Advanced RAM Analysis and Forensics - 4 Day Course

We are pleased to announce the updated 2021 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 data extraction and analysis techniques including reconstruction of file systems, password location, decryption and deconstruction of memory resident Malware such as Stuxnet. Also interesting, is creating and scripting your own memory analysis toolkit.

A 32 GIG ruggedized USB key (download for online course) is supplied for each student to keep with all software and RAM dumps.

Syllabus

- Live Forensic procedures
- Live Windows RAM imaging (Cmd line and GUI based)
- Imaging Linux RAM
- Imaging Intel Mac's (OSX)
- Testing downloaded tools
- Creating and scripting your own toolkits
    - Script disk imaging
    - Scripting memory imaging
    - Volatile data extraction
    - Reverse copying key files and folders
- Advanced Memory (RAM) analysis
    - Extraction of data to enhance a disk investigation
    - Extraction of elements such as Internet History, timelines and passwords
    - Extracting data from Hiberfil and Crashdump files
    - Recreating the entire file system with automated forensic data extraction

- 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
    - Extracting process spaces with their associated files
    - 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 operating system files
    - Extracting and analysing user files
    - Extracting the MFT
    - Virus checking RAM dumps
    - Extraction of network packet data and analysis
        - Enhanced network analysis

- New Decryption section
    - Hands-on extraction of Truecrypt and 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)
    - Again, loads more

- OSX Memory analysis
  - Data carving
  - Process recovery
  - New Volatility commands

- Linux RAM investigation
  - Data carving
  - Recovering processes
  - Login sessions
  - Network information
  - Routing tables
  - Malware investigation

- 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

---