DUMPSBOSS.

CompTIA PenTest+ Certification Exam

CompTIA PT0-001

Version Demo

Total Demo Questions: 15

Total Premium Questions: 244

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A penetration tester has been assigned to perform an external penetration assessment of a company. Which of the following steps would BEST help with the passive-information-gathering process?

(Choose two.)

A. Wait outside of the company's building and attempt to tailgate behind an employee.

B. Perform a vulnerability scan against the company's external netblock, identify exploitable vulnerabilities, and attempt to gain access.

C. Use domain and IP registry websites to identify the company's external netblocks and external facing applications.

D. Search social media for information technology employees who post information about the technologies they work with.

E. Identify the company's external facing webmail application, enumerate user accounts and attempt password guessing to gain access.

ANSWER: C D

QUESTION NO: 2

A recently concluded penetration test revealed that a legacy web application is vulnerable to SQL injection. Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not in a position to risk the availability on the application. Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Choose two.)

A. Identity and eliminate inline SQL statements from the code.

B. Identify and eliminate dynamic SQL from stored procedures.

C. Identify and sanitize all user inputs.

D. Use a whitelist approach for SQL statements.

E. Use a blacklist approach for SQL statements.

F. Identify the source of malicious input and block the IP address.

ANSWER: C D

QUESTION NO: 3

A penetration tester is performing a code review. Which of the following testing techniques is being performed?

A. Dynamic analysis

B. Fuzzing analysis

C. Static analysis

D. Run-time analysis

ANSWER: C

Explanation:

Reference: https://smartbear.com/learn/code-review/what-is-code-review/

QUESTION NO: 4

An Internet-accessible database server was found with the following ports open: 22, 53, 110, 1433, and 3389. Which of the following would be the BEST hardening technique to secure the server?

A. Ensure all protocols are using encryption.

B. Employ network ACLs.

C. Disable source routing on the server.

D. Ensure the IDS rules have been updated.

ANSWER: B

QUESTION NO: 5

A security consultant receives a document outlining the scope of an upcoming penetration test. This document contains IP addresses and times that each can be scanned. Which of the following would contain this information?

A. Rules of engagement

B. Request for proposal

C. Master service agreement

D. Business impact analysis

ANSWER: A

QUESTION NO: 6 - (SIMULATION)

SIMULATION

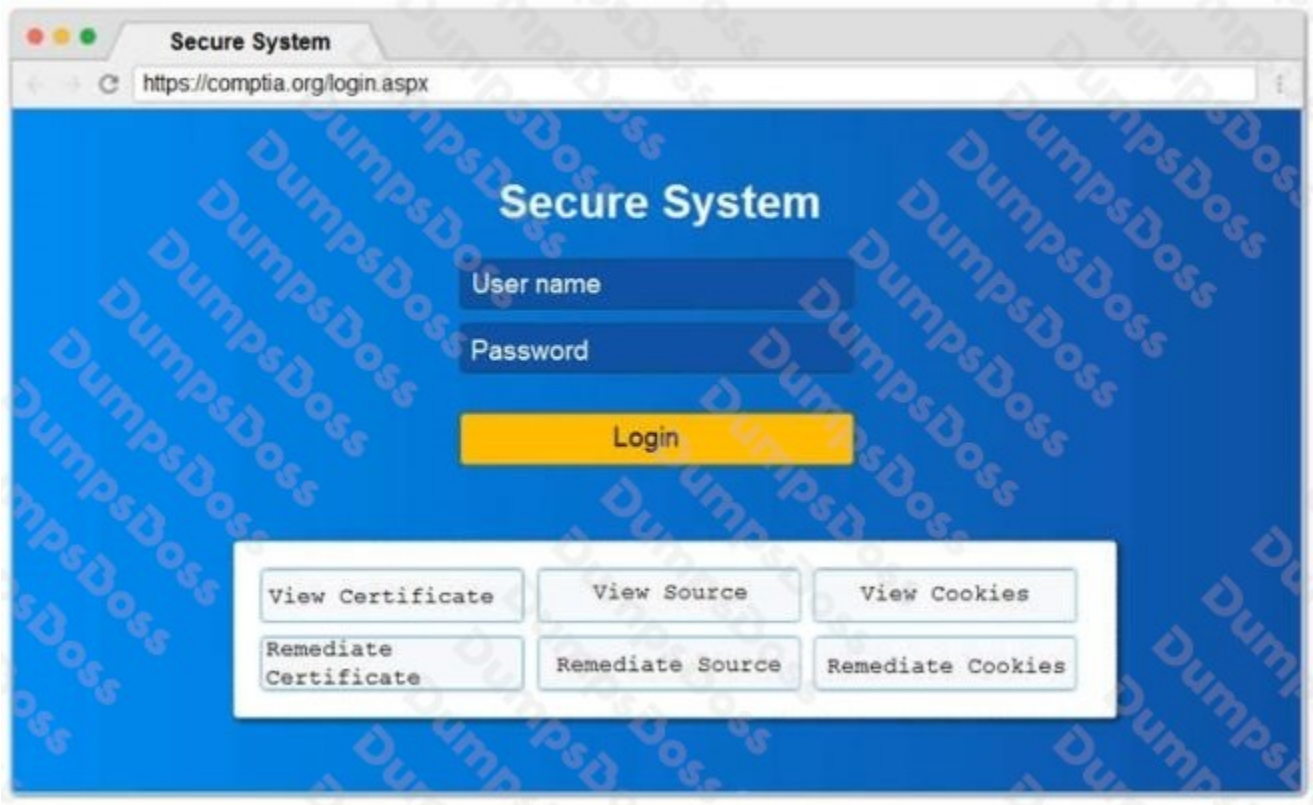
You are a penetration tester reviewing a client's website through a web browser.

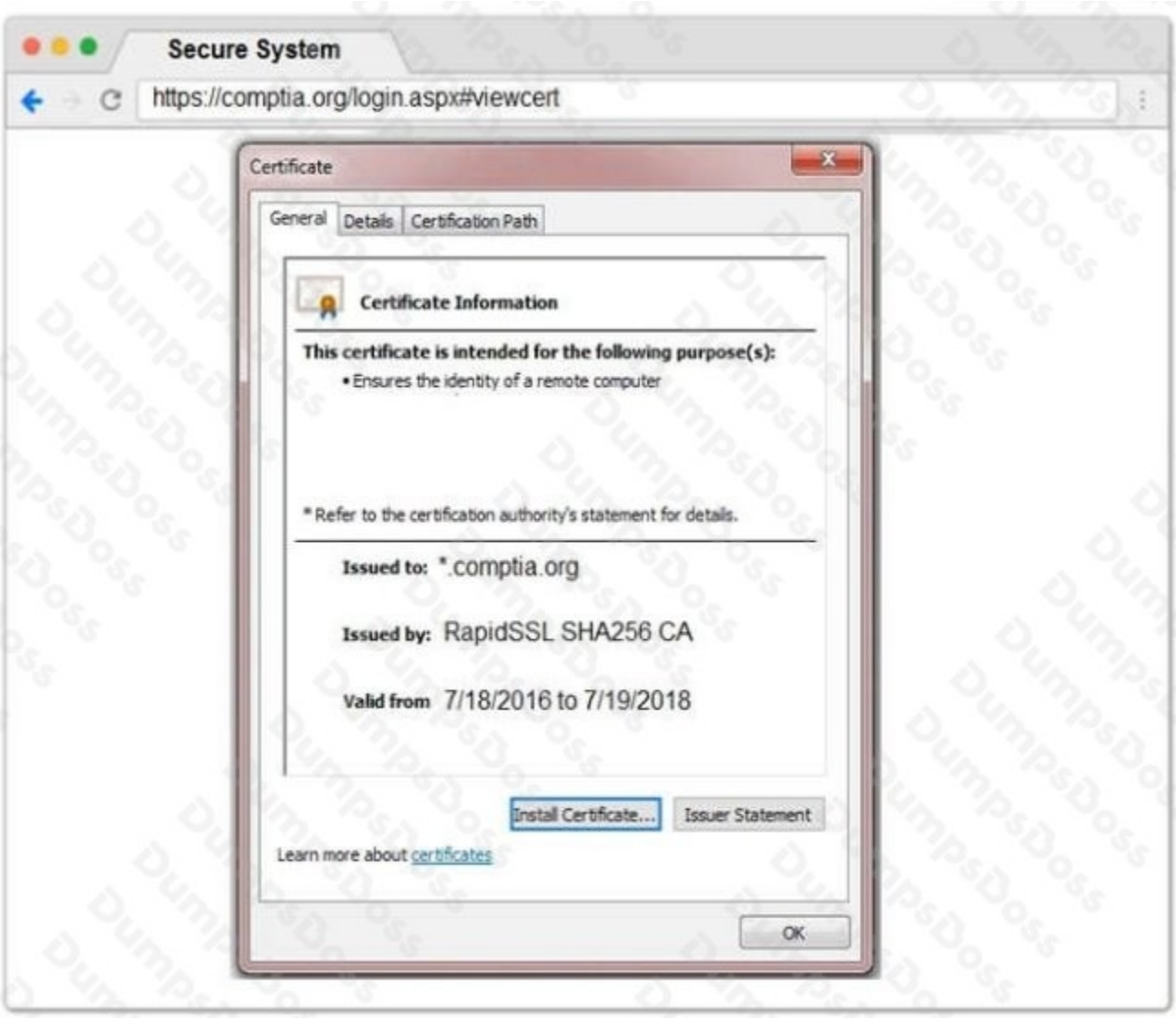
INSTRUCTIONS

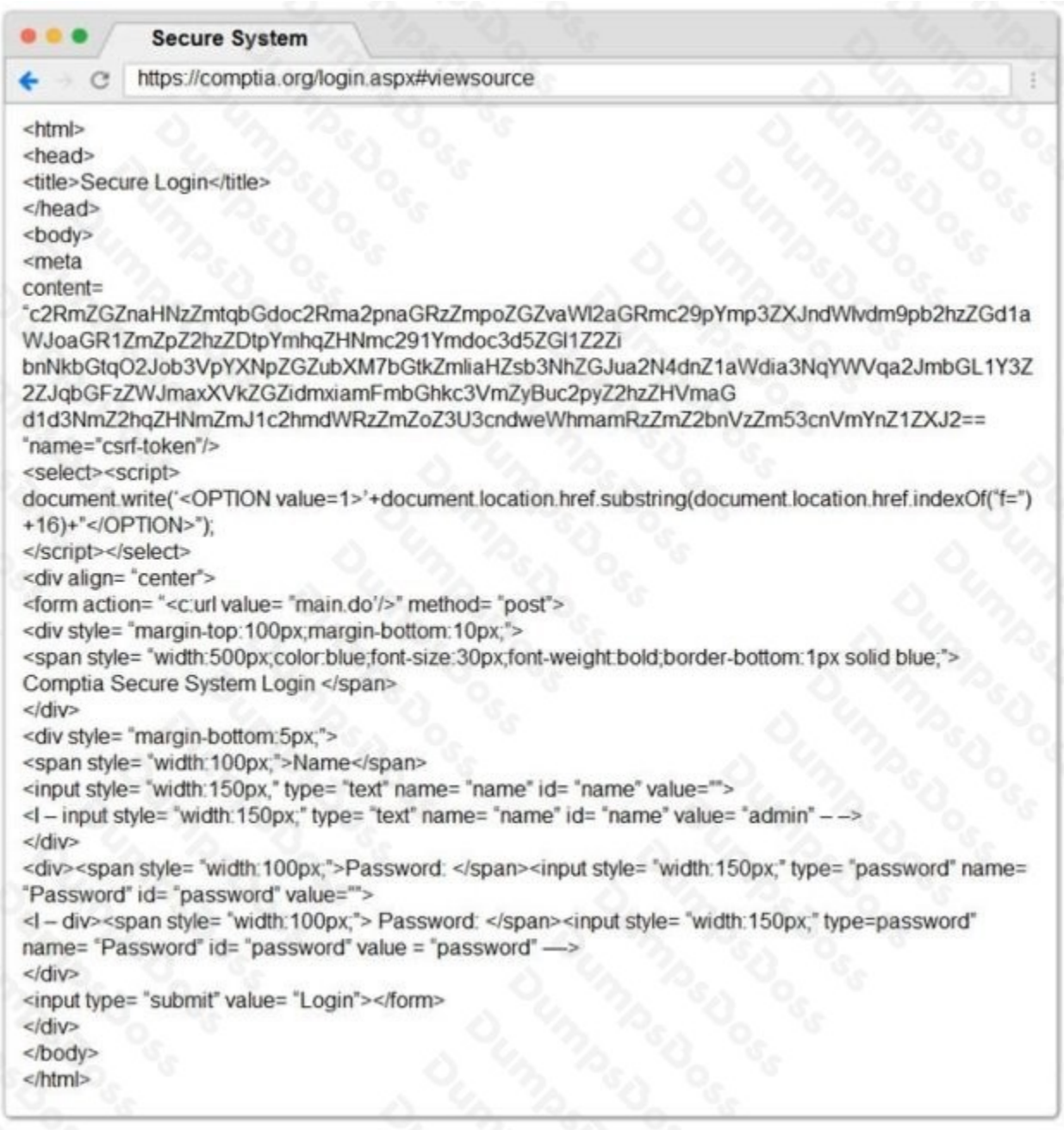
Review all components of the website through the browser to determine if vulnerabilities are present.

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
https://comptia.org/login.aspx#viewcert
Certificate
General
Details
Certification Path
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
Install Certificate...
Issuer Statement
Learn more about certificates
OK


Secure System
https://comptia.org/login.aspx#viewsource
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content=
"c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1a
WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
2ZJqbGFzZWJmaxXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2=="
"name="csrf-token"/>
<select><script>
document.write('<OPTION value=1>'+document.location.href.substring(document.location.href.indexOf("f=")
+16)+"</OPTION>");
</script></select>

<form action= "<c:url value= "main.do'/>" method= "post">

Comptia Secure System Login

Name
<input style= "width:150px," type= "text" name= "name" id= "name" value="">
<I – input style= "width:150px," type= "text" name= "name" id= "name" value= "admin" – –>

Password: <input style= "width:150px," type= "password" name=
"Password" id= "password" value="">
<I – div> Password: <input style= "width:150px," type=password"
name= "Password" id= "password" value = "password" —>

<input type= "submit" value= "Login"></form>

</body>
</html>

Secure System

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

Name	Value	Domain	Path	Expires /...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2ewvqaf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59			
__utmb	36104370.7.9.1508267988443	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	4a84866c6fff51c.1508266964.1.1508268019.1508266964.81f04f7...	comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	comptia.o...	/	2017-10-1...	13			

Secure System

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

Certificate

General | Details | Certification Path

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

Install Certificate... | Issuer Statement

Learn more about certificates

OK

Drag and Drop Options

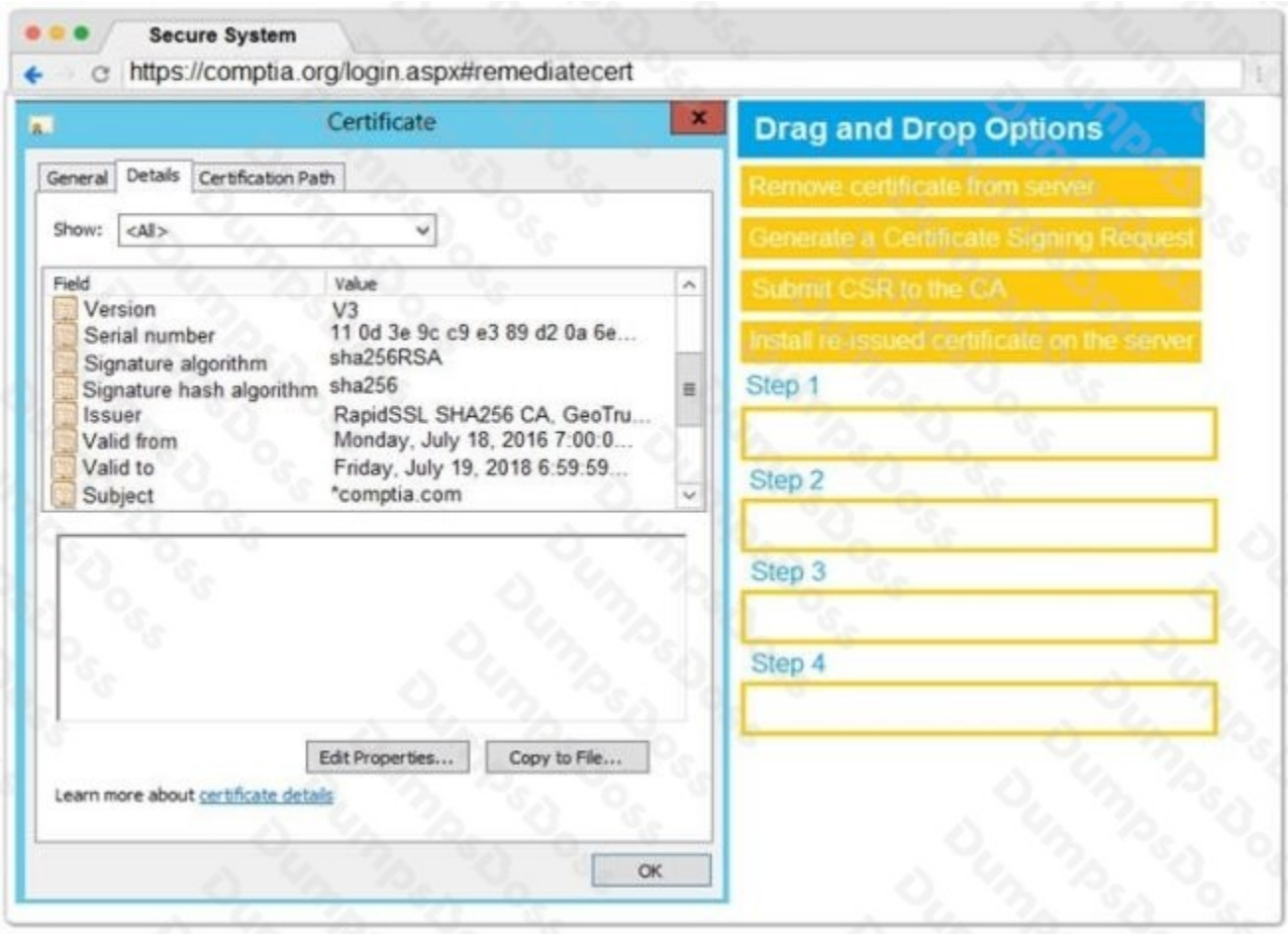
- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

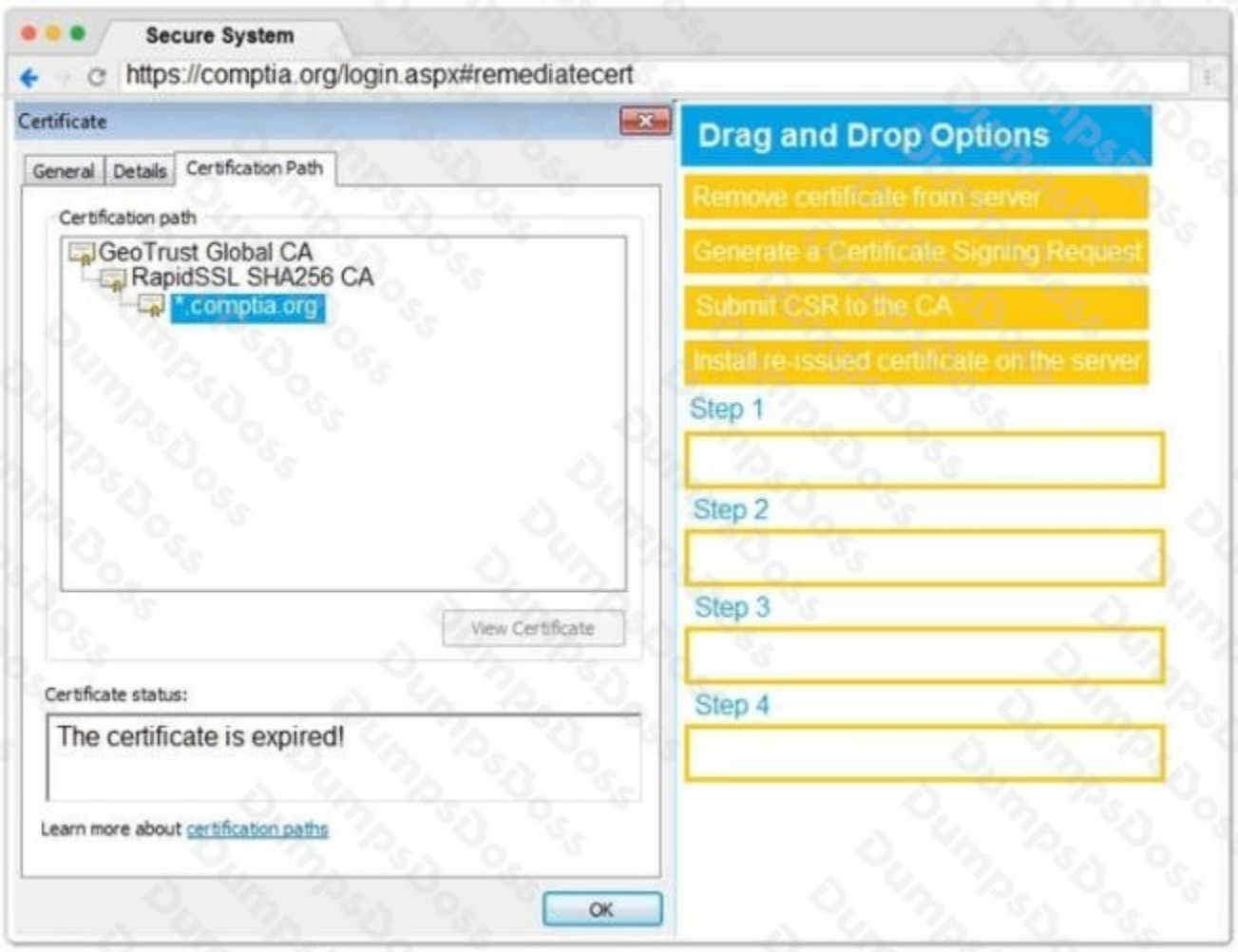
Step 1

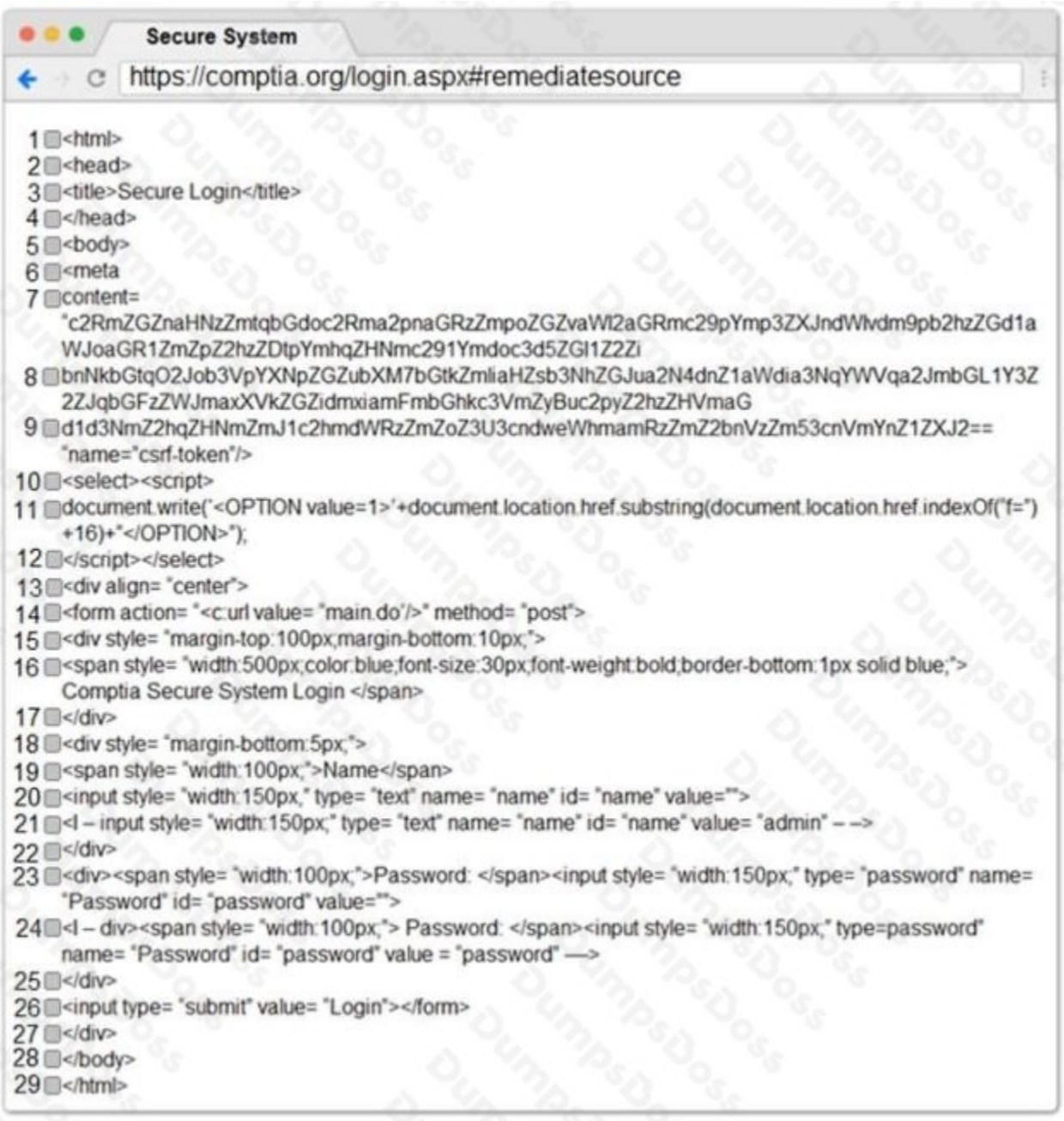
Step 2

Step 3

Step 4


Secure System
https://comptia.org/login.aspx#remediatecert
Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
11 0d 3e 9c c9 e3 89 d2 0a 6e...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
RapidSSL SHA256 CA, GeoTru...
Valid from
Monday, July 18, 2016 7:00:0...
Valid to
Friday, July 19, 2018 6:59:59...
Subject
*comptia.com
Edit Properties...
Copy to File...
Learn more about certificate details
OK
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


Secure System
https://comptia.org/login.aspx#remediatecert
Certificate
General
Details
Certification Path
Certification path
GeoTrust Global CA
RapidSSL SHA256 CA
*.comptia.org
View Certificate
Certificate status:
The certificate is expired!
Learn more about certification paths
OK
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


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=
"c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1a
WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
2ZJqbGFzZWJmaxXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==
"name="csrf-token"/>
10 <select><script>
11 document.write('<OPTION value=1>'+document.location.href.substring(document.location.href.indexOf("f=")
+16)+"</OPTION>");
12 </script></select>
13
14 <form action= "<c:url value= "main.do'/>" method= "post">
15
16
Comptia Secure System Login
17
18
19 Name
20 <input style= "width:150px," type= "text" name= "name" id= "name" value="">
21 <I – input style= "width:150px," type= "text" name= "name" id= "name" value= "admin" – –>
22
23 Password: <input style= "width:150px," type= "password" name=
"Password" id= "password" value="">
24 <I – div> Password: <input style= "width:150px," type=password"
name= "Password" id= "password" value = "password" —>
25
26 <input type= "submit" value= "Login"></form>
27
28 </body>
29 </html>

ANSWER: See explanation below.

Explanation:

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

QUESTION NO: 7

Which of the following has a direct and significant impact on the budget of the security assessment?

A. Scoping

B. Scheduling

C. Compliance requirement

D. Target risk

ANSWER: D

QUESTION NO: 8

A penetration tester is checking a script to determine why some basic math errors are persisting. The expected result was the program outputting “True”.

```
root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ 'source' = 'dest' ]; then
     echo "True"
else
     echo "False"
fi
#End of File

root:~# ./test.sh
False
```

Given the output from the console above, which of the following explains how to correct the errors in the script? (Choose two.)

A. Change 'fi' to 'Endlf'.

B. Remove the 'let' in front of 'dest=5+5'.

C. Change the '=' to '-eq'.

D. Change 'source' and 'dest' to "$source" and "$dest".

E. Change 'else' to 'elif'.

ANSWER: B D

QUESTION NO: 9

A penetration tester discovers SNMP on some targets. Which of the following should the penetration tester try FIRST?

A. Sniff SNMP traffic.

B. Use default credentials.

C. Upload a new config file.

D. Conduct a MITM.

ANSWER: B

QUESTION NO: 10 - (DRAG DROP)

DRAG DROP

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.

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.

Select and Place:


Drag and Drop Options
exec_scan(sys.argv[1], $PORTS)
port_scan(sys.argv[1], ports)
export $PORTS = 21, 22
self .ports {
try:
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
except socket.timeout
print("%s:$s - TIMEOUT" % (ip, port))
except socket.error as e:
print("%s:%s - CLOSED" % (ip, port))
finally:
s.close()
}
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()
}
#!/usr/bin/python
#!/usr/bin/ruby
ports = [21, 22]
run_scan(sys.argv[1], ports)
#!/usr/bin/bash
(:ports => 21 :ports => 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 len(sys.argv) < 2
print('Execution requires a target IP address.
Exiting...')
exit(1)
else:

ANSWER:

Explanation:

QUESTION NO: 11

A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack. Which of the following remediation steps should be recommended? (Select THREE).

A. Mandate all employees take security awareness training.

B. Implement two-factor authentication for remote access.

C. Install an intrusion prevention system.

D. Increase password complexity requirements.

E. Install a security information event monitoring solution.

F. Prevent members of the IT department from interactively logging in as administrators.

G. Upgrade the cipher suite used for the VPN solution.

ANSWER: B C G

QUESTION NO: 12

A penetration tester has gained access to a marketing employee's device. The penetration tester wants to ensure that if the access is discovered, control of the device can be regained. Which of the following actions should the penetration tester use to maintain persistence to the device? (Select TWO.)

A. Place an entry in HKLM\Software\Microsoft\CurrentVersion\Run to call au57d.ps1.

B. Place an entry in C:\windows\system32\drivers\etc\hosts for 12.17.20.10 badcomptia.com.

C. Place a script in C:\users\%username\local\appdata\roaming\temp\au57d.ps1.

D. Create a fake service in Windows called RTAudio to execute manually.

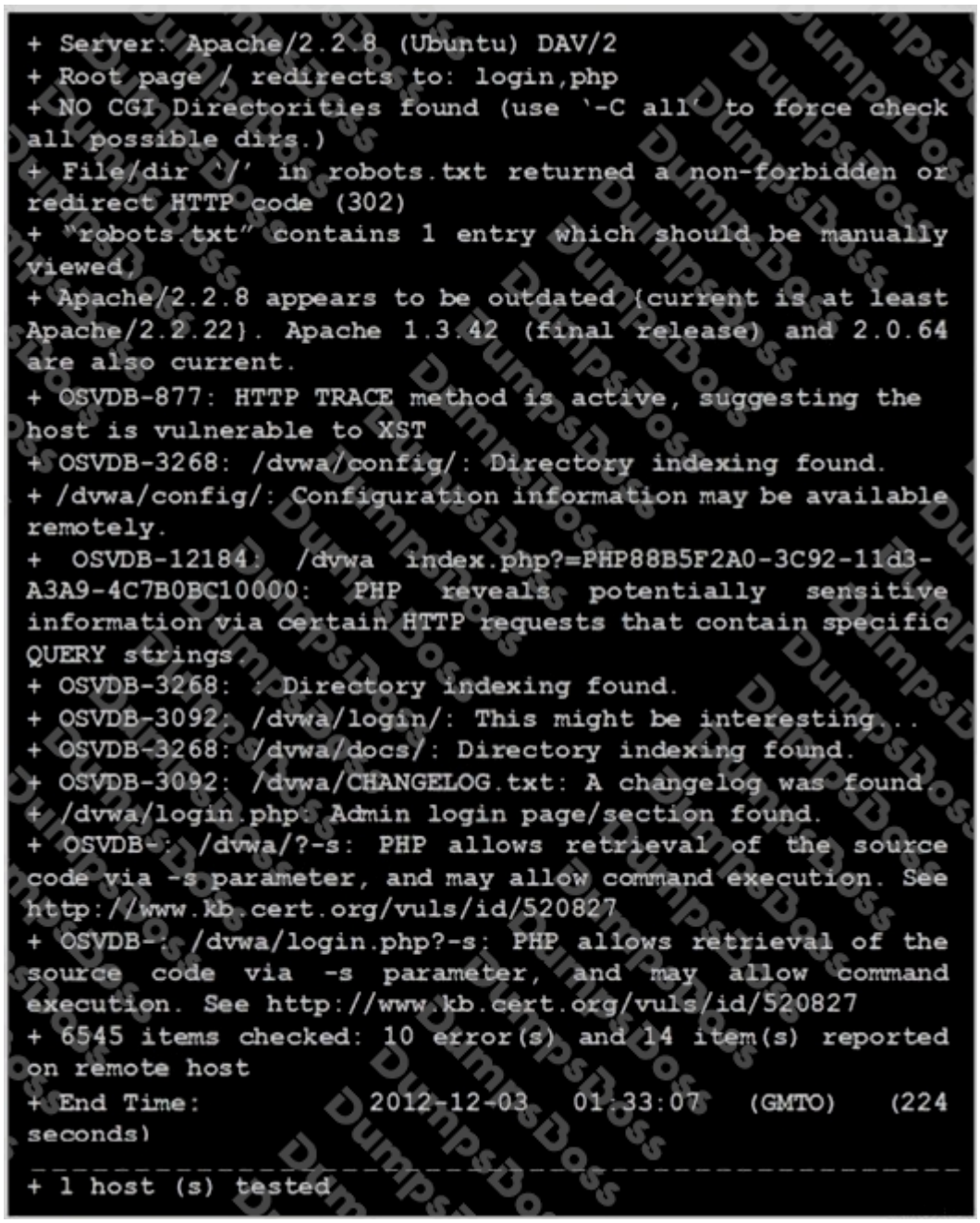
E. Place an entry for RTAudio in HKLM\CurrentControlSet\Services\RTAudio.

F. Create a schedule task to call C:\windows\system32\drivers\etc\hosts.

ANSWER: A C

QUESTION NO: 13

Click the exhibit button.



Given the Nikto vulnerability, scan output shown in the exhibit, which of the following exploitation techniques might be used to exploit the target system? (Choose two.)

A. Arbitrary code execution

B. Session hijacking

C. SQL injection

D. Login credential brute-forcing

E. Cross-site request forgery

ANSWER: B D

QUESTION NO: 14

A penetration tester is in the process of writing a report that outlines the overall level of risk to operations. In which of the following areas of the report should the penetration tester put this?

A. Appendices

B. Executive summary

C. Technical summary

D. Main body

ANSWER: B

QUESTION NO: 15

A penetration tester is outside of an organization's network and is attempting to redirect users to a fake password reset website hosted on the penetration tester's box. Which of the following techniques is suitable to attempt this?

A. Employ NBNS poisoning.

B. Perform ARP spoofing.

C. Conduct a phishing campaign.

D. Use an SSL downgrade attack.

ANSWER: C