# PT0-002<sup>Q&As</sup>

CompTIA PenTest+ Certification Exam

### Pass CompTIA PT0-002 Exam with 100% Guarantee

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

https://www.leads4pass.com/pt0-002.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

Leads4Pass

800,000+ Satisfied Customers





### **QUESTION 1**

CORRECT TEXT SIMULATION Using the output, identify potential attack vectors that should be further investigated.



| Weak Apache Tomcat Credentia | ls |
|------------------------------|----|
| Null session enumeration     |    |
| Weak SMB file permissions    |    |
| Webdav file upload           |    |
| ARP spoofing                 |    |
| SNMP enumeration             |    |
| Fragmentation attack         |    |
| FTP anonymous login          |    |

|   | ost is up (0.00079s latency).   |
|---|---|
| Ś | ot shown: 96 closed ports   |
| 2 | ORT STATS SERVICE VERSION   |
| 3 | B/tcp open kerberos-sec?  |
| 1 | 39/tcp open netbios-ssn   |
| 8 | 89/tcp open Idap?   |
| 1 | 45/tcp open microsoft-ds?   |
| V | AC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)                                       |
| D | evice type: general purpose   |
| ₹ | unning: Linux 2.4.X   |
| 3 | S CPE: cpe./o:linux_kemel:2.4.21  |
| 2 | S details: Linux 2.4.21   |
| N | etwork Distance: 1 hop  |
| Ċ | S and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. |
| f | Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds           |
| 1 |   |
|   |   |

| -Pn             | O NMAP Scan Output   |
|-----------------|--|
| -sV             | Host is up (0.00079s latency).<br>Not shown: 96 closed ports   |
| -p 1-1023       | PORT STATS SERVICE VERSION<br>88/top open kerberos-sec?  |
| 192.168.2.1-100 | 139/tcp open netbios-ssn<br>389/tcp open Idap?   |
| nmap            | 445/tcp open microsoft-ds?<br>MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)<br>Device type: general purpose |
| nc              | Running: Linux 2.4.X   |
| top-ports=100   | OS CPE: cpe:/o:linux_kemel:2.4.21<br>OS details: Linux 2.4.21<br>Network Distance: 1 hop                                     |
| top-ports=1000  | OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.                         |
| hping           | # Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds                                  |
| -sL             |  |
| -sU             |  |
| -0              |  |
| 192.168.2.2     |  |

| ports - [21, 22]   | O Immutables   |
|--|--|
| {:ports => 21:ports => 22}   | •  |
| #!/usr/bin/python  | import socket<br>import sys  |
| for \$PORT in \$PORTS:<br>try:<br>s.connect((ip, port))<br>print("%s:%s – OPEN" % (ip, port))<br>except socket timeout             | <pre>def port_scan(ip, ports):<br/>s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)<br/>s.settimeout(z.e)</pre>                 |
| print("%s:%s - TIMEOUT" % (ip, port))<br>except socket error as e<br>print("%s:%s - CLOSED" % (ip, port))<br>finally:<br>s close() |  |
| export \$PORTS = 21,22   |  |
| #I/usr/bin/ruby  |  |
| #I/usr/bin/bash  |  |
| for port in ports:   | <pre>ifname 'main': if len(sys.argv) &lt; 2     print('Execution requires a target IP address. Exiting')     exit(1)     else:</pre> |

### Leads4Pass

| • •   | Secure System  |    |
|-------|--|----|
| ÷     | C https://comptia.org/login.aspx#remediatesource   | ž  |
| 1.03  | <html></html>  |    |
| 210   | <pre> <head></head></pre>  |    |
| 3 🗐   | : <title>Secure Login</title>  |    |
| 4 🖽   | <pre><head></head></pre>   |    |
| 5 🗐   | <body></body>  |    |
| 6 (1) | I <meta< p=""></meta<>   |    |
| 7.0   | content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZG112   | Zi |
| 8 (3) | bnNkbGlgO2Job3VpYXNpZG2ubXM7bGlkZmllaHZsb3NhZGJua2N4drZ1aWdw3NgYWVqa2JmbGl1Y3Z22ZJqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBwc2pyZzhzZHVi  | Ð  |
| 9 🗐   | d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==* name=*csr1+oken* />  |    |
| 10 回  | <pre><kelect+<scnpt></kelect+<scnpt></pre>   |    |
| 11 10 | document write(" <option value="1">"+document location href substring(document location href indexO("h=")+16)+"</option> ");   |    |
| 12 🗐  | <pre>/scrot&gt;</pre>  |    |
| 13回   | i <divalign="center"></divalign="center">  |    |
| 14 EI | I <form action="&lt;c.u// value=" main.do?="">* method="post"&gt;</form>   |    |
| 15 🗊  | <div style="margin-top 200px margin-bottom 10px."></div>   |    |
| 16 🗍  | span style="width 500px.color.blue.font-size-30px font-weight bold,border-bottom 1px solid blue.">Comptia Secure System Login (span>   |    |
| 17 回  | ] edwa   |    |
| 18 📖  | <div spx."≻<="" style*"margin-bottom="" td=""><td></td></div>  |    |
| 19 🗐  | ] <span style="width:100px;">Name</span>   |    |
| 20 🗊  | ] <input 150px,"="" id="name" name="name" style="`width" type="text" value=""/>  |    |
| 21 🗭  | 5 <4 input style="width:150px" type="text" name="name" id="name" value="admin">  |    |
| 22 🖂  | ] <td></td>  |    |
| 23 🗍  | dv> <span style="width 100px,">Password </span> <input 100px"="" d="password" name="Password" style="width 150px," type="password" value="&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;24 🕄&lt;/td&gt;&lt;td&gt;5 &lt; div&gt;&lt;span style=" width:=""/> Password: |    |
| 25 🔃  |  |    |
| 26 🗐  | Input type="submit" value="Login">   |    |
| 27 🗐  | l <td></td>  |    |
| 28 🗐  | l «hody»   |    |
| 29 団  | Ahtmi>   |    |

|             | Se    | cure Syste       | m                 |  |
|-------------|-------|------------------|-------------------|--|
|             |       | r name           |                   |  |
|             | Pas   | sword            |                   |  |
|             |       | Login            |                   |  |
| View Certif | icate | View Source      | View Cookies      |  |
| Remedia     |       | Remediate Source | Remediate Cookies |  |

Correct Answer: Answer: See explanation below.



Weak SMB file permissions

Fragmentation attack

2: nmap

-sV

-р 1-1023

192.168.2.2

3: #!/usr/bin/python

export \$PORTS = 21,22

for \$PORT in \$PORTS:

try:

s.connect((ip, port))

print("%s:%s ?OPEN" % (ip, port))

except socket.timeout

print("%:%s ?TIMEOUT" % (ip, port))

except socket.error as e:

print("%:%s ?CLOSED" % (ip, port))

finally

s.close()

port\_scan(sys.argv[1], ports)

### **QUESTION 2**

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

- A. Acceptance by the client and sign-off on the final report
- B. Scheduling of follow-up actions and retesting
- C. Attestation of findings and delivery of the report
- D. Review of the lessons learned during the engagement

```
Correct Answer: C
```

## Leads4Pass

#### **QUESTION 3**

A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?

- A. Halt the penetration test.
- B. Contact law enforcement.
- C. Deconflict with the penetration tester.
- D. Assume the alert is from the penetration test.

Correct Answer: B

#### **QUESTION 4**

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

- A. Multiple handshakes
- B. IP addresses
- C. Encrypted file transfers
- D. User hashes sent over SMB

Correct Answer: B

### **QUESTION 5**

A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?

- A. Send deauthentication frames to the stations.
- B. Perform jamming on all 2.4GHz and 5GHz channels.
- C. Set the malicious AP to broadcast within dynamic frequency selection channels.
- D. Modify the malicious AP configuration to not use a pre-shared key.

Correct Answer: A

https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless- networks-with-wifislax

PT0-002 Practice Test

PT0-002 Exam Questions

### PT0-002 Braindumps