GIAC Experienced Forensic Analyst

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1.Analyzing Artifacts of Lateral Movement

Recognize and analyze events created by malicious lateral movement.

2.Examining Evidence of Execution

Recognize and analyze evidence of programs, scripts and other files being launched from the review of Windows host artifacts.

3.Examining Volatile Evidence

Analyze memory resident artifacts to identify both normal and malicious events.

4.Examining Windows Event Log Data

Windows event log data to provide analysis and identification of both normal and malicious events.

5.Examining Windows File System Artifacts

Windows host artifacts to provide analysis of both normal and malicious activity.

6.Identifying Evasion Techniques

Perform the tasks required to identify the use of commands or applications to remove or disguise evidence of malicious activity.

7.Investigating Credential Theft

Demonstrate the ability to recognize & analyse artifacts created during the collection and compromise of host credentials.

8.Investigating Persistence Mechanisms

Recognize and analyze configuration changes, script creation and use & program execution designed to allow malicious activity to survive, launch or restart based on the analysis of host based logs, system configurations and volatile data.

9.Temporal Event Analysis

Windows host event data to provide analysis of both normal & malicious activity.

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