Online Forensics

Joe Hemmerlein
Security Support Engineer
Microsoft CSS Security
joe.hemmerlein@microsoft.com

Microsoft | Services
Law Enforcement Support

Forensics vs Incident Response

- *Different goals*
  - IR - Restoration and prevention
  - *Forensics - Evidence preservation and legal action*
- *Different attitude*
  - IR - Fix as quick as possible
  - *Forensics - Cover and document all details*
- *Different results*
  - IR - Normal operation
  - *Forensics - Sets of documents and evidence*

The forensics schism

- Pull the Plug and do post-mortem analysis
  - Traditionally mostly disk analysis
    Disk Analysis
    - Imaging
    - Forensics by Hex Editor
    - Partitions
    - FAT32
    - Toolkits for Disk Forensics
  - Firewall-, IDS-, honey pot log analysis
- Gather data on the running system

What can Offline Forensics do?

- Recovers:
  - Deleted files
    - Slack space and free space
  - Passwords
  - Cryptographic keys
- Analyze file access, modification and creation (MAC) times.
- View/analyze System, Security and App logs.
- Identify users, applications and system activity.
- Analyze e-mails for source info and content.

What can Online Forensics do?

- Volatile data before forensic image
  - – Volatile data
    - Data in memory - Registers, cache contents
    - Running processes
    - Executed console commands
    - Passwords (clear text in memory)
    - Unencrypted data
    - Instant Messages
    - IP Addresses
    - Currently logged on users
    - Open ports and listening applications
    - Registry information
    - System information
    - Currently attached devices **especially networked devices**
  - - Contents of storage media: (Caution!)
    - Pssexec \\target –u Administrator p- password dd.exe **if**=\\.\PhysicalDrive0 **of**=\\mymachine\share\target.drive0.dd bs=8k conv=noerror
      - OR Netcat OR Cryptcat

Online Forensic Risks

- Data can be altered
  - Accidentally
  - By the tool
  - Intentionally (anti-forensics)
- A footprint of the forensic tool remains
- Accuracy of the tool could be challenged
- Could compromise offline analysis
  - ie. modification of MACe times

The Order of Volatility: OOV

Collecting some data impacts other data.

http://rfc.net/rfc3227.html

The expected lifespan of data.

Registers, peripheral memory, caches, etc.	nanoseconds
Main Memory	nanoseconds
Network state	milliseconds
Running processes	seconds
Disk	minutes
Floppies, backup media, etc.	years
CD-ROMs, printouts, etc.	tens of years

D Farmer, W Venema "Forensic Discovery" Addison-Wesley 2005

The Order of Volatility: OOV

- 1. RAM
- 2. Running Processes
- 3. Network connections
- 4. System settings
- 5. Hard Disk

Volatile Data Collection Process

- Collect uptime, date, time, and command history for the security incident
- When executing forensic tools or commands, generate the date and time to establish an audit trail
- Begin a command history that will document all forensic collection activities
- Collect all volatile system and network information
- End forensic collection with date, time and command history.

Example Steps:

- Create a step-by-step plan, document it:
  - Establish a new shell: cmd.exe
  - Record the system date and time:
    - now.exe
  - Record open sockets: netstat -ano
  - Processes that open sockets: fport
  - Currently running processes: pslist
  - System that recently connected: Nbtstat\netstat
  - Who is logged on: logonsessions
  - Re-run now.exe
  - Record step taken: doskey /history

How do we capture Memory?

- Hardware-based methods
  - DMA
  - IEEE 1394

- Software-based methods
  - Ctrl-ScrollLock keyboard sequence (Microsoft Knowledge Base Article 244139)
  - Benefit of “typical” memory dump

Physical Memory Devices

- **\\.\PhysicalMemory**
  - DD for Windows - Forensic Acquisition Utilities available at:

http://users.erols.com/gmgarner/forensics/

dd.exe if=\\.\PhyiscalMemory of=\\<remote share>\memorydump.img

- DD on 2000 and XP
- Not on Vista or 2003 SP1

Physical Memory Devices

- **\\.\DebugMemory**
  - WinDBG
- The upshot is that in order to really capture a snapshot of a Windows system, you need to cause a crashdump.

Memory Analysis Projects

- http://forensic.seccure.net
  - Analysis of Windows memory images
  - **WMFT - Windows Memory Forensics Toolkit**
- DFRWS Challenge 2005
  - The Memory Analysis Challenge
  - Results: 2 new tools
    - Memparser reconstructs a process list and extracts information from a process memory (Chris Betz)
    - Kntlist interprets structures of memory (George M. Garner Jr. and Robert Jan Mora)

Just checking: Any questions, yet?

Tools Walkthrough

- **Time:**
  - Now! Date, Time,
- **Network:**
  - Netstat, PortMon, Fport, Nbtstat
- **Processes:**
  - Pslist, Process Explorer
    - Using Process Explorer for removing malware
    - http://www.microsoft.com/emea/spotlight/sessionh.aspx?videoid=359
- Autoruns & Boot Logging

More tools...

- LogonSessions
- EFSdump
- Doskey
- Others:
  - Process Monitor
  - PsLogList
  - Streams
  - Strings
  - Sigcheck
  - PsFile
  - PendMoves and MoveFile
  - NTFSInfo
  - LDMDump
  - DiskView
  - AccessCheck
  - DebugView

References

- [CHOW, 2004] "Understanding Data Lifetime via Whole System Simulation", Jim Chow, Ben Pfaff, Tal Garfinkel, Kevin Christopher, and Mendel Rosenblum, Proceedings of the 2004 Usenix Security Symposium.
  http://suif.stanford.edu/collective/taint.pdf
- [GARNER, 2003] The Forensic Acquisition Utilities, including dd, for Windows.
  http://users.erols.com/gmgarner/forensics/
- The Coroner's Toolkit by Dan Farmer and Wietse Venema
- Blackhat presentations