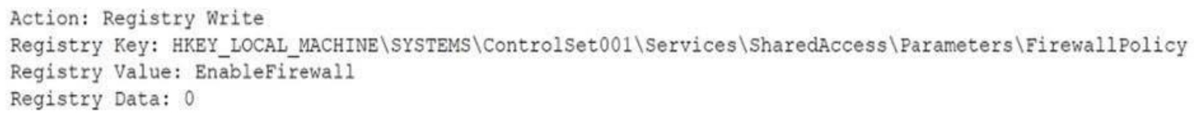
D. To define how each employee will be contacted after an event occurs

Correct Answer: A

Communicating with staff about the official public communication plan is important to avoid unauthorized or inaccurate disclosure of information that could harm the organization\'s reputation, security, or legal obligations. It also helps to ensure consistency and clarity of the messages delivered to the public and other stakeholders.
https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf

---

Question 6:
An analyst received an alert regarding an application spawning a suspicious command shell process Upon further investigation, the analyst observes the following registry change occurring immediately after the suspicious event:



```
Action: Registry Write
Registry Key: HKEY_LOCAL_MACHINE\SYSTEMS\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy
Registry Value: EnableFirewall
Registry Data: 0
```

Which of the following was the suspicious event able to accomplish?

A. Impair defenses.

B. Establish persistence.

C. Bypass file access controls.

D. Implement beaconing.

Correct Answer: A

Question 7:
Which of the following is the first step that should be performed when establishing a disaster recovery plan?

A. Agree on the goals and objectives of the plan

B. Determine the site to be used during a disaster

C. Demonstrate adherence to a standard disaster recovery process

D. Identity applications to be run during a disaster

Correct Answer: A

The first step that should be performed when establishing a disaster recovery plan is to agree on the goals and objectives of the plan. The goals and objectives of the plan should define what the plan aims to achieve, such as minimizing downtime, restoring critical functions, ensuring data integrity, or meeting compliance requirements. The goals and objectives of the plan should also be aligned with the business needs and priorities of the organization and be measurable and achievable.

Question 8:

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:

1.

TLS 1 2 is the only version of TLS running.

2.

Apache 2.4.18 or greater should be used.

3.

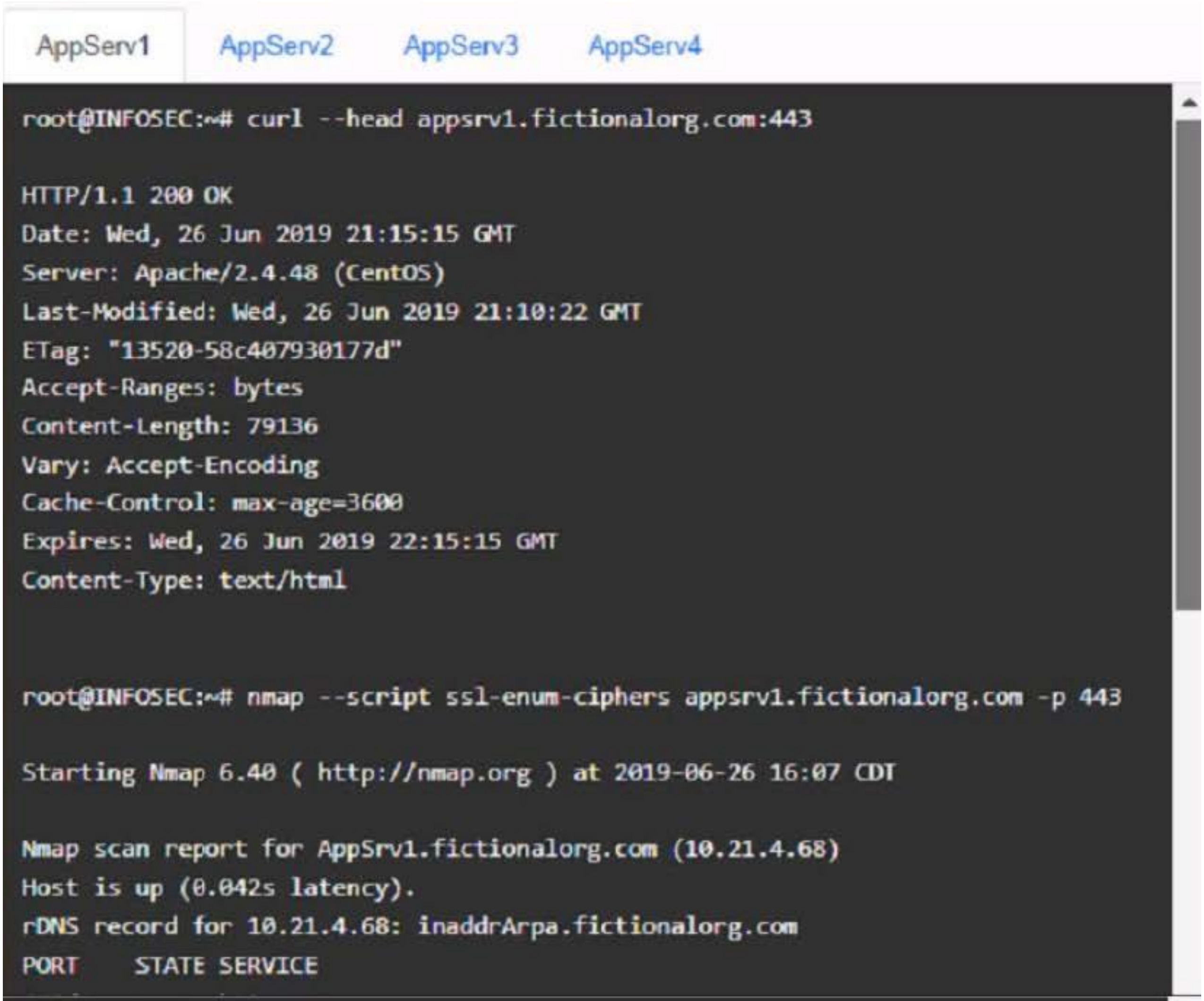
Only default ports should be used.

