Global Information Assurance Certification Paper

Obtaining And Protecting Electronic Information For Prosecution Purposes
Ken Kohl
August 14, 2001
Information Security KickStart Practical Assignment

Introduction

Experiencing a hacking attack, a Denial of Service (DoS) attack, or some other hacking incident is one of the more frightening things that can happen to an organization. The uncertainty about the depth of the attack and what information was affected, destroyed, or possibly stolen can leave a company unsure of its next step, too possibly out of business. In the case of stolen passwords or credit card information, the ramifications of a security breach can affect millions of people far beyond the company itself. Proper preparation will enable a company to identify and recover from a security breach efficiently while protecting not only themselves, but also their clients and client data.

A critical factor in a company's incident response plan needs to be the decision about responding to the attack by prosecuting the offender.

- Does the company want the publicity that comes along with a lawsuit?
- Is it in the best interest of the company?
- Does the company even have the information in a state that can be used to prosecute the attacker?
- Can the company prove the data has been unaltered?

If the company decides to prosecute the offender they will need evidence to back their claim that the attack happened and that the individual in question was the responsible party. The gathering and protection of electronic information is the key for a company to successfully proceed with a prosecution. This paper discusses some technical and legal aspects of preserving data for prosecution purposes.

There are some State and Federal laws and guidelines related to the legal collection and submission of electronic evidence. This document assumes that a company will define it policies and procedures, incident response plan, and other appropriate security measures, but will look at the high level legal regulations and technical requirements, and outline suggestions about needed activities in the collection and protection of evidence in a security incident. Any decisions and activities regarding collection, protection, and submission of evidence for legal purposes need to be reviewed and approved by appropriate legal counsel prior to implementation.

Definitions

For prosecution purposes, information collected must be relevant evidence to the incident. Rule 401 of the Federal Rules Of Evidence defines relevant evidence as "Having any tendency to make any fact that is of consequence… more or less probable than it would be without the evidence". In other words, evidence that makes a relevant contribution to the case may be submitted. Sources of evidence may consist of any of the following: system, firewall, intrusion detection, and written logs, system files and backup tapes of the event providing they can be validated.

Since so much information is contained on electronic media, and providing the original computers as evidence may not be possible, duplicates of the information may be needed. Rule 1001 of the Federal Rules Of Evidence describes an electronic duplicate as an "electronic re-recording by techniques, which accurately reproduces the original."

Rule 1003 of the Federal Rules Of Evidence defines that a duplicate is "admissible to the same extent as an original unless there is some question raised as to the authenticity of the original."

The concept of Preserving Chain of Custody was described in the article "Collecting Computer-Based Evidence, By Joan E. Feldman and Rodger I. Kohn. A chain of custody "tracks evidence that has been collected from the original source to the final evidence presented in court.

Preparation Prior To Attack

Activities to meet legal requirements for data collection must be met prior to the incident occurring. According to Rule 803(6) of the Federal Rules Of Evidence, report, record, or data compilation, in any form, may be admissible if kept in the course of a regularly conducted business activity.

In addition there are several activities that will add to the ability to meet the legal requirements of electronic forensic evidence.

Systems

Collecting and protecting electronic information does not start during or after an attack has occurred, but must start prior to the event. The best sources of available data of a security incident are system and network logs. To meet this need, logging will need to be activated and collected on all network elements and servers, including router logs, network intrusion detection logs, host intrusion and system logs, system backups, etc. and be monitored as part of normal daily routines. This will require investments in hardware to store and manage this information.

Policies & Processes

A company must have in place comprehensive, documented, consistent, and enforceable policies, procedures, and practices. These standards must be reviewed by the legal department to ensure completeness and compliance with applicable State and Federal laws.
Policies and procedures needed by a company include but are not limited to:

- A policy regarding activities to investigate an incident and prosecute the offender. If the decision has been made not to prosecute, many of the activities in this paper are not necessary. However you may still want to investigate each incident to determine the extent of any damage, what happened, and how protect yourself from future occurrences.
- A comprehensive security policy outlining the companies' security posture.
- Documented incident response plan and procedure which include identifying:
  - A list of information and media to collect and protect (system OS, file information, log data, backups, ISP logs, etc.).
  - A documented incident response team with responsibilities, authorities, and activities.
- Policies and procedures outlining the daily monitoring of system components.

