The Big Chill

Freezing Data for Analysis

The Magic Button

- Absolute Zero
- Processes
- Disks
- Memory
- Network
- Internet...

- Or, speed yourself up…

Heisenberg's Principle of System Analysis

- **Real** - impossible to know both momentum and location; examining one affects the other.
- **Computers** - examining or collecting one part of the system will disturb other components. It is impossible to completely capture the entire system at any point in time.

Prime Directive

Strive to capture as accurate a representation of the system(s), as free from distortion and bias as possible.

How Can You Trust Your Data if You Can’t Trust Your Tools?

- Compromised kernel == game over?
- Chain of Trust
- Dragging your own toolkit around
- Online vs. Offline

Chain of Trust
(What happens when you run a binary)

- The shell (incl. environment vars)
- The command
- Dynamic libraries
- Device drivers
- Kernel
- Controllers
- Hardware

Portable Toolkit

- Does it help?
- Be ready **beforehand!**
- Know the system
- Software tools
- OS distribution media
- Laptop, media, etc.

Contents of the Toolbag

- Depends on size of media
- Minimum -
  - statically linked data collection tools; dd, cp, cat, ls
  - ftp or other mechanism to get more tools or stash data
- Perl & the Coroner's Toolkit

Offline vs. Online

- Some things can’t be done
- Not working with original data/system
- Less time restrictions
- Errors in replication or interpretation of data
- Often can’t go back, so get all you can beforehand…

How/What to Grab, Theory

- Take the system offline
- Keep track of everything you type or do
- Consider space restrictions
- Grab first, analyze later
- Note hardware, software, system configuration
- Automation is necessary (time & consistency)
- Follow order of volatility
- Make copies (including tools) safeguard them

Before starting…

- **`script(1)`** & notebook
- **`dd(1)`** is your friend
- Setup and/or get tools
- Prepare storage location
- Sequential at host level, parallel at network

Netcat

- Written by der *hobbit*
- Easy transfer of data between two systems
- Typical usage in data stuffing:

```
[receive] nc -p 6666 -l > file
[send]cat data|nc -w 3 to 6666
```

- Network is slow compared to disk

Encrypted Netcat

```
[receive]  nc -p 6666 -l | \
      des -d -k key > file

[send]des -k key < data | \
      nc -w 3 to 6666
```

Memory

- Be cautious of memory mapped devices or holes in memory

```
# dd < /dev/kmem  > output
# dd < /dev/mem   > output2
# dd < /dev/rswap > output3
```

Power Management - The Ultimate State Freeze?

- Saves most states to disk
- Very popular, esp with laptops
- Extremely OS dependent
- Kernel & device driver support required
- Requires duplicate of hardware to reuse
- Highly promising

Capturing Network Information

- All local network states, such as -
  - netstat
  - route
  - arp
  - kernel info
  - logfiles

Remote Network Information

- Router flow logs
- Portmasters, dialup equipment, etc.
- Sniffer/tcpdump/etc
- Server information (DNS, NFS, NIS, mail, syslog, WWW, news, etc.)
- Any host's data that might be of interest - all the information gathered for this host

Processes

- What is running, capture state & binary
  - **`ps(1)`**
  - /proc
  - pcat
  - lsof

Disk Stuff

- NFS/Net stuff handled at server
- **`dd(1)`** all filesystems (if possible)
- **`stat(2v)&`** MD5 all files
- **`strings(1)`** on directories
- capture logfiles, sys configs, important files
- Kernel, dumps, corefiles (self-induced?)

Hardware, Additional Software, etc…

- **`uname(1)`**
- **`eeprom(8s)`**
- **`showrev -p`**/**`devinfo -vp`**/etc. (Solaris 2, 1, etc.)
- **`pkginfo(1)/rpm(8), etc.`**
- patches, kernel configuration, etc.

Auditing

- Host & network based audit (COPS/Tiger, SATAN/ISS, etc.), from both on system & externally
- Port scan
- Audit last, after capture all other info

Backups

- Don’t forget to recover & copy
- Can be crucial to investigation
- Costly and slow to examine

Grave Robber

- Automated way of collecting forensic info
- Gathers, in order -
  - Memory
  - Unallocated filesystem
  - netstat, route, arp, etc.
  - ps/lsof, capture all process data
  - stat & MD5 on all files, strings on directories
  - Config, log, interesting files (cron, at, etc.)