Windows Memory Forensics with Volatility

- Important Information for Attendees -

Agenda

1. Refresher
    a. Why memory analysis?
    b. Memory acquisition primer
    c. Memory image file formats
    d. Concepts of virtual and physical memory
    e. Windows kernel objects
    f. Windows memory pools
    g. Object enumeration techniques
    h. Examination techniques
2. Volatility memory analysis framework
    a. Overview
    b. Architecture
    c. Using built-in commands
3. Programming Volatility
    a. Address spaces
    b. Objects
    c. Your first plugin
    d. Building blocks (common problems and solutions)

Who should attend?

The course addresses forensic examiners and incident responders who already know about the basics of Windows memory analysis and who have used tools like a kernel debugger, PTFinder and Volatility in the past.

The course builds on the classes held by Pär Österberg-Medina and Andreas Schuster at previous FIRST conferences. Attendees should be familiar with the literature (see “Recommended reading” below) and expect a steep learning curve.

The main part of the course will deal with the architecture of the Volatility memory analysis framework. A basic analysis and programming environment will be provided as a Linux virtual machine. Attendees should know how to navigate a UNIX shell (bash) and how to edit a text file. Also, attendees should know how to program and debug Python 2.6 scripts.

Recommended reading

- Pär Österberg-Medina: Detecting Intrusions - The latest forensics tools and techniques to identify Windows malware infections http://members.first.org/conference/2008/papers/medina-osterberg-par-slides.pdf
- Harlan Carvey: Windows Forensic Analysis, Chapter 3: Windows Memory Analysis. http://www.elsevierdirect.com/product.jsp?isbn=9781597491563
- Aquilina, Casey and Malin: Malware Forensics, Chapter 3: Analyzing Physical and Process Memory Dumps for Malware Artifacts. http://www.elsevierdirect.com/product.jsp?isbn=9781597492683
- Andreas Schuster: Searching for Processes and Threads in Microsoft Windows Memory Dumps. http://computer.forensikblog.de/files/talks/DFRWS2006-Searching_for-Processes_and_Threads.pdf
- Andreas Schuster: Pool Allocations as an Information Source in Windows Memory Forensics http://computer.forensikblog.de/files/talks/IMF2006-PoolAllocations-paper.pdf
- Mark Lutz: Python pocket reference. O'Reilly 2005 http://oreilly.com/catalog/9780596009403/
- Richard Gruet: Python Quick Reference. http://rgruet.free.fr/#QuickRef

Hardware/Software prerequisites

Attendees are expected to bring their own Laptop.

- Minimum hardware requirements:
  - CPU 1.5 GHz
  - 1 GB RAM
  - 6 GB of free disk space
  - DVD drive
- Software:
  - Either VMware Player (free) Version 6.5.2
    or VMWare Workstation 6.5.2 (commercial, 30days trial version available)
    from http://www.vmware.com/
  - Any archiver for your host OS that can unpack ZIP archives, e.g. file roller, WinZip

Don't forget to bring power adaptors, extension cords, an USB hub, OS and driver installation media, your latest backup and whatever else might be helpful in an impromptu work environment.

Contact

Don't hesitate to contact me; I welcome your suggestions and questions.

Andreas Schuster
a.schuster@yendor.net
http://computer.forensikblog.de/en/