

Case Study: Using Security Audits as an adjunct to Computer Forensics

HTCIA International 2004



Case Study: Using Security Audits as an adjunct to Computer Forensics

- Christopher L. T. Brown, CISSP
- clbrown@TechPathways.com
- Phone: 619-435-0906 x111
- Technology Pathways, Founder and CTO
(www.TechPathways.com)

Outline

- Computer Forensics Overview
- State of Computer Forensics
- Investigative Techniques
- Sample Case I
- Recommended Expanded Investigative Techniques
- Sample Case I with expanded investigative techniques
- Recommended IT Organizational Protective Measures
- Conclusion

Computer Forensics Overview

Computer Forensics (1)

- Computer Forensics = Computer Science in support of the legal process
- So what does this really mean?

Computer Forensics (2)

- Tedious process of sifting through mounds of computer and network data
- Best understood when breaking down into the Four Phases...

Four Phases

- Collection
- Preservation
- Filtering
- Presentation

Collection

- Identify and Obtain the evidence
- Bag and Tag
- Much focus on hard disk imaging
- Can involve any magnetic or optical media and volatile network device data

Preservation

- Closely tied to the collection phase
- Iterative throughout the process
- Preserving and verifying
 - Write-blocking
 - Hashing
 - Checksums

Filtering

- Computers contain tens to hundreds of thousands of files
- The filtering phase is focused on getting to the real evidence by...
 - Keyword searching
 - Hashing
 - File signatures

Presentation

- Here evidence is ...
 - Organized & Indexed
- Reports are written
- Evidence & Reports are often burned to CD or DVD
- Declarations, depositions and testifying in court

State of the Computer Forensics

New Legislation Results in Change

- Corporate liability drives higher possibility of prosecution
- More prosecutions drive higher likelihood of success
- Both help drive corporate policies to support evidence collection and prosecution

Tools & Training Maturing

- Increasing number and quality of IR/Forensics tools
- Increasing availability of training
- All factors raise the bar for everyone
- *What passed in court last year may not this year*

The Disk and Only the Disk

- So much importance is placed on the disk other artifacts of evidentiary value are still often overlooked
 - Firewall logs
 - IDS logs
 - Directory Server logs
 - More...

Investigative Techniques

Current Case Processing (1)

- Focus on the four phases
- Seize the computer and anything with supporting evidence of interest
- Bag and Tag

Current Case Processing (2)

- Back at the lab image the original
- Collect any hardware specific data (BIOS, etc.)
- Begin processing from the image disk

Focus on Evidence from:

- Recoverable deleted files
- Disk slack space and unallocated space
- Internet history
- Email databases
- General user documents
- System configuration information (Windows Registry)
- Log files
- The last modified, accessed or created (MAC) times of files

Final Phase

- Stage and index evidence
- Write the report
- Burn the CD/DVD
- Wrap up in a nice neat package

Predictable Results

- These techniques were highly simplified
- But, provide a good overview
- with predictable results

Sample Case 1

Case Background (1)

- Much like many intellectual property theft cases
- X-Employee is suspected of “dumping” the entire customer database prior to quitting
- X-Employee is found to be working of primary competitor the following week

Case Background (2)

- Company desires a court order prohibiting the use of any data taken to strengthen signed employment agreement
- Company desires forensics analysis to support the above request

Working the Case (1)

- Casework reveals:
 - The report was run on xxx date and time
 - The former employee userid was the only one logged on to the computer on the days in question
 - The userid spent 5 hours on a day months before leaving searching for USB key drives, then bought one on line

Working the Case (2)

- USB Keydrive drivers were downloaded
- Userid spent a lot of time searching for secure delete software
- Userid spent a lot of time searching for file splitting software

Working the Case (3)

- File splitting software was downloaded
- File deletion software was downloaded
- Very few recoverable files existed

Working the Case (4)

- Large amounts of data was found in unallocated space showing split versions of the reports in question
- Another case closed... Right?

Recommended Expanded Investigative Techniques

Sound Procedures

- IACIS (International Association of Computer Investigative Specialist)
- HTCIA (High Technology Crime Investigation Association)
- Both provide sound training and guidelines, but often focus on the “disk”

Reasons for Change

- Two primary factors drive the need to do more:
 - Number of networked systems growing
 - Number of compromised systems growing (alarming growth)

Recommendations Easley Fit

- All recommendations are in support of the existing four phases

The Recommendations (1)

1. Prior to bag and tag diagram the network and key security devices.
2. Prior to bag and tag capture volatile data from target system.
3. Extract and analyze any router, intrusion detection system and firewalling rule sets in place along with any log data.

The Recommendations (2)

4. Examine anti-virus procedures in place (host based, server based and update periods).
5. Provide a full network vulnerability assessment with automated tools (optional).
6. Fully scan the evidence image disk for virus, Trojan, remote control and key stroke logging software. Note that anti-virus software will not find many Trojans, remote control and keystroke logging software.

Sample Case 1 with expanded investigative techniques

Cost Justification

- As expected cost can greatly increase using expanded methods
- Case I was actually conducted using the recommended expanded procedures

Let's see why...

Results Expanded Methods (1)

1. Router/firewall configuration & log files were extracted. No IDS system was in place. Router and firewall configurations were highly restrictive allowing only web, mail and ftp traffic both inbound and outbound.
2. Running processes on the target system found in the captured volatile data showed that two remote control Trojans were running.

Results Expanded Methods (2)

3. A virus scan showed that no viruses were present on the suspect system.
4. Trojan scans on the suspect system showed both remote control Trojans and their MAC times.

Results Expanded Methods (3)

5. A full audit of the entire network showed no other network system had been compromised.
6. Analysis of the specific remote control Trojans showed that they would not have been accessible from outside the local area network.

Case Conclusions

- Without the additional information an embarrassing situation could occur
- Simply adding a comprehensive virus/trojan/keylogger scan would have allowed the other items to have been performed

Recommended IT Organizational Protective Measures

Examining the Results

- What did the company learn and what can others learn?
- Defense In-depth (outbound filtering, firewalling, etc.) negated compromise from being effective

Corp. Recommendations (1)

1. Ensure acceptable use guidelines are in place.
2. Ensure authorization and accounting systems are in place to restrict and log user activity.
3. Give intensive thought to file system taxonomy and use file system access control lists.

Corp. Recommendations (2)

4. Ensure network topology includes layered security devices (firewalls, IDS, routers) which log to a centralized logging facility with tight access controls.
5. Control outbound as well as inbound network traffic on a granular (device or user) level.

Corp. Recommendations (3)

6. Implement a comprehensive patch management and anti-virus program which is network and host based.
7. Outfit Information security and incident response teams with proper tools and train the teams in proper tool use to include basic forensics bag & tag procedures.

Conclusion

Net Results

- Despite focus the entire network must be taken into account
- Compromised systems on the rise
- Compromised systems don't need to lead to compromised cases
- Using expanded procedures can save the case

Thank You!

Don't forget the feedback forms