LEAD2PASS

First Test, First Pass!

Vendor: CompTIA

Exam Code: PT0-003

Exam Name: CompTIA PenTest+ Exam: PT0-003 Exam

Version: DEMO

QUESTION 1
A penetration tester downloads a JAR file that is used in an organization's production environment. The tester evaluates the contents of the JAR file to identify potentially vulnerable components that can be targeted for exploit. Which of the following describes the tester's activities?

A. SAST
B. SBOM
C. ICS
D. SCA

Answer: D
Explanation:
The tester's activity involves analyzing the contents of a JAR file to identify potentially vulnerable components. This process is known as Software Composition Analysis (SCA).
Definition: SCA involves analyzing software to identify third-party and open-source components, checking for known vulnerabilities, and ensuring license compliance.
Purpose: To detect and manage risks associated with third-party software components.

QUESTION 2
During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

A. Segmentation
B. Mobile
C. External
D. Web

Answer: C
Explanation:
An external assessment focuses on testing the security of internet-facing services.
External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by attackers from outside the organization's network.
Segmentation: This type of assessment focuses on ensuring that different parts of a network are appropriately segmented to limit the spread of attacks. It's more relevant to internal network architecture.
Mobile: This assessment targets mobile applications and devices, not general internet-facing services.
Web: While web assessments focus on web applications, the scope of an external assessment is broader and includes all types of internet-facing services.

QUESTION 3
A penetration tester has just started a new engagement. The tester is using a framework that breaks the life cycle into 14 components. Which of the following frameworks is the tester using?

A. OWASP MASVS
B. OSSTMM
C. MITRE ATT&CK
D. CREST

Answer: B
Explanation:
The OSSTMM (Open Source Security Testing Methodology Manual) is a comprehensive framework for security testing that includes 14 components in its life cycle.
OSSTMM: This methodology breaks down the security testing process into 14 components, covering various aspects of security assessment, from planning to execution and reporting.
OWASP MASVS: This is a framework for mobile application security verification and does not have a 14-component life cycle.
MITRE ATT&CK: This is a knowledge base of adversary tactics and techniques but does not describe a 14-component life cycle.
CREST: This is a certification body for penetration testers and security professionals but does not provide a specific 14-component framework.

QUESTION 4
A penetration tester is evaluating a SCADA system. The tester receives local access to a workstation that is running a single application. While navigating through the application, the tester opens a terminal window and gains access to the underlying operating system. Which of the following attacks is the tester performing?

A. Kiosk escape
B. Arbitrary code execution
C. Process hollowing
D. Library injection

Answer: A
Explanation:
A kiosk escape involves breaking out of a restricted environment, such as a kiosk or a single application interface, to access the underlying operating system.
Kiosk Escape: This attack targets environments where user access is intentionally limited, such as a kiosk or a dedicated application. The goal is to break out of these restrictions and gain access to the full operating system.
Arbitrary Code Execution: This involves running unauthorized code on the system, but the scenario described is more about escaping a restricted environment.
Process Hollowing: This technique involves injecting code into a legitimate process, making it appear benign while executing malicious activities.
Library Injection: This involves injecting malicious code into a running process by loading a malicious library, which is not the focus in this scenario.

QUESTION 5
A penetration tester presents the following findings to stakeholders:

Control	Number of findings	Risk	Notes
Encryption	1	Low	Weak algorithm noted
Patching	8	Medium	Unsupported systems
System hardening	2	Low	Baseline drift observed
Secure SDLC	10	High	Libraries have vulnerabilities
Password policy	0	Low	No exceptions noted

Based on the findings, which of the following recommendations should the tester make? (Select two).

A. Develop a secure encryption algorithm.

B. Deploy an asset management system.
C. Write an SDLC policy.
D. Implement an SCA tool.
E. Obtain the latest library version.
F. Patch the libraries.

Answer: DE
Explanation:
Based on the findings, the focus should be on addressing vulnerabilities in libraries and ensuring their security.
Implement an SCA Tool:
SCA (Software Composition Analysis) tools are designed to analyze and manage open-source components in an application. Implementing an SCA tool would help in identifying and managing vulnerabilities in libraries, aligning with the finding of vulnerable libraries in the secure SDLC process. This recommendation addresses the high-risk finding related to the Secure SDLC by providing a systematic approach to manage and mitigate vulnerabilities in software dependencies.
Obtain the Latest Library Version:
Keeping libraries up to date is a fundamental practice in maintaining the security of an application. Ensuring that the latest, most secure versions of libraries are used directly addresses the high-risk finding related to vulnerable libraries.
This recommendation is a direct and immediate action to mitigate the identified vulnerabilities.

QUESTION 6
While conducting a reconnaissance activity, a penetration tester extracts the following information:

```
Emails: - admin@acme.com - sales@acme.com - support@acme.com
```

Which of the following risks should the tester use to leverage an attack as the next step in the security assessment?

A. Unauthorized access to the network
B. Exposure of sensitive servers to the internet
C. Likelihood of SQL injection attacks
D. Indication of a data breach in the company

Answer: A
Explanation:
When a penetration tester identifies email addresses during reconnaissance, the most immediate risk to leverage for an attack is unauthorized access to the network.
Phishing Attacks:
Email addresses are often used to conduct phishing attacks. By crafting a convincing email, an attacker can trick the recipient into revealing their login credentials or downloading malicious software, thereby gaining unauthorized access to the network.
Spear Phishing:
With specific email addresses (like admin@acme.com), attackers can perform spear phishing, targeting key individuals within the organization to gain access to more sensitive parts of the network.

QUESTION 7
A penetration tester gains access to a host but does not have access to any type of shell. Which

of the following is the best way for the tester to further enumerate the host and the environment in which it resides?

A. ProxyChains
B. Netcat
C. PowerShell ISE
D. Process IDs

Answer: B
Explanation:
If a penetration tester gains access to a host but does not have a shell, the best tool for further enumeration is Netcat.
Netcat:
Versatility: Netcat is known as the "Swiss Army knife" of networking tools. It can be used for port scanning, banner grabbing, and setting up reverse shells.
Enumeration: Without a shell, Netcat can help enumerate open ports and services running on the host, providing insight into the host's environment.

QUESTION 8
A penetration tester has found a web application that is running on a cloud virtual machine instance. Vulnerability scans show a potential SSRF for the same application URL path with an injectable parameter. Which of the following commands should the tester run to successfully test for secrets exposure exploitability?

A. curl <url>?param=http://169.254.169.254/latest/meta-data/
B. curl '<url>?param=http://127.0.0.1/etc/passwd'
C. curl '<url>?param=<script>alert(1)<script>/'
D. curl <url>?param=http://127.0.0.1/

Answer: A
Explanation:
In a cloud environment, testing for Server-Side Request Forgery (SSRF) vulnerabilities involves attempting to access metadata services.
Accessing Cloud Metadata Service:
URL: http://169.254.169.254/latest/meta-data/ is a well-known endpoint in cloud environments (e.g., AWS) to access instance metadata.
Purpose: By exploiting SSRF to access this URL, an attacker can retrieve sensitive information such as instance credentials and other metadata.

QUESTION 9
A penetration tester cannot find information on the target company's systems using common OSINT methods. The tester's attempts to do reconnaissance against internet-facing resources have been blocked by the company's WAF. Which of the following is the best way to avoid the WAF and gather information about the target company's systems?

A. HTML scraping
B. Code repository scanning
C. Directory enumeration
D. Port scanning

Answer: B
Explanation:

When traditional reconnaissance methods are blocked, scanning code repositories is an effective method to gather information.
Code Repository Scanning:
Leaked Information: Code repositories (e.g., GitHub, GitLab) often contain sensitive information, including API keys, configuration files, and even credentials that developers might inadvertently commit.
Accessible: These repositories can often be accessed publicly, bypassing traditional defenses like WAFs.

QUESTION 10
During a penetration test, the tester uses a vulnerability scanner to collect information about any possible vulnerabilities that could be used to compromise the network. The tester receives the results and then executes the following command:

```
snmpwalk -v 2c -c public 192.168.1.23
```

Which of the following is the tester trying to do based on the command they used?

A. Bypass defensive systems to collect more information.
B. Use an automation tool to perform the attacks.
C. Script exploits to gain access to the systems and host.
D. Validate the results and remove false positives.

Answer: D
Explanation:
The command snmpwalk -v 2c -c public 192.168.1.23 is used to query SNMP (Simple Network Management Protocol) data from a device.
SNMP Enumeration:
Function: snmpwalk is used to retrieve a large amount of information from the target device using SNMP.
Version: -v 2c specifies the SNMP version.
Community String: -c public specifies the community string, which is essentially a password for SNMP queries.
Purpose of the Command:
Validate Results: The tester uses SNMP to gather detailed information about the network devices to confirm the findings of the vulnerability scanner and remove any false positives.
Detailed Information: SNMP can provide detailed information about device configurations, network interfaces, and other settings that can validate the scanner's results.

QUESTION 11
A penetration tester is working on a security assessment of a mobile application that was developed in-house for local use by a hospital. The hospital and its customers are very concerned about disclosure of information. Which of the following tasks should the penetration tester do first?

A. Set up Drozer in order to manipulate and scan the application.
B. Run the application through the mobile application security framework.
C. Connect Frida to analyze the application at runtime to look for data leaks.
D. Load the application on client-owned devices for testing.

Answer: B
Explanation:
When performing a security assessment on a mobile application, especially one concerned with

information disclosure, it is crucial to follow a structured approach to identify vulnerabilities comprehensively.
Mobile Application Security Framework: This framework provides a structured methodology for assessing the security of mobile applications. It includes various tests such as static analysis, dynamic analysis, and reverse engineering, which are essential for identifying vulnerabilities related to information disclosure.
Initial Steps: Running the application through a security framework allows the tester to identify a broad range of potential issues systematically. This initial step ensures that all aspects of the application's security are covered before delving into more specific tools like Drozer or Frida.

QUESTION 12
Before starting an assessment, a penetration tester needs to scan a Class B IPv4 network for open ports in a short amount of time. Which of the following is the best tool for this task?

A. Burp Suite
B. masscan
C. Nmap
D. hping

Answer: B
Explanation:
When needing to scan a large network for open ports quickly, the choice of tool is critical.
masscan: This tool is designed for high-speed port scanning and can scan entire networks much faster than traditional tools like Nmap. It can handle large ranges of IP addresses and ports with high efficiency.
Nmap: While powerful and versatile, Nmap is generally slower than masscan for scanning very large networks, especially when speed is crucial.
Burp Suite: This tool is primarily for web application security testing and not optimized for network- wide port scanning.
hping: This is a network tool used for packet crafting and network testing, but it is not designed for high-speed network port scanning.

QUESTION 13
A penetration tester is performing an authorized physical assessment. During the test, the tester observes an access control vestibule and on-site security guards near the entry door in the lobby. Which of the following is the best attack plan for the tester to use in order to gain access to the facility?

A. Clone badge information in public areas of the facility to gain access to restricted areas.
B. Tailgate into the facility during a very busy time to gain initial access.
C. Pick the lock on the rear entrance to gain access to the facility and try to gain access.
D. Drop USB devices with malware outside of the facility in order to gain access to internal machines.

Answer: B
Explanation:
In an authorized physical assessment, the goal is to test physical security controls. Tailgating is a common and effective technique in such scenarios.
Tailgating: This involves following an authorized person into a secure area without proper credentials. During busy times, it's easier to blend in and gain access without being noticed. It tests the effectiveness of physical access controls and security personnel.
Cloning Badge Information: This can be effective but requires proximity to employees and specialized equipment, making it more complex and time-consuming.
Picking Locks: This is a more invasive technique that carries higher risk and is less stealthy

compared to tailgating.
Dropping USB Devices: This tests employee awareness and response to malicious devices but does not directly test physical access controls.

QUESTION 14
During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?

A. SQL injection
B. SSRF
C. XSS
D. Server-side template injection

Answer: C
Explanation:
Cross-Site Scripting (XSS) is an attack that involves injecting malicious scripts into web pages viewed by other users.
XSS (Cross-Site Scripting): This attack involves injecting JavaScript into a web application, which is then executed by the user's browser. The scenario describes injecting a JavaScript prompt, which is a typical XSS payload.
SQL Injection: This involves injecting SQL commands to manipulate the database and does not relate to JavaScript injection.
SSRF (Server-Side Request Forgery): This attack tricks the server into making requests to unintended locations, which is not related to client-side JavaScript execution.
Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in the user's browser.

