DUMPSARENA

Logical Operations CyberSec First Responder

Logical Operations CFR-210

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

During a network-based attack, which of the following data sources will provide the BEST data to quickly determine the attacker's point of origin? (Choose two.)

A. DNS logs

B. System logs

C. WIPS logs

D. Firewall logs

E. IDS/IPS logs

ANSWER: A D

QUESTION NO: 2

A malicious attacker has compromised a database by implementing a Python-based script that will automatically establish an SSH connection daily between the hours of 2:00 am and 5:00 am. Which of the following is the MOST common motive for the attack vector that was used?

A. Pivoting

B. Persistence/maintaining access

C. Exfiltration

D. Lateral movement

ANSWER: D

QUESTION NO: 3

Which of the following are legally compliant forensics applications that will detect ADS or a file with an incorrect file extension? (Choose two.)

A. Regedit

B. EnCase

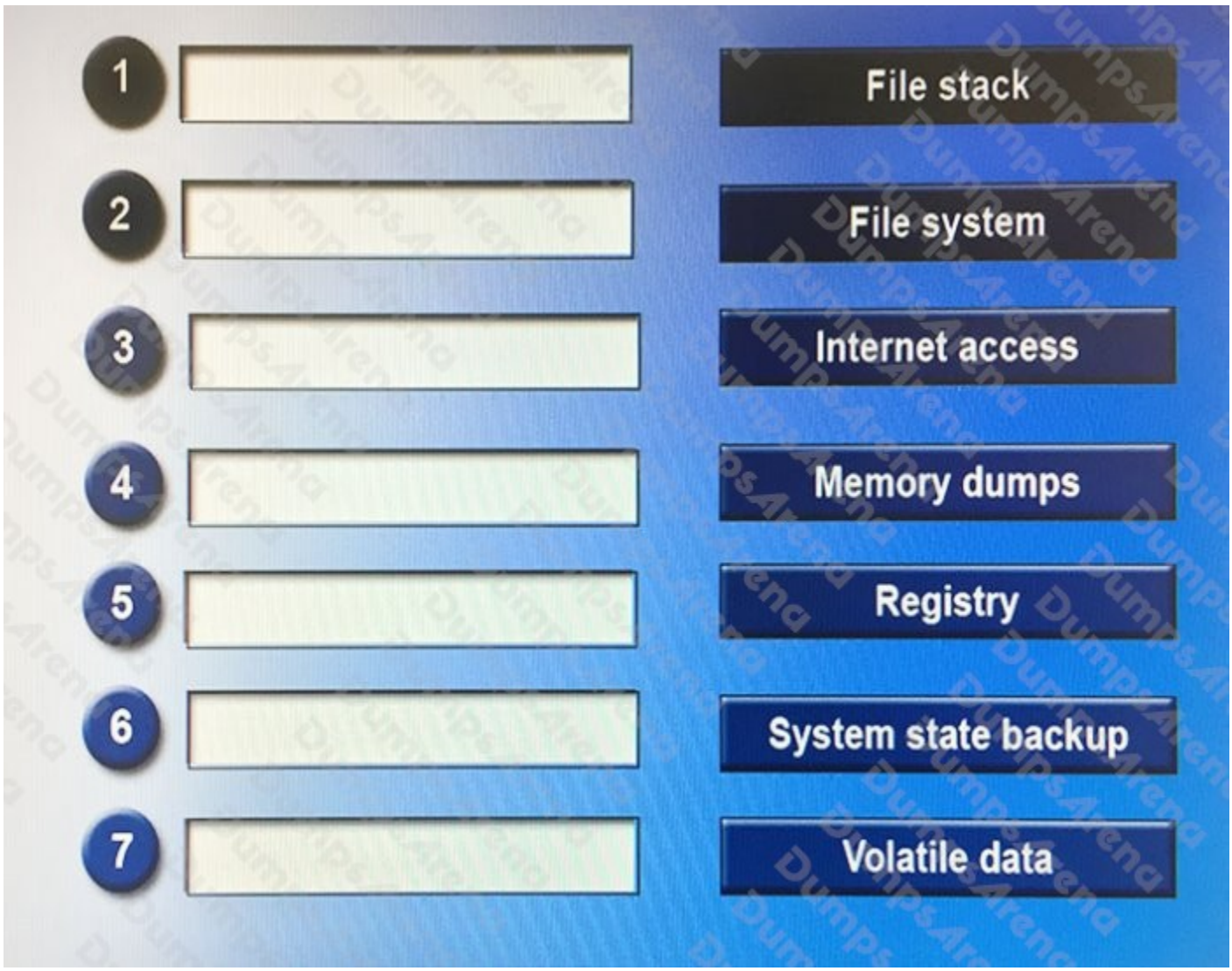
C. dd

D. FTK

E. Procmon

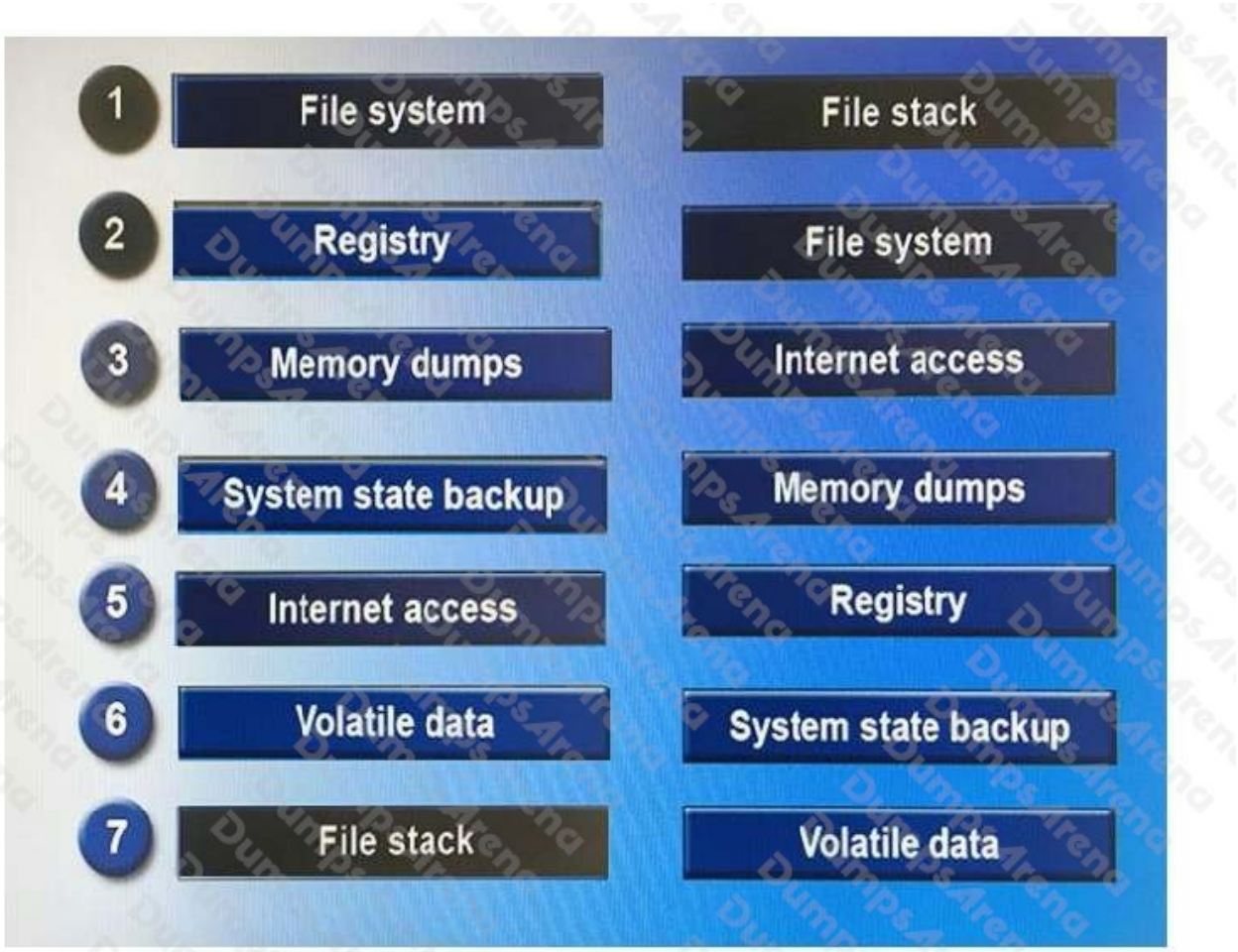
ANSWER: A C

QUESTION NO: 4 - (DRAG DROP)

