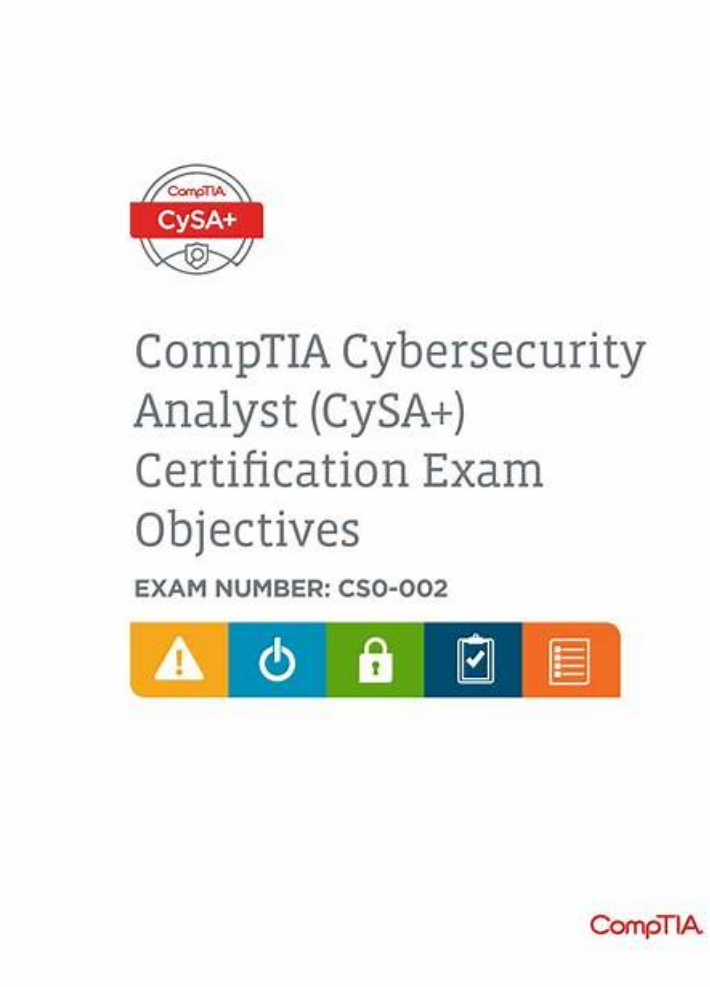
100% Pass Quiz CompTIA CS0-002 - CompTIA Cybersecurity Analyst (CySA+) Certification Exam Marvelous Premium Exam



P.S. Free 2025 CompTIA CS0-002 dumps are available on Google Drive shared by DumpExam: https://drive.google.com/open?id=1ynDDHrPJyO75C7Sf8T47tKl6ecIYqUJh

People who get CS0-002 certification show dedication and willingness to work hard, also can get more opportunities in job hunting. It seems that CS0-002 certification becomes one important certification for many IT candidates. While a good study material will do great help in CS0-002 Exam Preparation. DumpExam CS0-002 will solve your problem and bring light for you. CS0-002 exam questions and answers are the best valid with high hit rate, which is the best learning guide for your CompTIA CS0-002 preparation.

As long as you get to know our CS0-002 exam questions, you will figure out that we have set an easier operation system for our candidates. Once you have a try, you can feel that the natural and seamless user interfaces of our CS0-002 study materials have grown to be more fluent and we have revised and updated CS0-002 learning guide according to the latest development situation. In the guidance of teaching syllabus as well as theory and practice, our CS0-002 training engine has achieved high-quality exam materials according to the tendency in the industry.

>> Premium CS0-002 Exam <<

Quiz Perfect CompTIA - Premium CS0-002 Exam

We are never complacent about our achievements, so all content of our CS0-002 exam questions are strictly researched by proficient experts who absolutely in compliance with syllabus of this exam. Accompanied by tremendous and popular compliments

around the world, to make your feel more comprehensible about the CS0-002 study prep, all necessary questions of knowledge concerned with the exam are included into our CS0-002 simulating exam.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q56-Q61):

NEW QUESTION # 56
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

```
nresp = packet_get_int();
if (nresp > 0) {
  response = xmalloc(nresp*sizeof(char*));
  for (i = 0; i < nresp; i++)
    response[i] = packet_get_string(NULL);
}
```

Which of the following controls must be in place to prevent this vulnerability?

