GIAC
GX-FA
GIAC Experienced Forensics Analyst (GX-FA)

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**



Latest Version: 6.0

Question: 1

In a forensic analysis, the “%SystemRoot%\Prefetch” directory is examined primarily to discover:

A. Deleted registry keys
B. Executable files that have been run recently
C. Network share mappings
D. User password hashes

Answer: B

Explanation:
Prefetch files are created when an executable runs, storing metadata about the execution, helping investigators identify recently used programs.

Question: 2

Which of the following tools can be used to extract and parse Windows Event Log (EVTX) files into CSV format?

A. Evtxtract
B. RegRipper
C. MFTExp
D. Bulk Extractor

Answer: A

Explanation:
Evtxtract (or its Python counterpart) reads EVTX files and can export events to CSV for analysis.

Question: 3

The “lsass.exe” process typically runs under which user account?

A. Local System
B. Network Service
C. Local Service
D. Administrator

Answer: A

Explanation:
LSASS runs under the Local System account because it must access secure system resources for authentication

Question: 4

Which of the following is a characteristic of a “sandbox escape” technique often observed in advanced malware?

A. Use of standard Windows APIs only
B. Exploiting virtualization driver flaws to gain host OS control
C. Deleting all Prefetch files
D. Modifying the user’s desktop wallpaper

Answer: B

Explanation:
Sandbox escapes frequently target vulnerabilities in virtualization drivers (e.g., VMware, Hyper-V) to break out of the isolated environment.

Question: 5

The “Amcache.hve” hive is located in which directory on a Windows system?

A. %SystemRoot%\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Apps\Amcache.hve
B. %SystemRoot%\System32\config\Amcache.hve
C. %SystemRoot%\AppCompat\Programs\Amcache.hve
D. %SystemRoot%\System32\winevt\Logs\Amcache.hve

Answer: C

Explanation:
The Amcache.hve file resides in the “AppCompat\Programs” folder under the Windows directory.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/