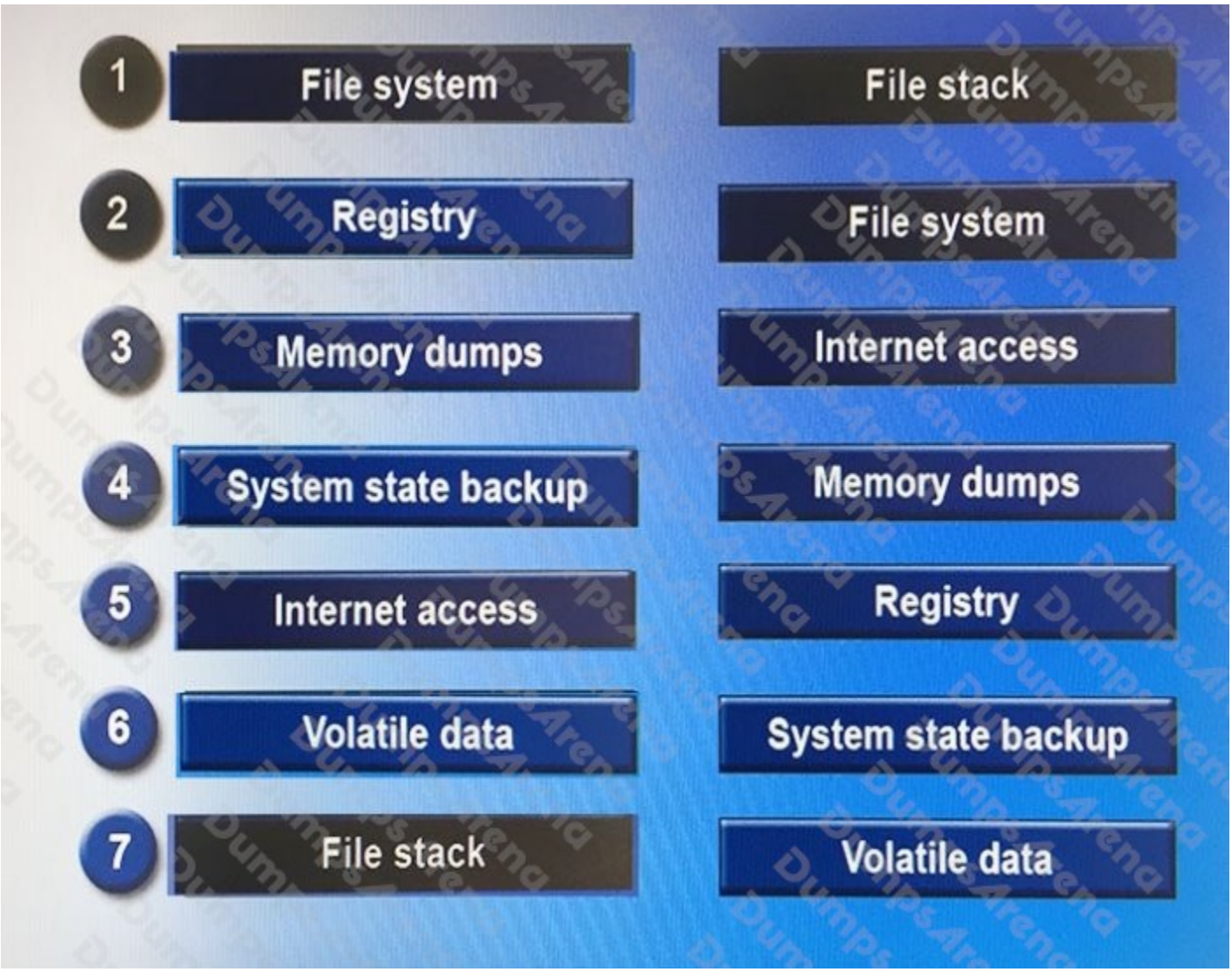


Drag and drop the following steps in the correct order from first (1) to last (7) that a forensic expert would follow based on data analysis in a Windows system.

ANSWER:



Explanation:



QUESTION NO: 5

An administrator wants to block Java exploits that were not detected by the organization's antivirus product. Which of the following mitigation methods should an incident responder perform? (Choose two.)

A. Utilize DNS filtering

B. Send binary to AV vendor for analysis

C. Create a custom IPS signature

D. Implement an ACL

E. Block the port on the firewall

ANSWER: C E

QUESTION NO: 6

During an annual penetration test, several rootkit-enabled systems are found to be exfiltrating data. The penetration test team and the internal incident response team work to begin cleanup. The company's operations team offers a new emails server to use for communications during the incident. As cleanup continues, the attackers seem to know exactly what the incident response plan is. Which of the following will prevent the attackers from compromising cleanup activities?

A. Check the DNS server for rootkits placed by the attackers.

B. Disconnect the Internet router until all systems can be checked and cleaned.

C. Use out-of-band communication until the end of the incident.

D. Disconnect the old emails server until they can be checked and cleaned.

ANSWER: A

QUESTION NO: 7

A logfile generated from a Windows server was moved to a Linux system for further analysis. A system administrator is now making edits to the file with vi and notices the file contains numerous instances of Ctrl-M (^M) characters. Which of the following command line tools is the administrator MOST likely to use to remove these characters from the logfile? (Choose two.)