INSTRUCTIONS

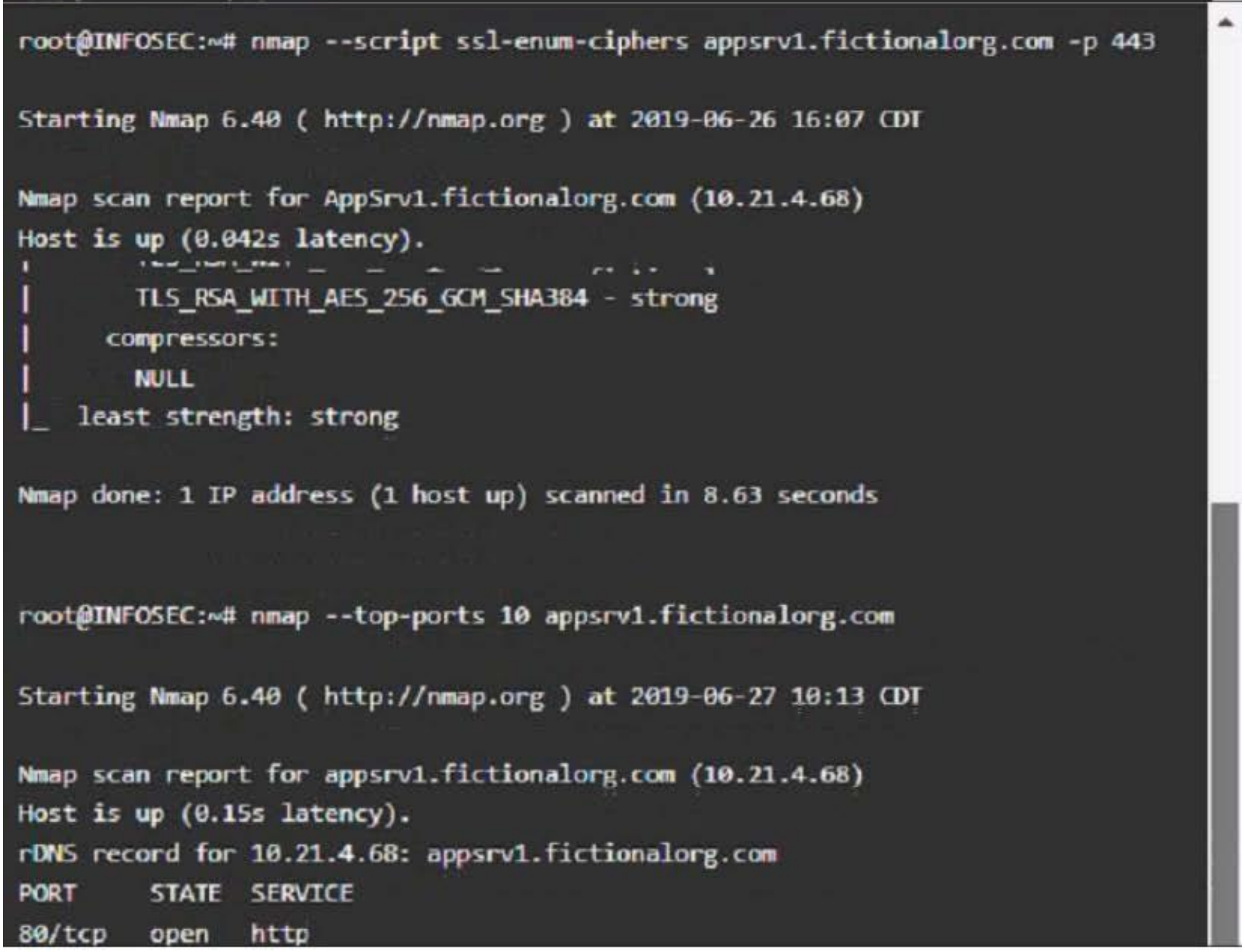
using the supplied data. record the status of compliance With the company\'s guidelines for each server.

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.

