



PT0-002^{Q&As}

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

A penetration tester exploited a vulnerability on a server and remotely ran a payload to gain a shell. However, a connection was not established, and no errors were shown on the payload execution. The penetration tester suspected that a network device, like an IPS or next-generation firewall, was dropping the connection. Which of the following payloads are MOST likely to establish a shell successfully?

- A. windows/x64/meterpreter/reverse_tcp
- B. windows/x64/meterpreter/reverse_http
- C. windows/x64/shell_reverse_tcp
- D. windows/x64/powershell_reverse_tcp
- E. windows/x64/meterpreter/reverse_https

Correct Answer: A

A reverse tcp connection is usually used to bypass firewall restrictions on open ports. A firewall usually blocks incoming connections on open ports, but does not block outgoing traffic. windows/meterpreter/reverse_tcp allows you to remotely control the file system, sniff, keylog, hashdump, perform network pivoting, control the webcam and microphone, etc.

QUESTION 2

Deconfliction is necessary when the penetration test:

- A. determines that proprietary information is being stored in cleartext.
- B. occurs during the monthly vulnerability scanning.
- C. uncovers indicators of prior compromise over the course of the assessment.
- D. proceeds in parallel with a criminal digital forensic investigation.

Correct Answer: C

This will then enable the PenTest to continue so that additional issues can be found, exploited, and analyzed.

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: D

QUESTION 4

A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data.

Which of the following should the tester verify FIRST to assess this risk?

- A. Whether sensitive client data is publicly accessible
- B. Whether the connection between the cloud and the client is secure
- C. Whether the client's employees are trained properly to use the platform
- D. Whether the cloud applications were developed using a secure SDLC

Correct Answer: A

QUESTION 5

In Python socket programming, SOCK_DGRAM type is:

- A. reliable.
- B. matrixed.
- C. connectionless.
- D. slower.

Correct Answer: C

Connectionless due to the Datagram portion mentioned so that would mean its using UDP.

[Latest PT0-002 Dumps](#)

[PT0-002 PDF Dumps](#)

[PT0-002 Exam Questions](#)