GIAC Certified Forensic Analyst

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES

www.zetlantech.com

GIAC Certified Forensic Analyst

Course Modules

1. Analyzing Volatile Malicious Event Artifacts

Understandg of abnormal activity within the structure of Windows memory and be able to identify artifacts such as malicious processes, suspicious drivers and malware techniques such as code injection and rootkits.

2. Analyzing Volatile Windows Event Artifacts

Understanding of normal activity within the structure of Windows memory and be able to identify artifacts such as network connectns, memory resident command line artifacts and processes, handles and threads.

3. Enterprise Environment Incident Response

Understanding of the steps of the incident response process, attack progression, and adversary fundamentals and how to rapidly assess and analyze systems in an enterprise environment scaling tools to meet the demands of large investigations.

4. File System Timeline Artifact Analysis

Understanding of the Windows filesystem time structure and how these artifacts are modified by system and user activity.

5. Identification of Malicious System and User Activity

Understanding of the techniques required to identify & document indicators of compromise on a system, detect malware and attacker tools, attribute activity to events and accounts, and identify and compnsat fr anti-forensic actions usg memory & disk residnt artifacts.

6. Identification of Normal System and User Activity

Understanding of the techniques required to identify, document, and differentiate normal and abnormal system and user activity using memory and disk resident artifacts.

7. Introduction to File System Timeline Forensics

Understanding of the methodology required to collect and process timeline data from a Windows system.

8. Introduction to Memory Forensics

Understanding of how and when to collect volatile data from a system and how to document and preserve the integrity of volatile evidence.

9. NTFS Artifact Analysis

Understanding of core structures of the Windows filesystems, and the ability to identify, recover, and analyze evidence from any file system layer, including the data storage layer, metadata layer, and filename layer.

10. Windows Artifact Analysis

Understanding of Windows system artifacts and how to collect and analyze data such as system back up and restore data and evidence of application execution.

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474