Part 1: AppServ1:

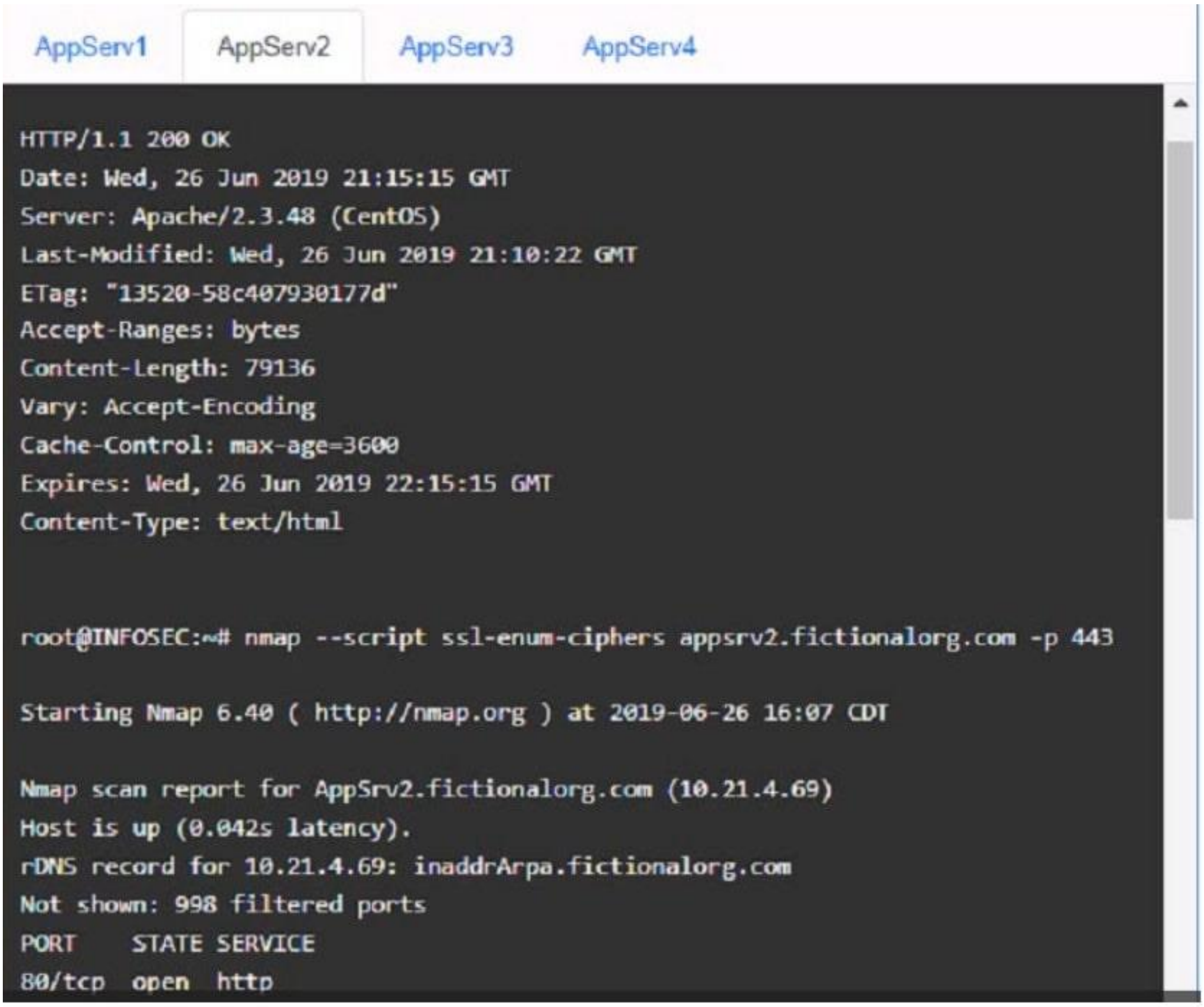


```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

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
```



