Security Incident Investigation

A Seminar Presented to CERIAS at Purdue University

Peter Stephenson, CPE, PCE
Director of Technology
Global Security Practice, Netigy Corp.
peter.stephenson@netigy.com

Agenda

• Background
• Legal
• Criminal profiling
• Investigation
• Forensics
What is Computer-Related Crime?

- Crimes directed against a computer
- Crimes where the computer contains evidence
- Crimes where the computer is used to commit the crime
- Average loss from an incident around $1 million

The Modern Computer Criminal

- Motivated by:
  - financial gain
  - political gain
  - revenge
- Accomplished code writers
- Create their own tool kits
- Will either steal from you or damage you
- 71% chance he/she is insider
Examples

- Credit card theft ring in Lithuania with multiple sites around the world attacks e-tailer
  - Downloads 900 cards per day and offers security assistance to plug holes for a fee
  - Sells and trades cards
- Script kiddie in Netherlands attempts to penetrate fortune 100 company and steal passwords - the victim had no firewall
- Internal employee crashes SCADA system in large metropolitan power company

How Criminals Get Their Info

- Observing equipment and events
- Using public information
- Dumpster diving
- Compromising systems
- Compromising people (social engineering)
Top Ten Vulnerabilities

- Denial of service exploits
- Weak accounts
- Microsoft Internet Information Server
- Open databases
- eBusiness web applications
- Open email
- File Sharing
- RPC
- BIND
- Linux buffer overflows

There Are Only 4 Kinds of Attacks

- Denial of service
- Social engineering
- Technical
- Sniffing
Techniques

• Masquerading as legitimate users
• Social engineering
• Any method of harvesting passwords
• System masquerades

Cleaning Up After an Attack

• Delete tools and work files
• Modify Unix logs
  – Syslog
  – messages files (especially the mail log)
  – su log
  – lastlog (including wtmp and utmp)
  – daemon logs
  – transfer logs
• Modify NT logs
Treat every incident as if it will end up in a criminal prosecution.

Standards for Investigations

• Criminal
  – establish case beyond a reasonable doubt
  – rules of evidence apply - proceedings formal
  – jury is finder of fact

• Civil
  – establish case on preponderance of evidence
  – rules of evidence apply - proceedings formal
  – judge or jury may be finder of fact

• Administrative
  – establish case on preponderance of evidence
  – proceedings may be informal
  – arbitrator(s), mediator(s), other finders of fact
Electronic Communications
Privacy Act - Your Enabling Law

• Owner may intercept communications between an *intruder and that owner's computer system*

Electronic Communications
Privacy Act - Your Enabling Law

• Owner providing others with the ability to use that computer to communicate with other computer systems may:
  – make routine backups and perform other routine monitoring
  – intercept with prior consent of the user
  – *intercept portions of communications necessary to determine origin and destination*
  – *intercept where necessary to protect owners rights or property*
Privacy Protection Act

- Part of 18 USC
- Jurisdiction
  - Federal
- Elements
  - covers materials intended for publication

Fourth Amendment

- Protection against unreasonable search and seizure
- Generally applies to law enforcement only
- Exception: When acting as an “agent” of law enforcement
Agent of the Government

- The private party performs a search which the government would need a search warrant to conduct;
- The private party performs that search to assist the government, as opposed to furthering its own interests (e.g., protecting its rights or property); and
- The government is aware of that party's conduct and does not object to it.

Rules of Evidence

- Hearsay rule
- Best evidence rule
- Must be probative
- Produced in the normal course of business
- Must be authentic
- Chain of custody
Tainted Fruit

- Evidence that results from improperly collected evidence
  - privacy violations
  - protective order violations
  - violations of law
- Everything in the chain from the improperly collected evidence on is tainted and may not be used at trial

Chain of Custody

- Accounts for access to evidence from collection to presentation in court
- Evidence should be sealed, physically and/or electronically
- Custodian signs, dates and seals – must be able to attest to custody
- Evidence is locked in evidence locker
- Data may be cryptographically signed
Criminal Profiling

• Criminal profiling
  – Using available information about a crime and crime scene to compose a psychological portrait of the unknown perpetrator of the crime

• Classical profiling goals
  – Provide a social and psychological assessment of the offender
  – Create a psychological evaluation of possessions found at the crime scene

Developing a Profile of an Intruder

• Crime scene analysis
  – how was access obtained? What skills were required?
  – how did the intruder behave on the system? Damage? Clean-up? Theft?

