Open Source and Incident Response

Joe Lofshult, CISSP, GCIH

Agenda

- Overview
- Open Source Tools
- FIRE
- Demonstration

Overview

Incident

- Adverse event that threatens security in computing systems and networks. Examples include system crashes, DOS attacks, unauthorized account access, web page defacement, or virus infection. [Schultz and Shumway]

Incident Response

- Actions taken to handle an incident that occurs.

Overview

Computer Forensics

- Definition – The process of methodically examining computer data for evidence.
- Network Forensics – Applying the computer forensic methods to the search for evidence in network traffic.
- Host Forensics – Applying computer forensic methods to the examination of computer media (hard disks, tapes, diskettes, etc).

Overview

Live System Response

- Goals
  - Determine if an incident has occurred or is in progress.
  - Take steps to contain the incident.
  - Record all steps taken.
- Tools Required
  - View processes, network ports, disk files.
  - Network sniffer and diagnostic tools.
  - Trusted binaries. Can’t trust any programs on the system.
  - Tools to help automate information gathering and reporting.

Overview

Forensic Analysis

- Goals
  - Gather evidence from computer media.
  - Gather evidence from network traffic logs.
  - Analyze data to to determine what happened.
  - Do not alter the evidence.
  - Maintain a chain of evidence.
  - Create record of all steps taken.
- Tools Required
  - Tools to acquire the digital data.
  - Tools to analyze the data.
  - Tools to help automate the analysis and create a record.

Open Source Tools

Pros

- Price is right
- Tools can be customized to meet needs
- Empowers analyst (can look under the covers)

Cons

- Commercial support rarely available
- Legal acceptability
- Documentation sometimes sparse
- Tools not integrated

Open Source Tools

Windows Live Response

- Standard Windows utilities
- Other free tools
  - Foundstone tools
    - fport, sfind, hfind, afind, ntlast, etc
  - Sysinternals tools
    - psloggedon, pslist, ntfsinfo, etc
  - Cygwin toolkit
- Preferably run from external media (disk, CD-ROM, etc)

Open Source Tools

Unix Live Response

- Standard Unix tools
  - ps, cat, find, dd, script, strings
- Other freeware tools
  - lsof, netcat, tcpdump
- Preferably statically compiled and mounted from external media

Open Source Tools

Forensic Analysis

- Linux makes a great platform because
  - It supports many file system types
  - It affords the ability to examine a file system without affecting it
  - The development community has created many terrific analysis tools for it
  - It can run from bootable media

Open Source Tools

Forensic Analysis

- Linux File System Support
  - Ext2, Ext3 (Linux)
  - FFS, UFS (BSD, Unix)
  - FAT, VFAT (DOS, Windows)
  - NTFS (Windows NT/2000/XP)
  - HPFS (OS/2)
  - ISO9660 (CD-ROM)

Open Source Tools

Forensic Analysis

- Control over file system access
  - Drives are not mounted by default
  - Can be mounted with options such as:
    - read-only to prevent modifying files
    - noatime to prevent modifying access time
    - noexec to prevent executing code by mistake

Open Source Tools

Forensic Analysis

- Data Acquisition Tools
  - dd – Rated "Best Buy" by SC Magazine for data acquisition in September 2000
  - dcfldd – DoD enhanced dd that performs md5sum hashing
  - rda – combines dd, md5sum, and netcat in one tool
- Data Validation Tools
  - md5sum, sha1sum – Generate md5 for sha2 hashes

Open Source Tools

Forensic Analysis

- Data Analysis Tools
  - Media analysis
    - Sleuthkit, Autopsy, mac-robber
    - foremost
    - fatback
  - Network analysis
    - tcpdump – The standard
    - Snort
    - Ethereal, Etherape, ngrep

Open Source Tools

Forensic Analysis

- Bootable distributions
  - Not just for incident response (diskless, old systems, low memory, etc)
  - Knoppix (http://www.knoppix.org)
  - Trinux (http://trinux.sourceforge.net)
  - FIRE (http://fire.dmzs.com)

FIRE

- F.I.R.E. – Forensic and Incident Response Environment
- Developed by William Salusky
- Available at http://fire.dmzs.com.
- Developed with forensics and incident response in mind
- System requirements – x86 system with at least 48 MB RAM

FIRE

- Bootable Linux CD-ROM
  - Good hardware support
    - IDE and SCSI devices
    - Firewire and USB drives
    - Support for x filesystems
    - PCMCIA devices
  - X Windows support
- Security tool collection
  - Everything mentioned so far and much, much more

FIRE

Use for Live Response

- Good addition to your “jump kit”
- Just pop it in the CD-ROM drive
- Trusted, read-only environment
- Static binaries for Windows, Solaris, Linux
- Incident response data collection scripts
  - Linux: linux-ir.sh
  - Solaris: solaris-ir.sh
  - Win32: F.R.E.D. scripts (fred.bat and fred-nc.bat)

FIRE

Use for Forensic Analysis

- Data Acquisition
  - Boot from the CD-ROM
  - Choose either console or GUI environment
  - Make a bit-level backup of media
    - dd, dcfldd, or rda
    - Send backup to an external disk, cdrom, or to trusted server across a network
  - VNC included for remote analysis

FIRE

Use for Forensic Analysis

- Data Acquisition
  - Example: Using dd and netcat to send an image to another server for analysis
  - On server:
    - $ nc –l –p 9000 > image
  - In FIRE:
    - $ dd if=/dev/hda1 | nc server 9000

FIRE

Use for Forensic Analysis

- Data Analysis
  - Preferably, analysis would be done on backup image
    - Could use tools on FIRE disk
  - If not practical, could perform analysis using FIRE disk on the original system

FIRE

Other Uses

- Penetration Testing
  - Tools such as Dsniff, firewalk, fragrouter, John the Ripper, Nemesis, Nessus, NBTScan, Nikto, Nmap, hunt, airsnort
- Emergency Recovery
  - Recover files
  - Reset passwords
  - Repair file systems

FIRE

Demonstration

Summary

- Open source tools can play an important role in incident response and forensic analysis.
  - They’re not just for cash-strapped organizations.
- There are many great free tools available.
  - Get familiar with some the tools we’ve discussed.
  - During an incident is not the time to learn new tools.
- Download F.I.R.E. and check it out. I recommend version 0.3.5b.

Where to Get More Information

Books

- Mandia, Kevin and Chris Prosise. Incident Response. Osborne/McGraw-Hill. 2001.
- Schultz, E. Eugene and Russell Shumway. Incident Response. New Riders. 2002.

Where to Get More Information

White Papers and Presentations

- Carrier, Brian. Open Source Software in Digital Forensics. http://www.atstake.com/carrier.
- SANS May Webcast on F.I.R.E. http://www.sans.org/webcasts.
- Preservation of Fragile Digital Evidence by First Responders. http://www.dfrws.org/dfrws2002/papers/Papers/Jesse_Kornblum.pdf

Where to Get More Information

Tools

- F.I.R.E. http://www.dmzs.com/fire.
- Incident Response Homepage. http://www.incident-reponse.org
- Sleuthkit, Autopsy, and mac-robber. http://www.sleuthkit.org.
- Remote Data Acquisition. http://www.md5sa.com/downloads/rda.
- Cygwin. http://www.cygwin.com.
- Foundstone tools. http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm