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.geekcert.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 web application scanner reports that a website is susceptible to clickjacking. Which of the following techniques would BEST prove exploitability?

A. Redirect the user with a CSRF.

B. Launch the website in an iFRAME.

C. Pull server headers.

D. Capture and replay a session ID.

Correct Answer: B

Reference: https://www.imperva.com/learn/application-security/clickjacking/

QUESTION 2

A tester was able to retrieve domain users\\' hashes. Which of the following tools can be used to uncover the users\\' passwords? (Choose two.)

A. Hydra

B. Mimikatz

C. Hashcat

D. John the Ripper

E. PSExec

F. Nessus

Correct Answer: BE

Reference: https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/

QUESTION 3

During the exploitation phase of a web application, a penetration tester finds XML files are being used to handle parameters that are sent for the server. Which of the following vulnerabilities can be exploited to try to access internal files of the affected web server using a web proxy?

A. XSS

B. SQL injection

C. CSRF

D. XXE

Correct Answer: B

Reference: https://www.sqlshack.com/sql-injection-what-is-it-causes-and-exploits/

QUESTION 4

A client has scheduled a wireless penetration test. Which of the following describes the scoping target information MOST likely needed before testing can begin?

A. The physical location and network ESSIDs to be tested

B. The number of wireless devices owned by the client

C. The client\\'s preferred wireless access point vendor

D. The bands and frequencies used by the client\\'s devices

Correct Answer: D

QUESTION 5

Which of the following types of physical security attacks does a mantrap mitigate-?

A. Lock picking

B. Impersonation

C. Shoulder surfing

D. Tailgating

Correct Answer: D