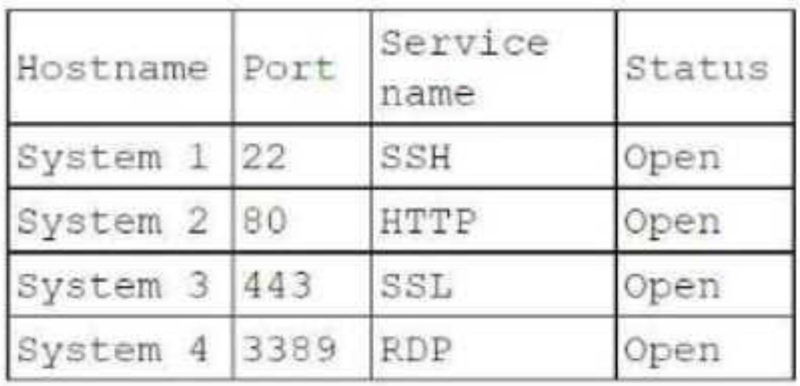
QUESTION 15
A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack. During the engagement, the tester is able to obtain an internal foothold on the target network. Which of the following is the next task the tester should complete to accomplish the objective?

A. Initiate a social engineering campaign.
B. Perform credential dumping.
C. Compromise an endpoint.
D. Share enumeration.

Answer: B
Explanation:
Given that the penetration tester has already obtained an internal foothold on the target network, the next logical step to achieve the objective of collecting confidential information and potentially exfiltrating data or performing a ransomware attack is to perform credential dumping.
Purpose: Credential dumping involves extracting password hashes and plaintext passwords from compromised systems. These credentials can be used to gain further access to sensitive data and critical systems within the network.
Tools: Common tools used for credential dumping include Mimikatz, Windows Credential Editor, and ProcDump.
Impact: With these credentials, the tester can move laterally across the network, escalate privileges, and access confidential information.

QUESTION 16

During a penetration test, the tester identifies several unused services that are listening on all targeted internal laptops. Which of the following technical controls should the tester recommend to reduce the risk of compromise?



Hostname	Port	Service name	Status
System 1	22	SSH	Open
System 2	80	HTTP	Open
System 3	443	SSL	Open
System 4	3389	RDP	Open

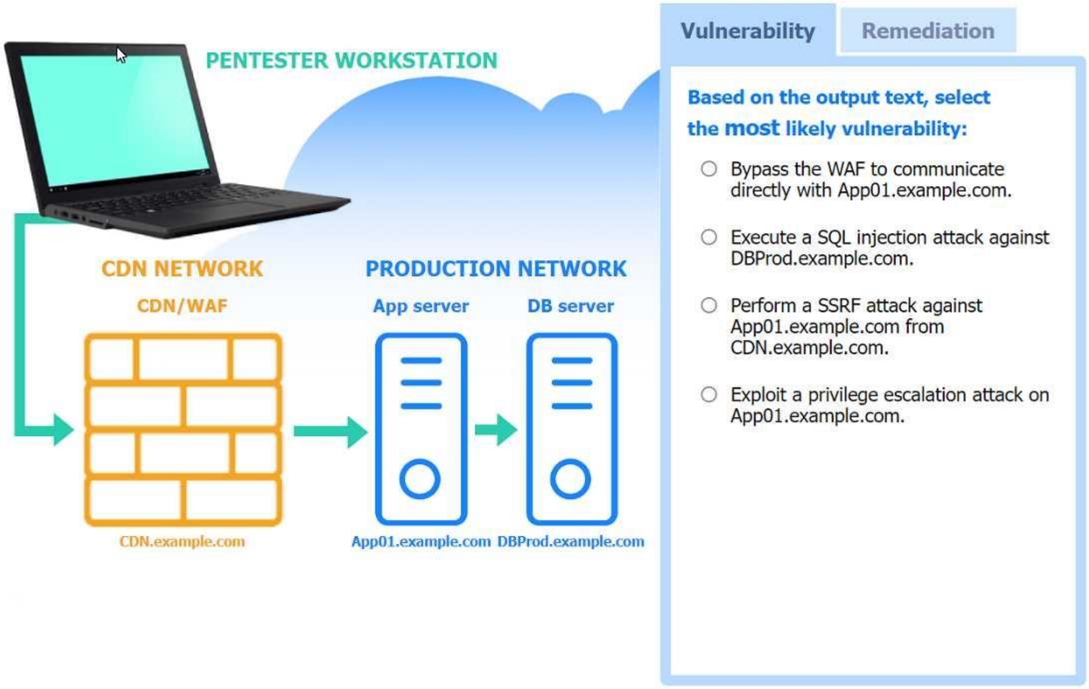
A. Multifactor authentication
B. Patch management
C. System hardening
D. Network segmentation

Answer: C
Explanation:
When a penetration tester identifies several unused services listening on targeted internal laptops, the most appropriate recommendation to reduce the risk of compromise is system hardening.
System Hardening:
Purpose: System hardening involves securing systems by reducing their surface of vulnerability. This includes disabling unnecessary services, applying security patches, and configuring systems securely.
Impact: By disabling unused services, the attack surface is minimized, reducing the risk of these services being exploited by attackers.

