Live Response for Windows Systems

Matt Churchill

Douglas County Sheriff’s Office

NebraskaCERT Conference 2007

Agenda

- Who am I?
- What is live response?
- Why is it important?
- What info can we acquire?
- What is the best method?
- Available Tools / Demo
- Analysis of RAM
- Resources

Who am I?

- 10 years LE experience
- Three and half years of computer forensics experience
- CFCE, CCE certified
- IACIS, ISFCE, HTCIA member

What is Live Response?

- Easy definition: Collecting data from a running computer
- Every action or inaction an investigator makes will result in changes to the system
- Will interacting with the running system produce enough results to justify the changes made?

Why is Live Response Important?

- Potential of information retrieved
- Some info won’t be available on a “dead” system
- Drive Encryption
- Hacker defense
- Case Law

What Info Can We Acquire?

- Network Information / Connections
- Running Processes
- Mapped Drives / Shares
- System Time, Logged on users
- RAM, to include:
  - Passwords
  - Instant Message Chats

What is the Best Method?

- Remember that some information will be lost quicker than others
- Varying degrees of volatility:
  - registers, cache
  - routing table, arp cache, process table, kernel statistics, memory
  - temporary file systems
  - Disk
  - remote logging and monitoring data that is relevant to the system in question
  - physical configuration, network topology
    - » *See RFC 3227*

What is the Best Method?

- Should we image RAM first and then run other tools or run some tools then collect RAM?
- Any tool run will displace information in RAM, but we may be able to find that information in the pagefile if it’s still being used

What is the Best Method?

- Test your tools first
- Know what actions they will have on the system
  - ProcessMonitor, ListDLLs, Dependency Walker
- Build a trusted toolkit, hash tools
- Test and validate toolkit
- What are you going to save the results to?

Available Tools

- Sysinternals / Microsoft
- Harlan Carvey's individual scripts
- George M. Garner Jr.'s tools, KnTTools
- Several tools to image RAM
  - DD
  - DMA firewire approach
  - Tribble
  - Crash Dumps
  - .vmem files

Available Tools

- Helix
  - Two sides: Windows and Bootable Live CD
  - Numerous incident response tools and "packages"
  - Free download

Available Tools

- Windows Forensic Toolchest
  - Excellent tool that can be used for incident response, auditing systems, or to check system configurations
  - Relies on tools not included in download, but everything is included on Helix CD
  - Non-network based output
  - New license structure as of June 07

Available Tools

- Incident Response Collection Report
- First Responder Utility
  - Both of these tools are similar to WFT, but require a listening computer on the network to send the output of the tools
- FRED, COFEE, Intel RPIER, Nigilant32
- Create your own .bat files to only run the items you specifically need

Helix Demo

INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS •
HELIX3™

Analysis of RAM

- Expectations
- Tools
  - Procloc, Tim Vidas
  - Ptfinder, Andreas Schuster
  - Harlan Carvey’s scripts
  - Microsoft debugging tools
  - Standard forensic programs, string search & data carving

Resources / Acknowledgements

- Most presentations referred to can be found by searching e-evidence.info
- Tim Vidas, Post-Mortem RAM Forensics
- Ricci Ieong, Freeware Live Forensics Tools Evaluation and Operation
- Antonio Martin, FireWire Memory Dump of Windows XP
- Robert Beggs, Live Response: Asking the Patient, Not the Corpse

Resources / Acknowledgements

- Harlan Carvey, book: Windows Forensic Analysis, website: windowsir.blogspot.com
- NIST SP800-86: Guide to Integrating Forensic Techniques into Incident Response
- Search:
  - Jesse Kornblum, Andreas Schuster, DFRWS
  - United States v. Heckenkamp
  - MPAA v. TorrentSpy