Comptia

PT0-001

CompTIA PenTest+ Exam

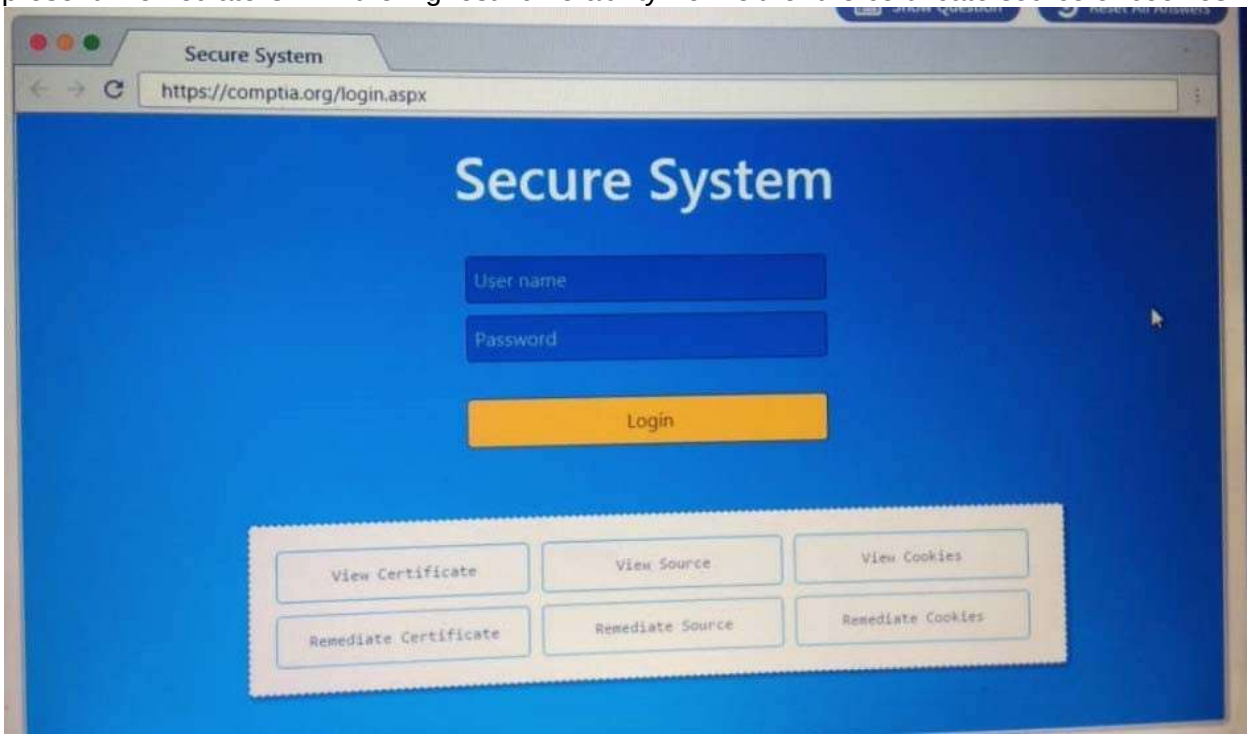
Verified by IT Experts

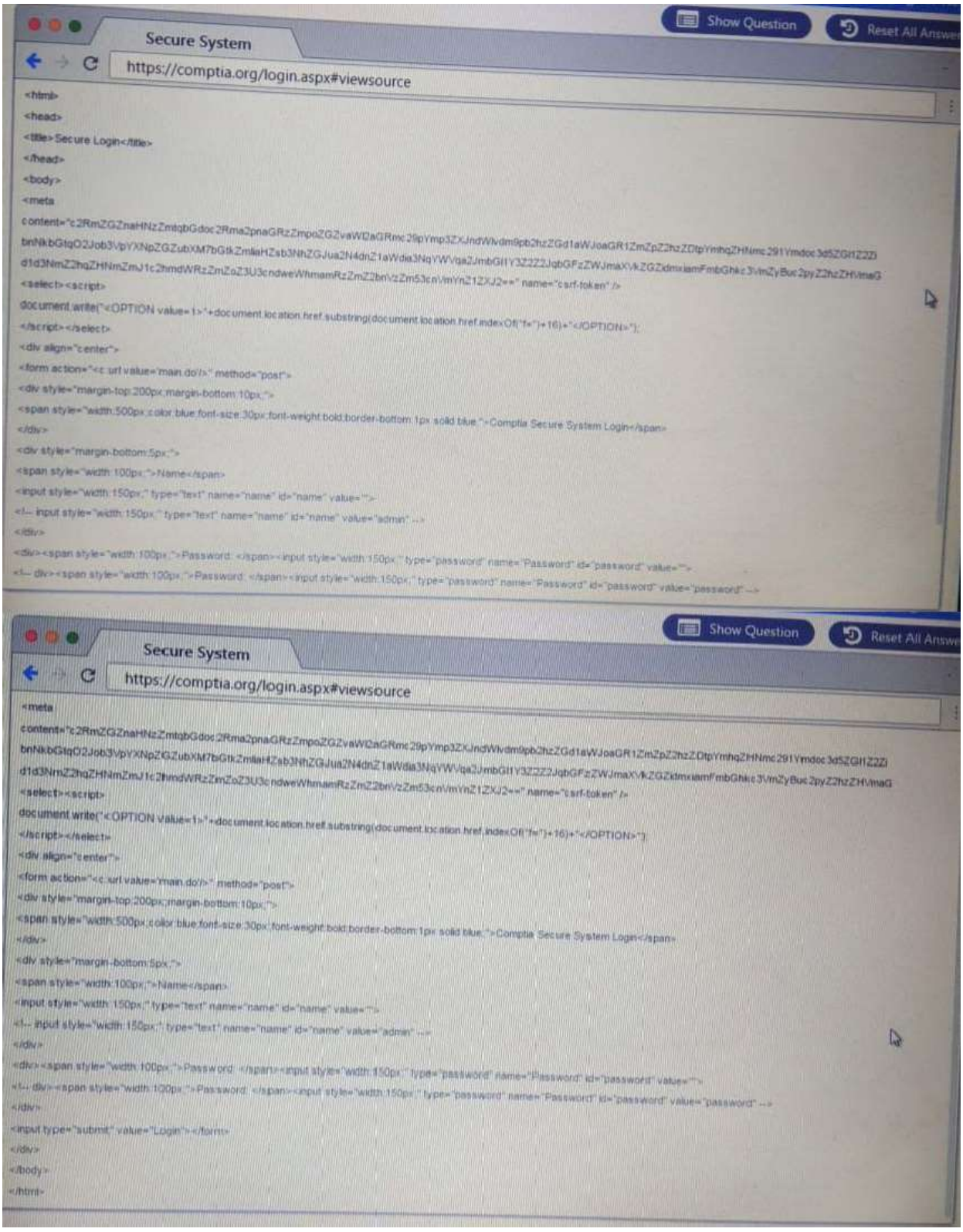
Pass your exam in first attempt

Demo Questions

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.




Show Question
Reset All Answe
Secure System
https://comptia.org/login.aspx#viewsource
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWlZaGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmlaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGlIY3Z2Z2JqbGFzZWJmaX\/kZGZkdmxiamFmbGhkc3\/mZyBuc2pyZ2hzZH\/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
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWlZaGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmlaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGlIY3Z2Z2JqbGFzZWJmaX\/kZGZkdmxiamFmbGhkc3\/mZyBuc2pyZ2hzZH\/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">

