CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company\\'s user accounts have been compromised. Users are also reporting that the company\\'s internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

A. There is an issue with the SSL certificate causinq port 443 to become unavailable for HTTPS access

B. An on-path attack is being performed by someone with internal access that forces users into port 80

C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80

D. An error was caused by BGP due to new rules applied over the company\\'s internal routers

Correct Answer: B

An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies network traffic between two parties. In this case, someone with internal access may be performing an on-path attack by forcing users into port 80, which is used for HTTP communication, instead of port 443, which is used for HTTPS communication. This would allow the attacker to compromise the user accounts and access the company\\'s internal portal.

QUESTION 2

Which of the following can be used to learn more about TTPs used by cybercriminals?

A. ZenMAP

B. MITRE ATTandCK

C. National Institute of Standards and Technology

D. theHarvester

Correct Answer: B

MITRE ATTandCK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It is used as a foundation for the development of specific threat models and methodologies in the private sector,

in government, and in the cybersecurity product and service community. It can help security professionals understand, detect, and mitigate cyber threats by providing a comprehensive framework of TTPs.

References: MITRE ATTandCK, Getting Started with ATTandCK, MITRE ATTandCK | MITRE

QUESTION 3

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

A. Hard disk

B. Primary boot partition

C. Malicious tiles

D. Routing table

E. Static IP address

Correct Answer: D

QUESTION 4

HOTSPOT

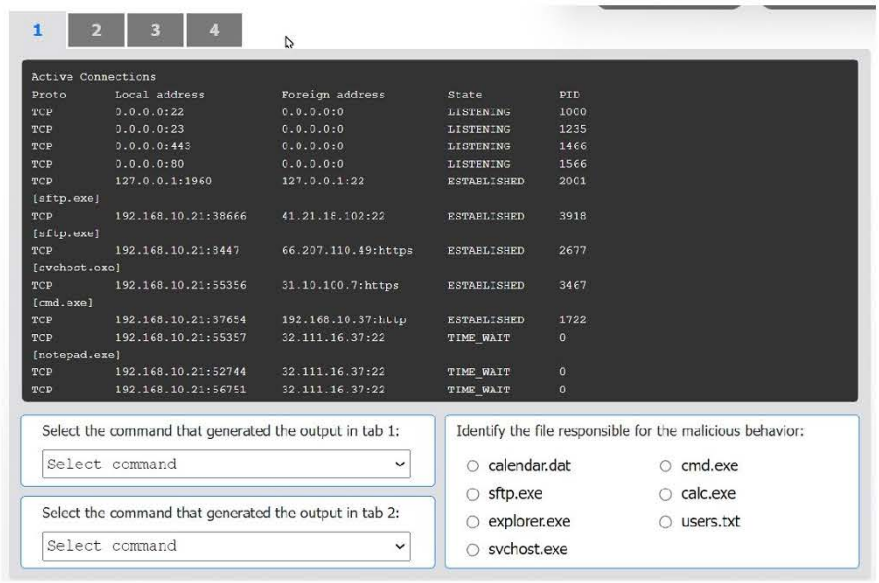
An organization has noticed large amounts of data are being sent out of its network. An analyst is identifying the cause of the data exfiltration.

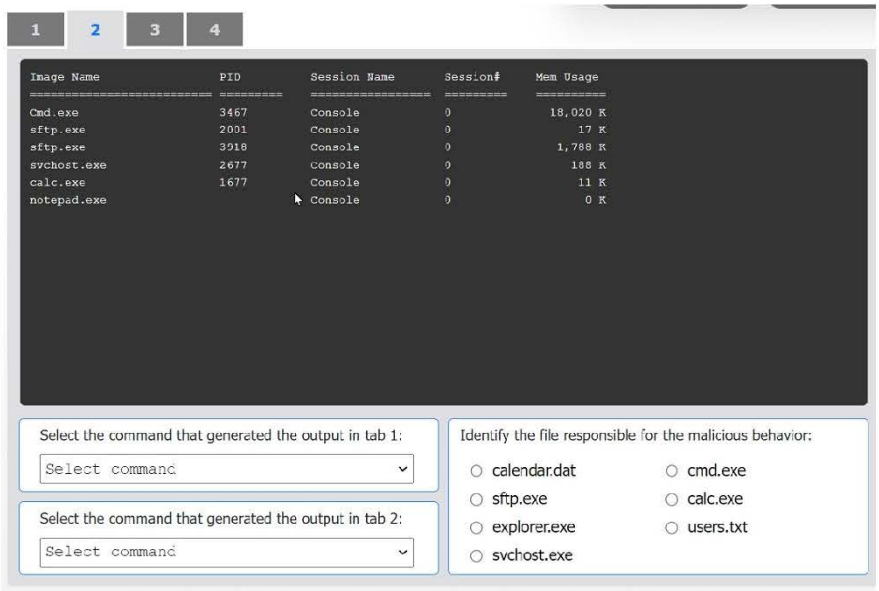
INSTRUCTIONS

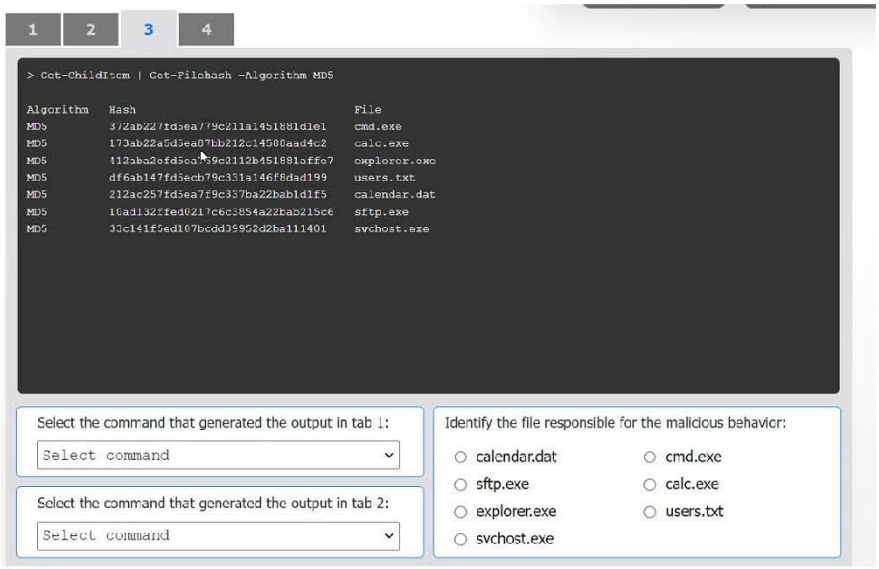
Select the command that generated the output in tabs 1 and 2.

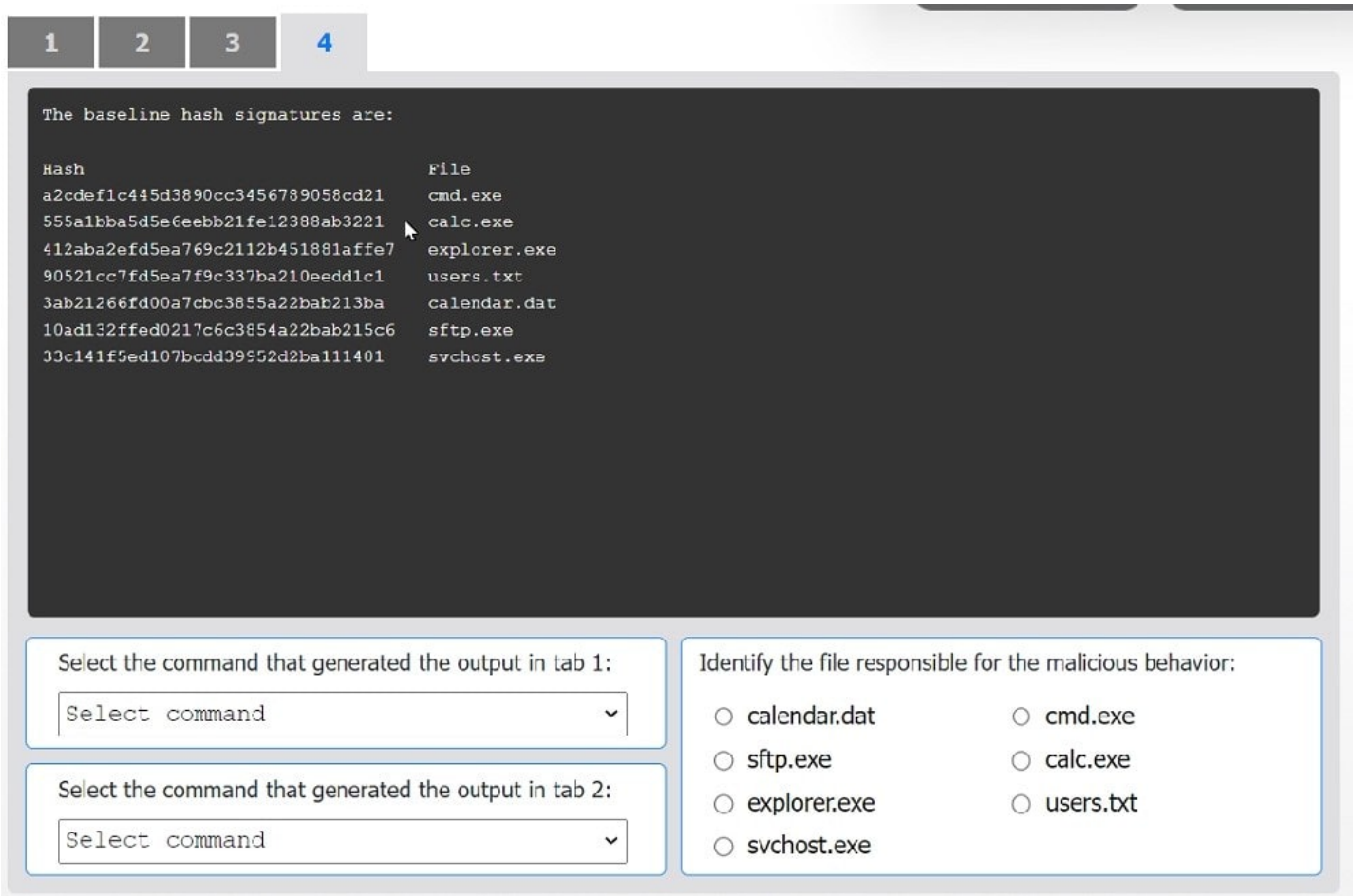
Review the output text in all tabs and identify the file responsible for the malicious behavior.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

