GIAC Reverse Engineering Malware Certification

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1. **Analyzing Malicious Office Macros**

   Analyze macros & scripts embedded in suspicious Microsoft Office files to understand their capabilities.

2. **Analyzing Malicious PDFs**

   Analyze suspicious PDFs and embedded scripts to understand the nature of the threat they might pose.

3. **Analyzing Malicious RTF Files**

   Analyze suspicious RTF files & embedded shellcode to understand their capabilities.

4. **Analyzing Obfuscated Malware**

   Able to identify packed Windows executables and obfuscated malicious JavaScript and unpack it to gain visibility of it's key capabilities.

5. Behavioral Analysis Fundamentals

Analyze static properties of a suspected malware sample, develop theories regarding its nature, & determine subsequent analysis steps.

6. Common Malware Patterns

Identify common API calls used by malware and understand what capabilities the APIs offer to the malware samples.

Identify common techniques used by malware including code injection, hooking, and process hollowing techniques.

7. Core Reverse Engineering Concepts

Dynamic analysis techniques to examine a malware sample in a debugger and will apply static analysis techniques to interpret common assembly instructions and patterns in Windows malware using a disassembler.

8. Examining .NET Malware

Analyze .NET programs to understand their capabilities.

9. Identifying and Bypassing Anti-Analysis Techniques

Identify & bypass common debugger detection & data protection measures used in malware, including the detection of security tools.

10. Malware Analysis Fundamentals

Describe key methods for analyzing malicious software & identify the needs of malware analysis lab.

11. Malware Flow Control and Structures

Analyze common execution flow contrl mechanisms, such as loops and conditional statements, in assembly language.

12. Overcoming Misdirection Techniques

Misdirecting execution workflow as an anti-analysis technique used in malware.

13. Reversing Functions in Assembly

Analyze malware functions in assembly language to understand use of parameters, return values and other structural elements.

14. Static Analysis Fundamentals

Analyze static properties of a suspected malware sample, develop theories regarding its nature, & determine subsequent analysis steps.

15. Unpacking and Debugging Packed Malware

Demonstrate process for unpacking malware using a debugger and repairing unpacked malware for further analysis.

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