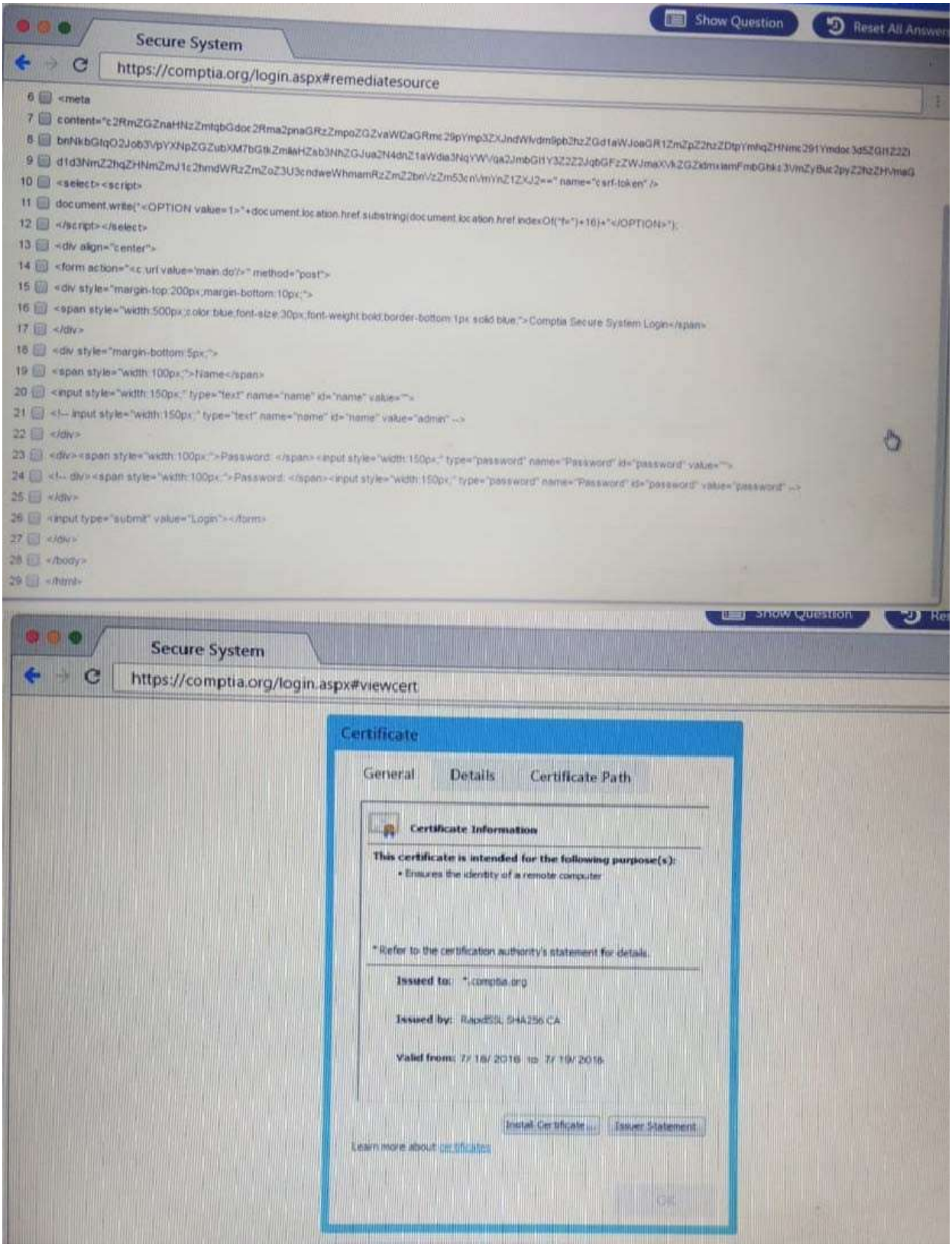
Comptia Secure System Login

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" -->

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

</body>
</html>


Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#remediatesource
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWZaGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGh1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmlaHZab3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JqbGFzZWJmaXVkZGZkdmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("fe")+16)+"</OPTION>");
</script></select>

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

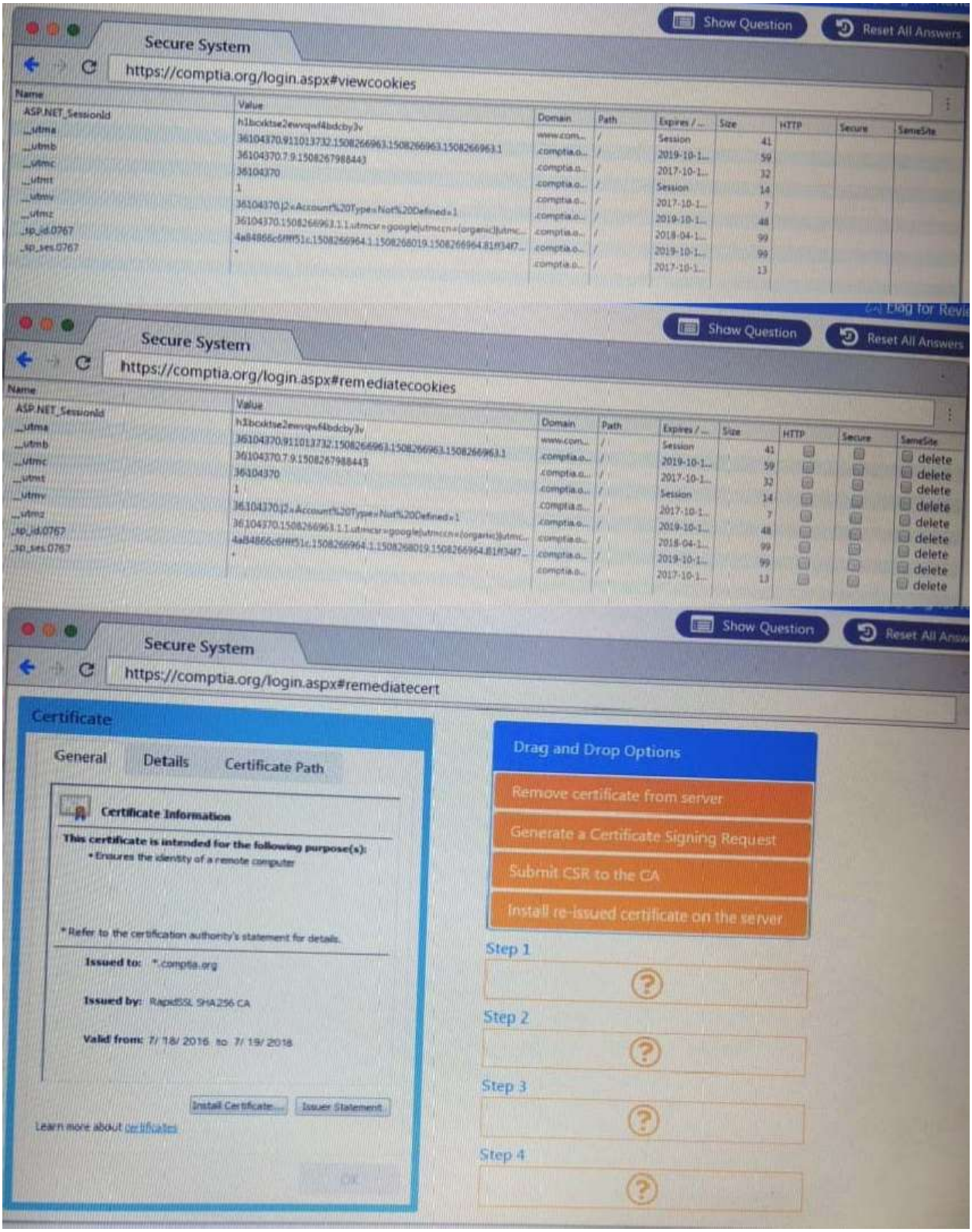
Comptia Secure System Login

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" -->

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

</body>
</html>
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/ 2019
Install Certificate...
Issuer Statement
Learn more about certificates
OK

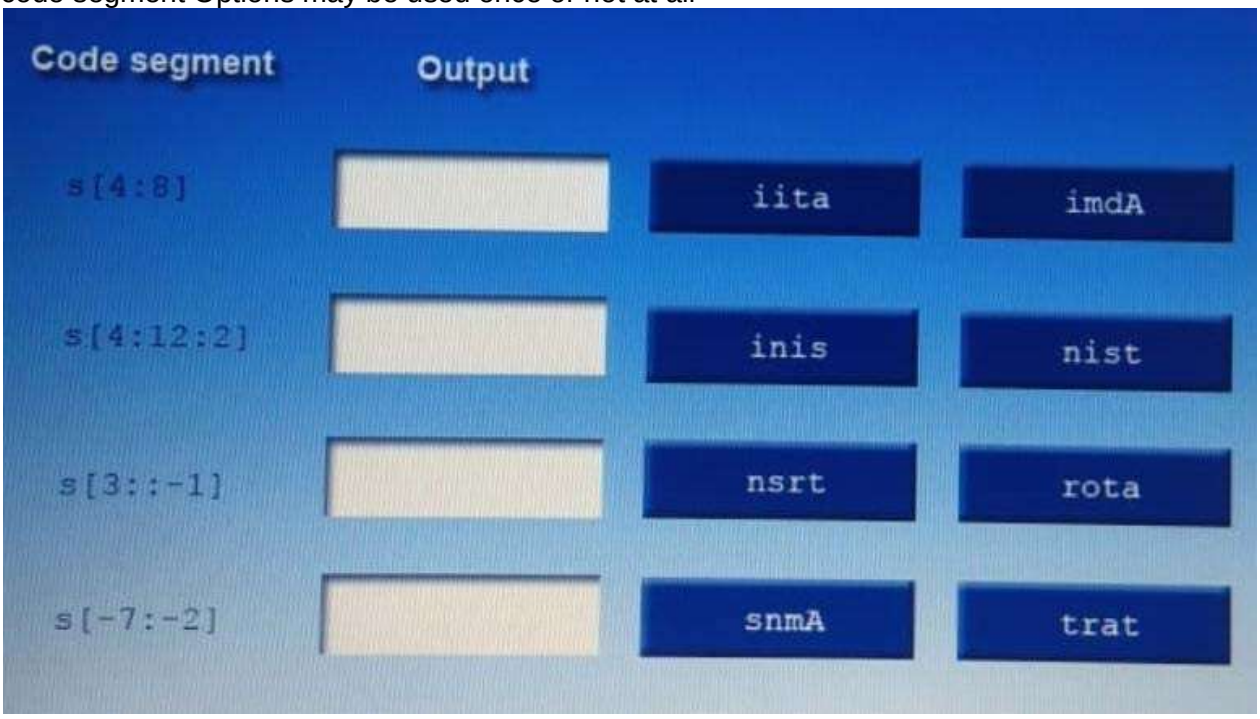

Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#viewcookies
Name
Value
Domain
Path
Expires / ...
Size
HTTP
Secure
SameSite
ASP.NET_SessionId
__utma
__utmb
__utmc
__utmt
__utmv
__utmz
_sp_id.0767
_sp_ses.0767
Secure System
https://comptia.org/login.aspx#remediatecookies
delete
Secure System
https://comptia.org/login.aspx#remediatecert
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	Generate a Certificate Signing
Step	Submit CSR to the
Step	Installed re-issued certificate on the
Step	Remove Certificate from

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

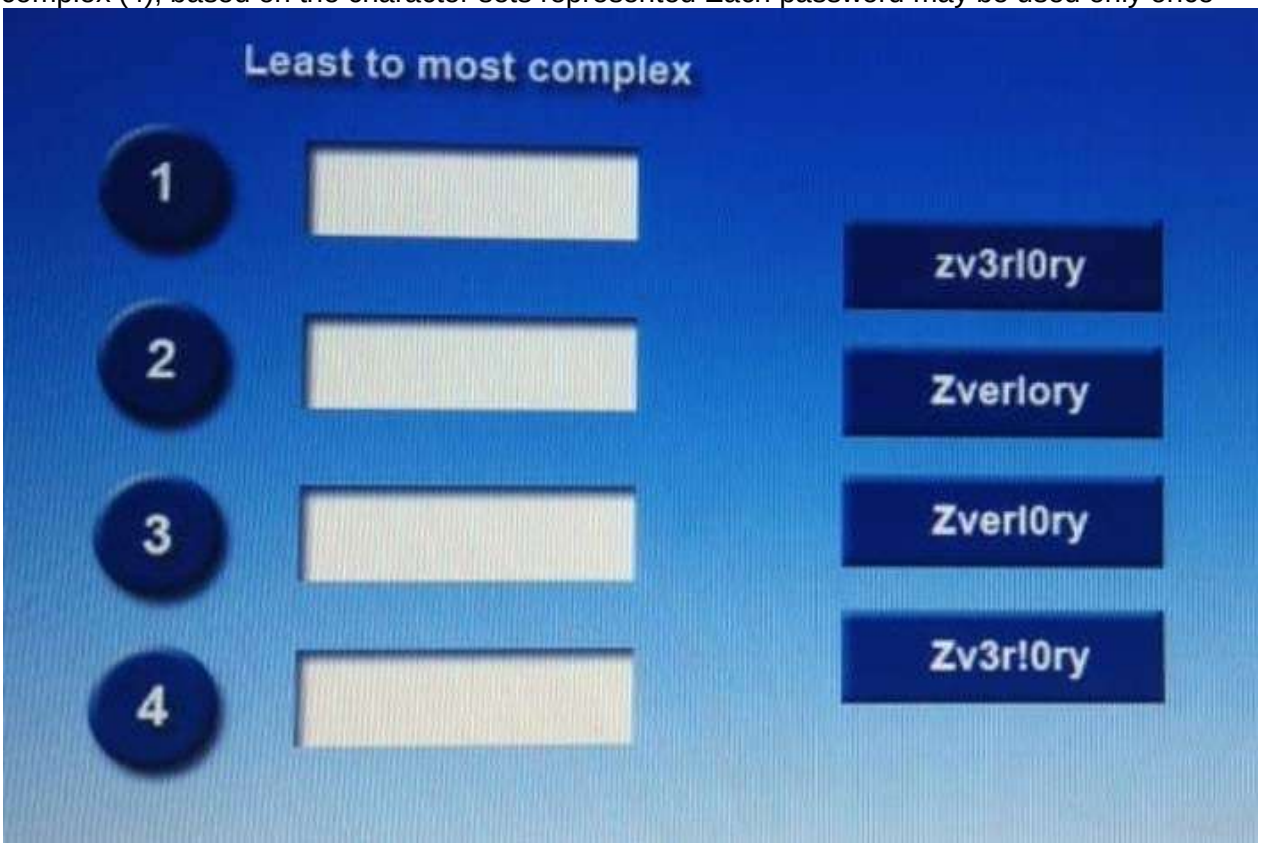


Answer:

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:

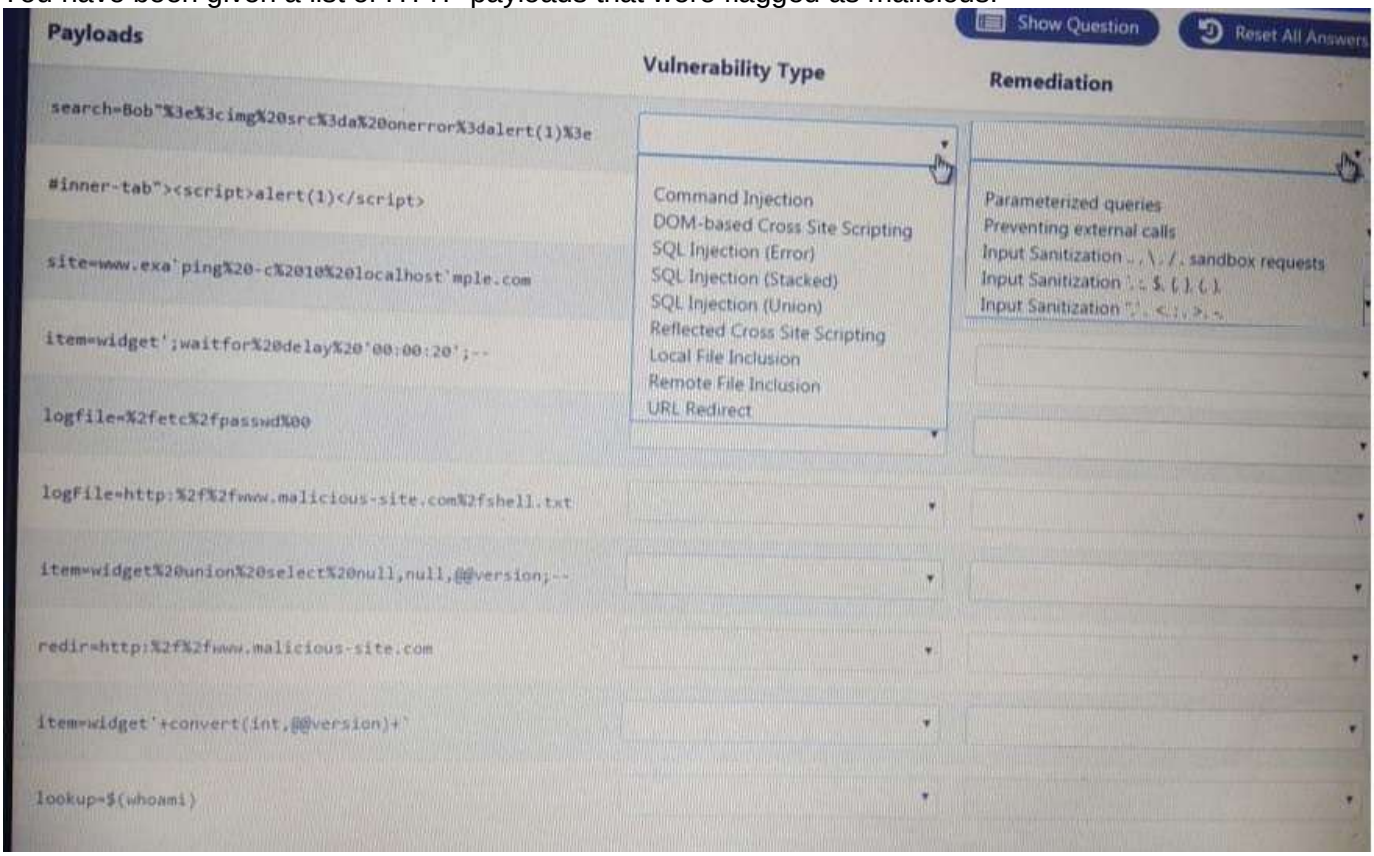
1.) Zverlory
2.) Zverl0ry
3.) zv3rl0ry
4.) Zv3r!0ry

Question: 4

HOTSPOT

You are a security analyst tasked with hardening a web server.

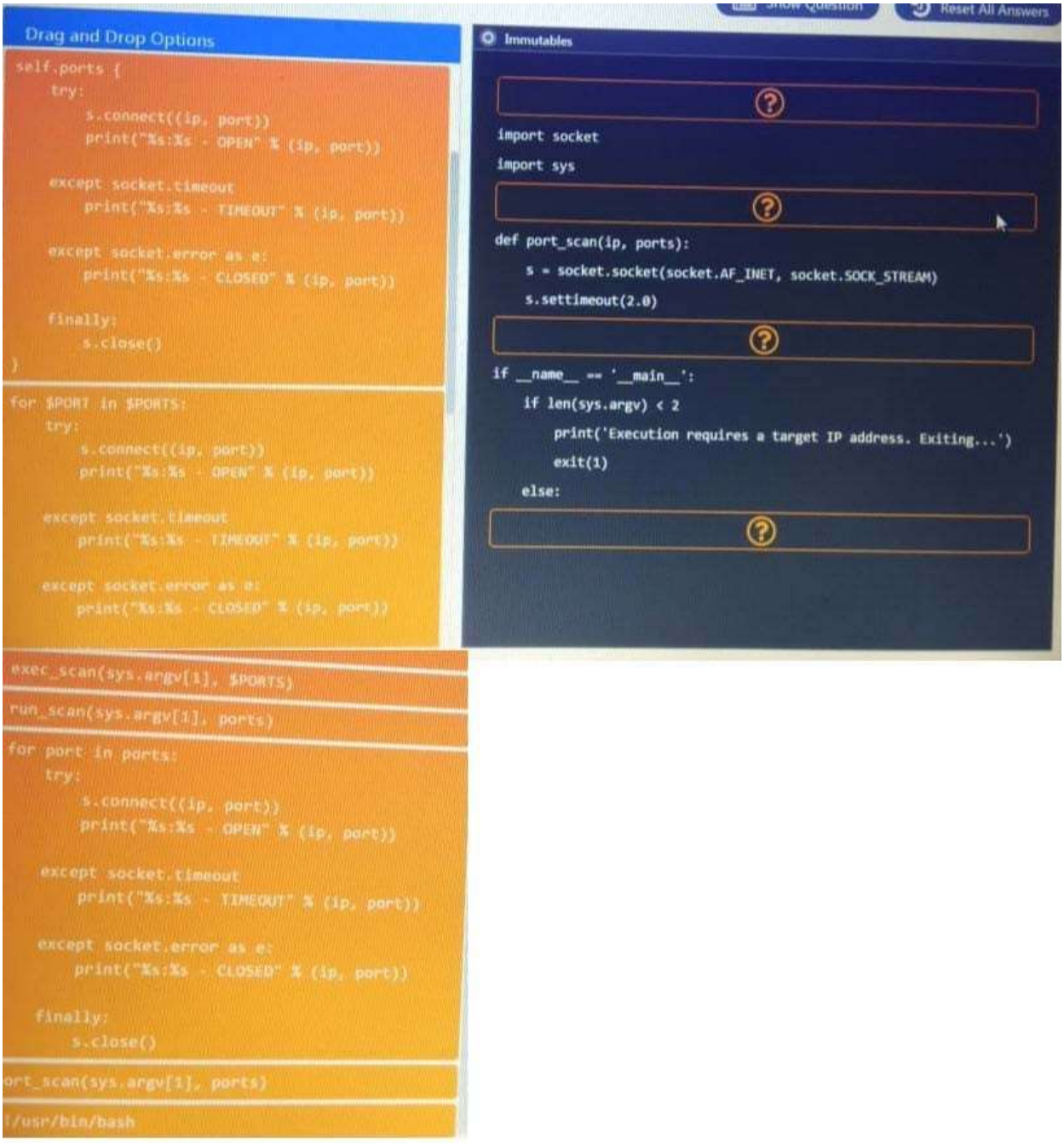
You have been given a list of HTTP payloads that were flagged as malicious.



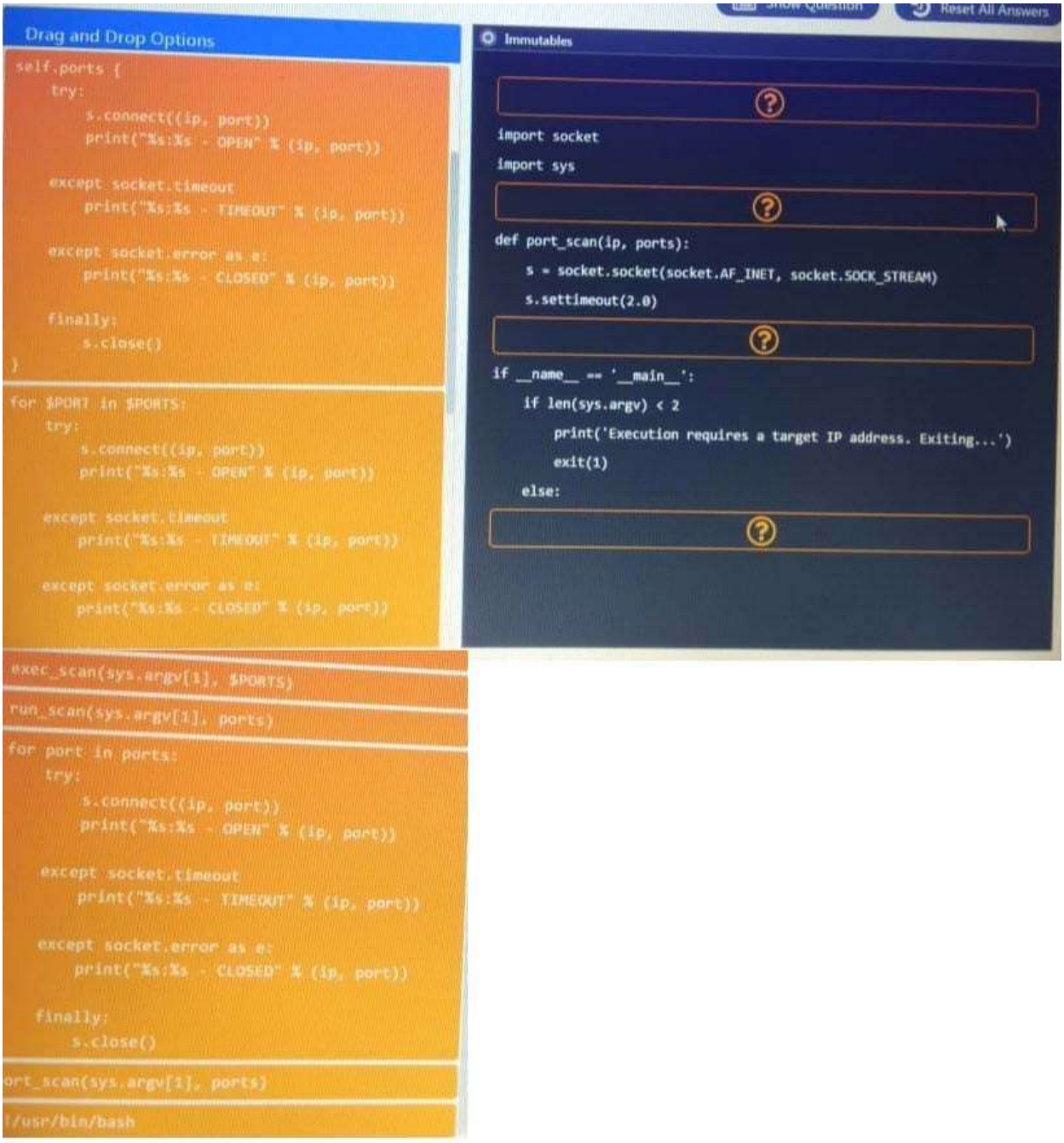
Answer:

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
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))
exec_scan(sys.argv[1], $PORTS)
run_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()
ort_scan(sys.argv[1], ports)
!/usr/bin/bash
Reset All Answers
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 address. Exiting...')
exit(1)
else:

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,

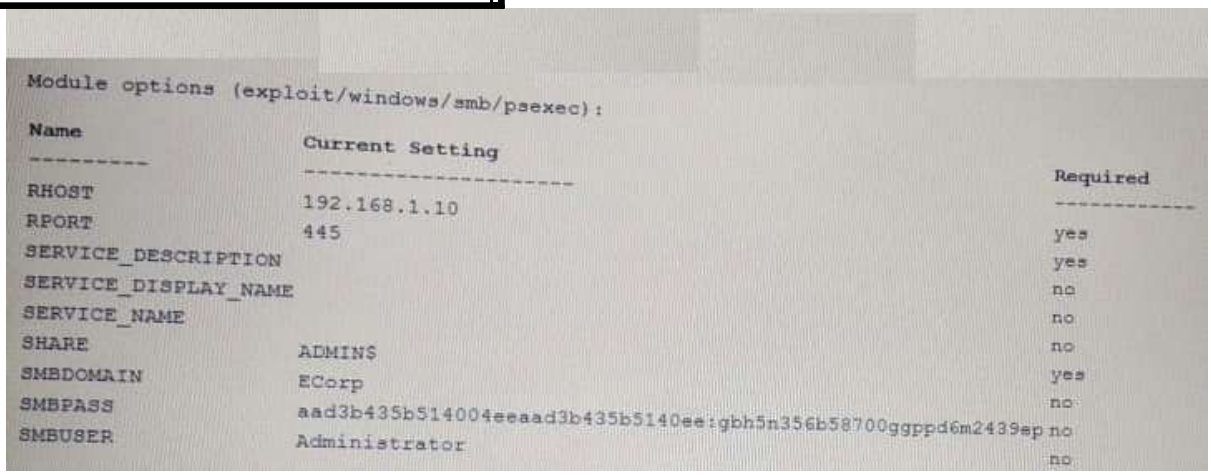
C. -p 1-65534

D. -port 1-65534

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

Answer: A

Question: 7



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