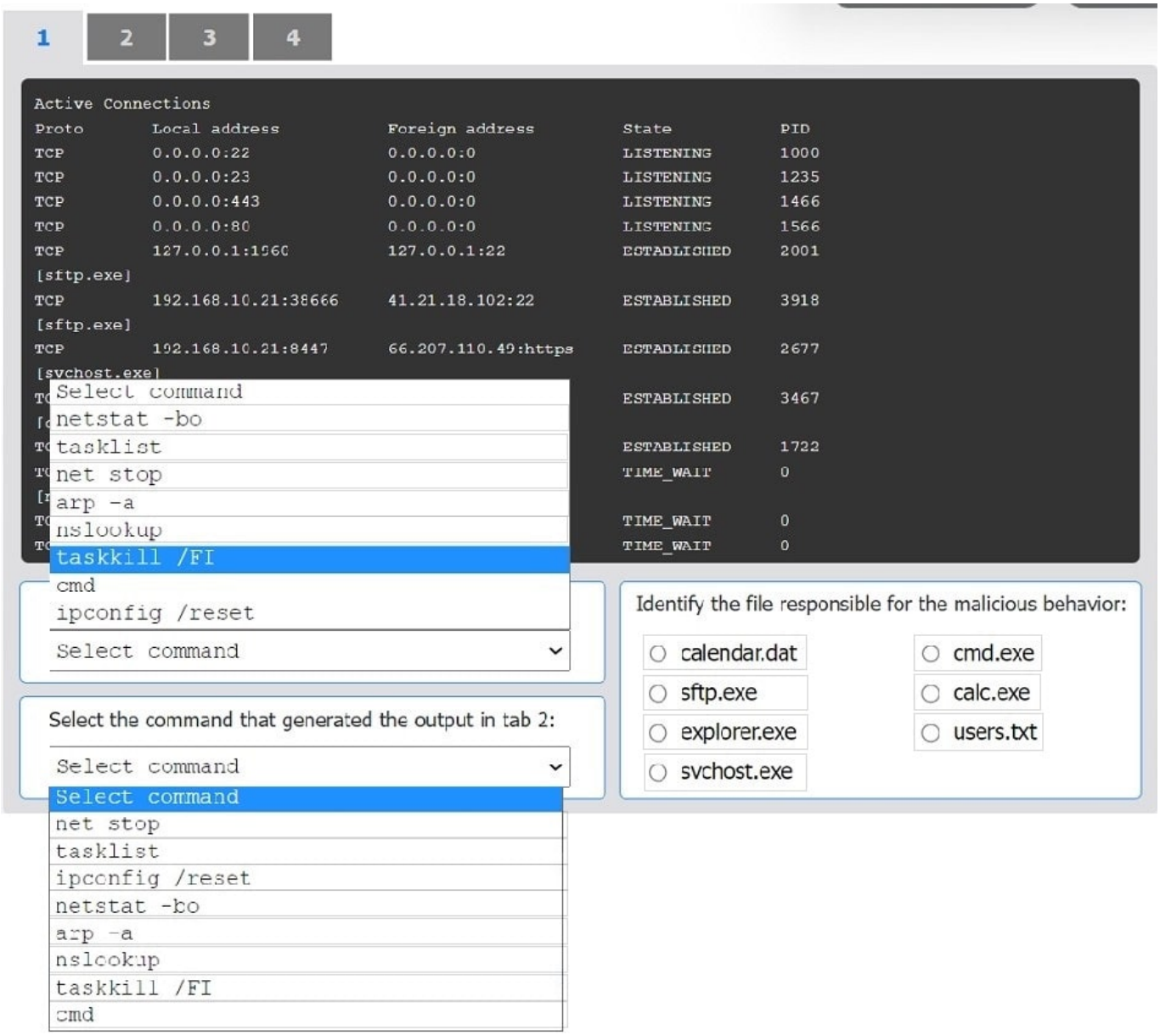

1
2
3
4
Active Connections
Proto Local address Foreign address State PID
TCP 0.0.0.0:22 0.0.0.0:0 LISTENING 1000
TCP 0.0.0.0:23 0.0.0.0:0 LISTENING 1235
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 1466
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 1566
TCP 127.0.0.1:1960 127.0.0.1:22 ESTABLISHED 2001
[sftp.exe]
TCP 192.168.10.21:38666 41.21.18.102:22 ESTABLISHED 3918
[sftp.exe]
TCP 192.168.10.21:3447 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
sftp.exe
explorer.exe
svchost.exe
cmd.exe
calc.exe
users.txt


1
2
3
4
Image Name PID Session Name Session# Mem Usage
Cmd.exe 3467 Console 0 18,020 K
sftp.exe 2001 Console 0 17 K
sftp.exe 3918 Console 0 1,788 K
svchost.exe 2677 Console 0 188 K
calc.exe 1677 Console 0 11 K
notepad.exe Console 0 0 K
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
sftp.exe
explorer.exe
svchost.exe
cmd.exe
calc.exe
users.txt

