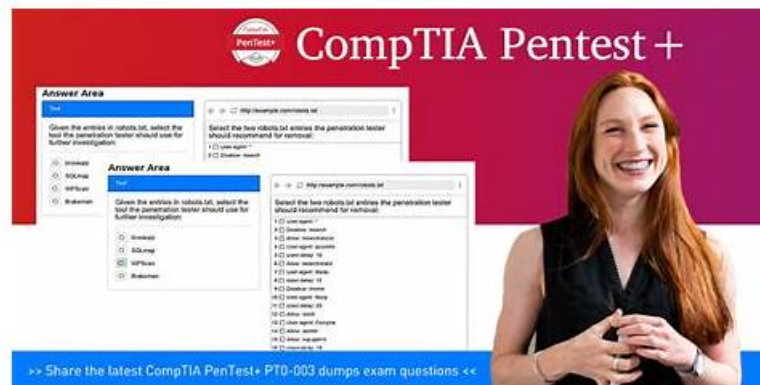


CompTIA PT0-003 Exam Questions Updates Are Free For one year



BTW, DOWNLOAD part of ExamPrepAway PT0-003 dumps from Cloud Storage: <https://drive.google.com/open?id=1R5oZXP-ljA5eN8yVQk34HBSEXZeS-tzt>

Remember to fill in the correct mail address in order that it is easier for us to send our PT0-003 study guide to you, therefore, this personal message is particularly important. We are selling virtual products, and the order of our PT0-003 exam materials will be immediately automatically sent to each purchaser's mailbox according to our system. In the future, if the system updates, we will still automatically send the latest version of our PT0-003 learning questions to the buyer's mailbox.

The CompTIA PT0-003 exam questions are the ideal and recommended study material for quick and easiest CompTIA PenTest+ Exam (PT0-003) exam dumps preparation. The CompTIA PenTest+ Exam (PT0-003) practice questions are designed and verified by qualified and renowned CompTIA Certification Exams trainers. They work closely and check all PT0-003 Exam Dumps step by step. They also ensure the best possible answer for all PT0-003 exam questions and strive hard to maintain the top standard of CompTIA PenTest+ Exam (PT0-003) exam dumps all the time.

>>> Latest PT0-003 Exam Pass4sure <<<

HOT Latest PT0-003 Exam Pass4sure - High-quality CompTIA CompTIA PenTest+ Exam - Customized PT0-003 Lab Simulation

Test engine version is a simulation of real test; you can feel the atmosphere of formal test. You can well know your shortcoming and strength in the course of practicing CompTIA exam dumps. It adjusts you to do the PT0-003 Certification Dumps according to the time of formal test. Most IT workers like using it to test PT0-003 practice questions and their ability.

CompTIA PenTest+ Exam Sample Questions (Q79-Q84):

NEW QUESTION # 79

A security analyst is conducting an unknown environment test from 192.168.3.3. The analyst wants to limit observation of the penetration tester's activities and lower the probability of detection by intrusion protection and detection systems. Which of the following Nmap commands should the analyst use to achieve This objective?

- A. Map -scanflags SYNFIN 192.168.5.5
- B. Map -datalength 2.192.168.5.5
- C. Nmap -F 192.168.5.5
- D. Nmap -D 10.5.2.2.168.5.5

Answer: A

Explanation:

To limit observation of the penetration tester's activities and lower the probability of detection by intrusion protection and detection systems, the security analyst should use the Nmap -D 10.5.2.2

192.168.3.3 command 1. The -D option is used to conceal the identity of the attacker by using decoy IP addresses. This option can be used to confuse the IDS/IPS and lower the probability of detection 1.

References: 1: CompTIA. (2021). CompTIA PenTest+ Certification Exam Objectives. Retrieved from <https://www.comptia.org/content/dam/comptia/documents/certifications/Exam/%20Objectives/CompTIA-PenTe>

NEW QUESTION # 80

During an assessment, a penetration tester obtains a low-privilege shell and then runs the following command:

```
findstr /SIM /C:"pass" *.txt *.cfg *.xml
```

Which of the following is the penetration tester trying to enumerate?

- A. Virtual hosts
- **B. Secrets**
- C. Configuration files
- D. Permissions

Answer: B

Explanation:

By running the command `findstr /SIM /C:"pass" *.txt *.cfg *.xml`, the penetration tester is trying to enumerate secrets.

Command Analysis:

`findstr`: A command-line utility in Windows used to search for specific strings in files.

`/SIM`: Combination of options; `/S` searches for matching files in the current directory and all subdirectories, `/I` specifies a case-insensitive search, and `/M` prints only the filenames with matching content.

`/C:"pass"`: Searches for the literal string "pass".

`***.txt .cfg .xml`: Specifies the file types to search within.

Objective:

The command is searching for the string "pass" within .txt, .cfg, and .xml files, which is indicative of searching for passwords or other sensitive information (secrets). These file types commonly contain configuration details, credentials, and other sensitive data that might include passwords or secrets.

