

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

<https://www.2passeasy.com/dumps/PT0-001/>



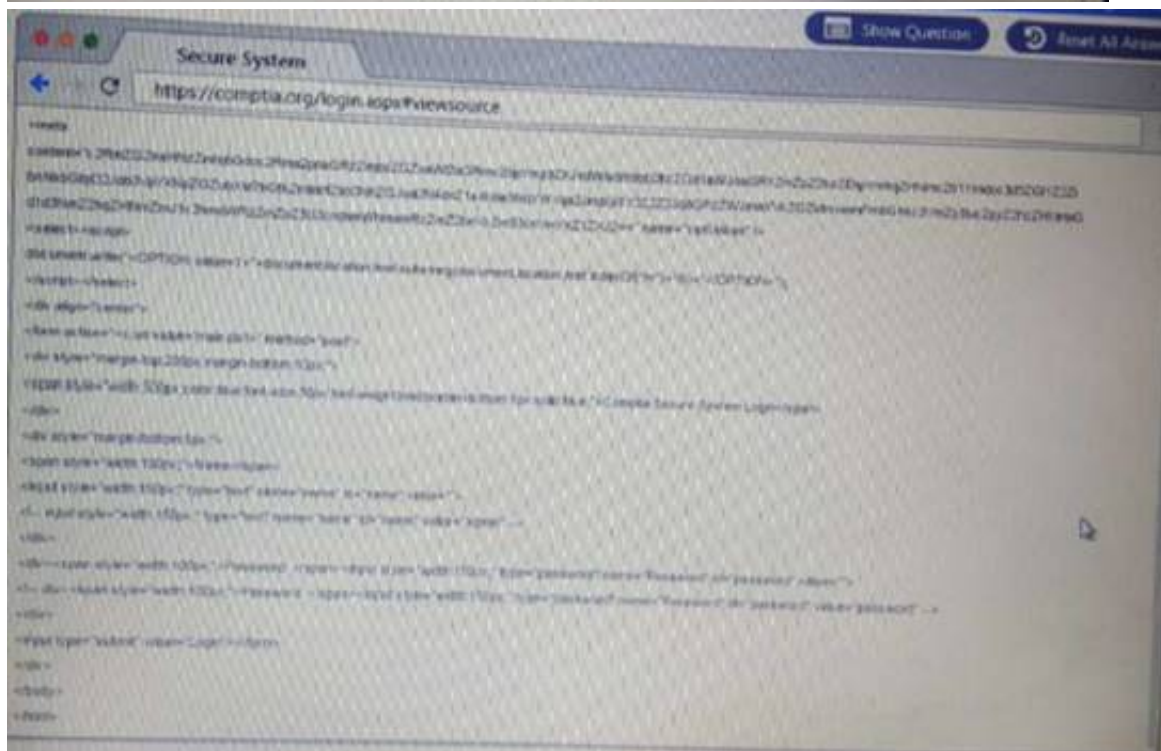
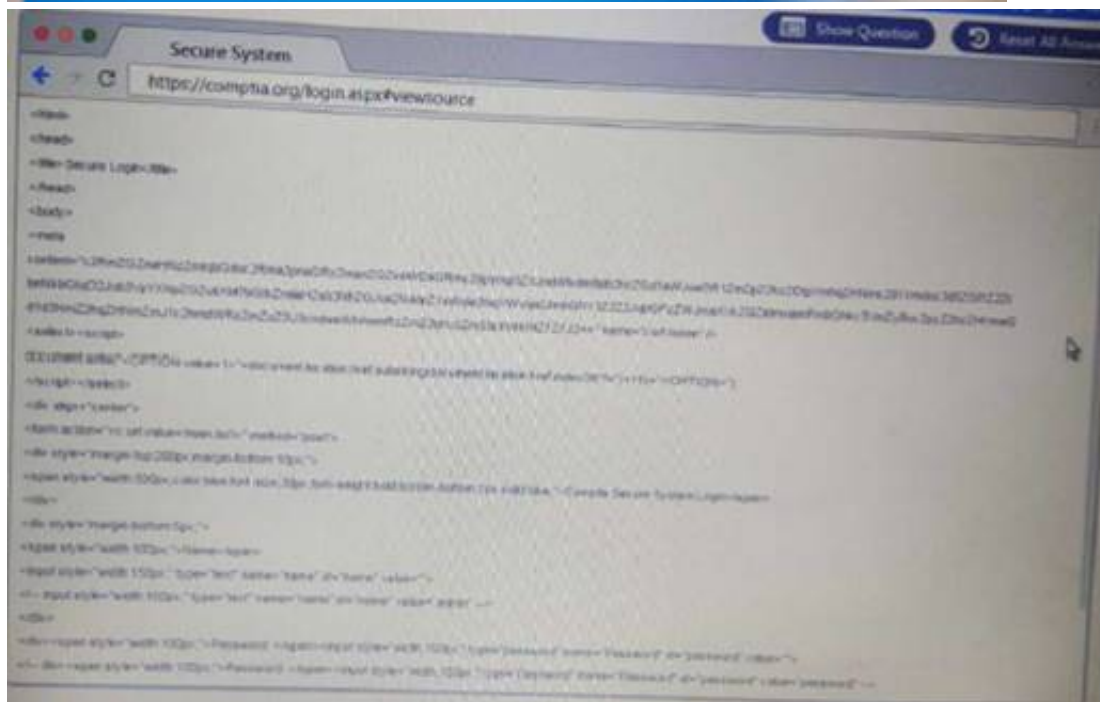
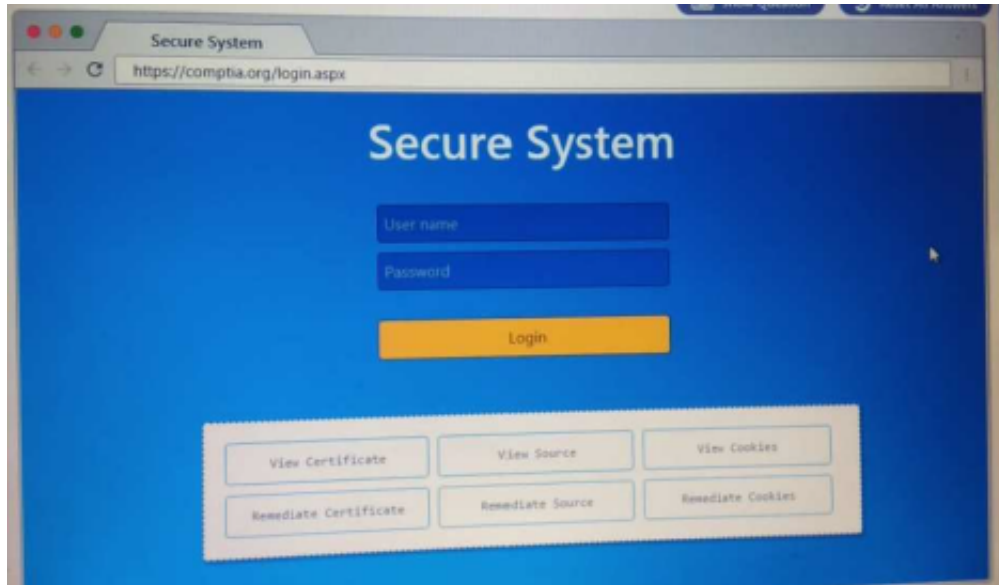
NEW QUESTION 1