QUESTION 17
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.



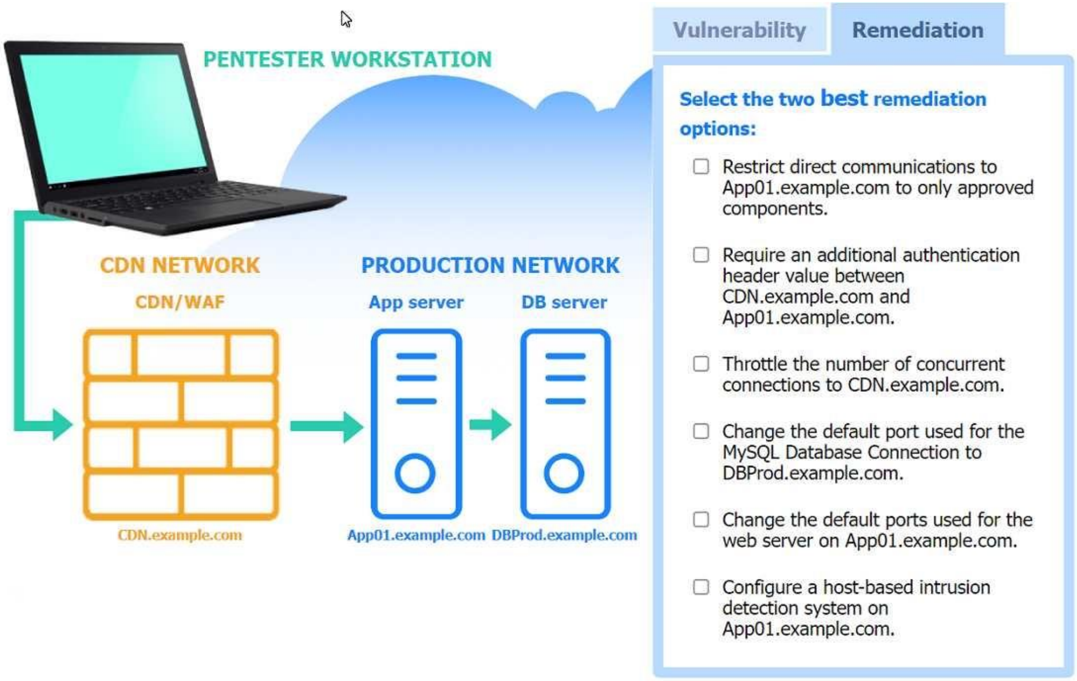
Based on the output text, select the most likely vulnerability:

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

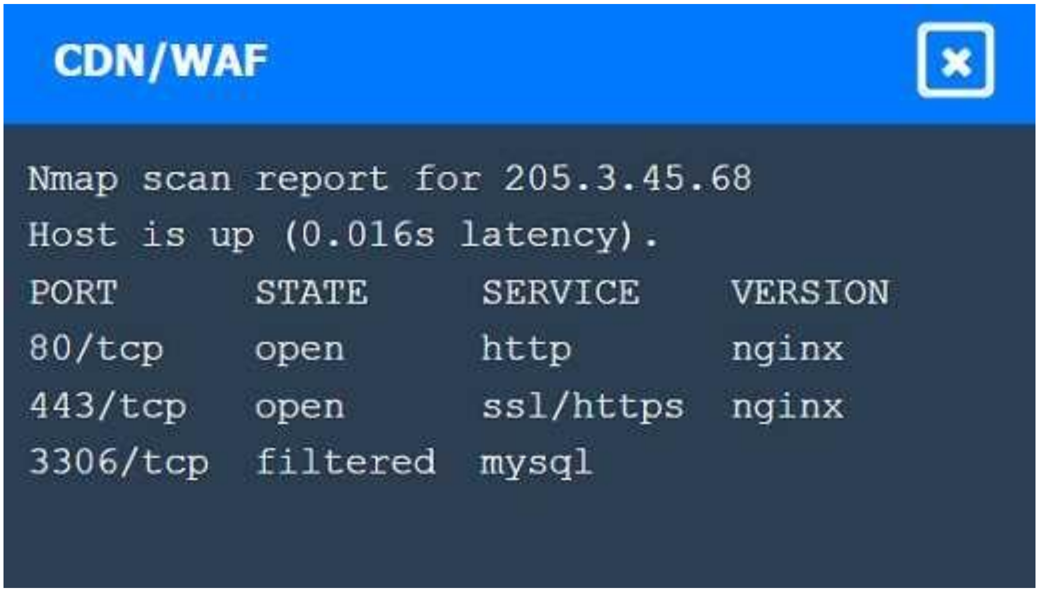
□ Require an additional authentication header value between CDN.example.com and App01.example.com.

