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.leads4pass.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

In which of the following components is an exploited vulnerability MOST likely to affect multiple running application containers at once?

A. Common libraries

B. Configuration files

C. Sandbox escape

D. ASLR bypass

Correct Answer: A

Reference: https://www.stackrox.com/post/2019/02/the-runc-vulnerability-a-deep-dive-on-protecting-yourself/

QUESTION 2

Which of the following commands will allow a tester to enumerate potential unquoted service paths on a host?

A. wmic environment get name, variablevalue, username | findstr /i "Path" | findstr /i "Service"

B. wmic service get /format:hform > c:\temp\services.html

C. wmic startup get caption, location, command |findstr /i "service" |findstr /v /i "%"

D. wmic service get name, displayname, pathname, startmode |findstr /i "auto" |findstr /i /v "c:\windows\\" |findstr /i /v """"

Correct Answer: D

Reference: https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae

QUESTION 3

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 4

Which of the following can be used to perform online password attacks against RDP?

A. Hashcat

B. John the Rippef

C. Aircrack-ng

D. Ncrack

Correct Answer: D

QUESTION 5

A penetration tester is scoping an engagement with a company that provided a list of firewall rules and a digital network diagram. Which of the following tests would require this data?

A. Network segmentation test

B. Network penetration test

C. Network vulnerability scan

D. Network baseline test

Correct Answer: A

Reference: https://www.pcidssguide.com/pci-network-segmentation-testing/