# Reliable PT0-002 Exam Simulator Fee & Leading Offer in Qualification Exams & Authorized CompTIA CompTIA PenTest+ Certification


DOWNLOAD the newest ActualTorrent PT0-002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1pgku3DcE77d1JZSaruZW8X_UC3WkYON-

We are a certificate exam materials providers, our company is also in a leading position in provide exam braindumps. With the experienced professionals to edit and examine, the PT0-002 exam dumps is high-quality. We have three versions for the PT0-002 Exam Dumps, and you can choose the right one according to your demands. Besides, we offer you free update for one year after buying the PT0-002 exam dumps, and pass guarantee and money back guarantee.

CompTIA PT0-002 exam is designed to test candidates' hands-on technical skills to conduct real-world penetration testing and vulnerability assessments. It's a performance-based exam that emphasizes testing the actual abilities and knowledge of the practitioner. That's why the CompTIA PenTest+ certification is in high demand from organizations who want individuals that can perform advanced penetration testing and vulnerability assessments. Practitioners who pass the CompTIA PT0-002 exam can evaluate designs, implement secure solutions, and identify weaknesses to help organizations mitigate risk.

CompTIA PenTest+ exam (PT0-002) is a globally recognized certification that is designed to validate your technical knowledge and skills in penetration testing. PT0-002 Exam is intended for cybersecurity professionals who possess intermediate to advanced-level knowledge of offensive cybersecurity testing, vulnerability management, and analytical techniques. PT0-002 exam covers five domains, which include planning and scoping, information gathering and vulnerability identification, attacks and exploits, and reporting and communication.

**>> PT0-002 Exam Simulator Fee <<**

## Free PDF 2025 CompTIA Unparalleled PT0-002 Exam Simulator Fee

We declare that we can ensure you 100% pass, because we have the real exam questions for the PT0-002 actual test. All the questions of CompTIA PT0-002 test pdf are taken from current pool of actual test, then after refined and checked, compiled into the complete dumps. Furthermore, the answers are correct and verified by our IT experts with decades of hands-on experience. So the high quality and accuracy of PT0-002 Cert Guide are without any doubt. With our 100 % pass rate history & money back guarantee, you can rest assured to choose our PT0-002 vce files.

## CompTIA PenTest+ Certification Sample Questions (Q177-Q182):

**NEW QUESTION # 177**
Which of the following situations would require a penetration tester to notify the emergency contact for the engagement?

- A. The team discovers another actor on a system on the network.

- B. The team exploits a critical server within the organization.
- C. The team loses access to the network remotely.
- D. The team exfiltrates PII or credit card data from the organization.

**Answer: A**

**NEW QUESTION # 178**
A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be
valid?

- A. Supervisors and controllers are on a separate virtual network by default.
- B. Controllers will not validate the origin of commands.
- C. Supervisory systems will detect a malicious injection of code/commands.
- D. PLCs will not act upon commands injected over the network.

**Answer: B**

Explanation:
PLCs are programmable logic controllers that execute logic operations on input signals from sensors and output signals to actuators. They are often connected to supervisory systems that provide human-machine interfaces and data acquisition functions. If both systems are connected to the company intranet, they are exposed to potential attacks from internal or external adversaries. A valid assumption is that controllers will not validate the origin of commands, meaning that an attacker can send malicious commands to manipulate or sabotage the industrial process. The other assumptions are not valid because they contradict the facts or common practices.

**NEW QUESTION # 179**
A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

- A. Meta tagging
- B. RFID tagging
- C. Tag nesting
- D. RFID cloning

**Answer: C**

Explanation:
since vlan hopping requires 2 vlans to be nested in a single packet. Double tagging occurs when an attacker adds and modifies tags on an Ethernet frame to allow the sending of packets through any VLAN. This attack takes advantage of how many switches process tags. Most switches will only remove the outer tag and forward the frame to all native VLAN ports. With that said, this exploit is only successful if the attacker belongs to the native VLAN of the trunk link.https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation Tag nesting is a technique that involves inserting two VLAN tags into an Ethernet frame to bypass VLAN hopping prevention mechanisms. The first tag is stripped by the first switch, and the second tag is processed by the second switch, allowing the frame to reach a different VLAN than intended. RFID cloning is a technique that involves copying the data from an RFID tag to another tag or device. RFID tagging is a technique that involves attaching an RFID tag to an object or person for identification or tracking purposes.
Meta tagging is a technique that involves adding metadata to web pages or files for search engine optimization or classification purposes.

**NEW QUESTION # 180**
Which of the following is the MOST important information to have on a penetration testing report that is written for the developers?

- A. Metrics and measures
- B. Methodology
- C. Remediation

- D. Executive summary

**Answer: C**

Explanation:
Explanation
The most important information to have on a penetration testing report that is written for the developers is remediation. Remediation is the process of fixing or mitigating the vulnerabilities or issues that were discovered during the penetration testing. Remediation should include specific recommendations, best practices, and resources to help the developers improve the security of their applications4.

**NEW QUESTION # 181**
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:

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

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

**Answer: D**

**NEW QUESTION # 182**
.....

In modern society, everything is changing so fast with the development of technology. If you do no renew your knowledge and skills, you will be wiped out by others. Our PT0-002 study materials also keep up with the society. After all, new technology has been applied in many fields. It is time to strengthen your skills. Our PT0-002 Study Materials will help you master the most popular skills in the job market. Then you will have a greater chance to find a desirable job. Also, it doesn't matter whether have basic knowledge about the PT0-002 study materials.

Test Tips

- study.stcs.edu.np, lms.ait.edu.za, muketm.cn, motionentrance.edu.np, ncon.edu.sa, learnvernac.co.za, tinnitusheal.com, www.stes.tyc.edu.tw, thewealthprotocol.io, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New PT0-002 dumps are available on Google Drive shared by ActualTorrent: https://drive.google.com/open?id=1pgku3DcE77d1JZSaruZW8X_UC3WkYON-