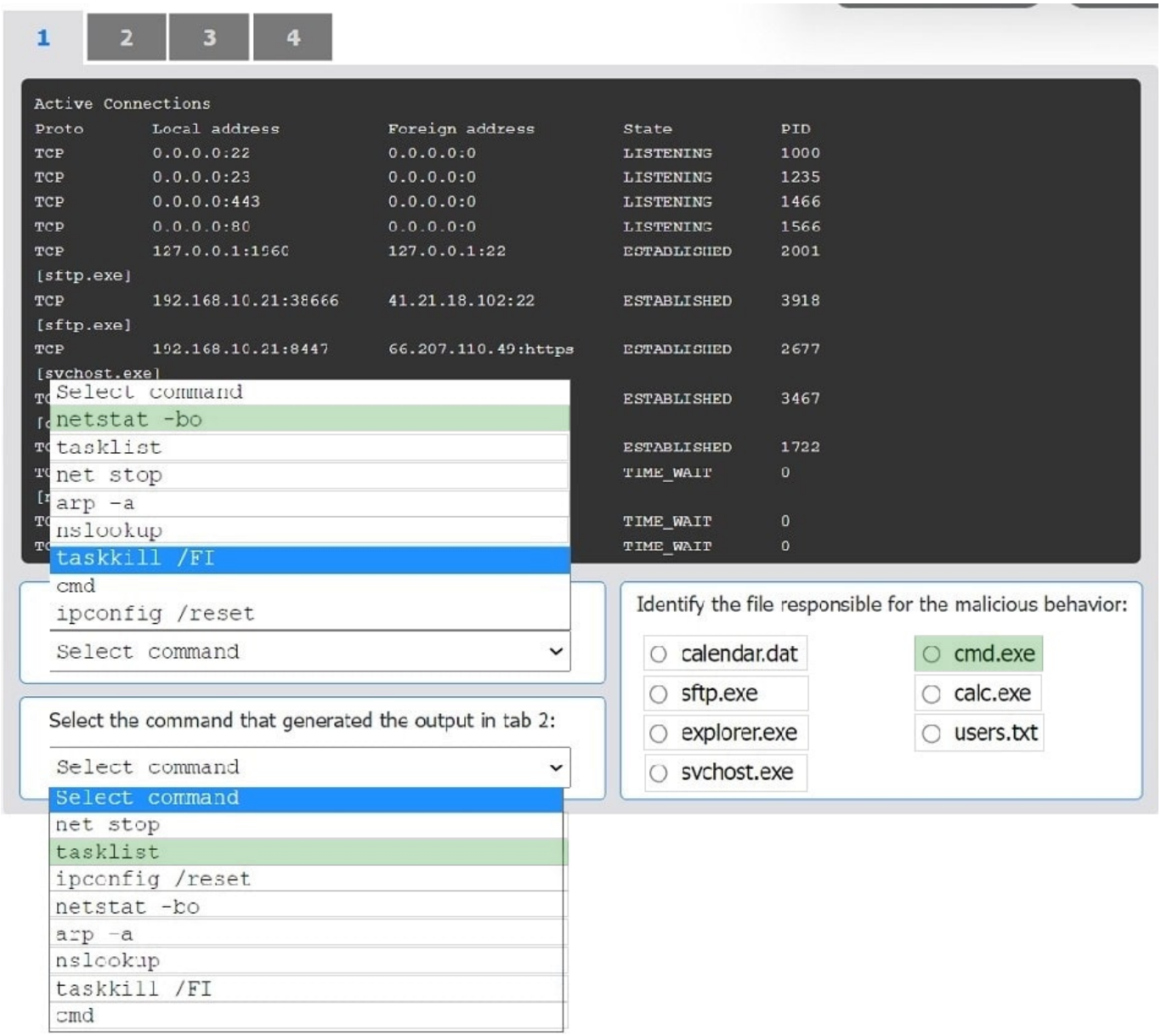

1
2
3
4
> Get-ChildItem | Get-FileHash -Algorithm MD5
Algorithm Hash File
MD5 372ab227fd3ea779c211a145181d1e1 cmd.exe
MD5 173ab22a5d3ea07bb212c14586aad4c2 calc.exe
MD5 412aba2ofd3ea39c2112b451881affe7 explorer.exe
MD5 df6ab147fd3ecb79c331a146f8dad199 users.txt
MD5 212ac257fd3ea7f9c337ba22bab1d1f5 calendar.dat
MD5 10ad132ffed0217c6c3854a22bab215c6 sftp.exe
MD5 33c141f3ed107bcdd39952d2ba111401 svchost.exe
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
sftp.exe
explorer.exe
svchost.exe
cmd.exe
calc.exe
users.txt


