Free Questions for PT0-002 by certsinside

Shared by Burris on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

During an assessment, a penetration tester found an application with the default credentials enabled. Which of the following best describes the technical control required to fix this issue?

Options:

A- Password encryption

B- System hardening

C- Multifactor authentication

D- Patchmanagement

Answer:

B

Explanation:

* System hardening involves securing a system by reducing its surface of vulnerability, which includes changing default credentials, disabling unnecessary services, and applying security patches.

* Details:

A . Password encryption: Secures passwords but does not address the issue of default credentials.

B . System hardening: Comprehensive approach to securing the system, including changing default credentials.

C . Multifactor authentication: Adds an additional layer of security but does not solve the problem of default credentials being enabled.

D . Patch management: Ensures software is up-to-date but does not directly address default credentials.

* Reference: System hardening is a fundamental practice in securing systems and preventing unauthorized access, as detailed in security best practices and guidelines.

Question 2

Question Type: MultipleChoice

As part of active reconnaissance, penetration testers need to determine whether a protection mechanism is in place to safeguard the target's website against web application attacks. Which of the following methods would be the most suitable?

Options:

A- Direct-to-origin testing

B- Antivirus scanning

C- Scapy packet crafting

D- WAF detection

Answer:

D

Explanation:

* Detecting a Web Application Firewall (WAF) helps penetration testers understand the protective measures in place and tailor their testing methods to bypass these defenses.

* Details:

A . Direct-to-origin testing: Useful for bypassing CDN but not specifically for detecting protective mechanisms like WAF.

B . Antivirus scanning: Not relevant for web application attacks.

C . Scapy packet crafting: Useful for network-level testing but not for detecting web application protections.

D . WAF detection: Identifies if a WAF is present, which is critical for understanding and bypassing web application defenses.

* Reference: WAF detection techniques are documented in web application security testing methodologies such as OWASP.

Question 3

Question Type: MultipleChoice

Which of the following is the most important to include in the scope of a wireless security assessment?

Options:

A- Frequencies

B- APs

C- SSIDs

D- Signal strengths

Answer:

B

Explanation:

* Access Points (APs) are crucial in a wireless security assessment as they are the main points through which devices connect to the network. Identifying and securing APs ensures network integrity and security.

* Details:

A . Frequencies: Important but not as critical as identifying and assessing APs.

B . APs: Central to the network's security; assessing AP configurations, placements, and security settings is essential.

C . SSIDs: Identifying SSIDs is part of the assessment but does not provide a complete picture without evaluating APs.

D . Signal strengths: Useful for understanding coverage but secondary to assessing AP security.

* Reference: Wireless security assessments prioritize AP evaluation as they are the entry points to the network, as outlined in various wireless security frameworks and methodologies.

Question 4

Question Type: MultipleChoice

During an engagement, a junior penetration tester found a multihomed host that led to an unknown network segment. The penetration tester ran a port scan against the network segment, which caused an outage at the customer's factory. Which of the following documents should the junior penetration tester most likely follow to avoid this issue in the future?

Options:

A- NDA

B- MSA

C- ROE

D- SLA

Answer:

C

Explanation:

* Rules of Engagement (ROE) documents outline the scope, boundaries, and rules for a penetration test to prevent unintended consequences such as network outages.

* Details:

NDA (Non-Disclosure Agreement): Protects confidential information but does not provide guidelines for engagement.

MSA (Master Service Agreement): General terms and conditions for services but does not detail specific engagement rules.

ROE (Rules of Engagement): Specifies the limits and guidelines for testing, including which systems can be tested, when, and how, to avoid disruptions.

SLA (Service Level Agreement): Defines the level of service expected but does not guide the testing process.

* Reference: ROE is a critical document in penetration testing engagements to ensure both the tester and client are aligned on the scope and limitations, as outlined in various penetration testing standards and methodologies.

Question 5

Question Type: MultipleChoice

Which of the following is the most secure way to protect a final report file when delivering the report to the client/customer?

