Murder on the Internet Express

Dan Farmer & Wietse Venema

Aug 6th, 1999

Emphasis [note to self, not slide]

- Gathering host based information
- Analysis of the same

Morning

- Setting the stage - dan
- First steps & kernel intro - Wietse
- Ceci N'est Pas une Pipe - dan
- Time travel & correlation - Wietse
- Reconstruction of actions - dan

Afternoon

- Processes - Wietse
- Networks - dan
- Filesystems, unrm, etc. - Wietse
- Lazarus - dan
- Best practices, conclusion - dan

The Coroner's Toolkit

- Set of software tools
- Unix
- Perl & C
- Gathering & reconstructing data
- Analysis

http://www.fish.com/security/forensics.html

Forensic Computing

Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system.

What We Won't Cover

- Trapping, tricking, pursuing
- Identifying perpetrators
- Dealing with law enforcement, courts, telcos, etc.
- Important but non-technical stuff

Ted Bundy

"What's one less person on the face of the earth, anyway?

The **BIG** Issues

- Systems are HUGE & complex, change rapidly
- Things can hide anywhere
- Very little technical knowledge anywhere
- No software available
- Knowledge & experience are important
- Gathering data easy, analysis harder (but mostly vastly time-consuming)
- Storage

Requirements for Digital Detectives

- Technical Awareness
- Knowing the tech implications of your actions
- Understand how data can be modified
- Clever, open-minded, & devious
- Highly ethical
- Continuing education, knowledge of history
- **Always** use highly redundant data sources when drawing conclusions

When Faced with a "Situation"…

- Secure and isolate
- Record the scene
- Conduct a systematic search for evidence
- Collect and package evidence
- Maintain chain of custody

Lemmas

- Speed is of the essence - but don’t overdo it
- **Anything** you do to a system disturbs it
- You can never trust the system
- Your policies must always be considered
- Resign yourself to failures
- Prepare to be Surprised

Searching for Evidence

- Preserving state
- We can never know the past
- Even the present is tricky
- Always collect data in accordance to the order of volatility

Order of Volatility

- Registers, peripheral memory, caches, etc.
- Memory (kernel, physical)
- Network state
- Running processes
- Disk
- Floppies, backup media, etc.
- CD-ROMs, printouts, etc.

Big Problems

- Lack of clairvoyance
- Don't know what happened
- Don't know who/what you're up against
- Don't know what to trust
- Harder problems require more preparation
- Heisenberg's legacy

If You don't Know the System…

- Know thy limitations
- Damaging evidence is easy to do
- If automation exists, data collection is *possible*
- Even simple analysis is dangerous
- Ask for help!

Battle Plan

- Think. Typing fast is not going to help.
- Security policy?
- Set goals
- Contact anyone?
- Assume the worst
- Log actions
- Work as little as possible with original data

Action	**Expertise**	**Time**
Go back to Work	None	1+ hours
Minimal Work	Install Sys Software	1/2-1 day
Minimum Recomm’d	Jr. System Admin	1-2 days
Serious Effort	System Admin	2+ days - weeks
Fanaticism	Exp Sys Admin	weeks-months+

Reconstruction of the Fables

- Most data has time-based component
- Some times are more fuzzy than others
- Construct a timeline
- Examine a window in time
- Attempt to determine what happened

Who to Contact?

- Security within your organization
- Management
- CERT?
- FBI, Police, etc.?

We Also Won't Cover…

- More than one investigator/incident/…
  - Lightning can strike twice
  - Multiple events at once can get confusing
  - Same incident, multiple parties
  - Separate incident, multiple parties
  - Tying events to the right datastream?
  - Multiple investigators, tying evidence together
- IDS, orange book, Microsoft

IDS & Orange Book

- A disturbing lack of faith…
- IDS - a four letter word
- Seldom used in the real world
- Currently no help in analysis

Microsoft++

- You’re on your own…
- 40 million and rising
- Rapidly changing
- Windowing system
- Plug and play
- Scarce technical data, the great unknown
- Lack of security & auditing features