• Investigative psychology
  – motivation
  – personality type
Goals of an Investigation

• To ensure that all applicable logs and evidence are preserved
• To understand how the intruder is entering the system
• To obtain the information you need to justify a trap and trace of the phone line the intruder is using or to obtain a subpoena to obtain information from an ISP

Goals of an Investigation

• To discover why the intruder has chosen the computer
• To gather as much evidence of the intrusion as possible
• To obtain information that may narrow your list of suspects
• To document the damage caused by the intruder
• Gather enough information to decide if law enforcement should be involved.
Immediate Objective:  
**PRESERVE THE EVIDENCE !!!**
- Begin a traceback to identify possible log locations
- Contact system administrators on intermediate sites to request log preservation
- Contain damage
- Collect local logs
- Image disks on victim computers

Crime Scene Management
- Clear everyone away from the computer under investigation
- Examine for communications connections (modem and network)
- Examine for other connections and observe the screen display - photograph or sketch the display for future reference
- Unplug communications connections from the computer - turn nothing off at this point
Crime Scene Management

- Disconnect the modem from the telephone - do not use the phone
- Document and label all connections to the computer
- Pull the plug(s)
- Reboot from an external source (bootable floppy or CD-ROM) and make physical images of hard drives
- Shut down and collect any potential evidence - bag and tag individually.

Building an Incident Hypothesis

- Start with witness accounts
- Consider how the intruder could have gained access
  - eliminate the obvious
  - use logs and other physical evidence
    - consider the skill level or inside knowledge required
- Create images of affected computers
Building an Incident Hypothesis

- Develop a profile of the intruder
- Consider the path into the victim computer
- Recreate the incident in the lab if necessary
  - use real images whenever possible
- Consider alternative explanations
  - test alternatives

Back Tracing

- Elements of a back trace
  - end points
  - intermediate systems
  - e-mail and packet headers
  - logs
- Objective: to get to a POP
- The only messages that can’t be back traced are those using a true anonymizer and those where no logs are present
Obtaining Subpoenas

- Notify involved organization that you are going to subpoena and request that they preserve evidence - find out who to deliver the subpoena to
- File John/Jane Doe lawsuit with an emergency order to subpoena appropriate records
- Subpoena the logs you need
  - Get everything you can on the first pass
  - May need depositions

Log Info - Unix

- Times of login and logout - LASTLOG
- Anomalies in the LASTLOG - use a log analysis tool such as CHKLASTLOG
- Source IP address - use SYSLOG or any other logs you have that record IP addresses
- Reboots - CRON LOG
- Other logs may be from TCP wrappers installed on critical services
Log Info - NT

- Times of login and logout - SECURITY EVENT LOG
- Source IP address - SECURITY EVENT LOG (not reliable)
- Other useful information may be in SYSTEM EVENT LOG

Log Info - Web Servers

- Http access logs
- Http referrer logs
- Http error logs
- Make sure logging is configured for source IP address, times and dates
- Make sure logs cover all pages on the site
Using Logs as Evidence

- Must not be modifiable
  - Spool off to protected loghost
  - Optical media
  - Backups
- Must be complete
  - All superuser access
  - Login and logout
  - Attempts to use any controlled services
  - Attempts to access critical resources
  - E-mail details
- Appropriate retention

Analyzing Logs

- If there are no logs
  - May be able to use forensic analysis
  - Check other involved computers
- Multiple log analysis
  - Corroboration
  - Fill in gaps
  - Step by step tracing between attacker, victim and intermediate computers
What Do We Mean by “Forensics”?