1
2
3
4
The baseline hash signatures are:
Hash File
a2cdef1c445d3890cc3456789058cd21 cmd.exe
555a1bba5d5e6eebb21fe12388ab3221 calc.exe
412aba2efd5ea769c2112b451881affe7 explorer.exe
90521cc7fd5ea7f9c337ba210eedd1c1 users.txt
3ab21266fd00a7cbc3855a22bab213ba calendar.dat
10ad132ffed0217c6c3854a22bab215c6 sftp.exe
33c141f5ed107bcdd39552d2ba111401 svchost.exe
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

Hot Area:



Correct Answer:



QUESTION 5

Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

A. Determine the sophistication of the audience that the report is meant for

B. Include references and sources of information on the first page

C. Include a table of contents outlining the entire report

D. Decide on the color scheme that will effectively communicate the metrics

Correct Answer: A

The best way to begin preparati"" regarding a recent incident involving a cybersecurity breach is to determine the

sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and businessoriented than a report for technical staff or peers.

QUESTION 6

Which of the following statements best describes the MITRE ATTandCK framework?

A. It provides a comprehensive method to test the security of applications.

B. It provides threat intelligence sharing and development of action and mitigation strategies.

C. It helps identify and stop enemy activity by highlighting the areas where an attacker functions.

D. It tracks and understands threats and is an open-source project that evolves.

E. It breaks down intrusions into a clearly defined sequence of phases.

Correct Answer: C

The MITRE ATTandCK framework is a knowledge base of adversary tactics and techniques based on real-world observations. It helps organizations identify and understand how attackers operate and where they focus their efforts, enabling more effective defense strategies. It highlights areas where an attacker functions during a cyber intrusion, which can help in identifying and stopping their activity.

QUESTION 7

A security analyst detects an email server that had been compromised in the internal network. Users have been reporting strange messages in their email inboxes and unusual network traffic. Which of the following incident response steps should be performed next?

A. Preparation

B. Validation

C. Containment

D. Eradication

Correct Answer: C

After detecting a compromised email server and unusual network traffic, the next step in incident response is containment, to prevent further damage or spread of the compromise. References: CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

QUESTION 8

An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason the firewall feed stopped working?

A. The firewall service account was locked out.

B. The firewall was using a paid feed.

C. The firewall certificate expired.

D. The firewall failed open.

Correct Answer: C

The firewall certificate expired. If the firewall uses a certificate to authenticate and encrypt the feed, and the certificate expires, the feed will stop working until the certificate is renewed or replaced. This can affect the data enrichment process and the security analysis. References: CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161.

QUESTION 9

A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

A. Code analysis

B. Static analysis

C. Reverse engineering

D. Fuzzing

Correct Answer: C

Reverse engineering is a technique that involves analyzing a binary file to understand its structure, functionality, and behavior. Reverse engineering can help security analysts perform malware analysis, vulnerability research, exploit development, and software debugging. Reverse engineering can be done using various tools, such as disassemblers, debuggers, decompilers, and hex editors.

