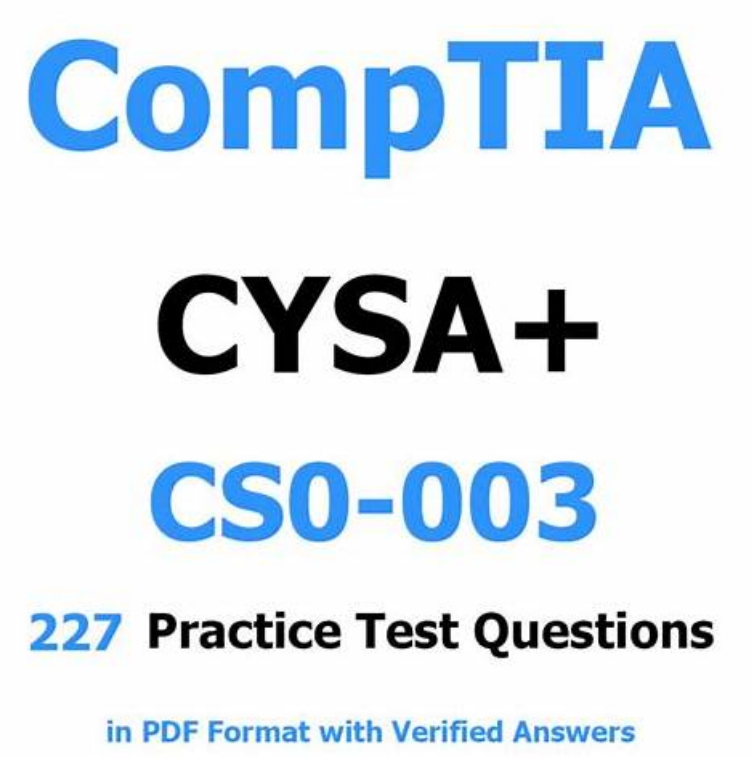
100% Pass Quiz 2025 CompTIA CS0-003: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Authoritative Actual Test Answers



DOWNLOAD the newest Actual4Dumps CS0-003 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1pFP6bHTmpZ-Epb9mDXQxB_q5yLnU3jty

If you are still worried about your exam, our exam dumps may be your good choice. Our CompTIA CS0-003 training dumps cover many real test materials so that if you master our dumps questions and answers you can clear exams successfully. Don't worry over trifles. If you purchase our CompTIA CS0-003 training dumps you can spend your time on more significative work.

CompTIA Cybersecurity Analyst (CySA+) Certification is one of the most in-demand certifications for cybersecurity analysts. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification exam has been designed to validate the aptitude of cybersecurity analysts in configuring and using threat detection techniques. It is an internationally recognized certification that demonstrates an individual's expertise in cybersecurity. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification exam is called CompTIA CS0-003.

CompTIA CS0-003 (CompTIA Cybersecurity Analyst (CySA+) Certification) Exam is designed to assess the knowledge and skills of candidates in the field of cybersecurity analysis. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification exam is an esteemed qualification for cybersecurity analysts and is globally recognized in the industry. It is an intermediate-level certification, which means that candidates are required to have some prior knowledge and experience in this field before attempting the exam.

To pass the CS0-003 Certification Exam, candidates must demonstrate their ability to perform real-world cybersecurity tasks. They must be able to analyze data to identify security threats, develop and implement effective security policies and procedures, and respond to security incidents in a timely and effective manner. Candidates are expected to have a strong understanding of cybersecurity concepts and principles, as well as hands-on experience in the field.

