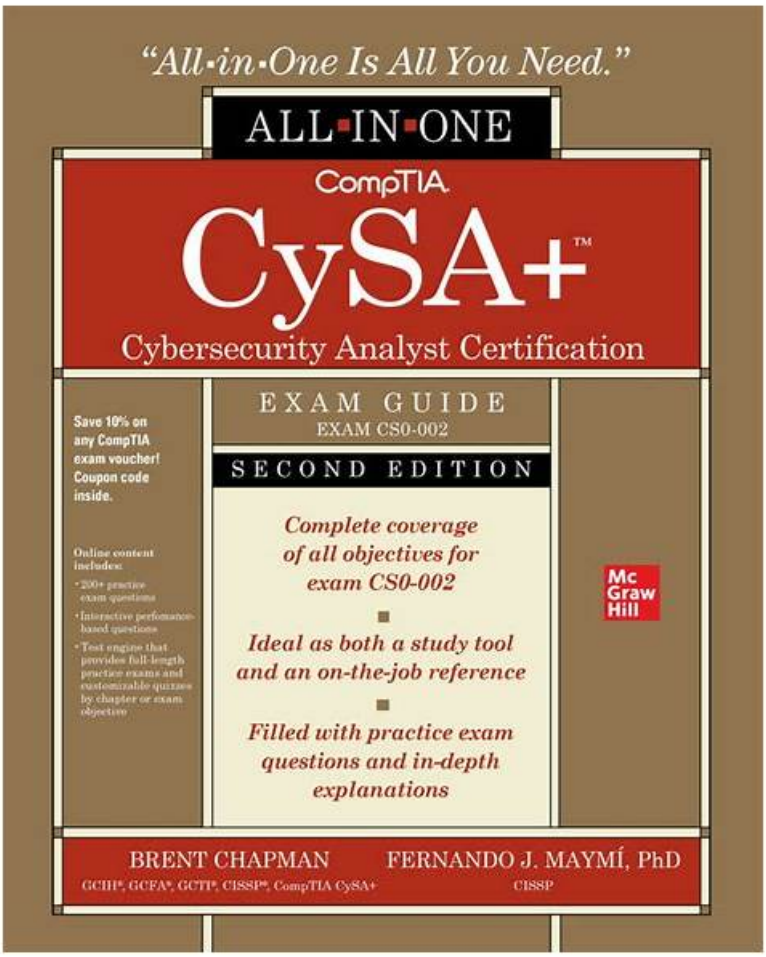
CS0-002 Training Materials & CS0-002 Dumps PDF & CS0-002 Exam Cram



DOWNLOAD the newest Exam4Tests CS0-002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1iKXDa2tDUa0O5334XyTYYU9ziG3_IA2_

It means you can use the CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-002) PDF version of Exam4Tests anywhere at any time on the smart device you have. Our team of professionals continuously updates the collection of CompTIA CS0-002 PDF Questions according to changes in the real test's content. Due to these regular updates, you will get a better experience.

Nowadays in this information-based world the definition of the talents mean that the personnel boost both the knowledge in CS0-002 area and the practical abilities now. So if you want to be the talent the society actually needs you must apply your knowledge into the practical working and passing the test CS0-002 Certification can make you become the talent the society needs. If you buy our CS0-002 study materials you will pass the exam successfully and realize your goal to be the talent.

>> CS0-002 Exam Voucher <<

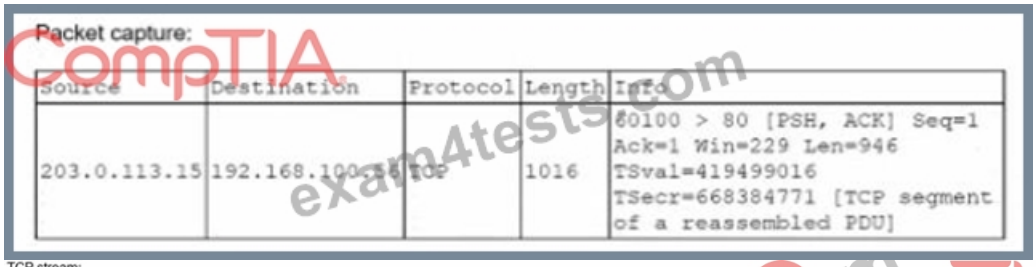
Unparalleled CS0-002 Exam Voucher - Easy and Guaranteed CS0-002 Exam Success

Do you want to pass your exam by using the least time? CS0-002 exam braindumps of us can do that for you. With skilled professionals to compile and verify, CS0-002 exam dumps of us is high quality and accuracy. You just need to spend 48 to 72 hours on practicing, and you can pass your exam. We are pass guaranteed and money back guaranteed. If you fail to pass the exam, we will give you full refund. Besides, we offer you free demo to have a try before buying CS0-002 Exam Dumps. We also have free update for one year after purchasing.

