SCMRE
Certified Malware Reverse Engineer

Synapse Certified Malware Reversing

Course objective:
The Aim of the Synapse's Certified Malware Reversing Course is to teach their Students the art reverse engineering and analyzing Malware in a fully hands on training.

Course Requirements:

- A Laptop running windows XP service pack 3 (or on VM)
- The Preferred VM (VirtualBox)

Suitable Requirements: (to be changed)
• Basic understanding of assembler language
• Basic programming skills

Course Duration:

Course Name	Duration	Instructors	Delivery Method	Delivery Date
SCMRE	One weeks (05 Days)	1/2	Onsite	

Contacts:
• Email: info@synapse-labs.com
• website: http://www.synapse-labs.com

Course Schedule:

- Day 1: 9am-4pm
- Day 2: 9am-4pm
- Day 3: 9am-4pm
- Day 4: 9am-4pm
- Day 5: 9am-4pm

Day 1

Chapter 0 : **The malware industry (1 hour)**

What is a Malware and their category

Malware history & evolution

Chapter 1 : **Inside Windows memory and PE structure (3 hours)**

- Windows memory layout
- The PE structure
- Windows process & threads
- Device drivers

Chapter 2: **Understanding assembler programming (2 hours)**

- A crash introduction to assembly programming

Day 2

Chapter 3: **The malware reverser toolkit (2 hours)**

- Overview of tools used by reverse engineers
- introduction to debuggers

Chapter 4: **Building the lab (1 hour)**

- Building the lab
- Security points to respect
- Kernel debugging lab

Chapter 5: **Static VS dynamic analysis (3 hours)**

- Static analysis of malware
- Dynamic analysis

Day 3

Chapter 6: **Disassembling and debugging malicious code (4 hours)**

- Two full malware specimen static & dynamic analysis

Chapter 7: **Bypassing protection mechanisms (2 hours)**

- Anti debugging techniques
- Bypassing Anti debugging techniques

Day 4

Chapter 8: **Reversing encryption techniques (3 hours)**

- encryption algorithms
- encoding techniques
- reversing encryption & encoding techniques

Chapter 9: **Malicious Code deobfuscation (3 hours)**

- Obfuscation techniques
- Deobfuscation techniques
- packers and unpackers
- Manual malware unpacking

Day 5

Chapter 10: **Analyzing polymorphic techniques (1 hour)**

- polymophic techniques
- metamorphic techniques
- get program counter

Chapter 11: **Advanced malware infection mechanisms (1 hour)**

- File infection techniques
- Memory infection and Process injection techniques
- Exploits and 0day payloads

Chapter 12: **Memory & Kernel debugging (4 hour)**

- use of memory analyzers & tools
- Playing with physical dumps
- kernel vs user mode debugging
- using Virtual KD
- Example of reversing a rootkit using kernel debugging