□ Throttle the number of concurrent connections to CDN.example.com.

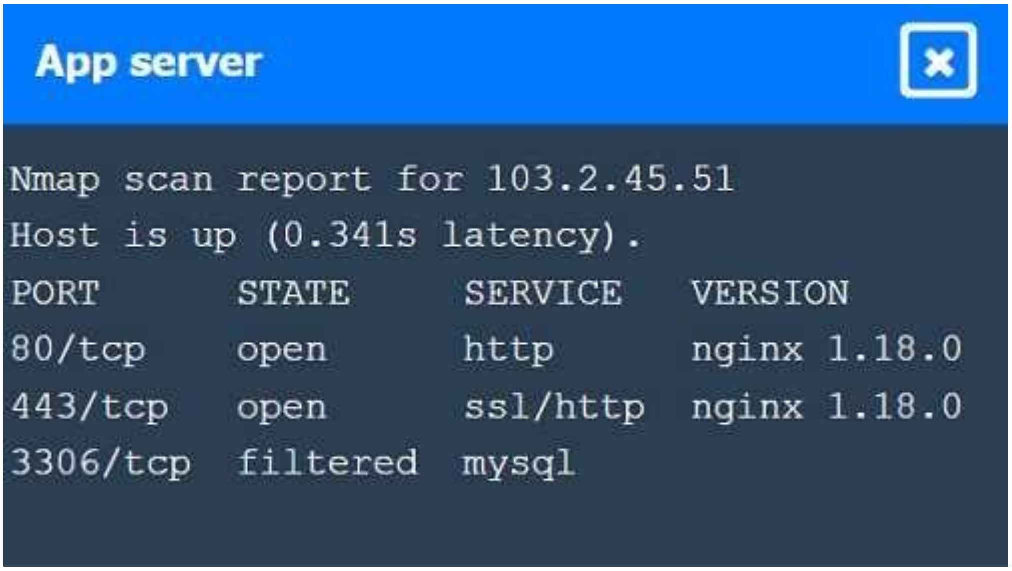
□ Change the default port used for the MySQL Database Connection to DBProd.example.com.

□ Change the default ports used for the web server on App01.example.com.

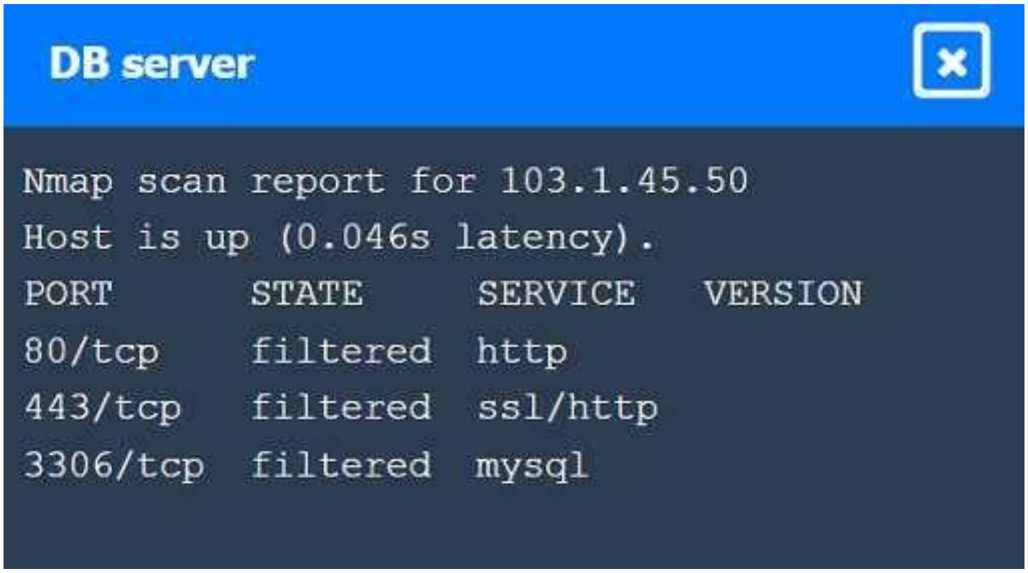
□ Configure a host-based intrusion detection system on App01.example.com.



```
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
```