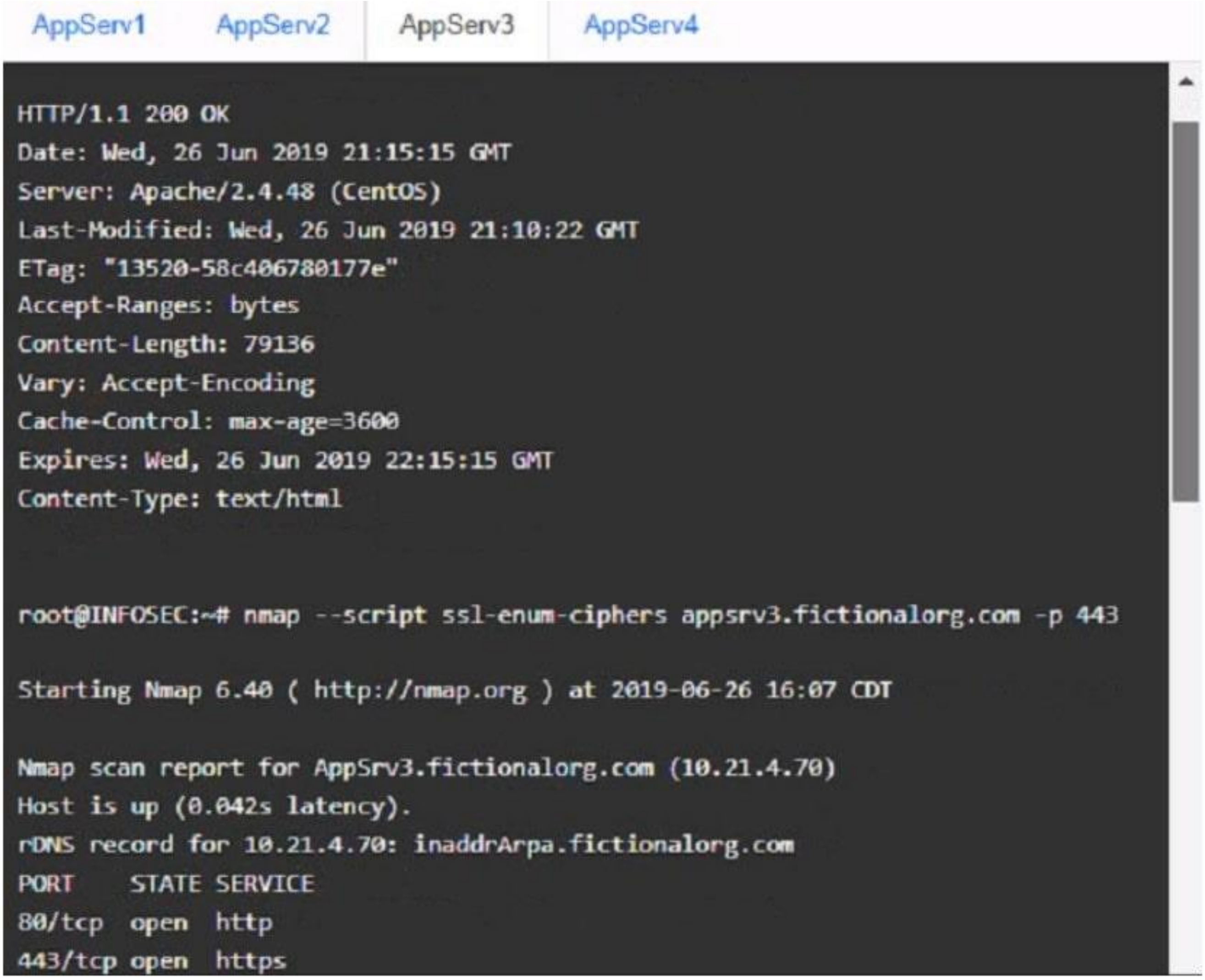
```
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

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)
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:



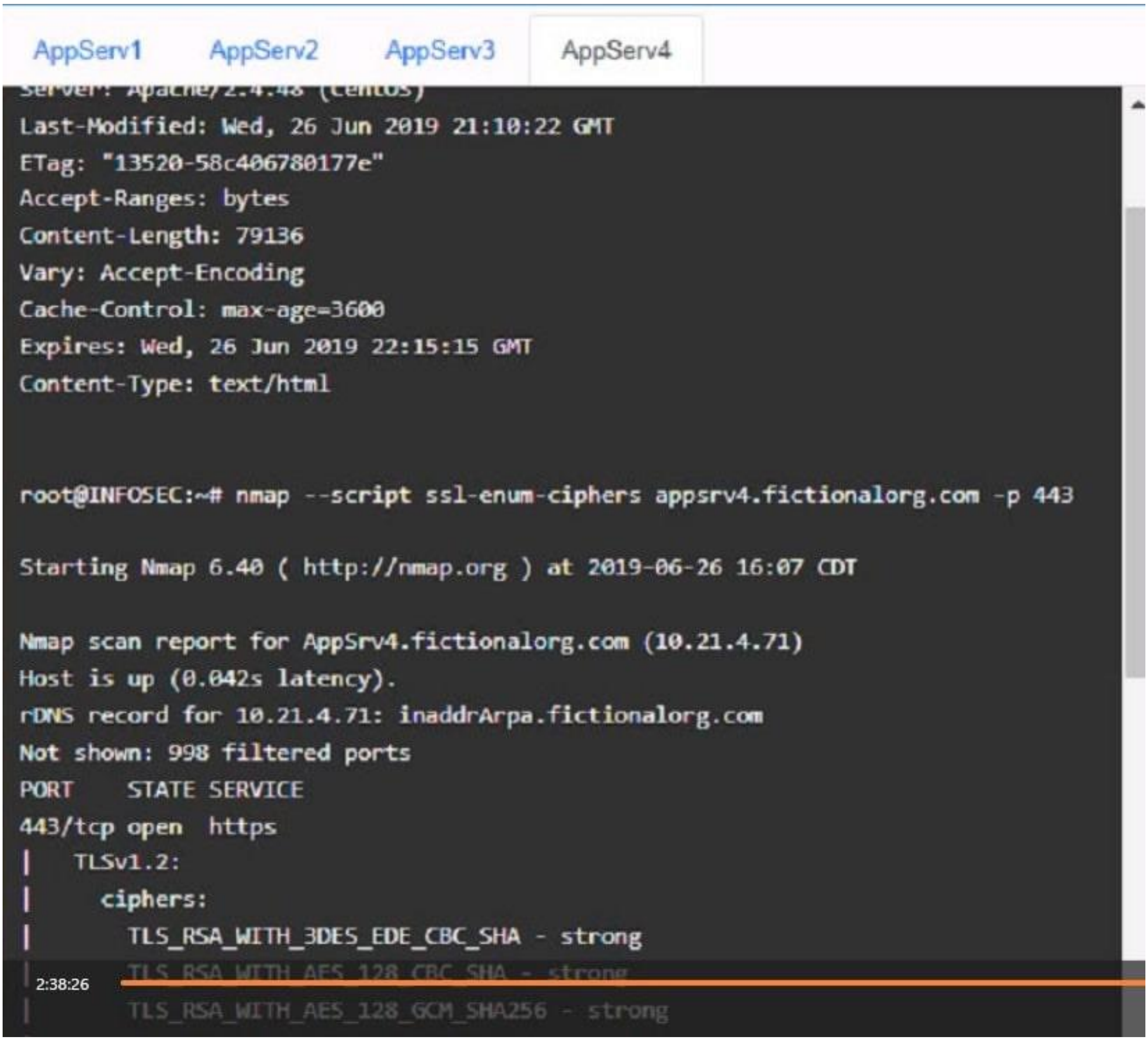
```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: 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
```

AppServ3:



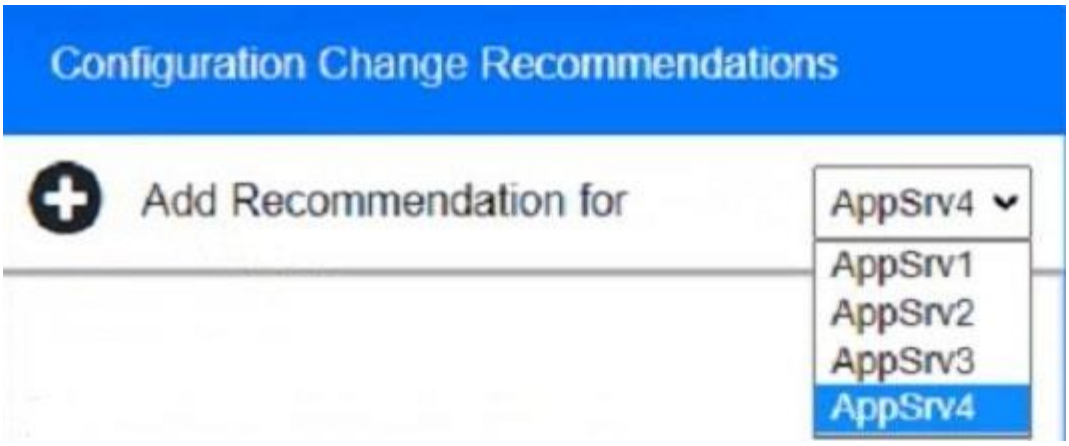
```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: 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:

