PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A penetration tester executes the following commands:

C:\>%userprofile%\jtr.exe

This program has been blocked by group policy

C:\> accesschk.exe -w -s -q -u Users C:\Windows

rw C:\Windows\Tracing

C:\>copy %userprofile%\jtr.exe C:\Windows\Tracing

C:\Windows\Tracing\jtr.exe

jtr version 3.2...

jtr>

Which of the following is a local host vulnerability that the attacker is exploiting?

A. Insecure file permissions

B. Application Whitelisting

C. Shell escape

D. Writable service

Correct Answer: A

References https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#john-the- ripper---jtr

QUESTION 2

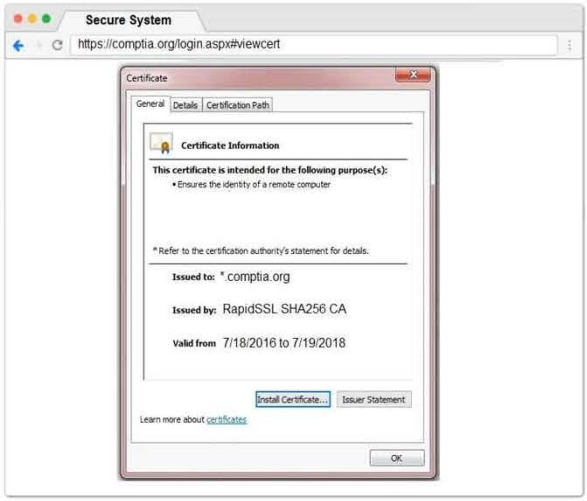
You are a penetration tester reviewing a client\\'s website through a web browser.

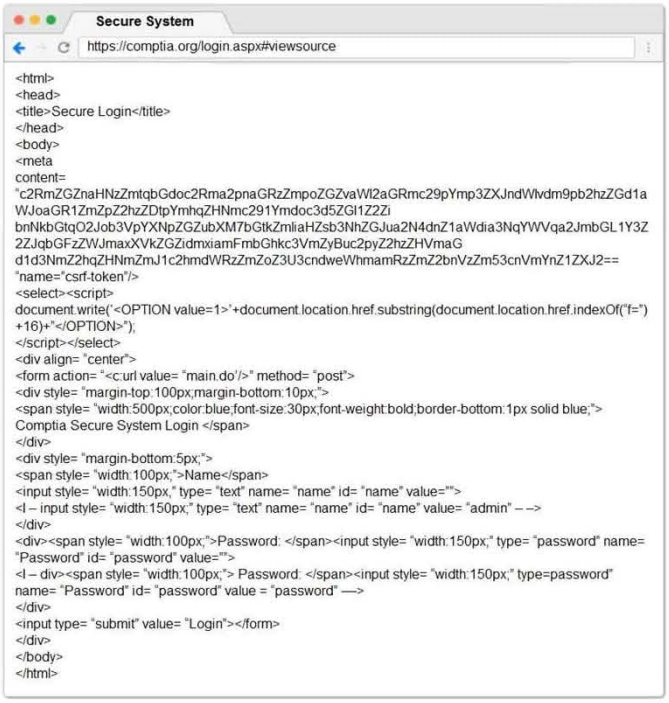
INSTRUCTIONS

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

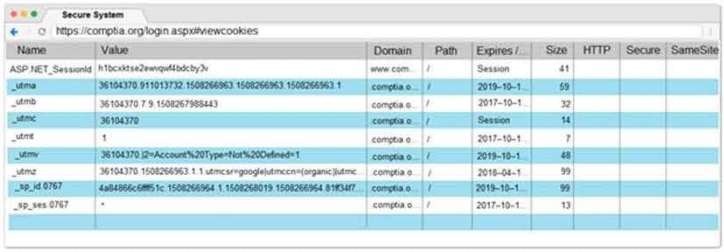
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

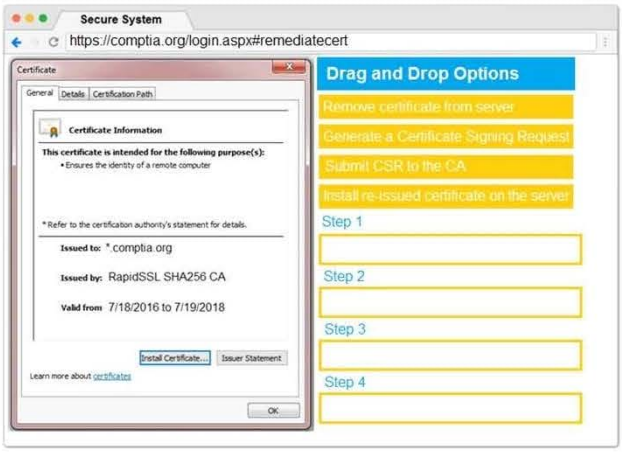
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

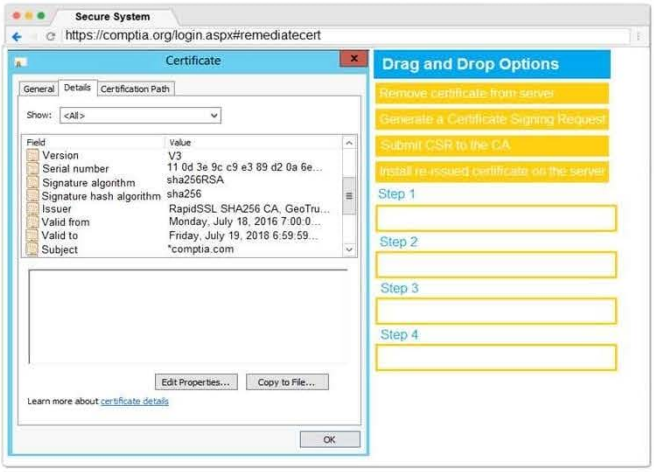


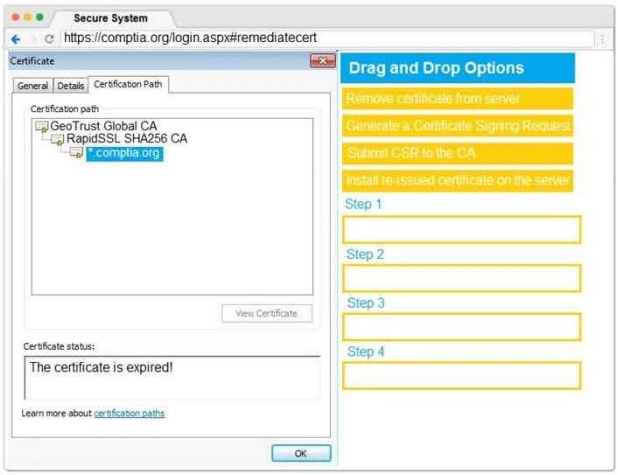


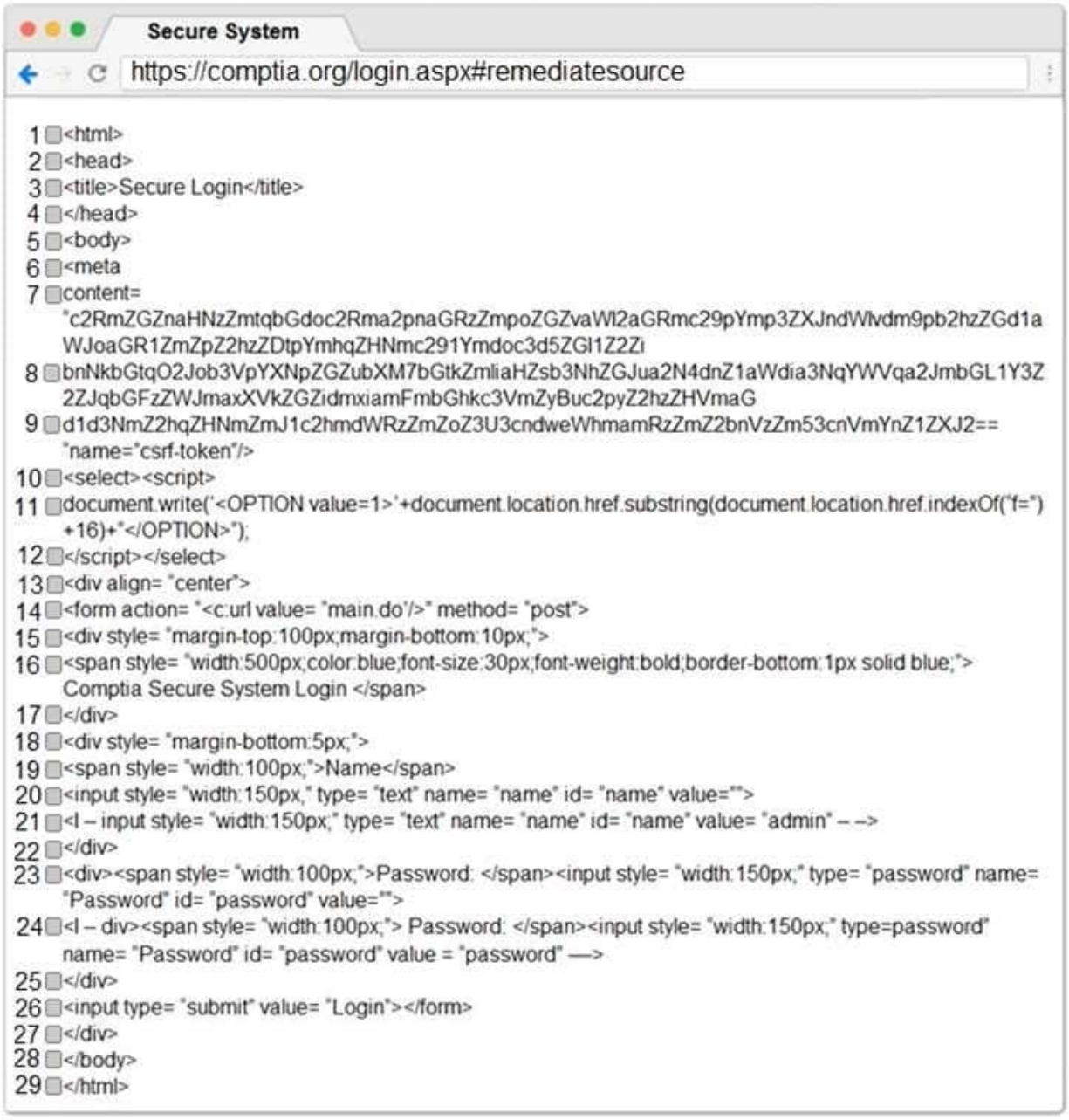

```
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content=
"c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1a
WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
2ZJqbGFzZWJmaxXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==
"name="csrf-token"/>
<select><script>
document.write('<OPTION value=1>'+document.location.href.substring(document.location.href.indexOf("f=")
+16)+"</OPTION>");
</script></select>
<div align= "center">
<form action= "<c:url value= "main.do'/>" method= "post">
<div style= "margin-top:100px;margin-bottom:10px;">
<span style= "width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px 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="">
<I – 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="">
<I – div><span style= "width:100px;"> Password: </span><input style= "width:150px;" type=password"
name= "Password" id= "password" value = "password" —>
</div>
<input type= "submit" value= "Login"></form>
</div>
</body>
</html>
```


Secure System
https://comptia.org/login.aspx#viewcookies
Name
Value
Domain
Path
Expires /...
Size
HTTP
Secure
SameSite


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

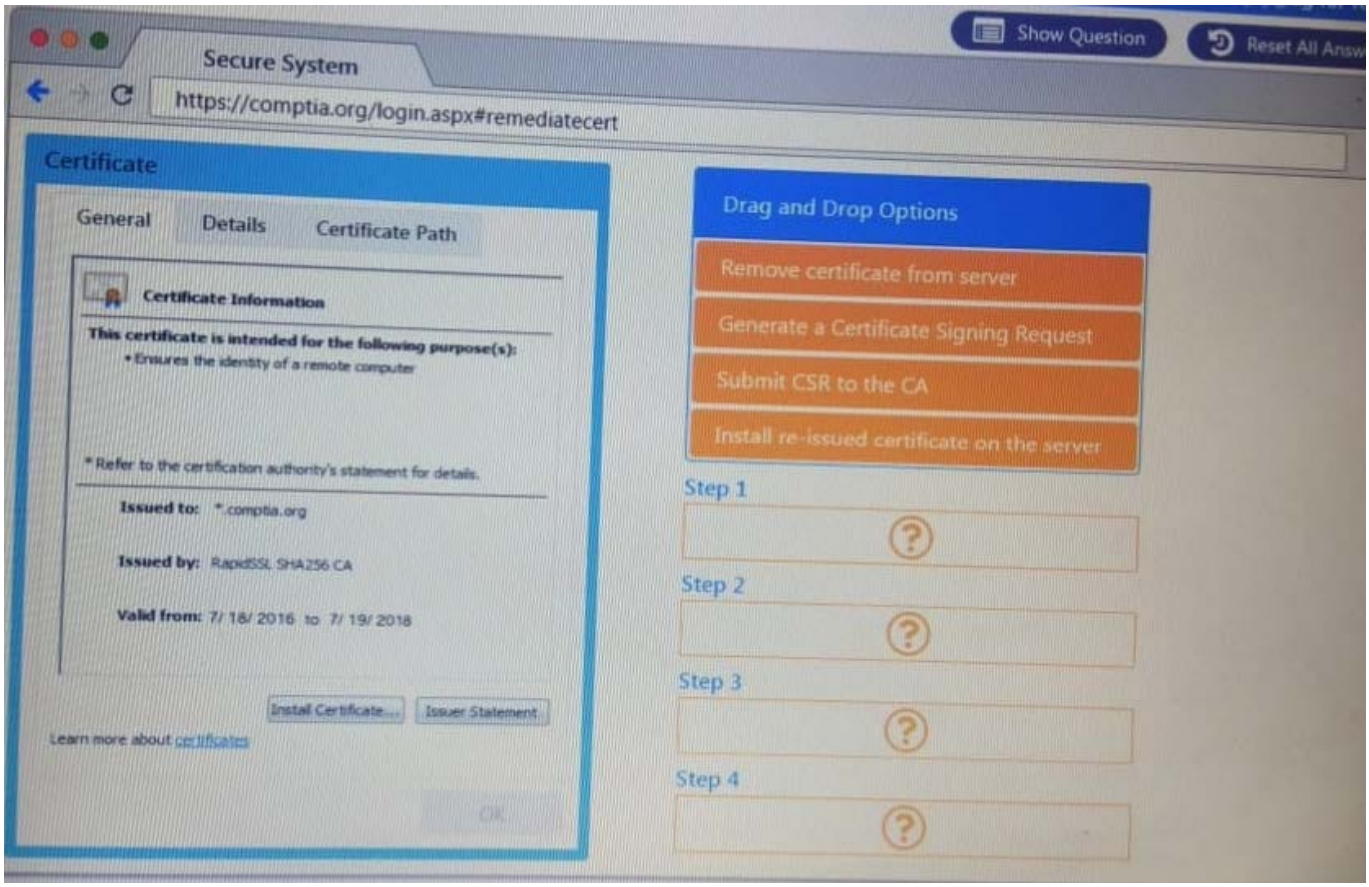

Secure System
https://comptia.org/login.aspx#remediatecert
Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Version
V3
Serial number
11 0d 3e 9c c9 e3 89 d2 0a 6e...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
RapidSSL SHA256 CA, GeoTru...
Valid from
Monday, 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

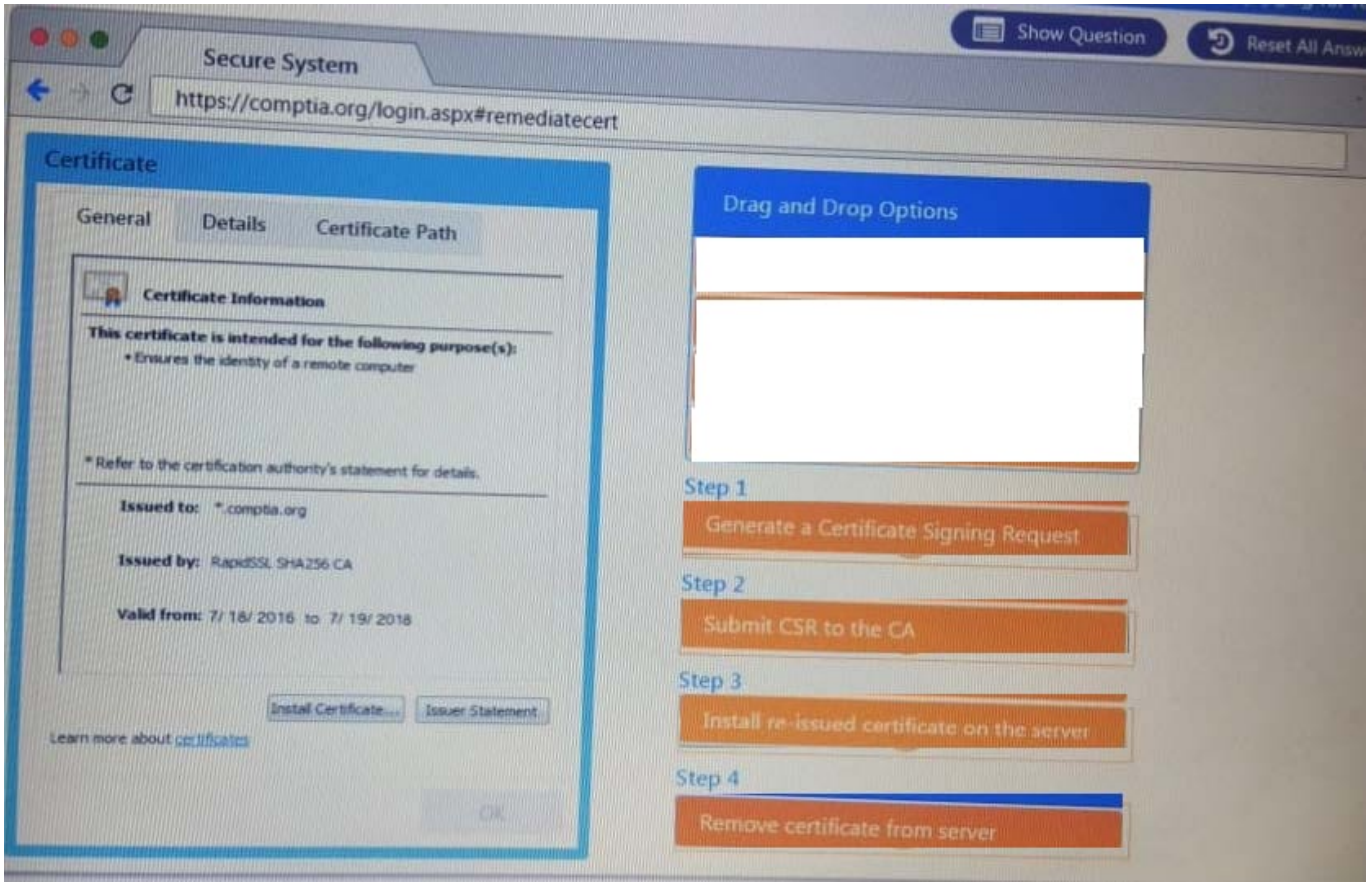

Secure System
https://comptia.org/login.aspx#remediatesource
1 <html>
2 <head>
3 <title>Secure Login</title>
4 </head>
5 <body>
6 <meta
7 content=
"c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1a
WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
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>


Secure System
https://comptia.org/login.aspx#remediatecookies
Name Value Domain Path Expires /... Size HTTP Secure SameSite
ASP.NET_SessionId h1bcxktse2ewvqwf4bdcby3v www.com... / Session 41 delete
_utma 36104370.911013732.1508266963.1508266963.1508266963.1 comptia.o... / 2019-10-1... 59 delete
_utmb 36104370.7.9.1508267988443 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 4a84866c6fff51c.1508266964.1.1508268019.1508266964.81ff34f7... comptia.o... / 2019-10-1... 99 delete
_sp_ses.0767 * comptia.o... / 2017-10-1... 13 delete

Select and Place:



Correct Answer:



QUESTION 3

Which of the following tools would a penetration tester leverage to conduct OSINT? (Select TWO).

A. Shodan

B. SET

C. BeEF

D. Wireshark

E. Maltego

F. Dynamo

Correct Answer: AE

References: https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint- tools/#gref

QUESTION 4

A penetration tester has compromised a Windows server and is attempting to achieve persistence. Which of the following would achieve that goal?

A. schtasks.exe /create/tr "powershell.exe" Sv.ps1 /run

B. net session server | dsquery -user | net use c$

C. powershell andand set-executionpolicy unrestricted

D. reg save HKLM\System\CurrentControlSet\Services\Sv.reg

Correct Answer: D

QUESTION 5

The scope of a penetration test requires the tester to be stealthy when performing port scans. Which of the following commands with Nmap BEST supports stealthy scanning?

A. -min-rate

B. -max-length

C. -host-timeout

D. -max-rate

Correct Answer: C

Reference: https://nmap.org/book/man-port-scanning-techniques.html