>> CS0-003 Actual Test Answers <<

CS0-003 Technical Training, CS0-003 New Braindumps

We will give you free update for 365 days after purchasing CS0-003 study guide from us, that is to say, in the following year, you don't need to spend extra money on update version, and the latest version for CS0-003 exam dumps will be sent to your email address automatically. Furthermore, CS0-003 exam dumps are high quality and accuracy, and they can help you pass the exam just one time. In order to strengthen your confidence to CS0-003 Study Guide, we are pass guarantee and money back guarantee, if you fail to pass the exam we will give you full refund, and there is no need for you to worry about that you will waste your money.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q537-Q542):

NEW QUESTION # 537
Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

- A. MOU
- B. SLA
- C. Organizational governance
- D. Best-effort patching

Answer: B

Explanation:
Explanation
An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer12 An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA. Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing.
Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

NEW QUESTION # 538
An analyst needs to provide recommendations based on a recent vulnerability scan:

Plug-in name	Family
SMB use domain SID to enumerate users	Windows : User management
SYN scanner	Port scanners
SSL certificate cannot be trusted	General
Scan not performed with admin privileges	Settings

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?

- A. SMB use domain SID to enumerate users
- B. SYN scanner
- C. SSL certificate cannot be trusted
- D. Scan not performed with admin privileges

Answer: D

Explanation:
This is because scanning without admin privileges can limit the scope and accuracy of the vulnerability scan, and potentially miss some critical vulnerabilities that require higher privileges to detect. According to the OWASP Vulnerability Management Guide1, "scanning without administrative privileges will result in a large number of false negatives and an incomplete scan". Therefore, the analyst should recommend addressing this issue to ensure potential vulnerabilities are identified.

NEW QUESTION # 539
During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

- A. Temporary files
- B. Backup data
- C. Disk contents
- D. Running processes

Answer: D

Explanation:
Explanation
The most volatile type of evidence that must be collected first in a computer system is running processes.
Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

NEW QUESTION # 540
An organization has noticed large amounts of data are being sent out of its network. An analyst is identifying the cause of the data exfiltration.
INSTRUCTIONS
Select the command that generated the output in tabs 1 and 2.
Review the output text in all tabs and identify the file responsible for the malicious behavior.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

1 2 3 4

```
Active Connections
Proto       Local address          Foreign address        State          PID
TCP         0.0.0.0:22             0.0.0.0:0              LISTENING      1000
TCP         0.0.0.0:23             0.0.0.0:0              LISTENING      1235
TCP         0.0.0.0:443            0.0.0.0:0              LISTENING      1466
TCP         0.0.0.0:80             0.0.0.0:0              LISTENING      1566
TCP         127.0.0.1:1960         127.0.0.1:22           ESTABLISHED    2001
[sftp.exe]
TCP         192.168.10.21:38666    41.21.18.102:22        ESTABLISHED    3918
[sftp.exe]
TCP         192.168.10.21:8447     66.207.110.49:https    ESTABLISHED    2677
[svchost.exe]
TCP         192.168.10.21:55356    31.10.100.7:https      ESTABLISHED    3467
[cmd.exe]
TCP         192.168.10.21:37654    192.168.10.37:http     ESTABLISHED    1722
TCP         192.168.10.21:55357    32.111.16.37:22        TIME_WAIT      0
[notepad.exe]
TCP         192.168.10.21:52744    32.111.16.37:22        TIME_WAIT      0
TCP         192.168.10.21:56751    32.111.16.37:22        TIME_WAIT      0
```

Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe

1 2 3 4

Active Connections
Proto Local address Foreign address State PID
TCP 0.0.0.0:22 0.0.0.0:0 LISTENING 1000
TCP 0.0.0.0:23 0.0.0.0:0 LISTENING 1235
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 1466
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 1566
TCP 127.0.0.1:1960 127.0.0.1:22 ESTABLISHED 2001
[sftp.exe]
TCP 192.168.10.21:38666 41.21.18.102:22 ESTABLISHED 3918
[sftp.exe]
TCP 192.168.10.21:8447 66.207.110.49:https ESTABLISHED 2677
[svchost.exe]
TCP 192.168.10.21:55356 31.10.100.7:https ESTABLISHED 3467
[cmd.exe]
TCP 192.168.10.21:37654 192.168.10.37:http ESTABLISHED 1722
TCP 192.168.10.21:55357 32.111.16.37:22 TIME_WAIT 0
[notepad.exe]
TCP 192.168.10.21:52744 32.111.16.37:22 TIME_WAIT 0
TCP 192.168.10.21:56751 32.111.16.37:22 TIME_WAIT 0