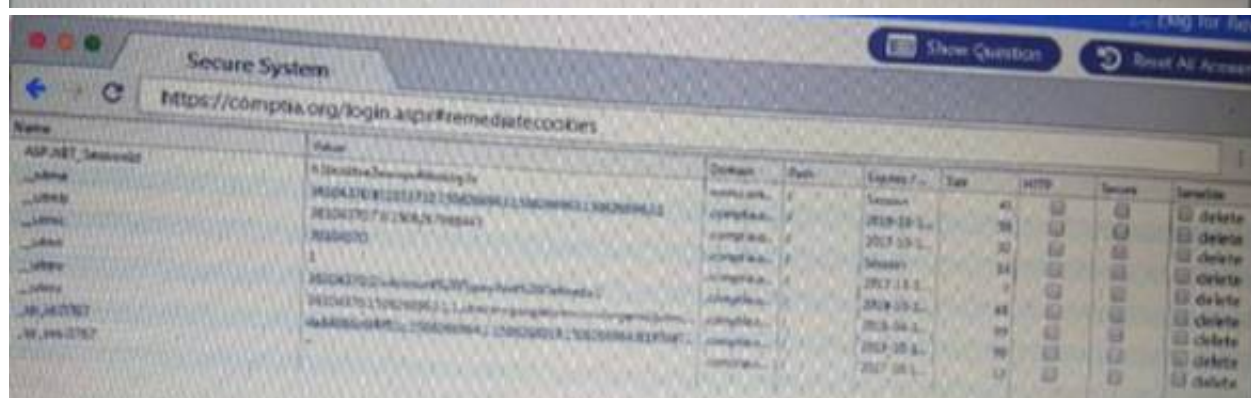
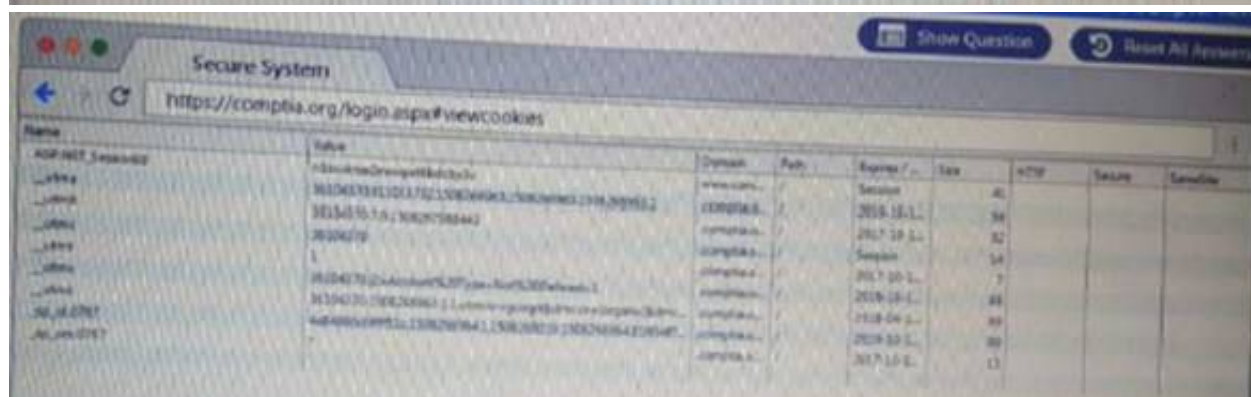