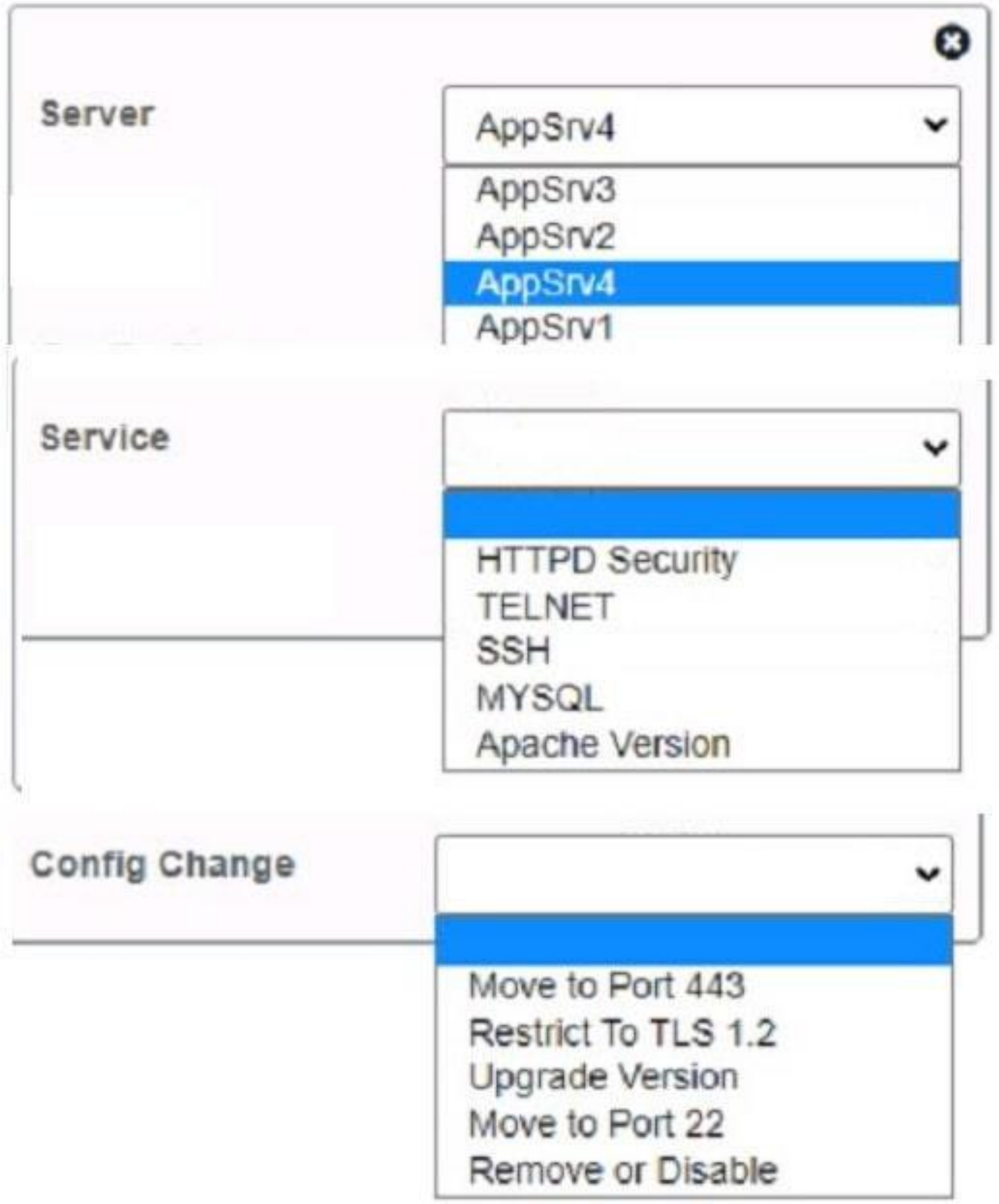


```
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


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
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
```