- Evaluate your ISP and other applicable vendors to ensure they have policies and processes in place to properly monitor for intrusions, protect data, and respond to an incident, as necessary. In some cases the ISP information will be able to provide additional documentation for your legal case.

These action plans, policies, and procedures must be cohesive with operations, and enforcement. When researching this paper, I contacted the local police department near where I work, and interviewed the individual in charge of the computer forensics area. He provided some interesting information regarding gathering and presentation of electronic evidence in court. He has seen issues that have arisen because a company's policies and procedures were not cohesive or were contradictory in ways that introduced uncertainty into the quality and completeness of the evidence.

- Which policy or process was used and why?
- How can you be sure you followed the right process in this particular circumstance?
- Justify your decision.

In his experience, this particular issue caused some cases to be dismissed. Consistency and completeness of policies and a company's preparedness to execute on these policies were key to successful prosecution.

Training

In addition to having the information available, education and training are also key components of preparedness. A security education program is needed which includes training for members of the incidence response team on technical tools and record keeping techniques (this will greatly assist in preparation for a security incident). Executing occasional simulations of security attacks and the resulting recovery responses and activities will allow the incident response team to evaluate the incident response plan and will allow all participating individuals to become familiarized with their responsibilities and duties. During an incident is not the time to discover the incident response plan is not complete or that people are unfamiliar with their responsibilities.

Communication

Communications processes need to be established to notify management of an incident and to keep them updated on any progress being made. Procedures and agreements need to be established with your local ISP for their assistance and cooperation in the event of a breach oh security. Their assistance, especially with the retention of logging information, will contribute to your ability to prosecute those attacking your system. And a final, major communication component will be to notify the applicable law enforcement agencies to seek assistance in tracking and trapping any offenders.

Resources

Establishment of a Security Response Team and an Incident Manager is necessary. The Incident Manager will be responsible for overall incident response, and individual incident team members. One additional item that may need to be considered is to have a security professional on retainer. This individual would have experience with incident response activities and would be a resource to provide assistance and direction during and intrusion, investigation, and information gathering activities.

Attack and Recovery

When it has been determined that a security incident is in progress, Follow the site security policy and the incident response plan that has been created. The Incident Manger will be responsible for assembling the team and verifying the incident. It is important that all activities during the incident investigation be recorded fully and completely.

Additionally, Rule 901(a) of the Federal Rules of Evidence states that submission of evidence must be authenticated or identified and that the evidence is what it is claimed to be. Documenting the activities identified in The SANS Computer Security Incident Handling: Step-by-Step guide can meet many of the technical and legal requirements needed. Create documentation for evidence that answers the following items:

- Who executed what activities? (A list of activities each individual on the incident response team is executing in order along with time, location, and results information)
- When were the activities performed and in what order were they executed?
- Where were the activities performed (local or remote)?
- Where was the information stored?
- How were the activities executed?
- Why were specific activities done?
- What policies and procedures were followed?
- What systems and network components are being investigated along with their configurations, operating systems, and applications?

As you document the information and complete any applicable activities, always keep in mind that any notes taken will probably become part of the presented evidence. Utilizing an audio recording device may be valuable in augmenting the documentation efforts.

The Incident Response Team will generally execute the following activities during their investigation. Several of the activities will include technical aspects that could impact information content and integrity, and affect its use for legal purposes.

1) Understand the extent of the incident
   - What systems appear to be compromised? Which ones are not? Understanding and documenting these findings not only provides a picture of what has happened to the systems and network components, but also contributes to the completeness of the investigation, and can support the legality of the collected information. Incomplete information can lead to other information being suspect. The technical tools utilized in determining the type and extent of the incident are also included here.
2) Protect sensitive data
   - In the case of an intrusion, sensitive data can include system and data files as well as the system logs and system configuration files. Modification or deletion of files can compromise or erase evidence. Protection may be accomplished by write protecting the disk or storage media, or removing the system containing the sensitive data from the network completely. Removing the unit from the network may also end further intrusion activity if this was the box compromised. The individual unit logs and the logging server

(if used) with its data needs protection as they contain the history of events. Having more complete and unaltered evidence will enhance your case in court.

3) Communicate the intrusion and including the progress of investigation and resolution to all necessary parties.
   - During the initial investigation of an incident, it is important that your IPS be notified. They can collect and protect the applicable log information if you intend to utilize it for prosecution purposes.
   - The applicable law enforcement agency needs to be contacted in order to set up the proper tracing and trapping efforts. Notifying them after the fact may invalidate any activities you have taken to investigate the incident. Law enforcement involvement is needed for prosecution.
   - Management needs to be informed of the incident so legal counsel can be engaged if needed.
4) Protect the systems and networks and their ability to continue operations
   - Keeping a system on the network may be counter-productive when protecting information. Data protection and integrity should be the main concern. The incident response plan should take into account the impact certain systems will have on the overall business if their functionality is lost. Contact your ISP for assistance in protecting your site from attacks and document this communication. Protect other internal systems from further intrusion.
5) Contain the intrusion
   - Remove the offending unit(s) from the network to prevent an attack against other network components. Insure that this action is documented and that the removal will not alter any information contained on the unit. Document the impact the removal of the unit has on your network.
6) Eliminate the means of intruder access
   - Defining the way the intruder is accessing the network is important because it will provide information on what additional protection your network needs and will possibly provide additional information to track the attacker (dial-in logs, router logs, ISP logs).
7) Collect and protect the information about the intrusion
   - Rebooting the unit can change a unit's configuration (understand this and protect this kind of information)
   - Never trust on operating system that may have been compromised. Utilize a forensic (clean) boot disk to access a system that has been compromised.
   - Activities as described in the article "Collecting Computer Based Evidence" by Joan E. Feldman and Roger I. Kohn come into play. The article outlines activities for collecting and preserving computer-based evidence. They included two steps:
     1) Identifying and collecting all available data including computers and computer disks, backup tapes, diskettes, other backup media, and paper copies if applicable.
     2) Preserving the chain of custody of the information obtained. Components of a chain of custody include:
        A) Ensuring that no information has been changed or added to (see Note B below about Ghost).
           - Write protect the media if possible to prevent changes. On hard disks this may necessitate the use of a software utility, or on floppies or tapes this could be as simple as engaging the write protect tab.

- Virus check the media, but do not clean it because doing so will alter information on it. Document the results of the virus check.
- Provide a method to determine that the data has not been altered. Proof of the integrity of electronic evidence is critical. Normally, hashing the data to insure data integrity will accomplish this. If the data is altered the hashing will not match. A product called Secure Hash Signature Generator S/W for Windows from ICS could be used for this purpose. MD5 hashing the information contained on the disk can also be done.

B) When copies are made, ensure that they are complete copies of the original information.
- An image copy is what is needed. The local law enforcement person indicated that they use Ghost from Symantec for Windows based units as it creates an image copy. For Unix they use the dd command as it can provide a reasonable bit-by-bit (image) copy of all disk information
- It is highly recommended that the team use new, unused media to make copies. New media is clean and there will be no possibility of left over information affecting the copy.
- Never work with original evidence. Make 2 copies of computer information.
  1) The master, sealed and placed in secure storage, and,
  2) The other used for the forensic activities.

C) Insure that a reliable copy process is used. A reliable copy has 3 characteristics:
- It meets industry standards for quality & reliability, the applicable copy capability is documented, and it is used in an appropriate manner. In the article titled "Ten Top Things To Do When Collecting Electronic Evidence" by Joan E. Feldman & Roger I. Kohn a good benchmark about whether software is good for copy purposes is whether law enforcement agencies use it. As previously stated dd for Unix, or Ghost from Symantec for Windows is used by the local law enforcement agency. One note, when Ghost makes an image it writes some information into the image disk. Additions like this can cause evidence to be suspect unless it is identified and explained in court. See Symantec knowledge base article titled "How to determine whether Ghost wrote to a disk or partition." DIVA and Encase are other more robust capabilities that can be used to create the required copies.
- Independent verification of the copies is needed. The copy application capabilities will need to support this.
- Copies must be tamper proof (usually by creating a hash of the data to insure that any modifications after the information has been collected can be identified). See Note A above.