Options:

A- Creating a link on a cloud service and delivering it by email

B- Asking for a PGP public key to encrypt the file

C- Requiring FTPS security to download the file

D- Copying the file on a USB drive and delivering it by postal mail

Answer:

B

Explanation:

* Using PGP (Pretty Good Privacy) encryption ensures that the report file is securely encrypted with the client's public key. Only the client can decrypt the file using their private key, ensuring confidentiality during transit.

* Details:

Option Analysis:

A . Creating a link on a cloud service and delivering it by email: This method is susceptible to interception or unauthorized access.

B . Asking for a PGP public key to encrypt the file: Provides end-to-end encryption ensuring that only the intended recipient can access the file.

C . Requiring FTPS security to download the file: While secure, it does not provide the same level of end-to-end encryption as PGP.

D . Copying the file on a USB drive and delivering it by postal mail: While physically secure, it is not practical and poses a risk of loss or theft.

* Reference: PGP encryption is a widely accepted method for securing sensitive data. It is recommended by many cybersecurity standards and best practice guides.

Question 6

Question Type: MultipleChoice

A penetration tester enters a command into the shell and receives the following output:

```
C:\Users\UserX\Desktop>vmic service get name, pathname, displayname, startmode | findstr /i auto | findstr /i /v |C:\\Windows\\" I findstr /i /v""
```

```
VulnerableService Some Vulnerable Service C:\Program Files\A Subfolder\B Subfolder\SomeExecutable.exe Automatic
```

Which of the following types of vulnerabilities does this system contain?

Options:

A- Unquoted service path

B- Writable services

C- Clear text credentials

D- Insecure file/folder permissions

Answer:

A

Explanation:

* The provided output reveals a common vulnerability in Windows services known as an unquoted service path. When the service executable path is not enclosed in quotes and contains spaces, Windows may incorrectly interpret the spaces, potentially leading to the execution of unintended programs.

* Details:

Command The command vmic service get name, pathname, displayname, startmode | findstr /i auto | findstr /i /v 'C:\\Windows\\' | findstr /i /v '' filters services that are set to start automatically and are not located in the Windows directory.

Output Interpretation: The output shows a service with a path C:\Program Files\A Subfolder\B Subfolder\SomeExecutable.exe which is not quoted. If a malicious user places an executable in C:\Program.exe, C:\Program Files\A.exe, or similar, it might get executed instead.

* Reference: Common Windows privilege escalation vulnerabilities include unquoted service paths. This vulnerability is well-documented in security resources and penetration testing guides.

Question 7

Question Type: MultipleChoice

SIMULATION

A penetration tester performs several Nmap scans against the web application for a client.