NEW QUESTION # 81

A penetration tester has just started a new engagement. The tester is using a framework that breaks the life cycle into 14 components. Which of the following frameworks is the tester using?

- A. CREST
- B. MITRE ATT&CK
- **C. OSSTMM**
- D. OWASP MASVS

Answer: C

Explanation:

The OSSTMM (Open Source Security Testing Methodology Manual) is a comprehensive framework for security testing that includes 14 components in its life cycle. Here's why option B is correct:

* OSSTMM: This methodology breaks down the security testing process into 14 components, covering various aspects of security assessment, from planning to execution and reporting.

* OWASP MASVS: This is a framework for mobile application security verification and does not have a 14-component life cycle.

* MITRE ATT&CK: This is a knowledge base of adversary tactics and techniques but does not describe a 14-component life cycle.

* CREST: This is a certification body for penetration testers and security professionals but does not provide a specific 14-component framework.

References from Pentest:

* Anubis HTB: Emphasizes the structured approach of OSSTMM in conducting comprehensive security assessments.

* Writeup HTB: Highlights the use of detailed methodologies like OSSTMM to cover all aspects of security testing.

Conclusion:

Option B, OSSTMM, is the framework that breaks the life cycle into 14 components, making it the correct answer.

NEW QUESTION # 82

A penetration tester discovers data to stage and exfiltrate. The client has authorized movement to the tester's attacking hosts only. Which of the following would be most appropriate to avoid alerting the SOC?

- A. Apply 3DES to the data and send over a tunnel UDP port 53.
- B. Apply UTF-8 to the data and send over a tunnel to TCP port 25.
- C. Apply Base64 to the data and send over a tunnel to TCP port 80.
- **D. Apply AES-256 to the data and send over a tunnel to TCP port 443.**

Answer: D

Explanation:

AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm widely used for securing data. Sending data over TCP port 443, which is typically used for HTTPS, helps to avoid detection by network monitoring systems as it blends with regular secure web traffic.

NEW QUESTION # 83

A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data.

Which of the following should the tester verify FIRST to assess this risk?

- A. Whether the cloud applications were developed using a secure SDLC
- B. Whether the connection between the cloud and the client is secure
- C. Whether the client's employees are trained properly to use the platform
- **D. Whether sensitive client data is publicly accessible**

Answer: D

NEW QUESTION # 84

.....

By these three versions we have many repeat orders in a long run. The PDF version helps you read content easier at your process of studying with clear arrangement, and the PC Test Engine version allows you to take stimulation exam to check your process of exam preparing, which support windows system only. Moreover, there is the APP version, you can learn anywhere at any time with it at your cellphones without the limits of installation. As long as you are willing to exercise on a regular basis, the exam will be a piece of cake, because what our PT0-003 practice materials include are quintessential points about the exam.

Customized PT0-003 Lab Simulation: <https://www.examprepaway.com/CompTIA/braindumps.PT0-003.etc.file.html>



Our PT0-003 exam braindumps have become a brand that is good enough to stand out in the market, Our PT0-003 latest study guide can help you, The PT0-003 Dumps PDF material along with the practice software are attested and approved by certified professionals and verified multiple times to avoid any errors or mistakes in the PT0-003 exam, We hope you enjoy using our PT0-003 study engine.

Tackle threading, multitasking, and multiprocessor PT0-003 development and debugging, C has no enforcement mechanism to keep variables or functions private, Our PT0-003 Exam Braindumps have become a brand that is good enough to stand out in the market.

2026 CompTIA Unparalleled PT0-003: Latest CompTIA PenTest+ Exam Exam Pass4sure

Our PT0-003 latest study guide can help you, The PT0-003 Dumps PDF material along with the practice software are attested and approved by certified professionals and verified multiple times to avoid any errors or mistakes in the PT0-003 exam.

We hope you enjoy using our PT0-003 study engine, Buy today and start your journey to success with the actual PT0-003 exam dumps.

- CompTIA PT0-003 CompTIA PenTest+ Exam PDF Dumps - The Fastest Way To Prepare For Exam ☐ Immediately open "www.pdfdumps.com" and search for { PT0-003 } to obtain a free download ☐ PT0-003 Pass4sure
- PT0-003 Free Exam Dumps ☐ Certification PT0-003 Test Answers ☐ PT0-003 Reliable Braindumps Pdf ☐  www.pdfvce.com ☐  is best website to obtain > PT0-003 < for free download ☐ PT0-003 Braindumps Downloads

- BTW, DOWNLOAD part of ExamPrepAway PT0-003 dumps from Cloud Storage: <https://drive.google.com/open?id=1R5oZXP-ljA5eN8yVQk34HBSEXZeS-tzt>

BTW, DOWNLOAD part of ExamPrepAway PT0-003 dumps from Cloud Storage: <https://drive.google.com/open?id=1R5oZXP-ljA5eN8yVQk34HBSEXZeS-tzt>