

I Know That You Know That I Know That You Read My E- mail: The Forensics / Anti- Forensics Paradox

Weasel
nomad mobile research centre



Introduction

Outline

- **Forensics Overview**
 - Concepts, Pros and Cons
 - Tools
 - Case Studies
- **Anti-Forensics Overview**
 - Concepts, Pros and Cons
 - Tools
- **Conclusion**
- **Q & A**
- **Links**

Introduction

- **What This Presentation is About**
 - Overview and discussion of Forensics/Anti-Forensics concepts, tools, and case studies.
- **What This Presentation isn't About**
 - In-depth overview of the forensics process from a LE angle.
- **Participate**
 - Ask questions
 - Comment
 - Share Experiences (time permitting)
 - Keep to current topic



Forensics

Forensics Overview

- Definition:
 - CISSP:
 - The Collection of information from and about computer systems that is admissible in a court of law.
 - Mine:
 - Gathering evidence to determine what the fuck happened; whether for just information or to nail the asshat who compromised you.

Forensics Concepts

- Classic Forensics Functions
 - Evidence Gathering
 - Life Cycle of Evidence
 - Chain of Custody
 - Primarily a Consultant Role
- Professional Witness

Forensics Concepts (cont.)

- Professional Witnesses
 - Often brought in at beginning of investigation
 - Interprets the evidence for prosecution or defense for presentation to jury
 - Often is not an expert on case subject but is usually a “jack of all security related trades”
 - Common misconception of professional witnesses: unbiased.

Forensics Concepts (cont.)

- Example Uses of Forensics
 - Post-compromise investigation of events for:
 - Submission to Law Enforcement
 - Determine Damage and Return to State
 - Identifying attacker/misuser
 - Submission to Law Enforcement
 - Civil Action / HR
 - General Assbeating
 - Identifying damage
 - Informational
 - Revenge

Forensics Concepts (cont.)

- Forensics Targets
 - Logs: Local, Target, In-between
 - wtmp, /var/log/*, eventlogs, etc.
 - Access Logs
 - ISP, target network, etc.
 - Tools
 - Sometimes the presence of tools is incriminating
 - Memory
 - Physical, Virtual, Swap
 - Communication
 - E-mail, IRC, etc.
 - Arcs to non-computer data
 - Phone logs, Credit Card Activity, Receipts, Surveillance (etc.)

Forensics Concepts (cont.)

- Types of Forensics Data
 - Past
 - Logs
 - Present
 - Sniffer Traces
 - System Monitoring
 - IDS/IPS (near-present)
 - Vulnerability Scan deltas
 - Future
 - Honeypots
 - Proper Logging

Forensics Pros & Cons

- Pros
 - Finding and prosecuting criminals
 - Provides a set of standards for investigation
 - Jobs
 - Less victims on the dark
- Cons
 - Finding and prosecuting “criminals”
 - Assumption of Guilt
 - LE dabbling in areas of minimal impact

Forensics Tools

- Data Gathering
 - grave-robber (TCT/TSK)
- Log View
 - vi, event viewer, spreadsheets, most proprietary FEs, regedit
- Timestamp Extraction
 - mac-times, mac-robber
- Data Recover
 - unrm (TCT/TSK), File Rescue, Drive Rescue, Foremost, gpart, mdump, memfetch
- Hex Editor
- Disk Analyzer
 - Hex analysis, bmap
- Hasher
 - Md5, md5deep

Forensics Tools (cont.)

