Nailing the Intruder

Author: Vinay Narayan Disley

Introduction

Computer technology has made fraud/internet crime a growth industry beginning in the 1990s. Incidents of fraud through the use of computers are increasing. In many organizations, anyone with rudimentary knowledge of a company's computer system is capable of illicitly accessing sensitive information--or worse. Estimates indicate that in this year fraud will cost U.S. businesses over half a trillion dollars, with much of that being the result of computer crime.

Computer fraud does not only affect a company's bottom line but many company executives and outside directors are learning the hard way that they may be held liable for the lack of internal programs to prevent or minimize the impact of computer fraud.

Law enforcement and the courts are grappling with new and difficult problems presented by the success of the Internet. Slowly, they are gaining experience dealing with the problems of detecting, investigating, and prosecuting Internet crime.

This paper is an attempt to link the various aspects of evidence relating to computer crime, the sources of such evidence and some tips on how to identify systems compromised and cull out evidence from the same.

Problem of anonymity

One of the unique features of computers is the fact that they provide the user with a degree of anonymity -- or, more accurately, pseudonymity -- which is unparalleled in the non-electronic environment. The network surfer can truly be any person he or she wishes to be, either by masquerading as another user, or by defining oneself as one sees fit.

This anonymity has significant criminal law consequences. Not only does it make the task of detecting computer crimes and the offenders more difficult, it complicates the various proof issues presented at a computer crime trial. [1]

Needless to say that the intruder cannot be nailed unless there is adequate evidence available to point out that a fraud/unauthorized activity has been perpetrated.

[1] http://www.cla.org/RuhBook/chp11.htm, Mark D. Rasch, The Internet and Business:

Computer evidence

Fortunately, relatively unsophisticated individuals commit most computer fraud. Evidence of the fraud is difficult to hide, especially where a specialist in computer forensics is involved in the search. These specialists are trained to identify and preserve electronic data that can later serve as evidence in court. The telltale evidence of fraud is commonly left behind on hard drives, systems logs etc.[2]

The search for such evidence and techniques to gather, analyze and interpret the results is a very complex and time bound exercise.

On the contrary, quick forensics are needed by both the police and the victim. The police need to find when and where the attack came from. The source and nature of the attack may be discernible from post-mortems on the attacked systems.

The evidence gathered at these first steps is often much too vague to prove a defendant's guilt, but it can give probable cause for further investigation. Rarely does an attacker explicitly give away his name and address.

Nearly all of the evidence are machine-readable. As any computer user will tell you, this makes it subject to easy, undetectable editing. The courts have to deal with this alarming and obvious possibility.

Legal requirements vary greatly between jurisdictions. The laws of one country may not have yet contemplated hacking activity that is quite illegal in another. With over 150 countries registered on the Internet; many are new to the game. Their own laws (much less treaties) don't explicitly cover hacking activity.[2]

Even in countries with more experience with hacking cases, the laws and case law are still emerging. But there are some rules that seem to be working.

The key resources where evidence can be found are:

- Information from service providers (ISP's)
- Information from system logs
- Data in various forms on the compromised systems and related equipment

[2] Internet Forensics and Cyber Crime in Court, Bill Cheswick

Information from service providers (ISP's)

Any attack or intrusion initiated over the net necessarily has to pass through some ISP and thus leaves a trail. Extensive logs with regard to user activity are maintained by ISP's indicating the access points, the IP addresses, the start and end time etc. This information is invaluable to law enforcement.

Nowadays chances are very good that you can, given an IP address, time, and search warrant, find the owner of the offending systems. When combined with a wiretap/raid this usually results in evidence. Some network providers have started logging such things as DNS server usage, if a certain machine "walks" through a DNS domain (tries all the common names/etc.) and then a few minutes later an attack is launched there is a strong correlation between these activities usually. Most ISP's can also make router data available which gives law enforcement a chance to track you down, if they are sufficiently determined.[2]

Law enforcement has to request for the data quickly, because ISPs generally keep their logs for only a few days. However lately given the downward cost of storage media, the duration for which logs are maintained are normally between a week to ten days.

Information from system logs

Logs kept in the ordinary course of business are also admissible as evidences. Log keeping is an important part of dealing with the Internet as they help identify usage patterns, administrative and configuration errors, misuse, and attacks. Mailers keep logs to help identify sources of Spam mail. Firewalls log rejected packets. Authentication server's record account usage, and DHCP server's record caller ID information, accounts, and IP addresses assigned. ISP records of this sort are particularly important in tracing attacks back to their source.

One can examine log files for connections from unusual locations or other unusual activity. For example, look at your 'last' log, process accounting, all logs created by syslog, and other security logs. If your firewall or router writes logs to a different location than the compromised system, remember to check these logs also. Note that this is not foolproof unless you log to append-only media; many intruders edit log files in an attempt to hide their activity.

