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

While trying to maintain persistence on a Windows system with limited privileges, which of the following registry keys should the tester use?

A. HKEY_CLASSES_ROOT

B. HKEY_LOCAL_MACHINE

C. HKEY_CURRENT_USER

D. HKEY_CURRENT_CONFIG

Correct Answer: C

Reference: https://www.redcanary.com/blog/windows-registry-attacks-threat-detection/

QUESTION 2

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 3

A MITM attack is being planned. The first step is to get information flowing through a controlled device. Which of the following should be used to accomplish this?

A. Repeating

B. War driving

C. Evil twin

D. Bluejacking

E. Replay attack

Correct Answer: C

Reference: https://www.veracode.com/security/man-middle-attack

QUESTION 4

A penetration tester has a full shell to a domain controller and wants to discover any user account that has not authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

A. dsrm -users "DN=compony.com; OU=hq CN=usera"

B. dsuser -name -account -limit 3

C. dsquery uaer -inactive 3

D. dsquery -o -rein -limit 21

Correct Answer: D

QUESTION 5

A penetration tester, who is not on the client\\'s network. is using Nmap to scan the network for hosts that are in scope. The penetration tester is not receiving any response on the command:

nmap 100.100/1/0-125

Which of the following commands would be BEST to return results?

A. nmap -Pn -sT 100.100.1.0-125

B. nmap -sF -p 100.100.1.0-125

C. nmap -sV -oA output 100.100.10-125

D. nmap 100.100.1.0-125 -T4

Correct Answer: A