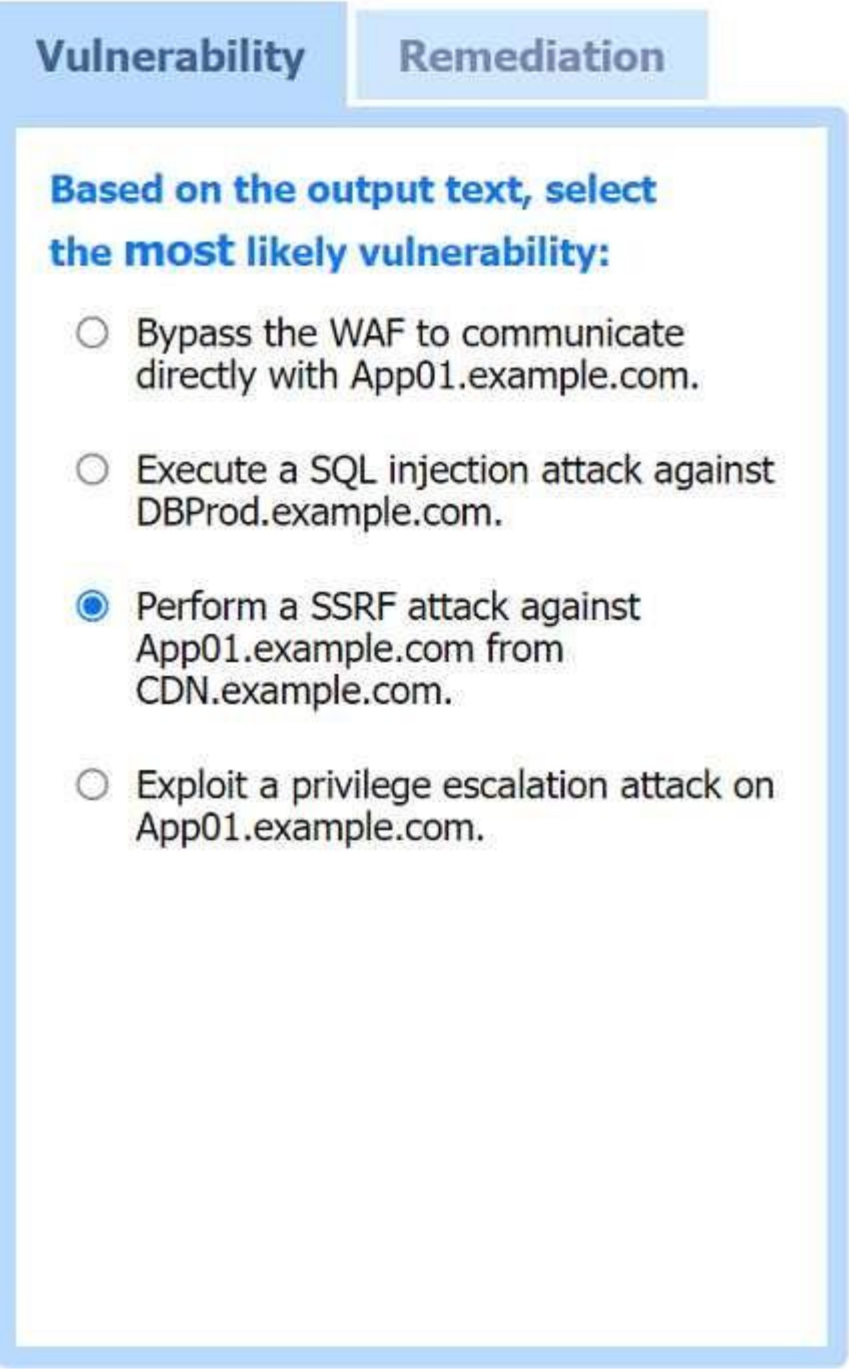


```
Nmap scan report for 103.2.45.51
Host is up (0.341s latency).
PORT      STATE     SERVICE   VERSION
80/tcp    open      http      nginx 1.18.0
443/tcp   open      ssl/http  nginx 1.18.0
3306/tcp  filtered  mysql
```



```
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
```

Answer:



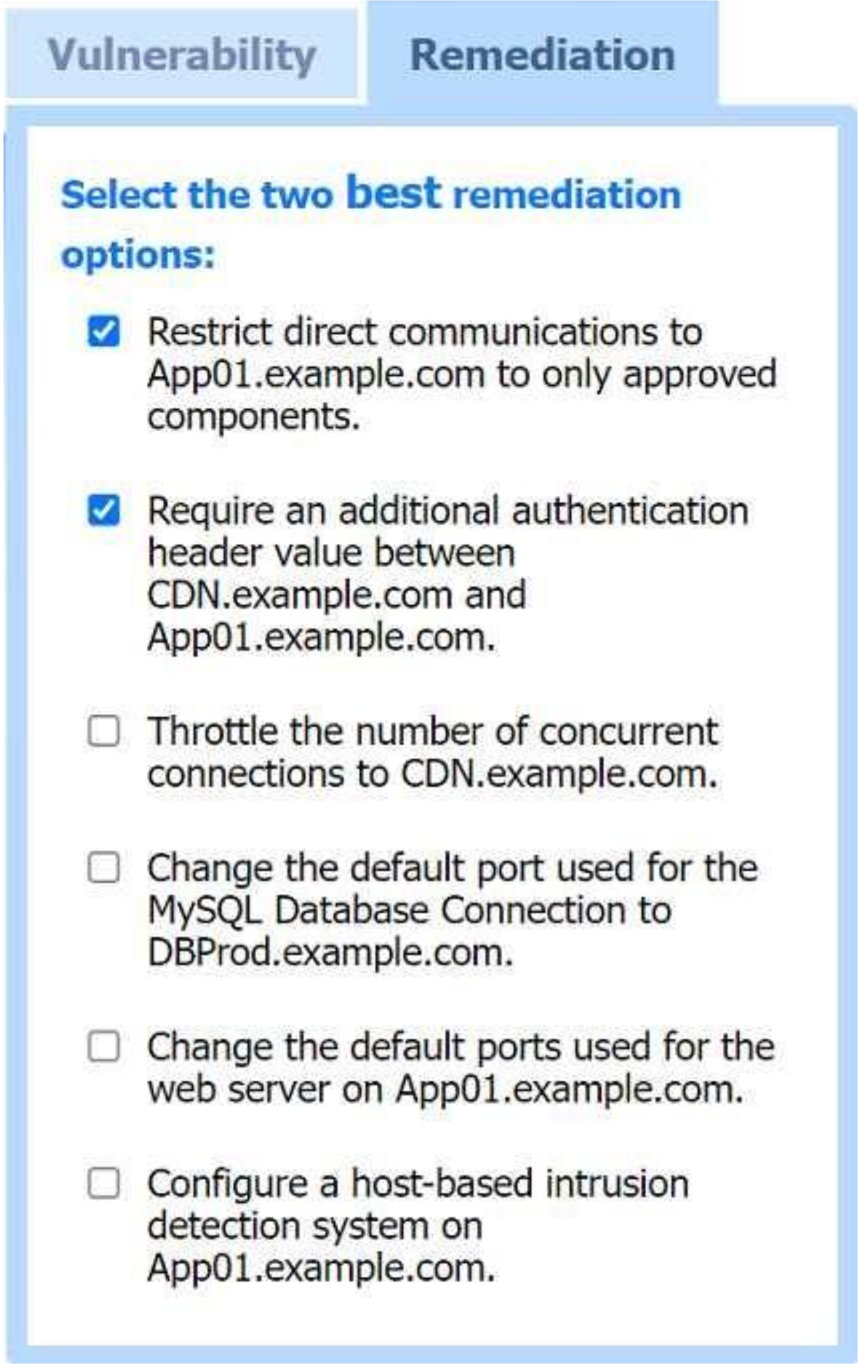
Based on the output text, select the most likely vulnerability:

○ 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.