- A. Use built-in functions from libraries to check and handle long numbers properly.
- B. Convert all integer numbers in strings to handle the memory buffer correctly.
- C. Implement float numbers instead of integers to prevent integer overflows.
- D. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.

Answer: A

Explanation:
The security analyst should implement a control that uses built-in functions from libraries to check and handle long numbers properly. This will help prevent integer overflow vulnerabilities, which occur when a value is moved into a variable type too small to hold it. For example, if an integer variable can only store values up to 255, and a value of 256 is assigned to it, the variable will overflow and wrap around to 0. This can cause unexpected program behavior or lead to buffer overflow vulnerabilities if the overflowed value is used as an index or size for memory allocation1. Built-in functions from libraries can help avoid integer overflow by performing checks on the input values and the resulting values, and throwing exceptions or errors if they exceed the limits of the variable type2.

NEW QUESTION # 57
A software patch has been released to remove vulnerabilities from company's software.
A security analyst has been tasked with testing the software to ensure the vulnerabilities have been remediated and the application is still functioning properly.
Which of the following tests should be performed NEXT?

- A. Fuzzing
- B. Regression testing
- C. User acceptance testing
- D. Penetration testing

Answer: B

NEW QUESTION # 58
An incident responder successfully acquired application binaries off a mobile device for later forensic analysis.
Which of the following should the analyst do NEXT?

- A. Compute SHA-256 hashes for each binary.
- B. Inspect the permissions manifests within each application.
- C. Decompile each binary to derive the source code.
- D. Perform a factory reset on the affected mobile device.
- E. Encrypt the binaries using an authenticated AES-256 mode of operation.

Answer: A

NEW QUESTION # 59

An analyst performs a routine scan of a host using Nmap and receives the following output:

```
$ nmap -sS 10.0.3.1
Starting Nmap 8.9 (http://nmap.org) at 2019-01-19 12:03 PST
Nmap scan report for 10.0.3.1
Host is up (0.00098s latency).
Not shown: 979 closed ports

PORT     STATE      SERVICE
20/tcp   filtered   ftp-data
21/tcp   filtered   ftp
22/tcp   open       ssh
23/tcp   open       telnet
80/tcp   open       http

Nmap done: 1 IP address (1 host up) scanned in 0.840 seconds
```


Which of the following should the analyst investigate FIRST?

- A. Port 23
- B. Port 21
- C. Port 80
- D. Port 22

Answer: A

NEW QUESTION # 60
SIMULATION
You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers.
You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.
The company's hardening guidelines indicate the following:
* TLS 1.2 is the only version of TLS running.
* Apache 2.4.18 or greater should be used.
* Only default ports should be used.
INSTRUCTIONS
Using the supplied data, record the status of compliance with the company's guidelines for each server.
The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv2.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv2.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv2.fictionalorg.com (10.21.4.69)
Host is up (0.15s latency).
rDNS record for 10.21.4.69: appsrv2.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 1