D) Secured all original media after being obtained and limit access through the use of:
- Locked vaults with few individuals having the keys or combination
- Establishing security procedures limiting physical access (physical access controls)
- Log and record methods of data creation, storage, and transport.

8) Recover systems

- After all data has been backed up and protected, activities to restore a system to an operational state can be initiated:
  - Install a clean copy of the operating system and applications.
  - Harden and install security patches and upgrades to bring the box up to the latest security levels and apply corrective measures for the issues that allowed the incident to initially occur (if possible).
  - Check the backup tapes to ensure they have not been compromised then restore your data and monitor the system closely.

9) Return system(s) to normal operation
   - Put the system(s) back online and monitor them to ensure proper operation. Additional effort for the short term should be placed on monitoring them for any follow-up attacks or security issues. Additional information may be obtained if attacks continue.
10) Continue to support the legal investigation if follow-on activities are required. This may involve the gathering of additional information or documentation of activities. Any activities, which may lead to the capture of additional information, will need to follow the same rules for collection and protection as before. Due diligence is needed.

After The Attack

Follow up activities after an attack has occurred will not protect data for legal purposes for that attack. Evaluating attack information and the activities of the incident response team will allow a company to:

- Better understand the attack and how it happened.
- Define what technical actions are needed to increase protection of the company and information for the future,
- Identify holes in data collection process,
- Identify issues with the monitoring processes and capabilities,
- Identify issues with the data collection and documentation issues.
- Identify holes in the policies and procedures.

A complete postmortem will increase a company's ability to protect future data, and allow them to more fully comply with the legal aspects of data collection and protection for prosecution purposes.

Summary

The hacking of computer systems and data can be a frustrating and financially damaging event. Protect yourself. However if a hacking event does occur, there can be actions taken to determine the sources of the attack, and to prosecution the individual. The necessary evidence must be gathered and protected in ways that allow it to be useful in a court of law. These efforts must be accomplished as part of the overall security preparation and implementation within a company. Make the effort. Every hacker prosecuted will reduce the number of hackers who can attack again.

References and Additional Information

1) The SANS Computer Security Incident Handling: Step-by-Step guide

2) Cert Coordination Center – Steps for Recovering From a Unix or NT System Compromise http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

3) "How the FBI investigates computer crimes" http://www.cert.org/tech_tips/FBI_investigates_crime.html

4) "DIVA^{tm} COMPUTER EVIDENCE - Digital Image Verification and Authentication", DIBS® Computer Forensics, Inc., http://www.computer-forensics.com/articles/diva.html

5) "The History of Image Copying Technology", DIBS® Computer Forensics, Inc., http://www.computer-forensics.com/history/welcome.html

6) Title 18A-Appendix, Federal Rules of Evidence, http://www.law.cornell.edu/rules/fre/overview.html

7) Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Computer Crime Policy and Programs, http://www.usdoj.gov/criminal/cybercrime/ccpolicy.html

8) "Collecting Computer-Based Evidence", New York Law Journal, January 26, 1998, BY JOAN E. FELDMAN AND RODGER I. KOHN, http://www6.law.com/ny/tech/012698t6.html

9) Symantec Knowledge Base article titled, "How to determine whether Ghost wrote to a disk or partition", http://service1.symantec.com/SUPPORT/ghost.nsf/034d12503a06d36c8525692d0046dbfa/60de0c600c46d34f882566bf005b9bac?OpenDocument

10) Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation 71 (2001), http://www.cybercrime.gov/searchmanual.pdf.

11) Information Security Magazine article, "Supporting Cyber Sleuths" by Todd G. Shipley, July 2001, http://www.infosecuritymag.com/articles/july01/features_cybercrime.shtml

12) "Computer Records and the Federal Rules of Evidence" by Orin S. Kerr, (March 2001) http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm

13) "Tracking a Computer Hacker" by Daniel A. Morris, http://www.usdoj.gov/criminal/cybercrime/usamay2001_2.htm

14) Center for Computer Forensics, "What is electronic evidence?", http://www.computer-forensics.net/faq.htm

15) Computer Crime and Intellectual Property Section (CCIPS), "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", January 2001, http://www.cybercrime.gov/searchmanual.htm

16) "Secure Hash Signature Generator S/W", http://www.ics-iq.com/show_item_222.cfm

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS