Advanced RAM Analysis & Live Forensics Training

We are pleased to announce the latest version of our 4 day Advanced RAM Analysis course.

As before the course is primarily hands on but provides much more flexibility.

A significant time is spent in advanced memory analysis techniques including a deconstruction of memory resident Malware such as Stuxnet. By the end of this course you will have created and scripted your own USB toolkit to extract volatile data and the RAM from a target machine, deploying covert techniques if required, as well as a toolkit to analyse that data back at the lab.

An 16 GIG USB key is supplied for each student to keep with all the software and RAM dumps needed for the course.

Syllabus

- Live Forensic procedures
    - Including how to detect encryption on both a BIOS and UEFI system
- Live RAM imaging (Cmd line and GUI based)
- Overview of Helix Pro for remote imaging
- Tool testing
- Circumventing password protection
- Creating and scripting your own USB toolkits (USB keys to keep included)
    - Script disk imaging
    - Volatile data extraction
    - Reverse copying key files and folders
- Advanced Memory (RAM) analysis
    - Extraction of bespoke file types
    - Extraction of Internet History
    - Extraction of Gmail contacts and other data
    - Extracting data from Hiberfil and Crashdump files

- Using Volatility to extract:-
    - Running processes
    - Open network sockets
    - Open network connections
    - DLLs loaded for each process
    - Open files for each process
        - Finding HTML pages in a Browser process
    - Open registry handles for each process
    - A process' addressable memory
    - OS kernel modules
    - Mapping physical offsets to virtual addresses (strings to process)
    - Understanding the PEB
    - Understanding the VAD
    - Extracting executables from memory samples
    - Extracting and analysing system files
    - Extracting the MFT
    - Virus checking RAM dumps
    - Extraction of network packet data and analysis
        - Enhanced network analysis

- Volatility 3.0
    - Setup
    - Differences between version 2 and 3
    - Useage

- New Decryption section
    - Hands-on extraction of Truecrypt/Veracrypt Master Keys and container decryption
    - Hands-on extraction of Bitlocker Master Keys and drive decryption
    - Cracking of OSX Keychain without password

- New Malware section
    - ID'ing suspect processes
    - Following the malware into Services and Registry
    - Mapping the IP connections
    - Extraction of the malware and analysis
    - Deconstruction of Stuxnet
    - Understanding what the Malware is doing
    - Much more…

- New Registry Section
  - Location and extraction of specific registry keys
  - Extracting the SAM and decrypting passwords
  - Finding other passwords
  - Locating useful keys (TypedURLS, System info etc)
  - Extracting Chrome and Firefox history

- Live Memory Analysis
  - Analysing live running memory using Memtriage
  - Using The Memory Process File System

- Linux RAM investigation
  - Extracting Linux Memory
    - LiME
    - AVML
  - Analysis of Linux memory using volatility
    - Recovering processes
    - Login sessions
    - Network information
    - Routing tables
    - Open files
    - And more

- OSX Memory analysis
  - Forensic process
  - Memory extraction
  - Volatility commands

- Creating your own RAM analysis script to take away
- Final day practical exam and review

To discuss your training needs, or to organize a course, please contact Nick Furneaux – nick@csitech.co.uk

---