Select command
netstat -bo
tasklist
net stop
arp -a
nslookup
taskkill /FI
cmd
ipconfig /reset

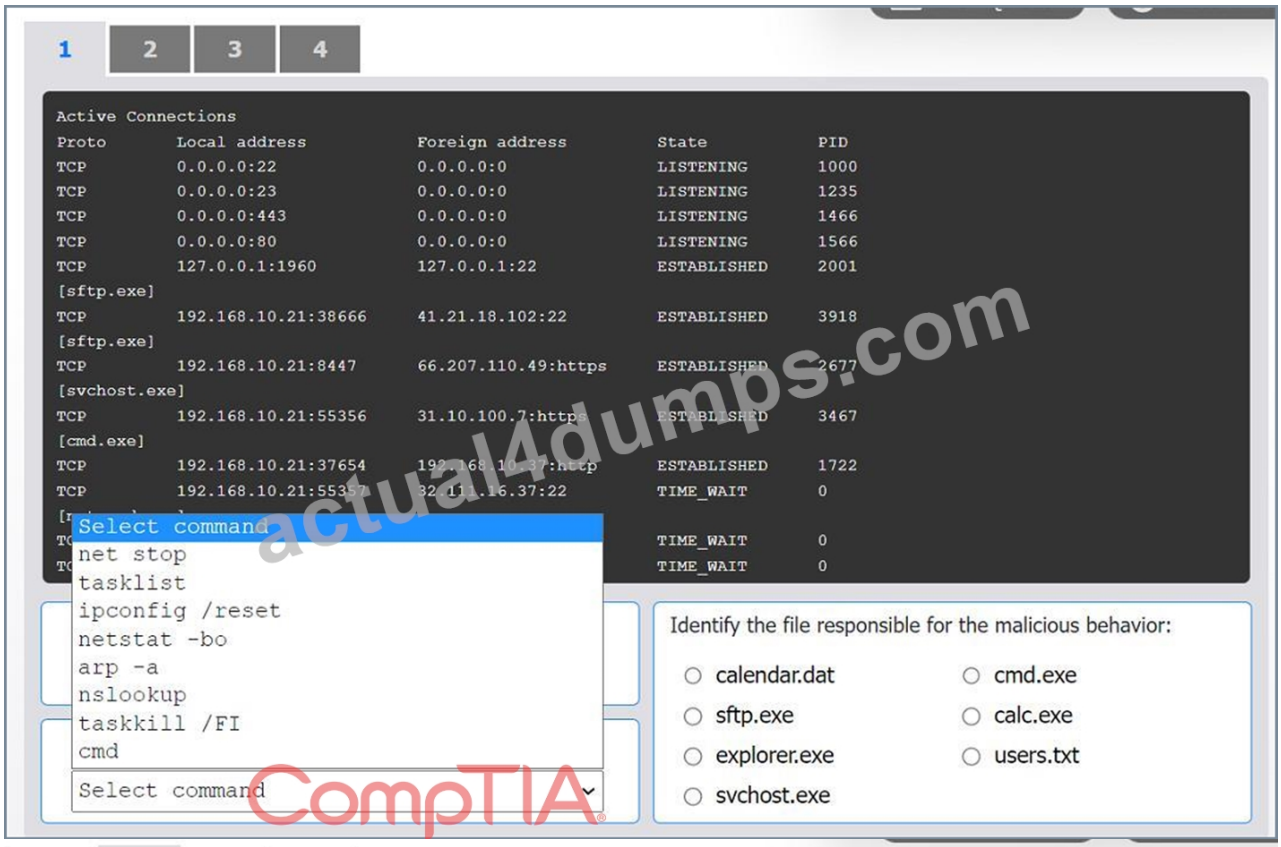