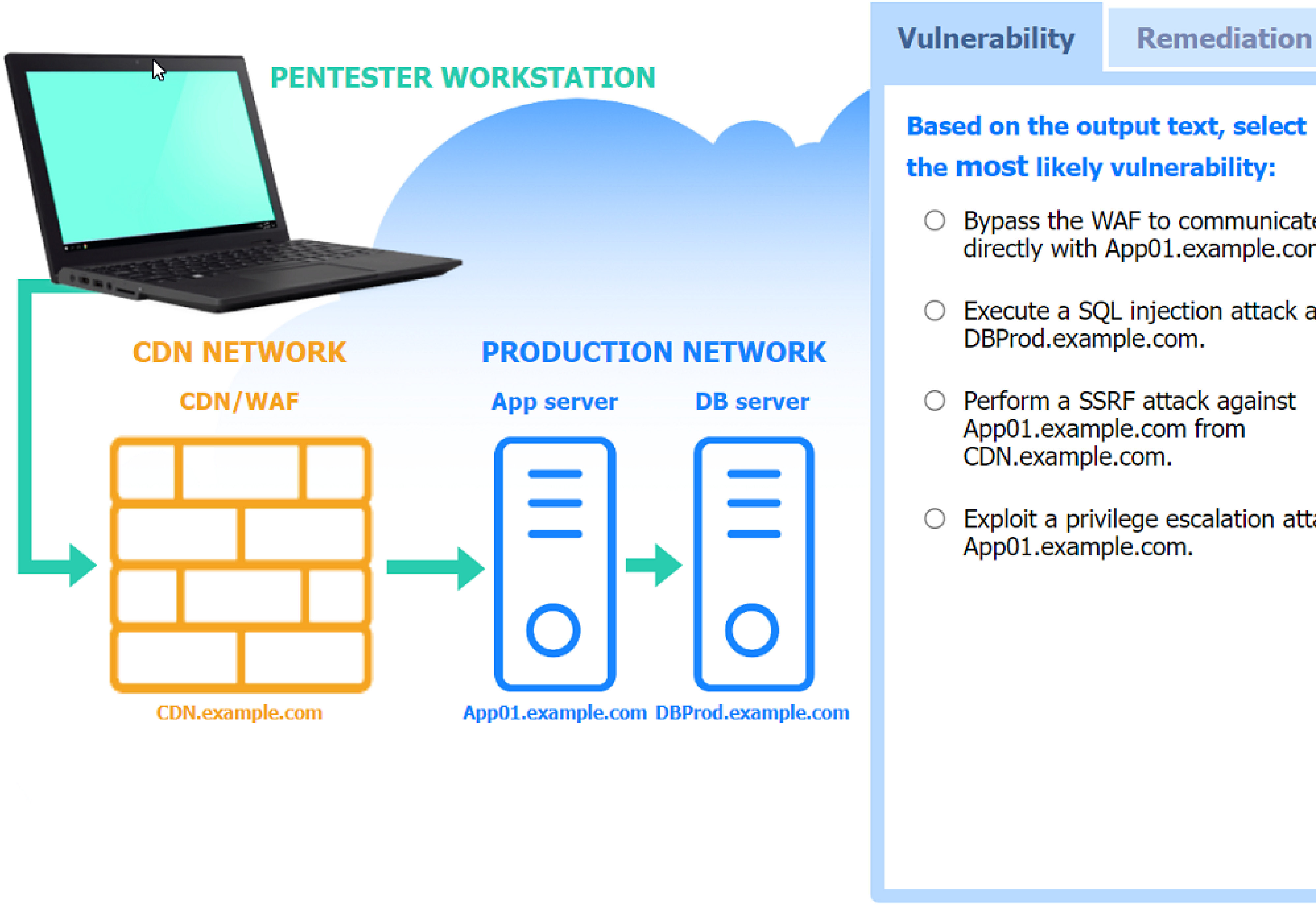
INSTRUCTIONS

Click on the WAF and servers to review the results of the Nmap scans. Then click on

each tab to select the appropriate vulnerability and remediation options.

If at any time you would like to bring back the initial state of the simulation, please

click the Reset All button.



