# PT0-001 Q&As

CompTIA PenTest+ Exam

## Pass CompTIA PT0-001 Exam with 100% Guarantee

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

**https://www.pass4itsure.com/pt0-001.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 tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

A. RID cycling to enumerate users and groups

B. Pass the hash to relay credentials

C. Password brute forcing to log into the host

D. Session hijacking to impersonate a system account

Correct Answer: D

**QUESTION 2**

A penetration tester runs the following on a machine:

```
a.txt:
corp/username%password
corp/John Doe%password
corp/Jane Doe %password

command:
for i in $ (cat a.txt); do echo $i; done | wc -1
```

Which of the following will be returned?

B. 3

C. 5

D. 6

Correct Answer: B

**QUESTION 3**

Which of the following CPU register does the penetration tester need to overwrite in order to exploit a simple butter overflow?

A. Stack pointer register

B. Index pointer register

C. Stack base pointer

D. Destination index register

Correct Answer: A

**QUESTION 4**

Which of the following should a penetration tester verify prior to testing the login and permissions management for a web application that is protected by a CDN-based WAF?

A. If an NDA is signed with the CDN company

B. If the SSL certificates for the web application are valid

C. If a list of the applicable WAF rules was obtained

D. If the IP addresses for the penetration tester are whitelisted on the WAF

Correct Answer: D

**QUESTION 5**

When considering threat actor scoping prior to an engagement, which of the following characteristics makes an APT challenging to emulate?

A. Development of custom zero-day exploits and tools

B. Leveraging the dark net for non-attribution

C. Tenacity and efficacy of social engineering attacks

D. Amount of bandwidth available for DoS attacks

Correct Answer: C