# Reconstruction of User Activity

# Goals

- Want to know **interesting** activity
- Reconstruct what was typed
- Determine what happened
- Understand/determine damage done
- Have access to all files used

# No Method is an Island

- Start with a time frame
- Must combine tactics to get an answer - **Correlation** is the key!
- Never will have everything, but could get enough…

# Tools & Methods

- Network sniffing
- Shell history
- Process accounting
- Log files
- MACtimes

# Network Sniffing & Spying (1/2)

- Cliff Stoll had the right idea!
- Close to perfect for **initial** attacks
- Hard to detect
- Can capture nearly all **network** traffic
- Simply logging connections is very useful
- Useless vs. dialups, other entry points
- High-speed/Active networks are tough

# Network Sniffing & Spying (2/2)

- Often useless by themselves - IDS is dead
- Useful for damage control, useless for data recovery
- Best as standalone monitoring system
- Requires lots of storage for complete traffic
- Must protect the system(s) doing the sniffing/storing data
- Encrypted or hidden connections a problem

# Shell History

- Don’t overlook!
- Some shells generate upon logout
- Command line, exactly as typed
- Fooled/bypassed by sub-shell or environ var
- Easily modified
- Commands inside scripts are not recorded
- Examine shell process memory

# Process Accounting

- Very complete
- Hard to read w/o automation
- Sorted by end of execution, will miss commands still running
- Easy to turn off or blow away, fairly simple to change

# Log files

- Too much or too little…
- Network logs
- TCP wrappers
- Daemon, program, kernel logs/accounting
- C2+ accounting

# By Itself, Nothing….

```
Jul 6 16:04 fish su: 'su root'
succeeded for zen on /dev/ttyp2
```

# But when…

```
% last
zen ttyp0 bar    Tue Jul 6 17:22–19:24 (02:01)
zen ftp   foo    Tue Jul 6 15:22–15:24 (00:01)
zen ttyp0 ultra  Tue Jul 6 10:13–11:07 (00:53)
reboot    ~      Tue Jul 6 20:10
```

# Intruder Modus Operandi

- Reconnaissance
- Strike
- Do the deed, hide tracks
- Get the hell out of Dodge

# MAC times

- atime     last access time
- mtime     last modify time
- ctime     last status change time

- Volatile
- If present & unaltered, **invaluable**

# Demo 1

- Show what intruder sees

http://www.fish.com/~zen/book/hacked/mini-talk/handout-1.html

- Show what mactimes tell

http://www.fish.com/~zen/book/hacked/mini-talk/handout-1b.html

# MAC times, redux

- Determine boot time activity
- Improve firewall/critical system security
- Debug system problems

# The Coroner’s Toolkit

- MAC times
- last
- lastcomm
- various logfiles