A. tr

B. cut

C. cat

D. unix2dos

E. awk

ANSWER: A C

QUESTION NO: 8

A DMZ web server has been compromised. During the log review, the incident responder wants to parse all common internal Class A addresses from the log. Which of the following commands should the responder use to accomplish this?

A. grep –x"(10.[0-9]+.[0-9]+.[0-9]+)" etc/rc.d/apache2/access.log | output.txt

B. grep –x"(192.168.[0.9]+[0-9])" bin/apache2/access.log | output.txt

C. grep –v"(10.[0-9]+.[0-9]+.[0-9]+)" /var/log/apache2/access.log > output.txt

D. grep –v"(192.168.[0.9]+[0-9]+)" /var/log/apache2/access.log > output.txt

ANSWER: C

QUESTION NO: 9

As part of an incident response effort, data has been collected and analyzed, and a malware infection has been contained. Which of the following is the NEXT step the incident response team should take within the incident response process?

A. Begin recovering all infected systems to return the organization to normal operations as soon as possible.

B. Ensure every instance of the malware has been removed across the organization.

C. Discuss lessons learned before proceeding with other steps.

D. Start writing the report to ensure a quality product is delivered by the end of the project.

ANSWER: B

QUESTION NO: 10

Which of the following technologies is used as mitigation to XSS attacks?

A. Intrusion prevention

B. Proxy filtering

C. Web application firewall

D. Intrusion detection

ANSWER: C