



# 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.passapply.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
-  **800,000+** Satisfied Customers





### QUESTION 1

Given the following code:

```
systems = {  
    "10.10.10.1" : "Windows 10",  
    "10.10.10.2" : "Windows 10",  
    "10.10.10.3" : "Windows 2016",  
    "10.10.10.4" : "Linux"  
}
```

Which of the following data structures is systems?

- A. A tuple
- B. A tree
- C. An array
- D. A dictionary

Correct Answer: C

---

### QUESTION 2

A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:

1.  
Have a full TCP connection
2.  
Send a "hello" payload
3.  
Wait for a response
4.  
Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

- A. Run `nmap-Pn-sV-script vuln` .



- B. Employ an OpenVAS simple scan against the TCP port of the host.
- C. Create a script in the Lua language and use it with NSE.
- D. Perform a credentialed scan with Nessus.

Correct Answer: C

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language ) to automate a wide variety of networking tasks. <https://nmap.org>

---

### QUESTION 3

Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?

- A. Dictionary
- B. Directory
- C. Symlink
- D. Catalog
- E. For-loop

Correct Answer: A

---

### QUESTION 4

A penetration tester created the following script to use in an engagement:



```
#!/usr/bin/python

import socket

ports = [21,22,23,25,80,139,443,445,3306,3389]

if len(sys.argv) == 2:
    target = socket.gethostbyname(sys.argv[1])
else:
    print("Few arguments.")
    print("Syntax: python {} <>".format(sys.argv[0]))
    sys.exit()

try:
    for port in ports:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(2)
        result = s.connect_ex((target,port))
        if result == 0:
            print("Port {} is opened".format(port))

except KeyboardInterrupt:
    print("Exiting...")
    sys.exit()
```

However, the tester is receiving the following error when trying to run the script:

```
$ python script.py 192.168.0.1
Traceback (most recent call last):
  File "script.py", line 7, in <module>
    if len(sys.argv) == 2:
NameError: name 'sys' is not defined
```

Which of the following is the reason for the error?

- A. The sys variable was not defined.
- B. The argv variable was not defined.
- C. The sys module was not imported.
- D. The argv module was not imported.

Correct Answer: A

---



### QUESTION 5

A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability. Which of the following is the BEST way to ensure this is a true positive?

- A. Run another scanner to compare.
- B. Perform a manual test on the server.
- C. Check the results on the scanner.
- D. Look for the vulnerability online.

Correct Answer: B

[Latest PT0-002 Dumps](#)

[PT0-002 VCE Dumps](#)

[PT0-002 Braindumps](#)