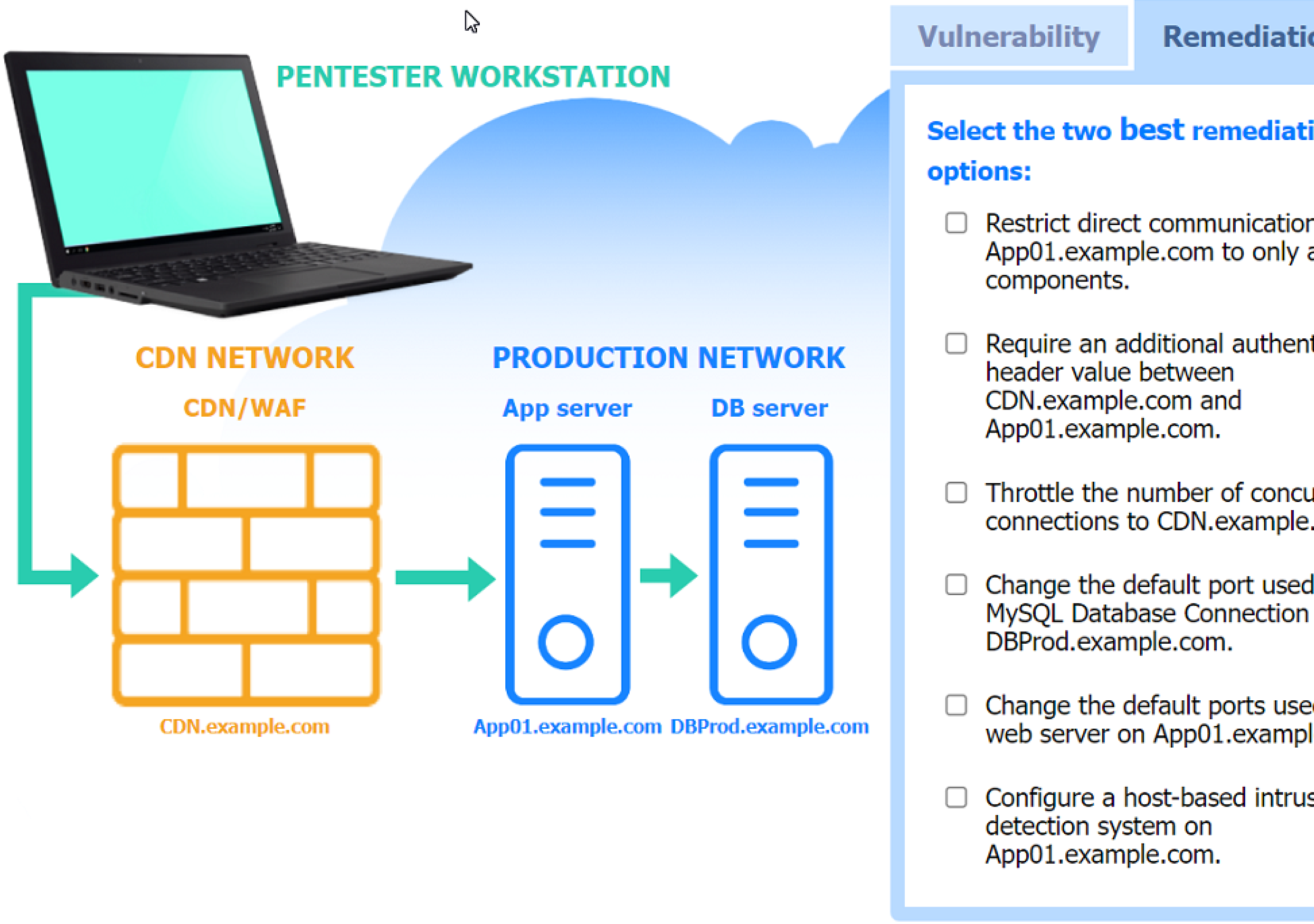
Based on the output text, select the most likely vulnerability:

○ Bypass the WAF to communicate directly with App01.example.cor

○ Execute a SQL injection attack a DBProd.example.com.

○ Perform a SSRF attack against App01.example.com from CDN.example.com.

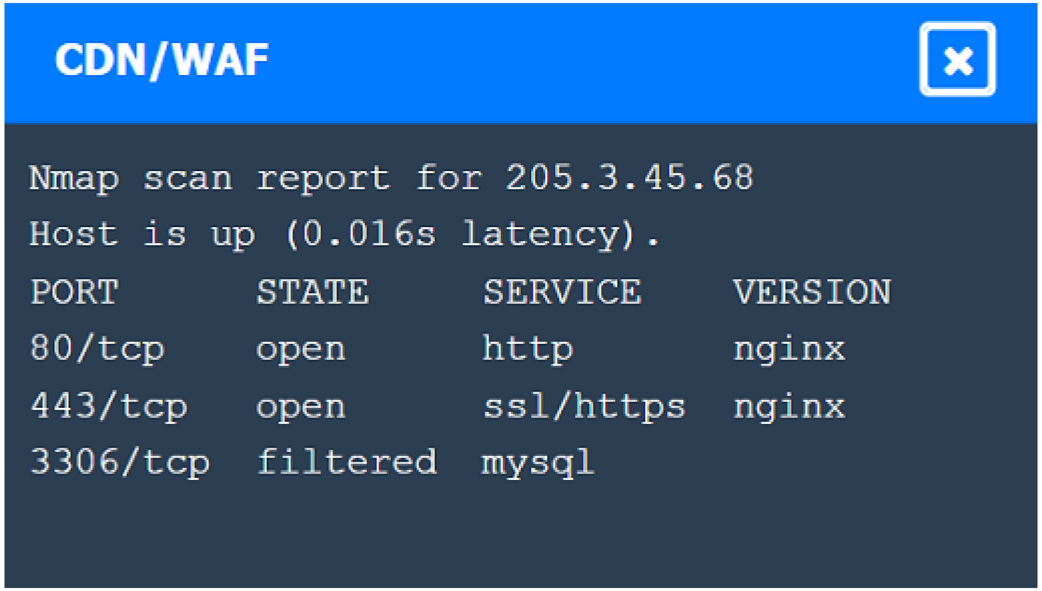
○ Exploit a privilege escalation atta App01.example.com.



Select the two best remediati

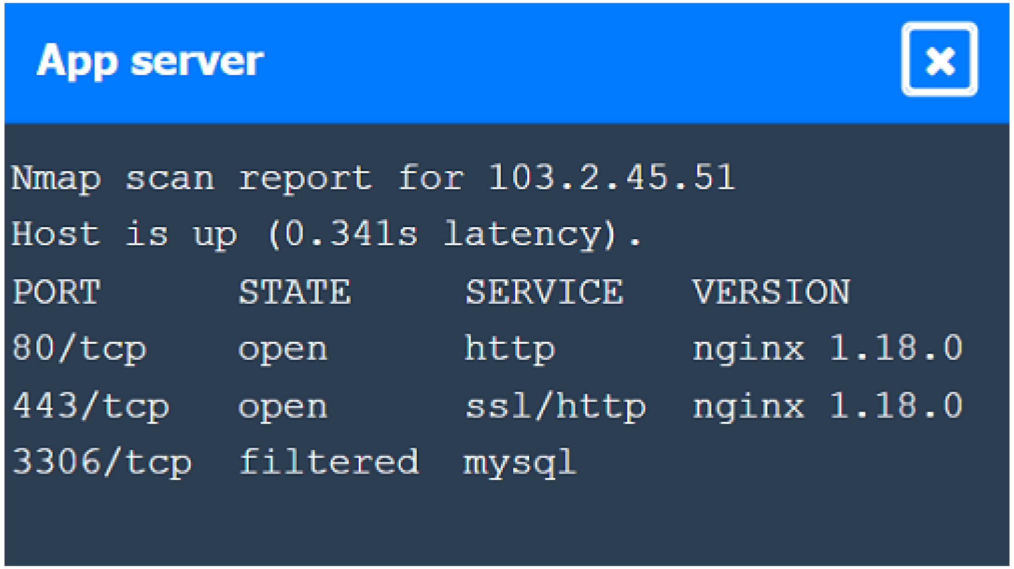
options:

- ☐ Restrict direct communicatior App01.example.com to only a components.
- ☐ Require an additional authent header value between CDN.example.com and App01.example.com.
- ☐ Throttle the number of concu connections to CDN.example.
- ☐ Change the default port used MySQL Database Connection DBProd.example.com.
- ☐ Change the default ports use web server on App01.exampl
- ☐ Configure a host-based intrus detection system on App01.example.com.



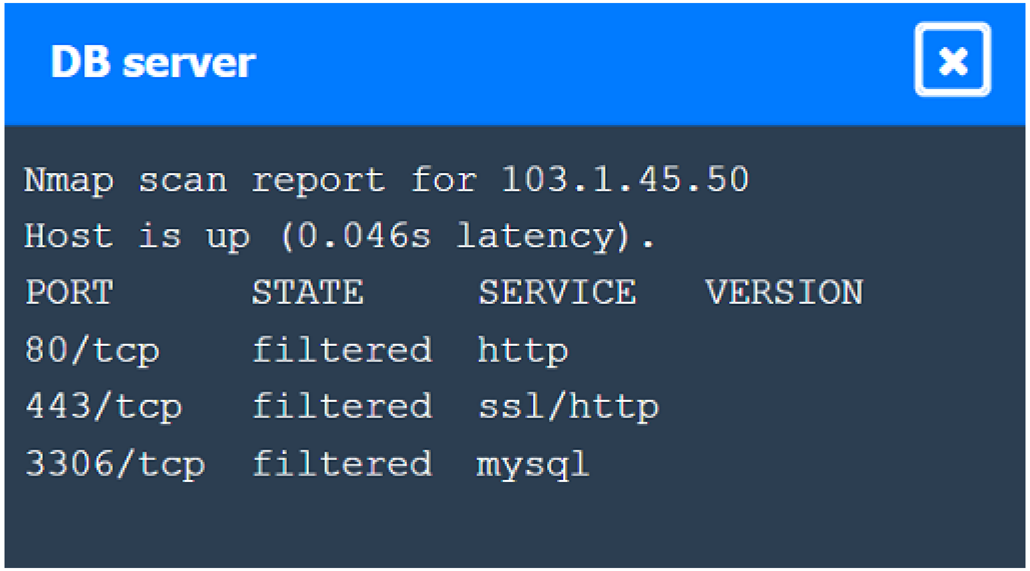
CDN/WAF

```
Nmap scan report for 205.3.45.68
Host is up (0.016s latency).
PORT      STATE     SERVICE    VERSION
80/tcp    open      http       nginx
443/tcp   open      ssl/https  nginx
3306/tcp  filtered  mysql
```



App server

```
Nmap scan report for 103.2.45.51
Host is up (0.341s latency).
PORT      STATE     SERVICE    VERSION
80/tcp    open      http       nginx 1.18.0
443/tcp   open      ssl/http   nginx 1.18.0
3306/tcp  filtered  mysql
```



```
Nmap scan report for 103.1.45.50
Host is up (0.046s latency).
PORT       STATE      SERVICE   VERSION
80/tcp     filtered   http
443/tcp    filtered   ssl/http
3306/tcp   filtered   mysql
```