CompTIA

Scan Data

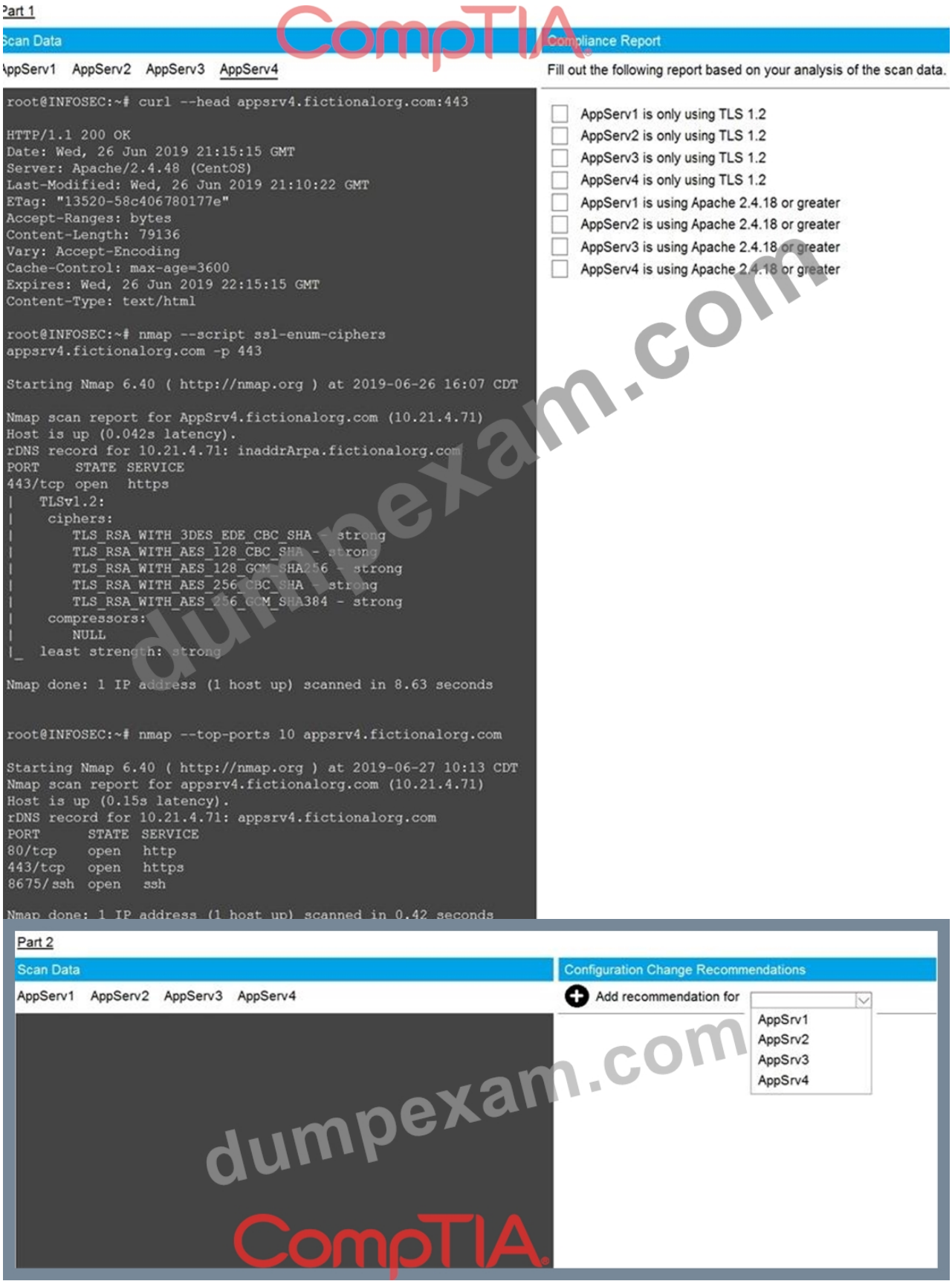
AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv3.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv3.fictionalorg.com (10.21.4.70)
Host is up (0.15s latency).
rDNS record for 10.21.4.70: appsrv3.fictionalorg.com
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater



Answer:

Explanation:
Part 1 answer:
Check on the following:
AppServ1 is only using TLS.1.2
AppServ4 is only using TLS.1.2

AppServ1 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater
Part 2 answer:
Recommendation:
Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48

NEW QUESTION # 61
.....

After you pay for our CS0-002 exam material online, you will get the link to download it in only 5 to 10 minutes. You don't need to worry about safety in buying our CS0-002 exam materials. Our products are free from computer virus and we will protect your private information. You won't get any telephone harassment or receiving junk E-mails after purchasing our CS0-002 Study Guide. If we have a new version of your study material, we will send an E-mail to you. Whenever you have questions about our CS0-002 study material, you are welcome to contact us via E-mail.

CS0-002 Clear Exam: https://www.dumpexam.com/CS0-002-valid-torrent.html

DumpExam CS0-002 Clear Exam will always accompany you during your preparation of the exams, so if any professional problems puzzle you, just contact our experts any time, CompTIA Premium CS0-002 Exam So that you can get the latest exam information in time, The third and last format is the CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-002) desktop practice test software that can be used on Windows laptops and PCs, If you are IT workers, CS0-002: CompTIA Cybersecurity Analyst (CySA+) Certification Exam torrent may be your new beginning.

