Answers PT0-002 Free, Demo PT0-002 Test

What's more, part of that 2Pass4sure PT0-002 dumps now are free: https://drive.google.com/open?id=1u8zxNd--d_9_gnglSJ9G2BnIc_8Sxn_X

The passing rate of our PT0-002 training braindump is 99% which means that you almost can pass the PT0-002 test with no doubts. The reasons why our PT0-002 test guide' passing rate is so high are varied. That is because our test bank includes two forms and they are the PDF test questions which are selected by the senior lecturer, published authors and professional experts and the practice test software which can test your mastery degree of our PT0-002 study question at any time. The two forms cover the syllabus of the entire PT0-002 test. You will pass the PT0-002 exam with it.

The privacy protection of users is an eternal issue in the internet age. Many illegal websites will sell users' privacy to third parties, resulting in many buyers are reluctant to believe strange websites. But you don't need to worry about it at all when buying our PT0-002 Learning Engine. We assure you that we will never sell users' information on the PT0-002 exam questions because it is damaging our own reputation. And we will help you on the PT0-002 study materials if you have any question.

>> Answers PT0-002 Free <<

2025 Reliable Answers PT0-002 Free | CompTIA PenTest+ Certification 100% Free Demo Test

Users are buying something online (such as PT0-002 learning materials), always want vendors to provide a fast and convenient sourcing channel to better ensure the user's use. Because without a quick purchase process, users of our PT0-002 learning materials will not be able to quickly start their own review program. So, our company employs many experts to design a fast sourcing channel for our PT0-002 Learning Materials. All users can implement fast purchase and use our learning materials.

If you're someone interested in pursuing a career in the field of cybersecurity, one of the certifications that you should consider getting is the CompTIA PT0-002 (CompTIA PenTest+) Certification Exam. PT0-002 examination is designed to measure your knowledge and understanding of penetration testing, and whether or not you have the skills necessary to perform them in a safe, ethical, and effective manner.

CompTIA PenTest+ Certification Sample Questions (Q98-Q103):

NEW QUESTION # 98
A penetration tester wrote the following script to be used in one engagement:

```
#!/usr/bin/python
import socket,sys
ports = [21,22,23,25,80,139,443,445,3306,3389]
if len(sys.argv) == 2:
        target = socket.gethostbyname(sys.argv[1])
else:
        print("Too few arguments.")
        print("Syntax: python {} <>".format(sys.argv[0]))
        sys.exit()
try:
        for port in ports:
                s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
                s.settimeout(2)
                results = s.connect_ex((target,port))
                if result == 0:
                        print("Port {} is opened".format(port))
except KeyboardInterrupt:
        print("Exiting...")
        sys.exit()
```


Which of the following actions will this script perform?

- A. Create an encrypted tunnel.
- B. Look for open ports.
- C. Attempt to flood open ports.
- D. Listen for a reverse shell.

Answer: B

Explanation:
The script will perform a port scan on the target IP address, looking for open ports on a list of common ports. A port scan is a technique that probes a network or a system for open ports, which can reveal potential vulnerabilities or services running on the host.

NEW QUESTION # 99
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Penetration Testing

Part 1 Part 2

Drag and Drop Options

- -sL
- -O
- 192.168.2.2
- -sU
- -sV
- -p 1-1023
- 192.168.2.1-100
- -Pn
- nc
- --top-ports=1000
- hping
- --top-ports=100
- nmap

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
scanned in 26.80 seconds
```

Command

Penetration Testing

Part 1 Part 2

Question Options

Using the output, identify potential attack vectors that should be further investigated.

- [ ] Weak SMB file permissions
- [ ] FTP anonymous login
- [ ] Webdav file upload
- [ ] Weak Apache Tomcat Credentials
- [ ] Null session enumeration
- [ ] Fragmentation attack
- [ ] SNMP enumeration
- [ ] ARP spoofing

NMAP Scan Output

Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
scanned in 26.80 seconds

2pass4sure.com
CompTIA

Answer:

Explanation:
Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns
Part 2 - Weak SMB file permissions
https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host

NEW QUESTION # 100
A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

- A. nmap -f -sV -p80 192.168.1.20
- B. nmap -O -v -p80 192.168.1.20
- C. nmap -sS -sL -p80 192.168.1.20
- D. nmap -A -T4 -p80 192.168.1.20

Answer: D

Explanation:
This command will scan the host 192.168.1.20 on port 80 using the following options:
* -A: This option enables OS detection, version detection, script scanning, and traceroute. This will help to determine if the host is running an approved version of Linux and a patched version of Apache, as well as other information about the host and the network path.
* -T4: This option sets the timing template to aggressive, which speeds up the scan by increasing the number of parallel probes, reducing the timeouts, and assuming faster responses.
* -p80: This option specifies the port to scan, which is 80 in this case. Port 80 is commonly used for HTTP services, such as Apache web server.

NEW QUESTION # 101
Which of the following types of information would MOST likely be included in an application security assessment report addressed to developers? (Choose two.)

- A. Poor input sanitization
- B. A cydomatic complexity score of 3
- C. Null pointer dereferences
- D. Use of non-optimized sort functions
- E. Use of deprecated Javadoc tags
- F. Non-compliance with code style guide

Answer: A,C

NEW QUESTION # 102
Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

- A. AS2
- B. DNSSEC
- C. S/MIME
- D. FTPS

Answer: C

Explanation:
Explanation
S/MIME stands for Secure/Multipurpose Internet Mail Extensions and is a standard for encrypting and signing email messages. It uses public key cryptography to ensure the confidentiality, integrity, and authenticity of email communications. FTPS is a protocol for transferring files securely over SSL/TLS, but it is not used for emailing. DNSSEC is a protocol for securing DNS records, but it

does not protect email content. AS2 is a protocol for exchanging business documents over HTTP/S, but it is not used for emailing.

NEW QUESTION # 103

.....

If you have never bought our PT0-002 exam materials on the website before, we understand you may encounter many problems such as payment or downloading PT0-002 practice quiz and so on, contact with us, we will be there. Our employees are diligent to deal with your need and willing to do their part on the PT0-002 Study Materials. And they are trained specially and professionlly to know every detail about our PT0-002 learning prep.

Demo PT0-002 Test: https://www.2pass4sure.com/CompTIA-PenTest/PT0-002-actual-exam-braindumps.html

- Exam PT0-002 Materials □ Valid Braindumps PT0-002 Book □ PT0-002 Exam Consultant □ Search for □ PT0-002 □ and download it for free immediately on ⇒ www.real4dumps.com ⇐ □PT0-002 Reliable Dumps Free
- 2025 High Hit-Rate CompTIA PT0-002: Answers CompTIA PenTest+ Certification Free □ Enter □ www.pdfvce.com □ and search for 【 PT0-002 】 to download for free □PDF PT0-002 Download
- PT0-002 Test Quiz □ New PT0-002 Test Question □ New PT0-002 Test Question □ Easily obtain free download of （ PT0-002 ） by searching on “ www.passtestking.com ” □PT0-002 Frequent Updates
- Hot Answers PT0-002 Free | High Pass-Rate CompTIA PT0-002: CompTIA PenTest+ Certification 100% Pass □ Search on □ www.pdfvce.com □ for ▹ PT0-002 ◃ to obtain exam materials for free download □Positive PT0-002 Feedback
- Answers PT0-002 Free - 100% Useful Questions Pool □ Open website 「 www.pass4leader.com 」 and search for （ PT0-002 ） for free download □New PT0-002 Test Question
- PT0-002 Reliable Dumps Free □ PT0-002 Practice Questions □ PT0-002 Practice Questions □□ Search for { PT0-002 } and download it for free on ▸ www.pdfvce.com ◂ website □PT0-002 Reliable Dumps Free
- PT0-002 Test Quiz □ Exam PT0-002 Materials □ Download PT0-002 Fee □ The page for free download of □ PT0-002 □ on ▸ www.torrentvalid.com ◂ will open immediately □Positive PT0-002 Feedback
- Answers PT0-002 Free | High-quality PT0-002: CompTIA PenTest+ Certification □ Download { PT0-002 } for free by simply searching on □ www.pdfvce.com □ □Original PT0-002 Questions
- Latest PT0-002 Exam Tips □ Positive PT0-002 Feedback ✏ PT0-002 Frequent Updates □ Search for 「 PT0-002 」 and easily obtain a free download on □ www.pdfdumps.com □ □Valid Braindumps PT0-002 Book
- PDF PT0-002 Download □ Valid Braindumps PT0-002 Book □ Original PT0-002 Questions □ Search for □ PT0-002 □ and download exam materials for free through ➽ www.pdfvce.com □ □PT0-002 Reliable Dumps Free
- Latest PT0-002 Exam Tips □ PT0-002 Vce Files □ Latest PT0-002 Exam Fee □ Search for “ PT0-002 ” and download it for free immediately on ➽ www.lead1pass.com □ □Valid PT0-002 Exam Syllabus
- 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, myportal.utt.edu.tt, cou.alnoor.edu.iq, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, academy.gaanext.lk, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, tomfox883.full-design.com, Disposable vapes

P.S. Free & New PT0-002 dumps are available on Google Drive shared by 2Pass4sure: https://drive.google.com/open?id=1u8zxNd--d_9_gnglSJ9G2BnIc_8Sxn_X