- Backup Utils
- Backup Hardware
- Network Analysis
 - Sniffers, tcpflow, Driftnet, netstat
- Application Analysis
 - Foundstone Forensics Utilities (Pasco, Galleta, Rifiuti)
- Rootkit Detection
 - chkrootkit, Rootkit Hunter
- Email Viewer
 - Mail Viewer, mboxgrep, uudecode
- Hash Libraries
 - Known Good, FUCK, Solaris Fingerprint Database
- Brute Force Tools
 - Jack the ripper, L0pht Crack, elcomsoft*

Forensics Tools

- Forensics Toolkits
 - The Coroner's Toolkit
 - grave-robber
 - mac-times
 - unrm and Lazarus
 - The Sleuth Kit (TCT++)
 - More platforms supported
 - Autopsy
 - Roll Your Own
 - Sourceforge
 - Freshmeat.net

Forensics Case Study 1

- Accused of Child Pornography Trading via IRC F-Server (DCC)
- Profile
 - Experienced/Power User
 - Admitted to owning legal pornography
 - Admitted to hanging in IRC
 - Claims he was “hacked”
- Described seeing a matrix-like screen once while in IRC
- Verdict: Guilty

Forensics Case Study 2

- Employee accused by wife (soon-to-be ex-wife) of pornography “use” at work
- Profile
 - 30+ year employee
 - Loved and respected by all co-workers (even investigating officer)
 - Little-league Coach
- 3-day thorough investigation
 - No evidence in proxy logs
 - No immediate evidence on system
 - Upon file recover, found .gifs (buttons) of child pornography, no other evidence on system or external media
- FBI notified for possible child pornography use/traffic
 - Warrant to home revealed broken/shattered CD-ROMs
 - Suspect intercepted upon arrival to work by FBI and confessed to child pornography.
- Result: Lost job; pension and benefits contested; federal prosecution pending.



Anti-Forensics

Anti-Forensics Overview

- Definition:
 - Phrack (59-6):
 - the removal, or hiding, of evidence in an attempt to mitigate the effectiveness of a forensics investigation.
 - Mine:
 - Preventing the discovery/recovery of evidential data.

Anti-Forensics Concepts

- Types of Anti-Forensics
 - Data Hiding
 - Header Stuffing, hidden files, permission changes
 - Data Destruction
 - Secure Deletion (do not assume permanent)
 - Data Encryption
- All Should Provide Protection for at least as long as the data is a threat (i.e. remain unrecoverable statute of limitations)

Anti-Forensics Concepts (cont.)

- Example Uses of Anti-Forensics
 - Post-compromise covering of Tracks:
 - Preventing LE or Employer from determining your “activities”
 - Protection from Oppression
 - Civil Rights Activists
 - Employer “Crackdown”
 - Whistle blowing
 - The Anti-pr0n Wife
 - Protection of Data From Misuse
 - Personal Data Protection (i.e. HR Data)

Anti-Forensics Pros & Cons

- Pros
 - Protection from prosecution by reducing substantial evidence
 - Privacy
 - Makes investigators earn their paycheck
 - Protection from non-LE oppressive entities
- Cons
 - Lost data
 - Lost alibi
 - Possession of tools “looks” guilty

Anti-Forensics Tools

- Secure Deletion
 - srm, dban, Necrofile, Evidence Eliminator, Tracks Eraser Pro
- Log File Modification
 - vi, notepad, wted, ClearLogs
- Data Hiding
 - Runefs (runewr, runerd), Outguess
- Encryption
 - Pgp, Steganos Security Suite
- Identity Spoofing/Hiding
 - IP spoofing, MAC spoofing, “borrowed” id/password, proxys, box hopping
- Rootkits
- Physical Destruction
 - Incinerator, degausers, chemicals



Conclusion



Q & A

Links

Dan Farmer and Wietse Venema (The Coroner's Toolkit)

- <http://www.porcupine.org/forensics/>

Fred Cohen

- <http://www.all.net>

Larry Leibrock (UT/eForensics)

- <http://www.eforensics.com>

Foundstone (Win32 Tools)

- <http://www.foundstone.com>

Links (cont.)

Talikser

- <http://www.networkintrusion.co.uk/foranti.htm>

ForInSecT

- <http://www.forinsect.de/forensics/>

L0phtcrack

- <http://www.atstake.com/products/lc>