

Free PDF Quiz 2025 PT0-002: CompTIA PenTest+ Certification—Trustable Mock Exams

CompTIA

PenTest+

PT0-002

256 Practice Test Questions

in PDF Format with Verified Answers

What's more, part of that DumpStillValid PT0-002 dumps now are free: <https://drive.google.com/open?id=1v-AHMReMxvhyLtvG0zyUbHhSzPpLkaqW>

Our product boosts many merits and high passing rate. Our products have 3 versions and we provide free update of the CompTIA exam torrent to you. If you are the old client you can enjoy the discounts. Most important of all, as long as we have compiled a new version of the PT0-002 Exam Questions, we will send the latest version of our CompTIA exam questions to our customers for free during the whole year after purchasing. Our product can improve your stocks of knowledge and your abilities in some area and help you gain the success in your career.

CompTIA PT0-002 exam seeks to evaluate the candidate's knowledge on the elaboration, implementation, management, and reporting on the whole penetration testing process, in addition to the different tools and techniques that are used to streamline and facilitate the process. It covers different areas such as network, application, and wireless penetration testing, in addition to reporting techniques, threat detection, and risk management.

CompTIA PT0-002 Certification Exam is vendor-neutral, which means that it is not tied to any particular product, technology, or manufacturer. It makes the certification valuable as it tests the candidate's abilities to apply the concepts and practices of penetration testing regardless of the employed technologies. Moreover, it opens up various job opportunities across different industries as this certification is widely recognized worldwide.

>> Mock PT0-002 Exams <<

PT0-002 Reasonable Exam Price & Verified PT0-002 Answers

DumpStillValid follows its motto to facilitate its consumer by providing them the material to qualify for the CompTIA PT0-002 certification exam with excellence. Therefore, it materializes its mission by giving them free of cost CompTIA PT0-002 demo of the dumps. This practical step taken by the DumpStillValid will enable its users to assess the quality of the CompTIA PT0-002 dumps.

CompTIA PenTest+ Certification Sample Questions (Q330-Q335):

NEW QUESTION # 330

A penetration tester is performing an assessment for an application that is used by large organizations operating in the heavily regulated financial services industry. The penetration tester observes that the default Admin User account is enabled and appears to be used several times a day by unfamiliar IP addresses. Which of the following is the most appropriate way to remediate this issue?

- A. Increase password complexity.
- B. Implement system hardening.
- C. Restrict simultaneous user log-ins.
- **D. Require local network access.**

Answer: D

Explanation:

Requiring local network access for the default Admin User account is a targeted measure to prevent unauthorized access from unfamiliar IP addresses, particularly those originating from outside the organization's network. This approach ensures that only devices physically connected to or authenticated within the local network can attempt to use the Admin User account, significantly reducing the risk of external attacks. Increasing password complexity and restricting simultaneous log-ins are good practices but do not directly address the issue of access from unfamiliar IPs. System hardening is broader and not specifically focused on the Admin User account issue.

NEW QUESTION # 331

During an engagement, a penetration tester found the following list of strings inside a file:

```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fcee6f640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421epabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503be8
d12e624a20d54fd3b34b89ee7169d17
```

Which of the following is the BEST technique to determine the known plaintext of the strings?

- **A. Rainbow table attack**
- B. Brute-force attack
- C. Credential-stuffing attack
- D. Dictionary attack

Answer: A

NEW QUESTION # 332

A CentOS computer was exploited during a penetration test. During initial reconnaissance, the penetration tester discovered that port 25 was open on an internal Sendmail server. To remain stealthy, the tester ran the following command from the attack machine:

```
nc 10.10.1.2 25
```

Which of the following would be the BEST command to use for further progress into the targeted network?

- A. nc 10.10.1.2
- B. ssh 127.0.0.1 5555
- **C. nc 127.0.0.1 5555**
- D. ssh 10.10.1.2