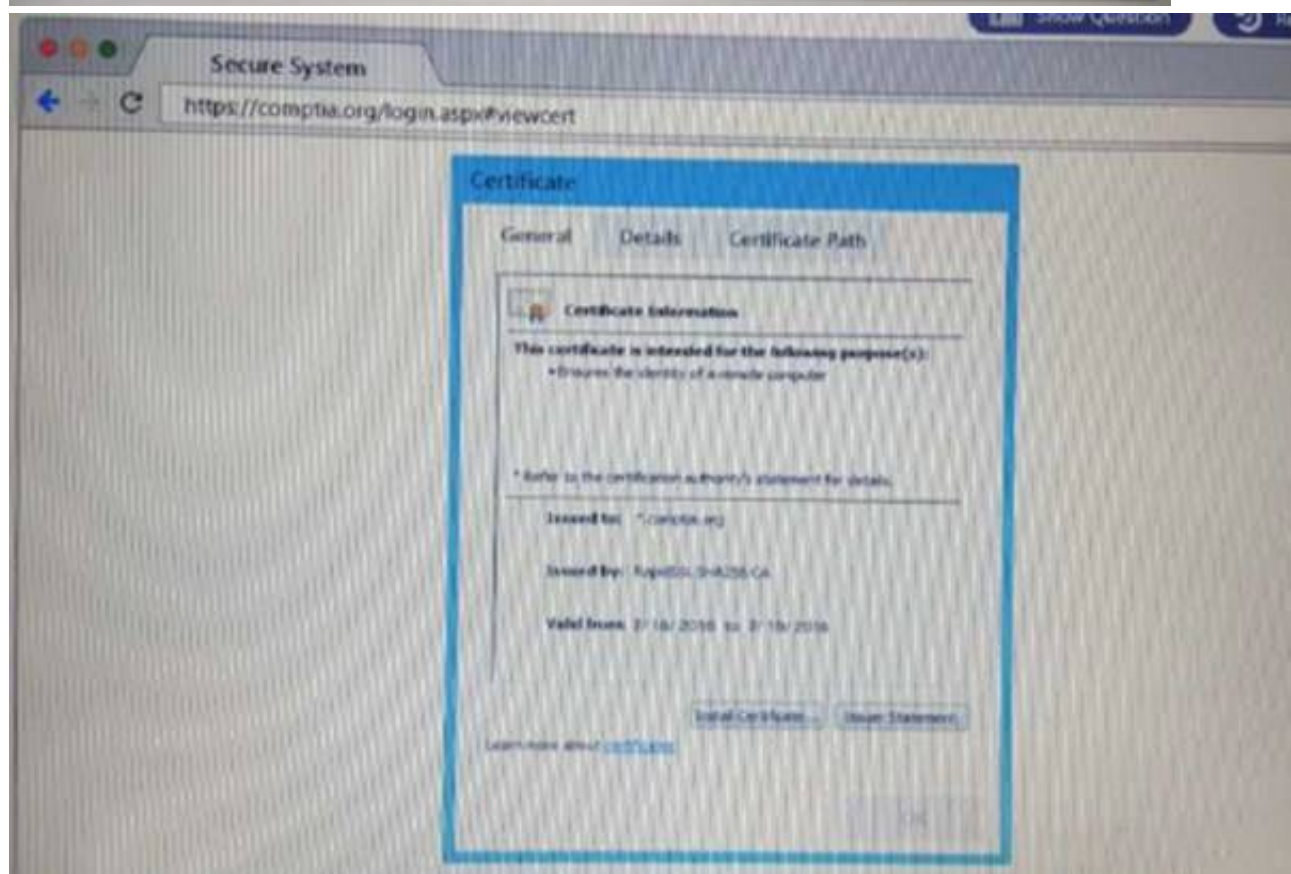
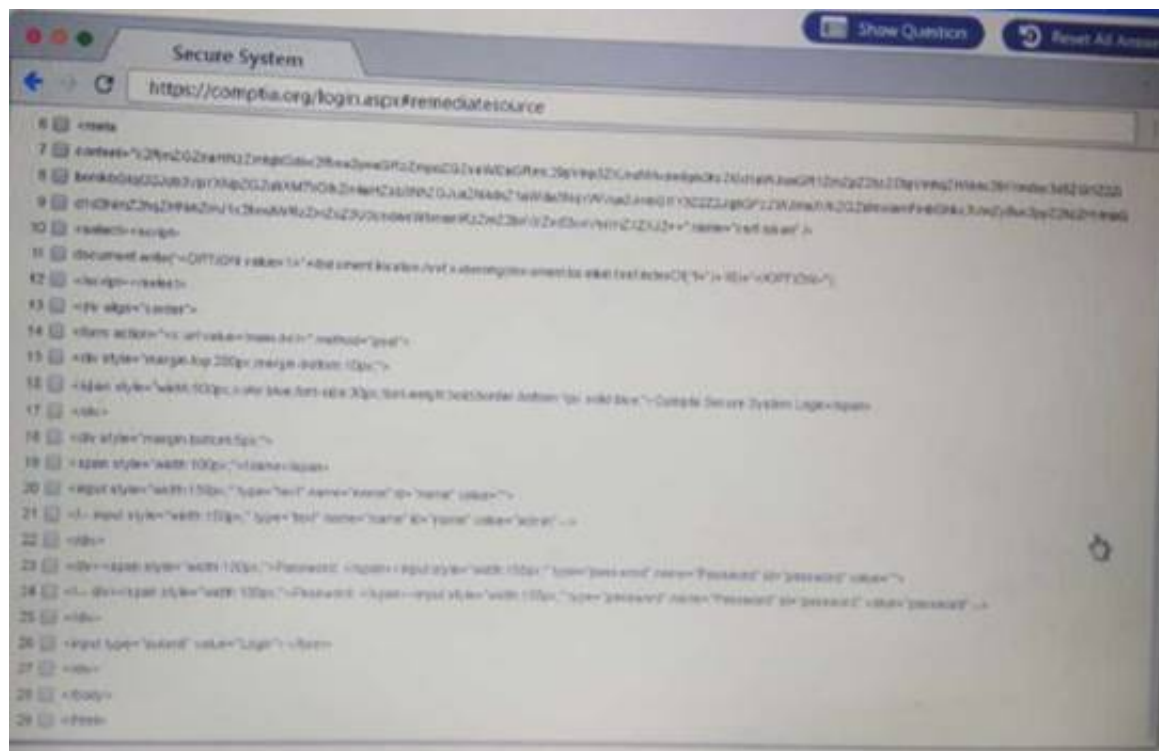
DRAG DROP