Part 2:



Configuration Change Recommendations



Server: AppSrv4

A. See the solution below in Explanation.

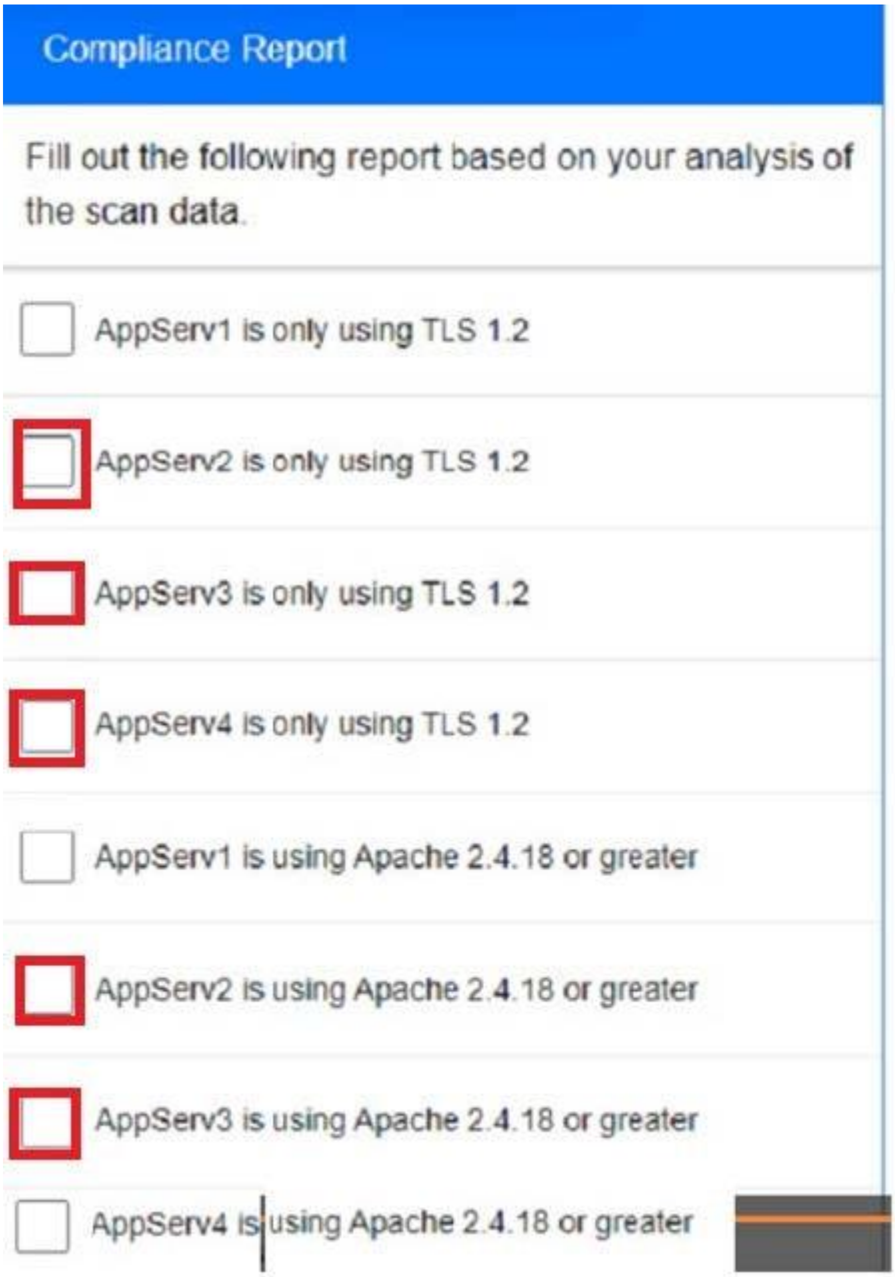
B. PlaceHoder

C. PlaceHoder

D. PlaceHoder

Correct Answer: A

Part 1:



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:

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.