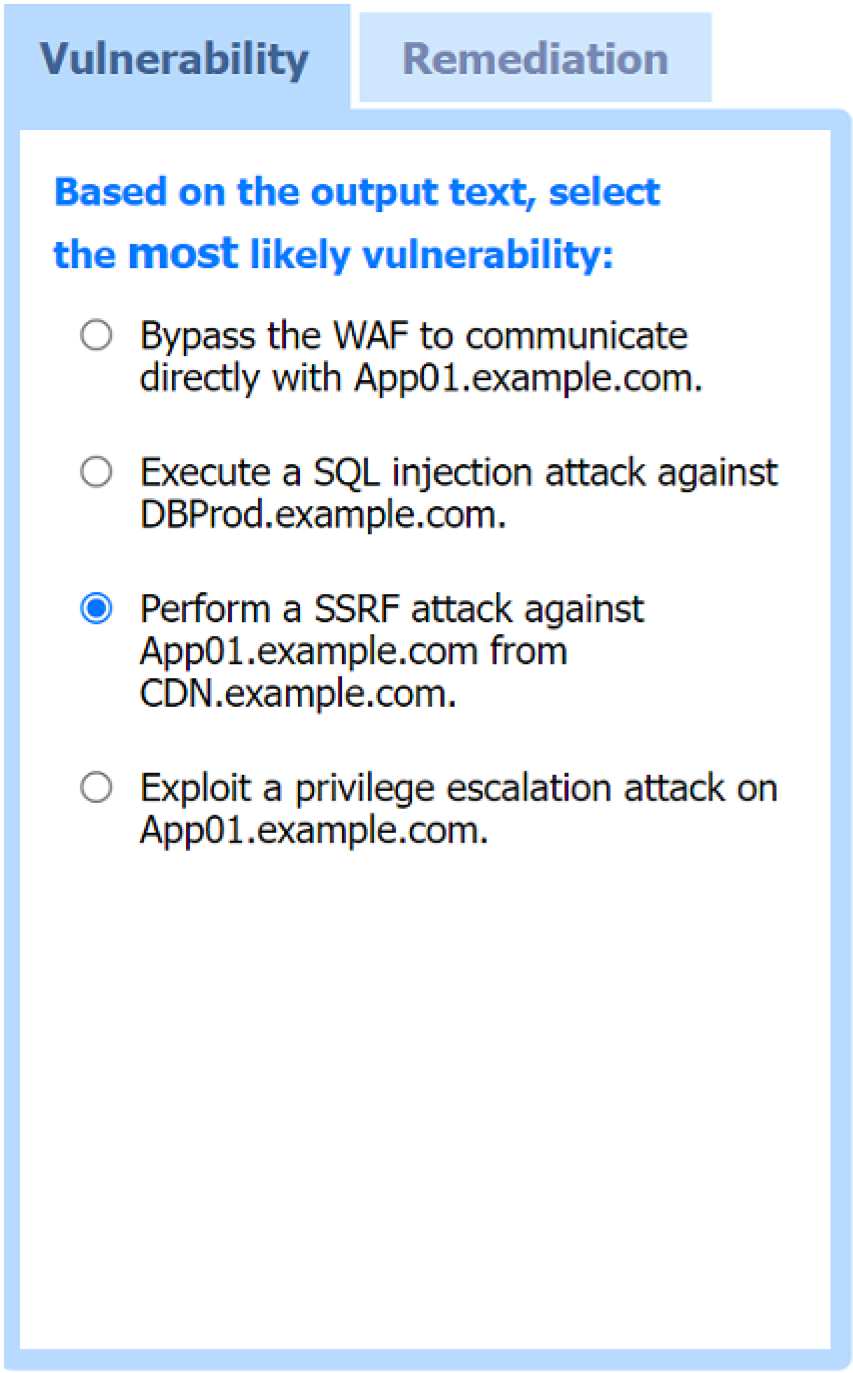
Options:

A- See the explanation part for detailed solution

Answer:

A

Explanation:



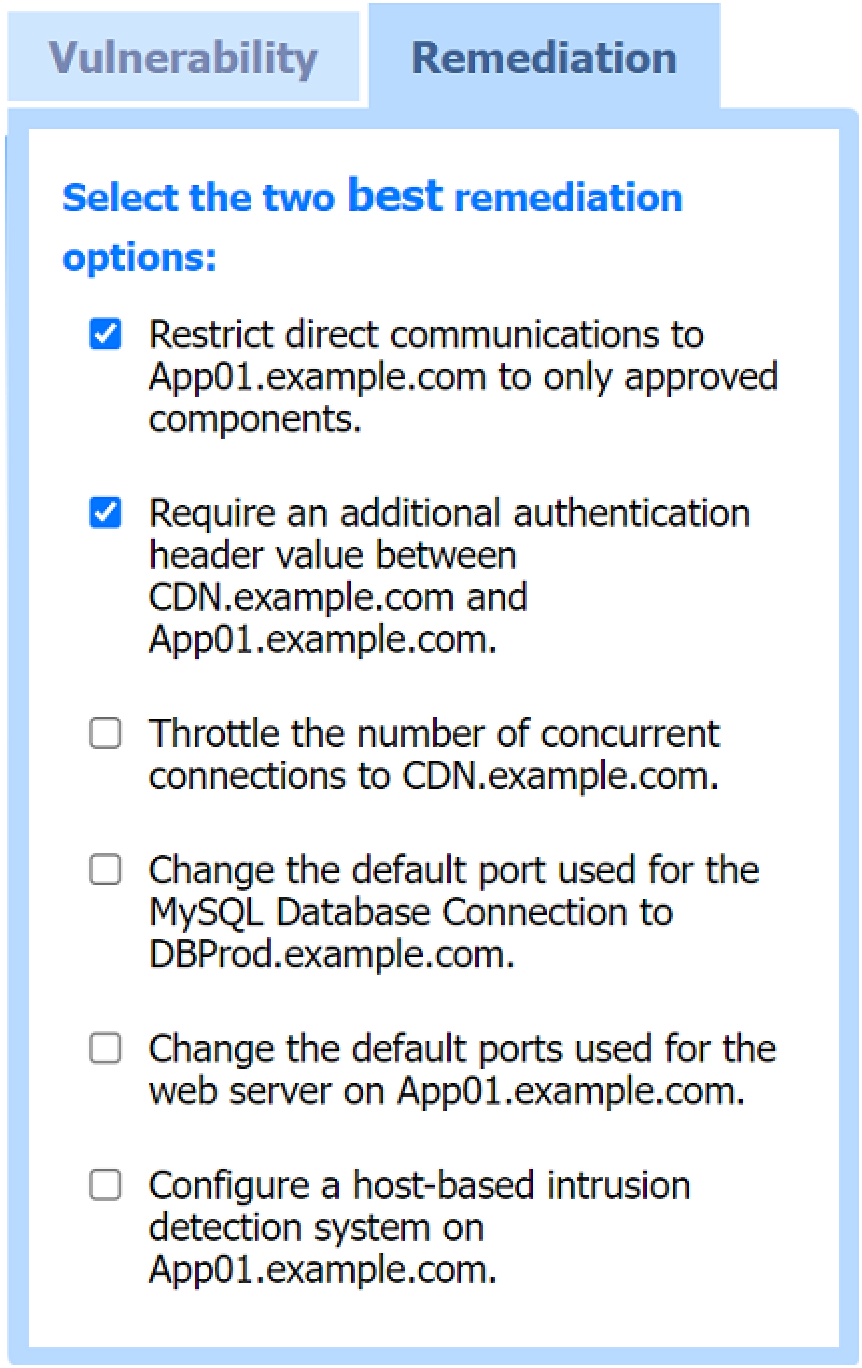
Based on the output text, select the most likely vulnerability:

○ Bypass the WAF to communicate directly with App01.example.com.

○ Execute a SQL injection attack against DBProd.example.com.

● Perform a SSRF attack against App01.example.com from CDN.example.com.

○ Exploit a privilege escalation attack on App01.example.com.



Select the two best remediation options:

- ☑ Restrict direct communications to App01.example.com to only approved components.
- ☑ Require an additional authentication header value between CDN.example.com and App01.example.com.
- ☐ Throttle the number of concurrent connections to CDN.example.com.
- ☐ Change the default port used for the MySQL Database Connection to DBProd.example.com.
- ☐ Change the default ports used for the web server on App01.example.com.
- ☐ Configure a host-based intrusion detection system on App01.example.com.

Most likely vulnerability: Perform a SSRF attack against App01.example.com from CDN.example.com.

The scenario suggests that the CDN network (with a WAF) can be used to perform a Server-Side Request Forgery (SSRF) attack. Since the penetration tester has the pentester workstation interacting through the CDN/WAF and the production network is behind it, the most plausible attack vector is to exploit SSRF to interact with the internal services like App01.example.com.

Two best remediation options:

Restrict direct communications to App01.example.com to only approved components.

Require an additional authentication header value between CDN.example.com and App01.example.com.

Restrict direct communications to App01.example.com to only approved components: This limits the exposure of the application server by ensuring that only specified, trusted entities can communicate with it.

Require an additional authentication header value between CDN.example.com and App01.example.com: Adding an authentication layer between the CDN and the app server helps ensure that requests are legitimate and originate from trusted sources, mitigating SSRF and other indirect attack vectors.

Nmap Scan Observations:

CDN/WAF shows open ports for HTTP and HTTPS but filtered for MySQL, indicating it acts as a filtering layer.

App Server has open ports for HTTP, HTTPS, and filtered for MySQL.

DB Server has all ports filtered, typical for a database server that should not be directly accessible.

These findings align with the SSRF vulnerability and the appropriate remediation steps to enhance the security of internal communications.

20%
DISCOUNT