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

An Internet-accessible database server was found with the following ports open: 22, 53, 110, 1433, and 3389. Which of the following would be the BEST hardening technique to secure the server?

A. Ensure all protocols are using encryption.

B. Employ network ACLs.

C. Disable source routing on the server.

D. Ensure the IDS rules have been updated.

Correct Answer: B

QUESTION 2

A recent vulnerability scan of all web servers in an environment offers the following results:

Severity	Vulnerability	Host Count	Network Zone
Critical	Unrestricted file upload	10	QA environment
High	SQL injection	5	DMZ
Medium	Clickjacking	10	Internal
Low	Verbose server banner	15	Cardholder data environment

Taking a risk-based approach, which of the following is the BEST order to approach remediation based on exposure?

A. Unrestricted file upload, clickjacking, verbose server banner, SQL injection

B. Unrestricted file upload, SQL injection, clickjacking, verbose server banner

C. Clickjacking, unrestricted file upload, verbose server banner, SQL injection

D. SQL injection, unrestricted file upload, clickjacking, verbose server banner

E. SQL injection, clickjacking, unrestricted file upload, verbose server banner

Correct Answer: B

QUESTION 3

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 4

Which of the following is the BEST initial attack against an identified FTP server on the remote network?

A. Perform fuzzing against a username field.

B. Use a MITM to sniff transferred credentials in cleartext.

C. Attempt to log in as anonymous.

D. Perform a dictionary attack.

Correct Answer: C

QUESTION 5

A penetration tester entered the following information into the browser URL:

https://www.example.com/login.php?file=../../../../../../../etc/passwd

The server responded with the data contained in the server\\'s sensitive data file. Which of the following types of vulnerabilities is MOST likely being exploited?

A. Weak credentials

B. Race conditions

C. Directory traversal

D. Command injection

Correct Answer: C

Reference: https://www.veracode.com/security/directory-traversal#:~:text=Directory%20traversal%20is%20a%20type,to%20restricted%20directories%20and%20files.andtext=Directory%20traversal%20attacks%20use%20web,of%20the%20web%20root%20folder