Question 9:
A security analyst discovers a standard user has unauthorized access to the command prompt, PowerShell, and other system utilities. Which of the following is the BEST action for the security analyst to take?

A. Disable the appropriate settings in the administrative template of the Group Policy.

B. Use AppLocker to create a set of whitelist and blacklist rules specific to group membership.

C. Modify the registry keys that correlate with the access settings for the System32 directory.

D. Remove the user\'s permissions from the various system executables.

Correct Answer: B

AppLocker: This is a Windows feature that allows administrators to control which applications and files users can run. By creating a set of whitelist (allowed applications) and blacklist (blocked applications) rules specific to group membership, the security analyst can effectively control access to the command prompt, PowerShell, and other system utilities based on the user\'s group membership. This provides a flexible and manageable solution to restrict unauthorized access.

Question 10:
An email hosting provider added a new data center with new public IP addresses. Which of the following most likely needs to be updated to ensure emails from the new data center do not get blocked by spam filters?

A. DKIM

B. SPF

C. SMTP

D. DMARC

Correct Answer: B

SPF (Sender Policy Framework) is a DNS TXT record that lists authorized sending IP addresses for a given domain. If an email hosting provider added a new data center with new public IP addresses, the SPF record needs to be updated to include those new IP addresses, otherwise the emails from the new data center may fail SPF checks and get blocked by spam filters References:

1: Use DMARC to validate email, setup steps

2: How to set up SPF, DKIM and DMARC: other mail and hosting providers providers

3: Set up SPF, DKIM, or DMARC records for my hosting email

Question 11:
An organization has the following risk mitigation policies

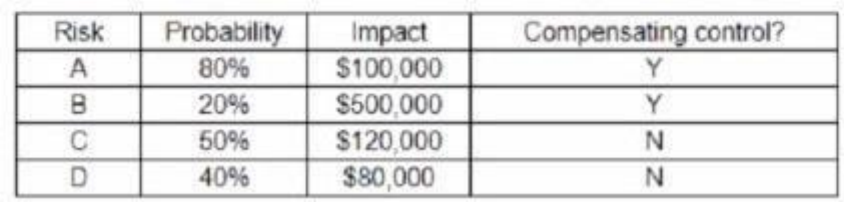
1.

Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000

2.

Other nsk mitigation will be pnontized based on risk value.

The following risks have been identified: Which of the following is the ordei of priority for risk mitigation from highest to lowest?



Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

A. A, C, D, B

B. B, C, D, A

C. C, B, A, D

D. C. D, A, B

E. D, C, B, A

Correct Answer: C

The order of priority for risk mitigation from highest to lowest is C, B, A, D. This order is based on applying the risk mitigation policies of the organization. According to the first policy, risks without compensating controls will be mitigated first if the risk value is greater than $50,000. Risk C has no compensating controls and a risk value of $75,000, so it is the highest priority. Risk B also has no compensating controls, but a risk value of $40,000, so it is the second priority. According to the second policy, other risk mitigation will be prioritized based on risk value. Risk A has a risk value of $60,000 and a compensating control of encryption, so it is the third priority. Risk D has a risk value of $50,000 and a compensating control of backup power supply, so it is the lowest priority.

Question 12:
Security awareness and compliance programs are most effective at reducing the likelihood and impact of attacks from:

A. advanced persistent threats.

B. corporate spies.

C. hacktivists.

D. insider threats.

Correct Answer: D

Question 13:
Which of following would best mitigate the effects of a new ransomware attack that was not properly stopped by the company antivirus?

A. Install a firewall.

B. Implement vulnerability management.

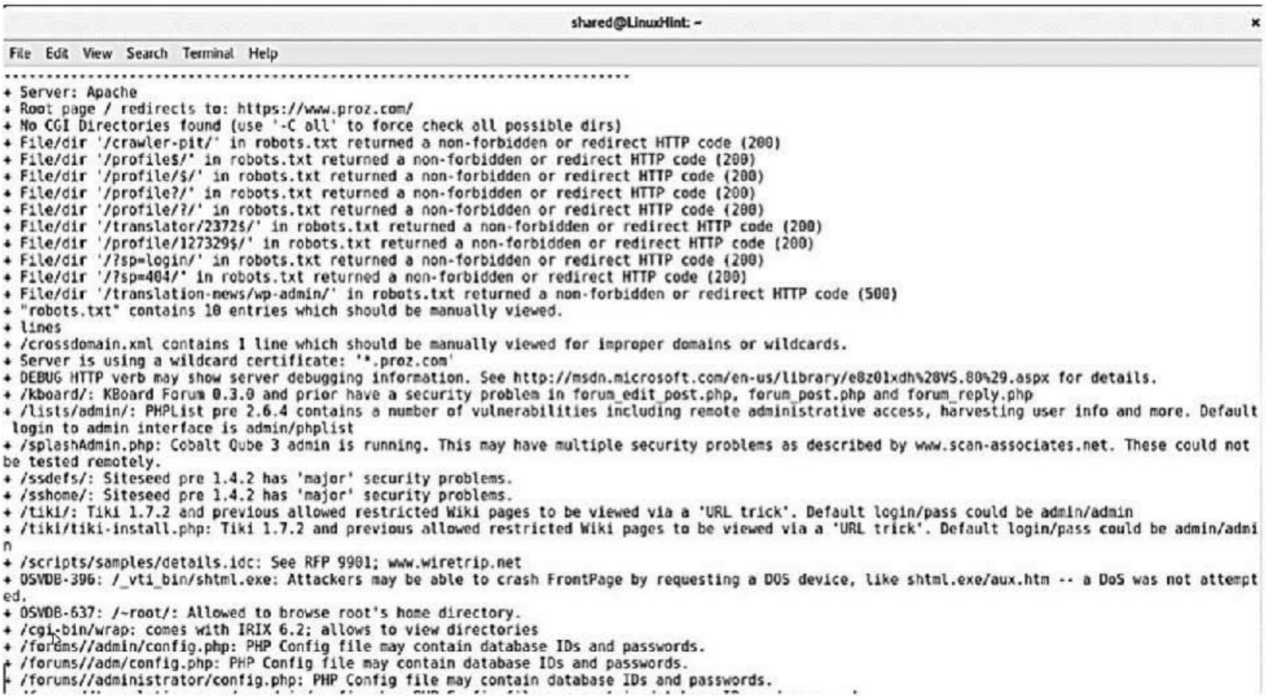
C. Deploy sandboxing.

D. Update the application blocklist.

Correct Answer: C

Sandboxing is a technique that isolates potentially malicious programs or files in a controlled environment, preventing them from affecting the rest of the system. It can help mitigate the effects of a new ransomware attack by preventing it from encrypting or deleting important data or spreading to other devices. References: CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 5, page 202; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 210.

Question 14:
A security analyst reviews the following results of a Nikto scan:



```
---------------------------------------------------------------------------
+ Server: Apache
+ Root page / redirects to: https://www.proz.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ File/dir '/crawler-pit/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/translator/2372$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/127329$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/?sp=login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/?sp=404/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/translation-news/wp-admin/' in robots.txt returned a non-forbidden or redirect HTTP code (500)
+ "robots.txt" contains 10 entries which should be manually viewed.
+ lines
+ /crossdomain.xml contains 1 line which should be manually viewed for improper domains or wildcards.
+ Server is using a wildcard certificate: '*.proz.com'
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default
 login to admin interface is admin/phplist
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan-associates.net. These could not
be tested remotely.
+ /ssdefs/: Siteseed pre 1.4.2 has 'major' security problems.
+ /sshome/: Siteseed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admi
n
+ /scripts/samples/details.idc: See RFP 9901; www.wiretrip.net
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempt
ed.
+ OSVDB-637: /~root/: Allowed to browse root's home directory.
+ /cgi-bin/wrap: comes with IRIX 6.2; allows to view directories
+ /forums//admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//adm/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//administrator/config.php: PHP Config file may contain database IDs and passwords.
```

Which of the following should the security administrator investigate next?

A. tiki

B. phpList

C. shtml.exe

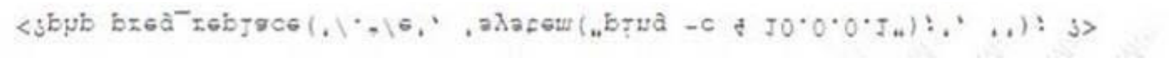
D. sshome

Correct Answer: C

The security administrator should investigate shtml.exe next, as it is a potential vulnerability that allows remote code execution on the web server. Nikto scan results indicate that the web server is running Apache on Windows, and that the shtml.exe file is accessible in the /scripts/ directory. This file is part of the Server Side Includes (SSI) feature, which allows dynamic content generation on web pages. However, if the SSI feature is not configured properly, it can allow attackers to execute arbitrary commands on the web server by injecting malicious code into the URL or the web page12. Therefore, the security administrator should check the SSI configuration and permissions, and remove or disable the shtml.exe file if it is not needed. References: Nikto-Penetration testing. Introduction, Web application scanning with Nikto

---

Question 15:
During the log analysis phase, the following suspicious command is detected



```
<?php preg_replace('/.*/e', 'system("ping -c 4 10.0.0.1");', ''); ?>
```

Which of the following is being attempted?

A. Buffer overflow

B. RCE

C. ICMP tunneling

D. Smurf attack

Correct Answer: B

RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program\'s execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified References: What Is Buffer Overflow? Attacks, Types and Vulnerabilities - Fortinet1, What Is a Smurf Attack? Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of ...3