- **Forensic Computer Science**
  - Discovery and analysis of ambient data on a computer disk
  - Using some form of science or technology to develop evidence in a legal setting
- **Operational Forensics**
  - Using ambient data, logs and forensic tools to restore a computer system to pre-damage condition
- **Network Forensics**
  - Network backtracing

The Role of Forensic Examination in an Investigation

- Computer forensics deals with the recovery of evidence from “hidden” areas of disks, data and systems
- Three major applications
  - developing leads
  - verifying hypotheses
  - recovering damaged systems
- Computer forensic evidence plays the role of physical evidence in a computer incident
When Forensic Evidence is Useful

• Developing leads
  – is there evidence of the incident connecting the suspect and the victim?
  – has the suspect accessed systems involved in the incident?
  – With whom has the suspect communicated?

• Verifying hypotheses

What to Expect From Forensic Evidence

• “Smoking guns” very rare
• Excellent lead generation
  – requires good “seeds” - starting points
• Corroboration of facts collected in other ways
• May require lots of patience - needle in the haystack
Evidence Collection

• All records of the unauthorized access.
• Make sure that your victim keeps those records in a secure area of a computer, preferably encrypted, or on a secured disk. Also caution the victim not to use e-mail to discuss the intrusion.
• All records of system activity on the day (or within a few hours) of the access.

Evidence Collection

• Backup tapes of the above.
• Make an exact copy of that data in the form in which it existed in the computer (i.e., onto a backup disk or tape - use SafeBack). Make more than one copy if possible.
• Disks, printouts, CDs, etc
Evidence Preservation

- **NEVER** work directly on the computer under test!!!!!
- Preserve the “crime scene” from alteration
- Document everything
  - photos, drawings, notes, etc.
- If you seize the PC, protect it from booting

Evidence Analysis

- Backups
  - Logical
    - files as reported by the FAT or other file system
  - Physical
    - bit stream data transferred from disk sectors directly
- Images
  - physical duplicate of the original disk
Selecting Forensic Tools

• The forensic examiner’s kit
  – Tools and techniques you use to collect the data
  – Tools and techniques you use to analyze the data

• Criteria
  – Must not alter data as a side effect of the collection process
  – Must collect all the data we want and only what we want
  – Must be able to establish that they worked as advertised
  – Must be accepted by the computer forensic community
  – Results they produce must be repeatable

Where Evidence Hides

• Slack space
• Unallocated space
  – true unallocated space
  – deleted file space
• Swap files
• Cache files
Disk Geometry

Track
Sector (Clusters are groups of Sectors)
Cylinder

Slack Space

End of File  Slack Space

Last Cluster in a File
Making & Using Backups

• Only physical backups are useful
  – use Safeback from NTI or enCase from Guidance Software
• The backup itself may be scanned for keywords and URLs
• The backup may be restored to a test disk for analysis of a true physical mirror of the original
  – better access to slack and unallocated space

The Backup Process

• Boot from a floppy
  – DOS operating system
  – copy of Safeback on the disk
  – enCase boot disk with drivers
• Use digital tape, Jaz or similar drive or CD-ROM for the backup medium
  – audit trail on the boot floppy
• Direct copy to another disk
  – set up a second hard disk as slave - original as master
  – boot from floppy with Safeback or enCase on it
Developing Leads - Tools

- URLs and e-mail addresses
  - IPFilter (NTI)
  - enCase Grep feature
- Text strings
  - Text Search (NTI)
  - enCase search
  - searches files, slack and unallocated space
  - know what you’re looking for first

Evidence Collection Step by Step

- Shut down computer - reboot with floppy - SafeBack or enCase bit stream or image
- Run FileList or use enCase
- Secure the computer - copy the backup
- Cryptographically sign evidence with CRCMD5 or use enCase
- Encrypt evidence & put into chain of custody
Extracting Evidence

- Run IPFilter against bitstream or enCase
grep against evidence file
  - E-mail and URL addresses & image file names
- Run Text Search with keyword list against
  physical disk on mirror
  - boot from DOS floppy
  - for NT use NTFS/DOS on DOS bootable floppy
- Boot from and analyze the image

Preserving Evidence

- Evidence must be able to be shown to be pristine
  - data - encrypt and sign with cryptographic signature
  - physical - bag, seal and tag
- Never perform forensics on evidence
  - always use images
- Never operate a computer containing possible evidence
Computer-Related Crime
Investigation = Job Security