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

After successfully enumerating users on an Active Directory domain controller using enum4linux a penetration tester wants to conduct a password-guessing attack Given the below output: Which of the following can be used to extract usernames from the above output prior to conducting the attack?

```
enum4linux_output.txt:
Starting enum4linux v0.8.2 ( https://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Feb 5 11:36:22 2018

---- Users on 192.168.2.55 ----
index: 0x1 RID: 0x1f4 acb: 0x210 Account: Administrator Name: Built-in account for administering the computer/domain
index 0x2 RID: 0x3ee acb: 0x10 Account test Name: test Desc:
index 0x3 RID: 0x3ed acb: 0x215 Account: Guest Name: Guest Desc: Built-in account for guest access to the computer/domain
index 0x4: RID: 0x1f5 acb: 0x214 Account: Test_User Name:Test User Account: Desc:

user:[Administrator] rid:[0x1f4]
user:[test] rid:[0x3ee]
user:[Guest] rid:[0x3ed]
user:[Test_User] rid:[0x1f5]
```

A. cat enum41inux_output.txt > grep -v user I sed `s/\[//\\' I sed `s/\]//\\' 2> usernames.txt

B. grep user enuza41inux_output.txt I awk \\'{print $1}\\' | cut -d[-? I cut -d] -f1>; username.txt

C. grep -i rid v; usernames. txt

D. cut -d: -f2 enum41inux_output.txt | awk \\'{print S2}\\' I cut -d: -f1 > usernaraes.txt

Correct Answer: B

QUESTION 2

A penetration tester was able to enter an SQL injection command into a text box and gain access to the information store on the database. Which of the following is the BEST recommendation that would mitigate the vulnerability?

A. Randomize the credentials used to log in

B. Install host-based intrusion detection

C. Implement input normalization

D. Perform system hardening

Correct Answer: D

QUESTION 3

Consumer-based IoT devices are often less secure than systems built for traditional desktop computers.

Which of the following BEST describes the reasoning for this?

A. Manufacturers developing IoT devices are less concerned with security.

B. It is difficult for administrators to implement the same security standards across the board.

C. IoT systems often lack the hardware power required by more secure solutions.

D. Regulatory authorities often have lower security requirements for IoT systems.

Correct Answer: A

QUESTION 4

When negotiating a penetration testing contract with a prospective client, which of the following disclaimers should be included in order to mitigate liability in case of a future breach of the client\\'s systems?

A. The proposed mitigations and remediations in the final report do not include a cost-benefit analysis.

B. The NDA protects the consulting firm from future liabilities in the event of a breach.

C. The assessment reviewed the cyber key terrain and most critical assets of the client\\'s network.

D. The penetration test is based on the state of the system and its configuration at the time of assessment.

Correct Answer: D

QUESTION 5

A penetration tester wants to target NETBIOS name service. Which of the following is the most likely command to exploit the NETBIOS name service?

A. arPspoof

B. nmap

C. responder

D. burpsuite

Correct Answer: B

Reference: http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/