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.pass2lead.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A penetration tester is performing a black box assessment on a web-based banking application. The tester was only provided with a URL to the login page. Given the below code and output: Which of the following is the tester intending to do?

```
import requests
from BeautifulSoup import BeautifulSoup
request = requests.get("https://www.bank.com/admin")
respHeaders, respBody = request[0], request[1]
if respHeader.statuscode = 200:
        soup = BeautifulSoup(respBody)
        soup = soup.FindAll("div", {"type": "hidden"})
        print respHeader.StatusCode, StatusMessage
else:
        print respHeader.StatusCode, StatusMessage

Output: 200 OK
```

A. Horizontally escalate privileges

B. Scrape the page for hidden fields

C. Analyze HTTP respond code

D. Search for HTTP headers

Correct Answer: D

QUESTION 2

Which of the following tools is used to perform a credential brute force attack?

A. Hydra

B. John the Ripper

C. Hashcat

D. Peach

Correct Answer: A

Reference https://www.greycampus.com/blog/information-security/brute-force-attacks- prominent-tools-totackle-such-

attacks

QUESTION 3

Joe, a penetration tester, was able to exploit a web application behind a firewall He is trying to get a reverse shell back to his machine but the firewall blocks the outgoing traffic Ports for which of the following should the security consultant use to have the HIGHEST chance to bypass the firewall?

A. HTTP

B. SMTP

C. FTP

D. DNS

Correct Answer: A

QUESTION 4

After a recent penetration test, a company has a finding regarding the use of dictionary and seasonal passwords by its employees. Which of the following is the BEST control to remediate the use of common dictionary terms?

A. Expand the password length from seven to 14 characters

B. Implement password history restrictions

C. Configure password filters

D. Disable the accounts after five incorrect attempts

E. Decrease the password expiration window

Correct Answer: A

QUESTION 5

A healthcare organization must abide by local regulations to protect and attest to the protection of personal health information of covered individuals. Which of the following conditions should a penetration tester specifically test for when performing an assessment? (Select TWO).

A. Cleartext exposure of SNMP trap data

B. Software bugs resident in the IT ticketing system

C. S/MIME certificate templates defined by the CA

D. Health information communicated over HTTP

E. DAR encryption on records servers

Correct Answer: DE