Performance based

You are a penetration Inter reviewing a client's website through a web browser. Instructions:

Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate source or cookies.







- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 2

DRAG DROP

Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented. Each password may be used only once.



- A. Mastered
- B. Not Mastered

Answer: A

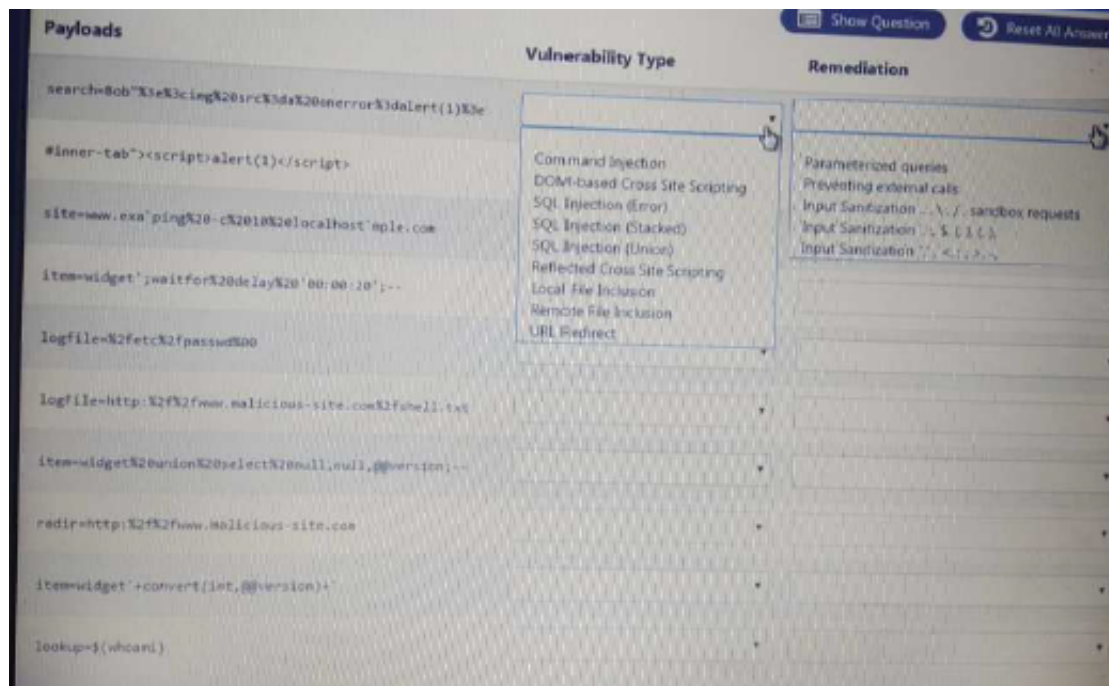
Explanation:

Zverlory
Zverl0ry
zv3rlory
Zv3rl0ry

NEW QUESTION 3

HOTSPOT

You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious.



- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 4

A constant wants to scan all the TCP Ports on an identified device. Which of the following Nmap switches will complete this task?

- A. -p-
- B. -p ALX,
- C. -p 1-65534
- D. -port 1-65534

Answer: A

NEW QUESTION 5

A client is asking a penetration tester to evaluate a new web application for availability. Which of the following types of attacks should the tester use?

- A. TCP SYN flood
- B. SQL injection
- C. xss
- D. XMAS scan

Answer: A

NEW QUESTION 6

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

Answer: D

NEW QUESTION 7

An assessor begins an internal security test of the Windows domain internal.comptia.net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A)

```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)

```
dig -q any _lanman._tcp.internal.comptia.net
```

C)

```
dig -q any _ntlm._tcp.internal.comptia.net
```

D)

```
dig -q any _smtp._tcp.internal.comptia.net
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 8

The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

- A. Storage access
- B. Limited network access
- C. Misconfigured DHCP server
- D. Incorrect credentials
- E. Network access controls

Answer: A

NEW QUESTION 9

When performing compliance-based assessments, which of the following is the MOST important Key consideration?

- A. Additional rate
- B. Company policy
- C. Impact tolerance
- D. Industry type

Answer: A

NEW QUESTION 10

An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever sending the email. Which of the following types of motivation was used in this attack?

- A. Principle of fear
- B. Principle of authority
- C. Principle of scarcity

- D. Principle of likeness
- E. Principle of social proof

Answer: E

NEW QUESTION 10

A recently concluded penetration test revealed that a legacy web application is vulnerable to SQL injection. Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not in a position to risk the availability of the application. Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Select TWO).

- A. Identify and eliminate inline SQL statements from the code.
- B. Identify and eliminate dynamic SQL from stored procedures.
- C. Identify and sanitize all user inputs.
- D. Use a whitelist approach for SQL statements.
- E. Use a blacklist approach for SQL statements.
- F. Identify the source of malicious input and block the IP address.

Answer: DE

NEW QUESTION 12

Given the following script:

```
import pyHook, pythoncom, logging, sys
f="f.txt"
def OnKeyboardEvent(event):
    logging.basicConfig(filename=f, level=logging.DEBUG, format='%(message)s')
    chr(event.Ascii)
    logging.log(10, chr(event.Ascii))
    return True

hm = pyHook.HookManager()
hm.KeyDown=OnKeyboardEvent
hm.HookKeyboard()
pythoncom.PumpMessages()
```

Which of the following BEST describes the purpose of this script?

- A. Log collection
- B. Event logging
- C. Keystroke monitoring
- D. Debug message collection

Answer: C

NEW QUESTION 17

A penetration tester is performing a remote scan to determine if the server farm is compliant with the company's software baseline. Which of the following should the penetration tester perform to verify compliance with the baseline?

- A. Discovery scan
- B. Stealth scan
- C. Full scan
- D. Credentialed scan

Answer: A

NEW QUESTION 19

A penetration test was performed by an on-staff technician's junior technician. During the test, the technician discovered the application could disclose an SQL table with user account and password information. Which of the following is the MOST effective way to notify management of this finding and its importance?

- A. Document the findings with an executive summary, recommendations, and screenshots of the web application disclosure.
- B. Connect to the SQL server using this information and change the password to one or two noncritical accounts to demonstrate a proof-of-concept to management.
- C. Notify the development team of the discovery and suggest that input validation be implemented on the web application's SQL query strings.
- D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Answer: B

NEW QUESTION 22

A tester has captured a NetNTLMv2 hash using Responder. Which of the following commands will allow the tester to crack the hash using a mask attack?

- A. hashcat -m 5600 -r rulea/beat64.rule hash.txt wordlist.txt
- B. hashcat -m 5600 hash.txt
- C. hashcat -m 5600 -a 3 hash.txt ?a?a?a?a?a?a
- D. hashcat -m 5600 -o result.txt hash.txt wordlist.txt

Answer: A

NEW QUESTION 25

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PT0-001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PT0-001 Product From:

<https://www.2passeasy.com/dumps/PT0-001/>

Money Back Guarantee

PT0-001 Practice Exam Features:

- * PT0-001 Questions and Answers Updated Frequently
- * PT0-001 Practice Questions Verified by Expert Senior Certified Staff
- * PT0-001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PT0-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year