Computer Forensics
Integrating Technical and Procedural Tasks

Nils Magnus

secunet Security Networks AG
The Trust Company

IT-Incident Management und IT-Forensics
Stuttgart, Germany, 24.-25. November 2003

Motivation

- Morris worm
- KGB hack
- technically easy
- legally complicated

- hands-on:
  - how to be prepared for incidents
  - how to actually do in your own organization
- focus on procedural tasks

- “Trix are for kids, you silly rabbit …”:
  - This is not an exhausive lecture on tools or techniques

Forensics

- derived from medicine and criminology
- collect and correlate evidence
- a lot of names:
  - electronic,
  - computer,
  - digital forensic
- how to deal after an incident?
  - investigate or
  - ignore

Related fields

- Penetration Testing
- Intrustion detection
- Data Recovery
- Reverse Engineering
- Incident Response
- "Legal Aftermath"

- Integration in processes and procedures
- Security Management

Limitations

- Data Recovery needs special tools
  - specializing companies
- Decipher data
  - needs numbercruncher
- Reverse Engineering
  - Needs deep programming skills

- why not hire an expert? ;)

Practical Forensics

- Three things to take into account

- general knowledge
  - about your computers and networks
- special knowledge
  - about speacial tools and methods
- organizational knowledge
  - About how to plan and conduct

General knowledge

- compare with detectives and private investigators

- standard tools
  - looking glass
  - iron powder
  - Worms (the other kind!)
- Methods
  - Sherloc Holmes
  - Hercule Poirot
  - Magnum PI

Operating system

- detect manipulations
  - modification in configuration file
  - modification or installation of software
- integrity checkers
  - md5sum
  - tripwire
- who checks the checkers?

Processes and memory

- running processes: ps
- processes don't need necessarily files in the file system
- serching for open files: lsof
- formerly running processes: dd if=/proc/kcore
- installed modules
- installed kernel

Programming skills

- understand basic methods of permissions
- priviledge escalation
- example: SUID/GUID
- investigate paths of information
- practise this stuff

File system

- Unix is file oriented
  - analyzing content
  - analyzing names
  - analyzing attributes
  - analyzing timestamps (modification, access time)

- what was modified, by whom, when?
- create time lines

- commands: ls, find, lsattr, touch, chmod, chown, ...

Log files

- a lot of log files
  - /var/log/messages
  - /var/log/wtmp
  - Apache log
  - IDS logs or network flows
- easy to tamper
  - relay to loghost
  - print to attached printer
- Correlation
  - look for interaction between Logs
  - look out for preparation before the first attack

Network Access

- network as access point
  - find out the origin (spoofing)
  - find out open connections
  - Find out about the content
- commands: netstat, tcpdump, ethereal, traceroute

- problem: relaying, bot-nets
- no access to all systems worldwide
- CERTs or IRTs, ISPs maintain relationships
- Forum of Incident Response Teams (FIRST)

Special Tools

- there are not many special tools
- tools vs. applications
- little helpers

- apt-cache search forensic
  - tct
  - Sleuthkit
  - Autopsy

The Coroner's Toolkit (TCT)

- Farmer/Venema
- selection of smaller programs in Perl/Shell
  - collects a lot of detail information
  - places everything in small files
  - keeps track of timestamping
  - not much correlation
- tool: grave-robber, builds "body"

Sleuthkit/TASK and autopsy

- extension of the file system component of TCT
- works also on dumps (dd if=/dev/hda5)
- allows browsing in deleted files, meta data
- many file system types supported (Unix and also NTFS)
- access to signature databases
- multiple cases, multiple investigators
- automatic timelines
- web based front end: autopsy

Methods

- Almost useless to deal with Forensics once your under attack
- all steps need to be practised
- all tools should be prepared and collected
- don't play or practise with hot data, always work on copies
- useful: Knoppix boots directly from CDROM/DVD
- convenient: Knoppix-STD has a lot of tools integrated

Tracking

- Find addresses (netstat, traceroute)
- Deal with insufficient or incorrect data
- Find contacts (whois)
- preservere data
- document everything
- contact your legal department
- contact law enforcement
- good luck

Law and Order

- different approaches of techies and lawyers
- no mandatory policies or regulations for forensic evidence of computer crimes exist
- some projects:
  - www.ctose.org
  - RFC 3227
  - state or national law enforcement policies
- identify contacts before incidents occur
- important before court: good documentation and overview

Privacy

- you may discover information from third parties
- during the investigation
- obey to privacy laws
- special rules may apply at companies or universities

Planning

- much more important than most people think
- evidence is easily lost
- be prepared in advance, you don't have the time at the scene
- inform
  - users what to do when they discover breaches
  - team members how to react
- example: “don't reboot, better pull the network plug”
- prepare a policy what to do, whom to contact

- Security Management

Conduct

- use only reliable communication (email may be monitored)
- decide whether to interrupt the attack or to study it online
- make copies early
- store master copies at a safe place
- work only on copies

Wrap up

- Forensics is about collecting and correlating
- Good general technical know how is necessary
- There exists a small number of good tools
- Dealing with law folk can turn out complicated
- Good preparation is crucial

Questions?

Comments.

Discussion!

Referent

Dipl.-Inform. Nils Magnus
Senior-Consultant IT-Security

secunet
Security Networks AG
Osterbekstr. 90b
22083 Hamburg, Germany

Tel.: +49 40 69 65 99 - 13
Fax: +49 40 69 65 99 - 29
E-Mail: magnus@secunet.de
URL: www.secunet.com