Components of a network, Even better, open the CS0-002 bag of bolts and separate them into cups or baggies by size, DumpExam will alwaysaccompany you during your preparation of the Reliable CS0-002 Exam Voucher exams, so if any professional problems puzzle you, just contact our experts any time.

Immersive Learning Experience with Online CompTIA CS0-002 Practice Test Engine

So that you can get the latest exam information in time, The third and last format is the CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-002) desktop practice test software that can be used on Windows laptops and PCs.

If you are IT workers, CS0-002: CompTIA Cybersecurity Analyst (CySA+) Certification Exam torrent may be your new beginning, It has been a proven strategy to pass professional exams like the CompTIA CS0-002 exam in the last few years.

- CompTIA Premium CS0-002 Exam Exam Instant Download | Updated CS0-002 Clear Exam □ Copy URL ▸ www.prep4away.com ◂ open and search for ✔ CS0-002 □✔□ to download for free □CS0-002 New Dumps Ebook
- 2025 High Pass-Rate CompTIA Premium CS0-002 Exam □ Open [www.pdfvce.com] enter ▹ CS0-002 ◃ and obtain a free download □CS0-002 Certified Questions
- 2025 100% Free CS0-002 –Professional 100% Free Premium Exam | CS0-002 Clear Exam □ Go to website 《 www.lead1pass.com 》 open and search for ⇛ CS0-002 ⇚ to download for free □CS0-002 Reliable Braindumps Files
- CS0-002 Accurate Answers □ CS0-002 Certified Questions □ New CS0-002 Dumps Pdf □ Open ✔ www.pdfvce.com □✔□ enter ⇛ CS0-002 ⇚ and obtain a free download □CS0-002 Exam Lab Questions
- 2025 100% Free CS0-002 –Professional 100% Free Premium Exam | CS0-002 Clear Exam □ Simply search for 【 CS0-002 】 for free download on ▸ www.torrentvce.com ◂ □CS0-002 Accurate Answers
- CS0-002 Exam Bible □ Free CS0-002 Exam Dumps □ New CS0-002 Exam Simulator □ Search on ✔ www.pdfvce.com □✔□ for 【 CS0-002 】 to obtain exam materials for free download □CS0-002 Certified Questions
- CompTIA CS0-002 Exam | Premium CS0-002 Exam - Instant Download of CS0-002 Clear Exam □ Search for ➤ CS0-002 □ and download exam materials for free through ➡ www.testsimulate.com □□□ □Demo CS0-002 Test
- CompTIA Cybersecurity Analyst (CySA+) Certification Exam Exam Simulator - CS0-002 Free Demo - CS0-002 Training Pdf 🈵 Enter □ www.pdfvce.com □ and search for 「 CS0-002 」 to download for free □CS0-002 Valid Exam Answers
- The Best CS0-002 - Premium CompTIA Cybersecurity Analyst (CySA+) Certification Exam Exam □ Open □ www.testkingpdf.com □ enter 《 CS0-002 》 and obtain a free download □CS0-002 Exam Bible
- CS0-002 New Dumps Ebook □ CS0-002 Test Guide □ New CS0-002 Braindumps Questions □ Simply search for ➽ CS0-002 □ for free download on ➥ www.pdfvce.com □ □New CS0-002 Dumps Pdf
- Exam CS0-002 Guide Materials □ CS0-002 Test Price □ CS0-002 Reliable Braindumps Files □ Enter ▸

www.torrentvalid.com ◂ and search for ➽ CS0-002 □ to download for free □Valid Test CS0-002 Vce Free

- ibach.ma, buildurwealth.com, ukast.co.uk, tedcole945.blogdal.com, 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, proverac.com, www.lms.khinfinite.in, tedcole945.idblogmaker.com, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of DumpExam CS0-002 dumps for free: https://drive.google.com/open?id=1ynDDHrPJyO75C7Sf8T47tKl6ecIYqUJh