Answer: C

NEW QUESTION # 333

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:

```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?

- A. Run an application vulnerability scan and then identify the TCP ports used by the application.
- B. Disassemble the binary code and then identify the break points.
- **C. Start a packet capture with Wireshark and then run the application.**
- D. Run the application attached to a debugger and then review the application's log.

Answer: C

NEW QUESTION # 334

Which of the following OSSTM testing methodologies should be used to test under the worst conditions?

- A. Reversal
- B. Semi-authorized
- C. Tandem
- **D. Known environment**

Answer: D

Explanation:

Explanation

The OSSTM testing methodology that should be used to test under the worst conditions is known environment, which is a testing approach that assumes that the tester has full knowledge of the target system or network, such as its architecture, configuration, vulnerabilities, or defenses. A known environment testing can simulate a worst-case scenario, where an attacker has gained access to sensitive information or insider knowledge about the target, and can exploit it to launch more sophisticated or targeted attacks. A known environment testing can also help identify the most critical or high-risk areas of the target, and provide recommendations for improving its security posture. The other options are not OSSTM testing methodologies that should be used to test under the worst conditions. Tandem is a testing approach that involves two testers working together on the same target, one as an attacker and one as a defender, to simulate a realistic attack scenario and evaluate the effectiveness of the defense mechanisms. Reversal is a testing approach that involves switching roles between the tester and the client, where the tester acts as a defender and the client acts as an attacker, to assess the security awareness and skills of the client. Semi-authorized is a testing approach that involves giving partial or limited authorization or access to the tester, such as a user account or a network segment, to simulate an attack scenario where an attacker has compromised a legitimate user or device.

NEW QUESTION # 335

.....

Learning knowledge is not only to increase the knowledge reserve, but also to understand how to apply it, and to carry out the theories and principles that have been learned into the specific answer environment. Studying for attending CompTIA PenTest+ Certification exam pays attention to the method. The good method often can bring the result with half the effort, therefore we in the examination time, and also should know some test-taking skill. The PT0-002 Quiz guide on the basis of summarizing the past years, found that many of the questions, the answers have certain rules can be found, either subjective or objective questions, we can find in the corresponding module of similar things in common.

PT0-002 Reasonable Exam Price: <https://www.dumpstillvalid.com/PT0-002-prep4sure-review.html>

- PT0-002 Test Guide ☐ PT0-002 Reliable Test Objectives ☐ Reliable PT0-002 Test Objectives ☐ Search for 《 PT0-002 》 and download it for free on ⇒ www.lead4pass.com ⇐ website ☐ PT0-002 Exams Torrent
- Quiz Professional PT0-002 - Mock CompTIA PenTest+ Certification Exams ☐ Enter ⇒ www.pdfvce.com ☐ and search for ⇒ PT0-002 ☐ ☐ ☐ to download for free ☐ Valid Dumps PT0-002 Book
- PT0-002 Valid Exam Preparation ☐ Valid Test PT0-002 Tutorial ☐ PT0-002 Valid Exam Preparation ☐ Download ▷

- PT0-002 < for free by simply searching on ✓ www.prep4away.com ✓ □ □ Latest PT0-002 Study Materials
- Free PDF Quiz PT0-002 - Pass-Sure Mock CompTIA PenTest+ Certification Exams □ Search for > PT0-002 □ and download exam materials for free through ➡ www.pdfvce.com □ □ □ Formal PT0-002 Test
 - CompTIA PT0-002 Exam| Mock PT0-002 Exams - Bring you The Best PT0-002 Reasonable Exam Price □ Easily obtain ⇒ PT0-002 ⇐ for free download through ▶ www.exams4collection.com ◀ □ Exam PT0-002 Study Guide
 - 2025 CompTIA PT0-002: Unparalleled Mock CompTIA PenTest+ Certification Exams □ Search for (PT0-002) on ➡ www.pdfvce.com □ immediately to obtain a free download □ PT0-002 Exams Torrent
 - Valid PT0-002 Dumps Demo □ PT0-002 New APP Simulations Ⓢ Reliable PT0-002 Test Objectives □ Go to website □ www.examcollectionpass.com □ open and search for 「 PT0-002 」 to download for free □ PT0-002 New APP Simulations
 - Valid Test PT0-002 Tutorial □ PT0-002 Exams Torrent □ Latest Study PT0-002 Questions □ Search for ➡ PT0-002 □ □ □ and download exam materials for free through [www.pdfvce.com] □ PT0-002 Test Guide
 - 2025 CompTIA PT0-002: Unparalleled Mock CompTIA PenTest+ Certification Exams □ Immediately open ☀ www.itcerttest.com □ ☀ □ and search for ▶ PT0-002 ◀ to obtain a free download □ PT0-002 Latest Exam Guide
 - 100% Pass Quiz PT0-002 - CompTIA PenTest+ Certification Accurate Mock Exams □ Simply search for ▷ PT0-002 ◀ for free download on ▷ www.pdfvce.com ◀ □ PT0-002 Exams Torrent
 - CompTIA PenTest+ Certification Exam Dumps Question is the Successful Outcomes of Professional Team - www.lead1pass.com □ Search for ➡ PT0-002 □ and download it for free immediately on [www.lead1pass.com] □ □ Exam PT0-002 Study Guide
 - edu.openu.in, www.stes.tyc.edu.tw, pct.edu.pk, seginternationalcollege.com, daninicourse.com, joshwhi204.bloggadores.com, e-cademy.online, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, courses.learnwells.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New PT0-002 dumps are available on Google Drive shared by DumpStillValid: <https://drive.google.com/open?id=1v-AHMReMxvhyLtvG0zyUbHhSzPpLkaqW>