Select command

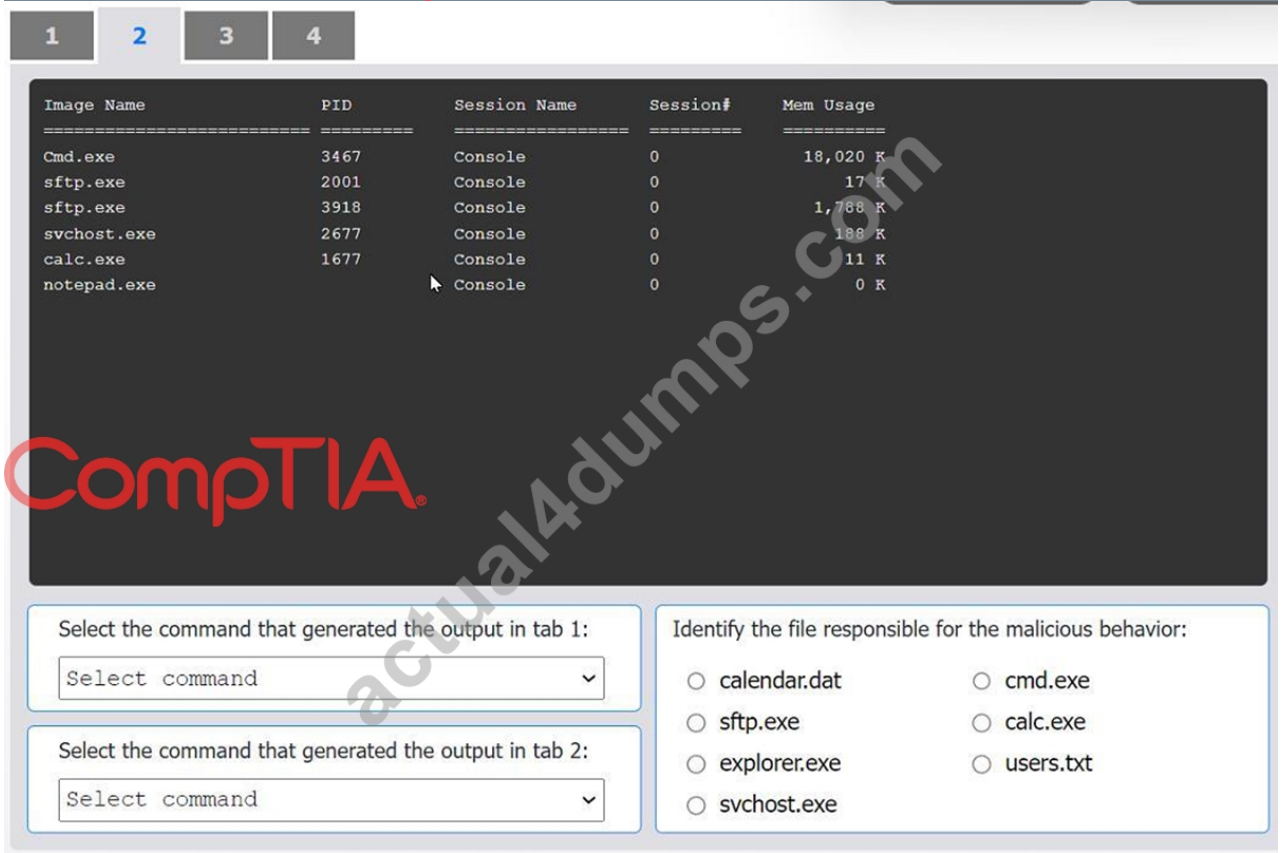
Select the command that generated the output in tab 2:

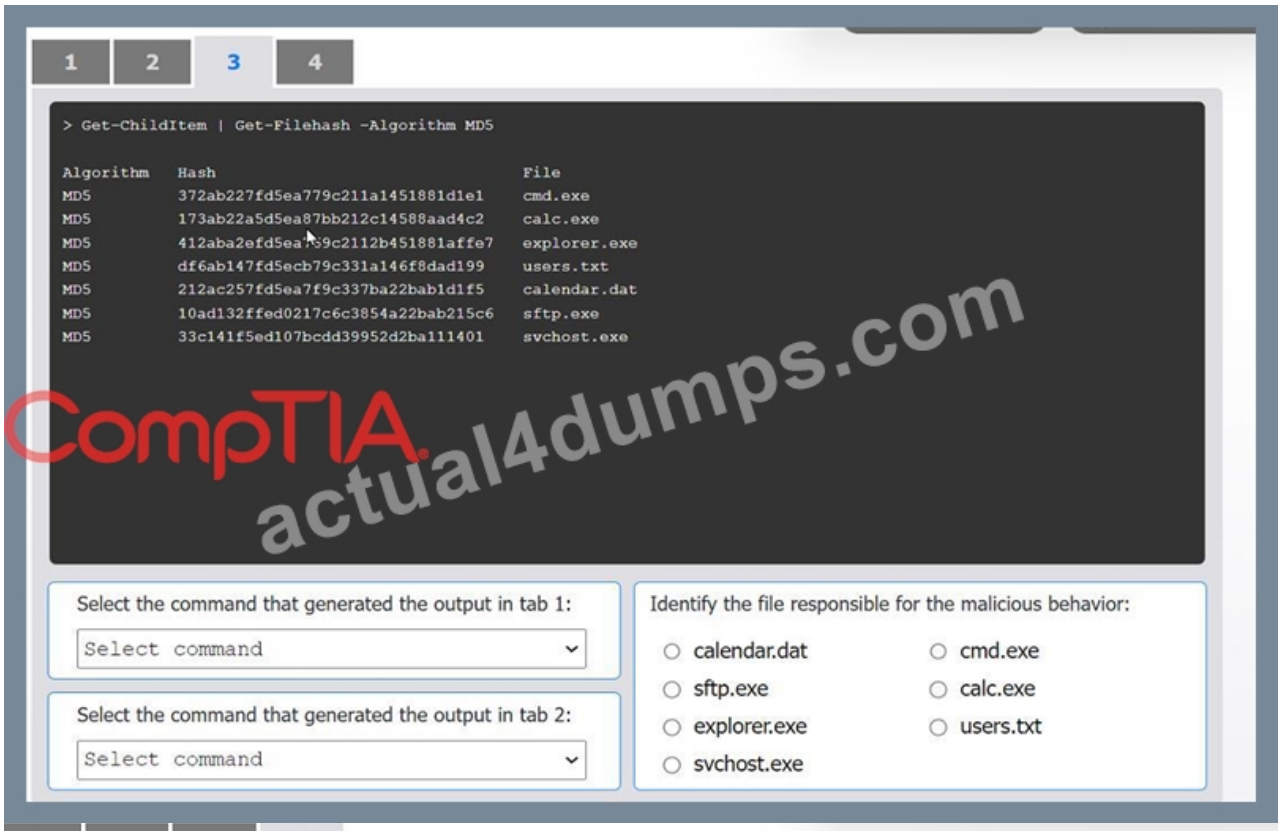
Select command

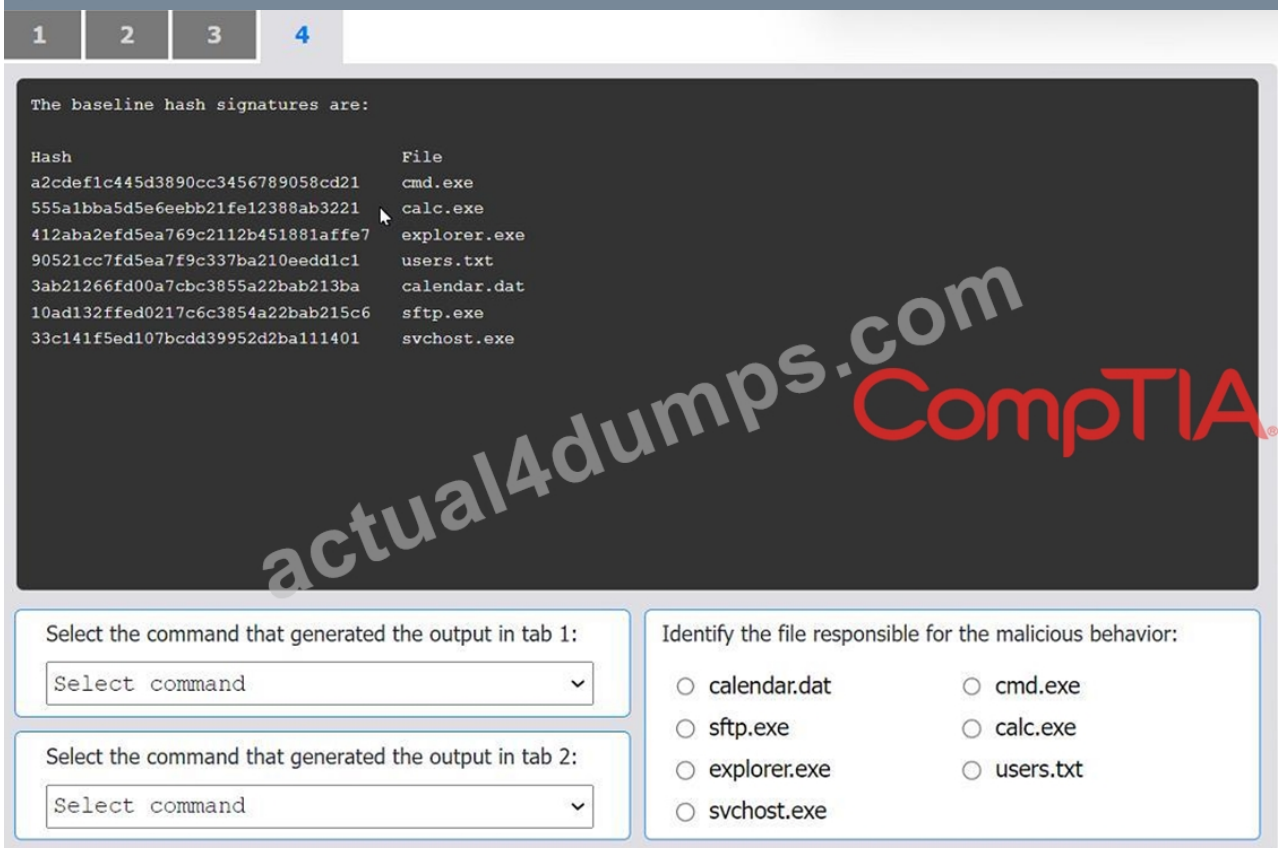
Identify the file responsible for the malicious behavior:

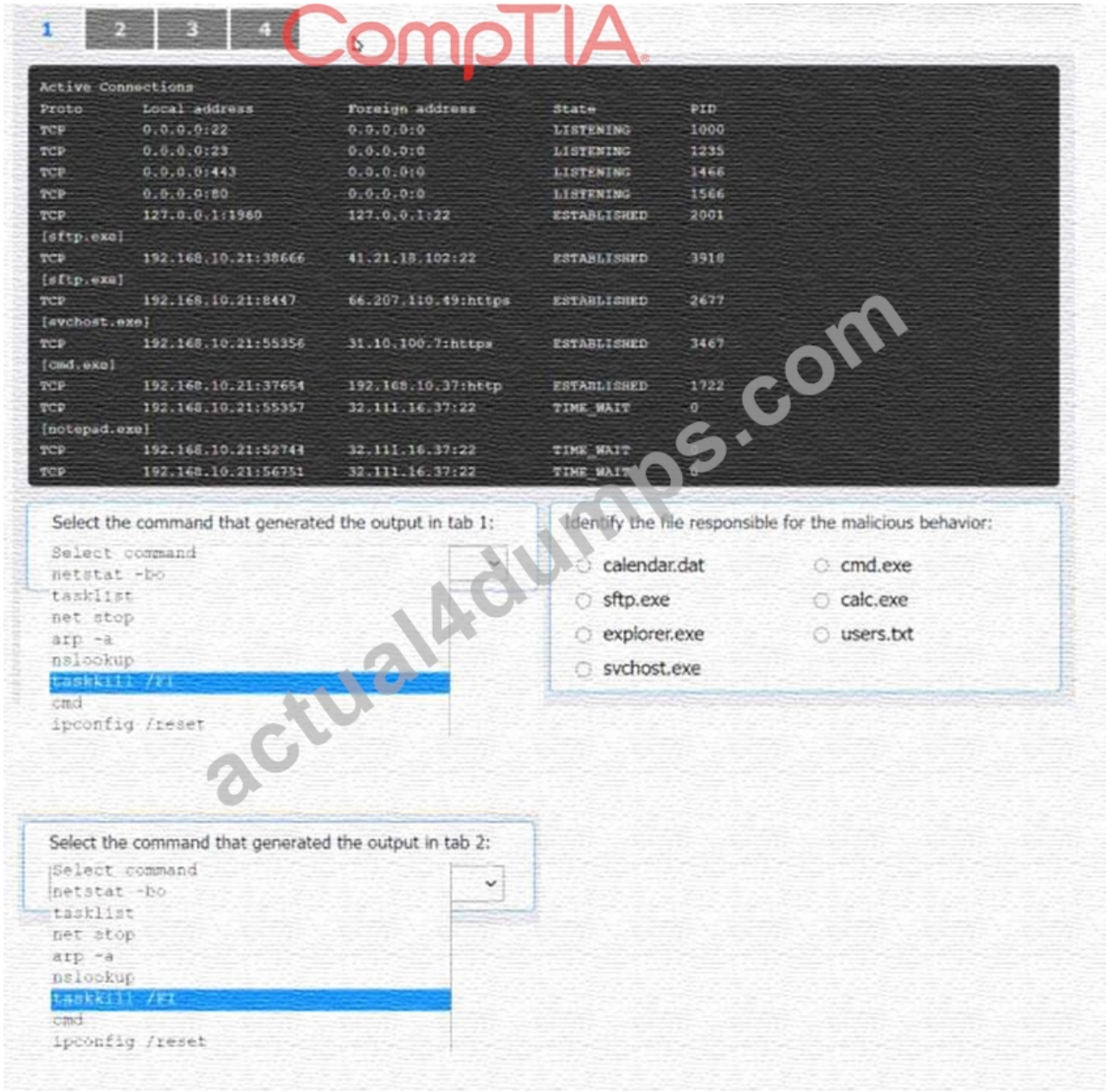
- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe





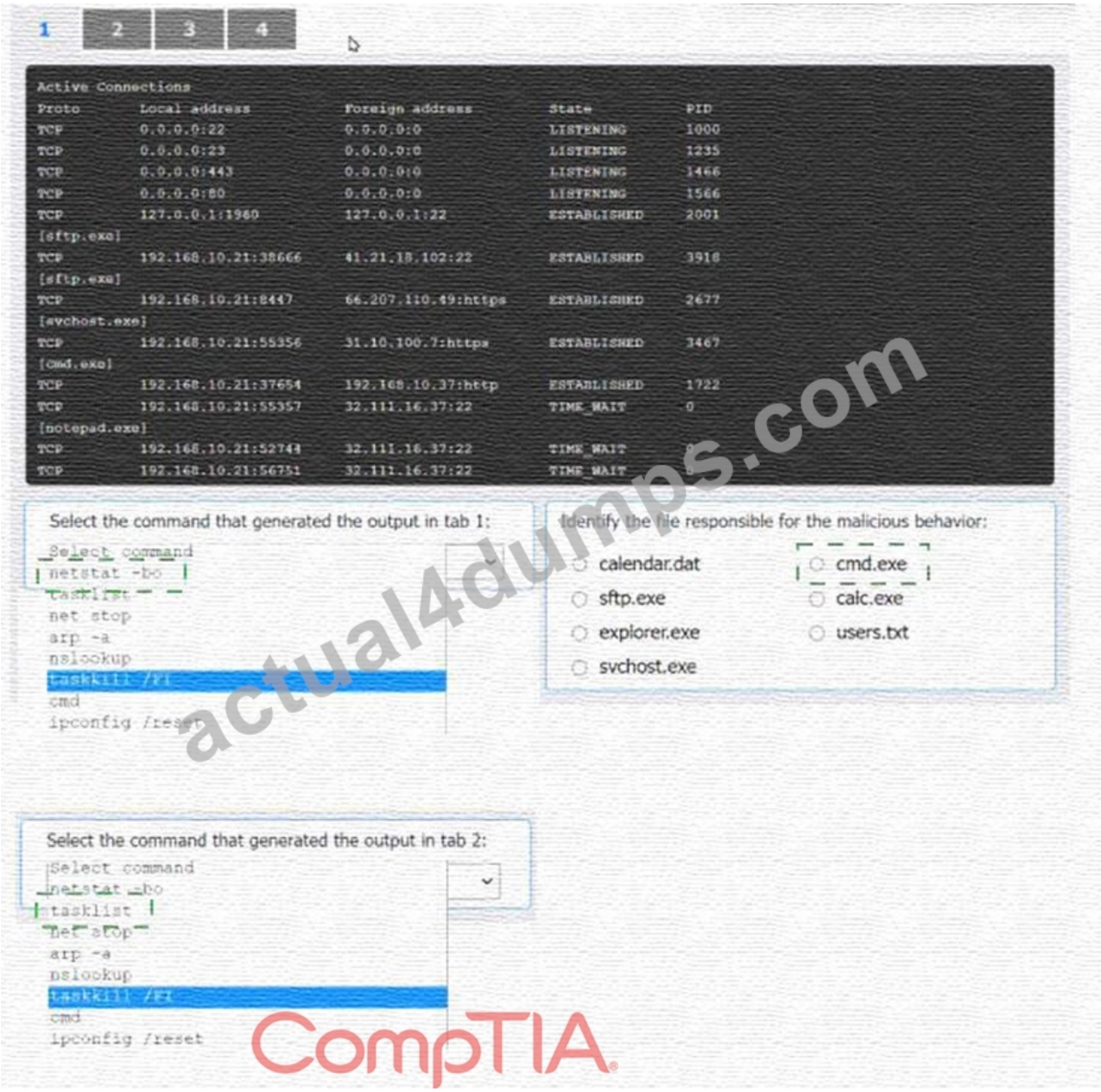






Answer:

Explanation:



Explanation:
Select the command that generated the output in tab 1:
* netstat -bo
Select the command that generated the output in tab 2:
* tasklist
Identify the file responsible for the malicious behavior:
* cmd.exe
Select the command that generated the output in tab 1: The output in tab 1 displays active network connections, which can be generated using the netstat command with options to display the owning process ID.
Select the command that generated the output in tab 1:
* netstat -bo
Select the command that generated the output in tab 2: The output in tab 2 lists the running processes with their PIDs and memory usage, which can be generated using the tasklist command.
Select the command that generated the output in tab 2:
* tasklist
Identify the file responsible for the malicious behavior: To identify the malicious file, we compare the hashes of the current files against the baseline hashes. From the provided data:
* The hash for cmd.exe in the current state (tab 3) is 372ab227fd5ea779c211a1451881d1e1.
* The baseline hash for cmd.exe (tab 4) is a2cdef1c445d3890cc3456789058cd21.
Since these hashes do not match, cmd.exe is the file responsible for the malicious behavior.

NEW QUESTION # 541
A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

- A. Integrate an IT service delivery ticketing system to track remediation and closure
- B. Accept the risk and decommission current assets as end of life
- C. Create a compensating control item until the system can be fully patched
- D. Request an exception and manually patch each system

Answer: A

NEW QUESTION # 542
.....

For purchasing the CS0-003 study guide, the cndidates may have the concern of the safety of the websites, we provide you a safety network environment for you. We have occupied in this business for years, and the website and the CS0-003 Study Guide of our company is of good reputation. We also have professionals offer you the guide and advice. CS0-003 study guide will provide you the knowledge point as well as answers, it will help you to pass it.