CompTIA CS0-002 (CompTIA Cybersecurity Analyst (CySA+) Certification) Exam is an advanced level certification exam that evaluates the candidate's ability to identify and respond to threats using various security tools and techniques. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification is aimed at IT professionals who specialize in security analysis and response and are seeking to demonstrate their expertise in the field. By passing this certification exam, candidates can demonstrate their technical knowledge and be recognized as cybersecurity professionals.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q267-Q272):

NEW QUESTION # 267
A security analyst at exampte.com receives a SIEM alert for an IDS signature and reviews the associated packet capture and TCP stream:


Packet capture:

Source	Destination	Protocol	Length	Info
203.0.113.15	192.168.100.34	TCP	1016	60100 > 80 [PSH, ACK] Seq=1 Ack=1 Win=229 Len=946 TSval=419499016 TSecr=668384771 [TCP segment of a reassembled PDU]

TCP stream:

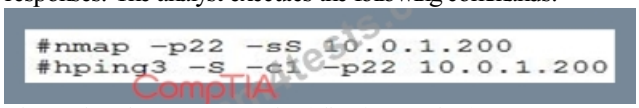
```
GET /admin/auth/Register.do HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
connection: close
content-type: %{(#test='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#ros=
(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(#ros.println(31337*31337)).(#ros.flush())}
host: connect.example.local
iv-user: Unauthenticated
user-agent: Security Operations Center; X-SOC-Scan (soc@example.com);
via: HTTP/1.1 revproxy.dmz.example.local:443
iv_server_name: connect-webseald-revproxy.dmz.example.local
x-
```

Winch of the following actions should the security analyst lake NEXT?

- A. Mark the alert as a false positive scan coming from an approved source.
- B. Review the known Apache vulnerabilities to determine if a compromise actually occurred
- C. Raise a request to the firewall team to block 203.0.113.15.
- D. Contact the application owner for connect example local tor additional information

Answer: C

NEW QUESTION # 268
A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands:



```
#nmap -p22 -sS 10.0.1.200
#hping3 -S -c1 -p22 10.0.1.200
```

The analyst then compares the following results for port 22:
nmap returns "Closed"
hping3 returns "flags=RA"
Which of the following BEST describes the firewall rule?

- A. DROP
- B. REJECT with --tcp-reset
- C. LOG --log-tcp-sequence
- D. DNAT --to-destination 1.1.1.1:3000

Answer: A

NEW QUESTION # 269
A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named Webserverlist. Xml. The host list is provided in a file named

werbserverlist,text. Which of the fallowing Nmap commands would BEST accomplish this goal?
A)

B)

C)

D)

- A. Option D
- B. Option B
- C. Option C
- D. Option A

Answer: D

NEW QUESTION # 270
A security analyst is concerned the number of security incidents being reported has suddenly gone down. Daily business interactions have not changed, and no following should the analyst review FIRST?

- A. The firewall ACL
- B. The IDS rule set
- C. Privileged accounts
- D. The DNS configuration

Answer: B

Explanation:
The security analyst should review the IDS rule set first. The IDS (Intrusion Detection System) is a tool that monitors network traffic and alerts on any suspicious or malicious activity. The IDS rule set is a set of conditions or patterns that define what constitutes normal or abnormal behavior on the network. The IDS rule set can affect the number of security incidents being reported, as it determines what triggers an alert or not3. The security analyst should review the IDS rule set to check if it is up to date, accurate, and comprehensive. If the IDS rule set is outdated, inaccurate, or incomplete, it may miss some incidents or generate false positives or negatives.

NEW QUESTION # 271
A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?
A)

B)

C)

D)

- A. Option D
- B. Option B
- C. Option A
- D. Option C

Answer: D

Explanation:

Option C shows a device that can perform a forensic copy of a hard drive. A forensic copy, also known as a forensic image or a bit-stream image, is an exact, unaltered digital copy of a piece of digital evidence. A forensic copy captures everything on the hard drive, including active and latent data, and preserves the integrity of the original evidence. A forensic copy can be used for forensic analysis without risking any changes to the original drive1. Option C shows a device that can connect to two hard drives and create a forensic copy from one drive to another using a write-blocker. A write-blocker is a tool that prevents any data from being written to the destination drive, ensuring that only a read-only copy is made2.

NEW QUESTION # 272

.....