QUESTION 10

The security team reviews a web server for XSS and runs the following Nmap scan:

```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

PORT     STATE    SERVICE REASON
80/tcp   open     http    syn-ack
| http-unsafe-output-escaping:
|_ Characters [> " '] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

Which of the following most accurately describes the result of the scan?

A. An output of characters > and " as the parameters used m the attempt

B. The vulnerable parameter ID hccp://l72.31.15.2.php?id-2 and unfiltered characters returned

C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe

D. The vulnerable parameter and characters > and " with a reflected XSS attempt

Correct Answer: D

A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back t" case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL http:/.31.15.2.php?id=2.

QUESTION 11

A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

A. nessie.explosion

B. vote.4p

C. sweet.bike

D. great.skills

Correct Answer: D

QUESTION 12

A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:

1.

Security Policy 1006: Vulnerability Management

2.

The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.

3.

In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.

4.

The Company shall prioritize patching of publicly available systems and services over patching of internally available system.

According to the security policy, which of the following vulnerabilities should be the highest priority to patch?

A. Name: THOR HAMMER CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H internal System

B. Name: CAP.SHIELD CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N External System

C. Name: LOKI.DAGGER CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H External System

D. Name: THANOS.GAUNTLET CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Internal System

Correct Answer: B

Based on the security policy and the CVSSv3.1 Base Scores, vulnerability B (CAP.SHIELD) with a high impact on confidentiality should be the highest priority to patch. It is an externally accessible system, and since confidentiality takes precedence over availability, it should be addressed before other vulnerabilities.

QUESTION 13

A threat hunter seeks to identify new persistence mechanisms installed in an organization\\'s environment. In collecting

scheduled tasks from all enterprise workstations, the following host details are aggregated: Which of the following actions should the hunter perform first based on the details above?

Task name	Target process	Number of hosts	Task user account
RtkAudUService64_BG	C:\Windows\System32\RtkAudUService64.exe	502	NT Authority/SYSTEM
BatteryGaugeMaintenance	%ProgramData%\Lenovo\Plugins\BGHelper.exe	410	NT Authority/SYSTEM
RtHVBg_PushButton	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	870	NT Authority/SYSTEM
UpdateService	C:\Users\sam\AppData\Roaming\Temp\taskhw.exe	1	PROD\sam

A. Acquire a copy of taskhw.exe from the impacted host

B. Scan the enterprise to identify other systems with taskhw.exe present

C. Perform a public search for malware reports on taskhw.exe.

D. Change the account that runs the -caskhw. exe scheduled task

Correct Answer: B

QUESTION 14

Which of the following would likely be used to update a dashboard that integrates.....?

A. Webhooks

B. Extensible Markup Language

C. Threat feed combination

D. JavaScript Object Notation

Correct Answer: D

JavaScript Object Notation (JSON) is commonly used for transmitting data in web applications and would be suitable for updating dashboards that integrate various data sources. It\\'s lightweight and easy to parse and generate.

QUESTION 15

An employee is no longer able to log in to an account after updating a browser. The employee usually has several tabs open in the browser. Which of the following attacks was most likely performed?

A. RFI

B. LFI

C. CSRF

D. XSS

Correct Answer: C

The most likely attack that was performed is CSRF (Cross-Site Request Forgery). This is an attack that forces a user to execute unwanted actions on a web application in which they are currently authenticated1. If the user has several tabs open in the browser, one of them might contain a malicious link or form that sends a request to the web application to change the user\\'s password, email address, or other account settings. The web application will not be able to distinguish between the legitimate requests made by the user and the forged requests made by the attacker. As a result, the user will lose access to their account. To prevent CSRF attacks, web applications should implement some form of anti-CSRF tokens or other mechanisms that validate the origin and integrity of the requests2. These tokens are unique and unpredictable values that are generated by the server and embedded in the forms or URLs that perform state-changing actions. The server will then verify that the token received from the client matches the token stored on the server before processing the request. This way, an attacker cannot forge a valid request without knowing the token value. Some other possible attacks that are not relevant to this scenario are: RFI (Remote File Inclusion) is an attack that allows an attacker to execute malicious code on a web server by including a remote file in a script. This attack does not affect the user\\'s browser or account settings. LFI (Local File Inclusion) is an attack that allows an attacker to read or execute local files on a web server by manipulating the input parameters of a script. This attack does not affect the user\\'s browser or account settings. XSS (Cross-Site Scripting) is an attack that injects malicious code into a web page that is then executed by the user\\'s browser. This attack can affect the user\\'s browser or account settings, but it requires the user to visit a compromised web page or click on a malicious link. It does not depend on having several tabs open in the browser.