The requirement of logging and retaining the logs has been a source of tension for companies, particularly those who do not wish to become involved in the legal process. If logs are discarded routinely, without backup, there is less

[2] Internet Forensics and Cyber Crime in Court, Bill Cheswick

information to obtain through the discovery process and as such no strong evidence against the intruder can be obtained.

The main problem however with information from systems logs is that the log files are first traces that an experienced intruder would remove from the compromised systems. It is therefore very important to ensure that the logs files are first secured. There are various mechanisms available to secure the log files, but the most effective mechanism would be having a centralized logging system.

Data in various forms on the compromised systems and related equipment

Examination of the file systems/hard disk etc may well give experienced investigators some hint about the attacker. The personality of the attack: the programs used, file names and passwords chosen, and similar idiosyncrasies, can match the modus operandi of other attacks.

In order to search for such evidence, it is required to put oneself in the shoes of the intruder and think alike to ascertain the nature of threat, the methods available to exploit, the probable motives and the anatomy of the attack. A series of articles titled "Know Your Enemy" the outcome of 'Honeynet Project' though aimed at explaining how to secure one's resources is a good reference for one to understand as to how an intruder will attack and how to capture the required evidence.

The Know Your Enemy series is dedicated to teaching the tools, tactics, and motives of the blackhat community. Know Your Enemy: II focuses on how you can detect these threats, identify what tools they are using and what vulnerabilities they are looking for. Know Your Enemy: III focuses on what happens once they gain root. Specifically, how they cover their tracks and what they do next. Know Your Enemy: Forensics covers how you can analyze such an attack. Know Your Enemy: Motives, uncovers the motives and psychology of some members of the black-hat community by capturing their communications amongst each other. Finally, Know Your Enemy: Worms at War covers how automated worms attack vulnerable Window systems.

Some tips on identifying compromised systems(Unix) and gathering evidence[3]

- Look for setuid and setgid files (especially setuid root files) everywhere on your system. Intruders often leave setuid copies of /bin/sh or /bin/time around to allow them root access at a later time. The UNIX find(1) program can be used to hunt for setuid and/or setgid files. For example, you can use the following commands to find setuid root files and setgid kmem files on the entire file system:

  ```
  find / -user root -perm -4000 -print
  find / -group kmem -perm -2000 -print
  ```

  Note that the above examples search the entire directory tree, including NFS/AFS mounted file systems. Some find(1) commands support an "-xdev" option to avoid searching those hierarchies. For example:

  ```
  find / -user root -perm -4000 -print -xdev
  ```

- Another way to search for setuid files is to use the ncheck(8) command on each disk partition. For example, use the following command to search for setuid files and special devices on the disk partition /dev/rsd0g:

  ```
  ncheck -s /dev/rsd0g
  ```

- Check your system binaries to make sure that they haven't been altered. We've seen intruders change programs on UNIX systems such as login, su, telnet, netstat, ifconfig, ls, find, du, df, libc, sync, any binaries referenced in /etc/inetd.conf, and other critical network and system programs and shared object libraries. Compare the versions on your systems with known good copies, such as those from your initial installation media. Be careful of trusting backups; your backups could also contain Trojan horses.

  Trojan horse programs may produce the same standard checksum and timestamp as the legitimate version. Because of this, the standard UNIX sum(1) command and the timestamps associated with the programs are not sufficient to determine whether the programs have been replaced. The use of cmp(1), MD5, Tripwire, and other cryptographic checksum tools is sufficient to detect these Trojan horse programs, provided the checksum tools themselves are kept secure and are not available for modification by the intruder. Additionally, you may want to consider using a tool (PGP, for example) to "sign" the output generated by MD5 or Tripwire, for future reference.

- Check your systems for unauthorized use of a network monitoring program,

[3] http://www.cert.org/tech_tips/intruder_detection_checklist.html#A7, Cert.org,

commonly called a sniffer or packet sniffer. Intruders may use a sniffer to capture user account and password information. For related information, see CERT advisory CA-94:01 available in http://www.cert.org/advisories/CA-94.01.ongoing.network.monitoring.attacks.html

- Examine all the files that are run by 'cron' and 'at.' We've seen intruders leave back doors in files run from 'cron' or submitted to 'at.' These techniques can let an intruder back on the system (even after you believe you had addressed the original compromise). Also, verify that all files/programs referenced (directly or indirectly) by the 'cron' and 'at' jobs, and the job files themselves, are not world-writable.

- Check for unauthorized services. Inspect /etc/inetd.conf for unauthorized additions or changes. In particular, search for entries that execute a shell program (for example, /bin/sh or /bin/csh) and check all programs that are specified in /etc/inetd.conf to verify that they are correct and haven't been replaced by Trojan horse programs.

- Also check for legitimate services that you have commented out in your /etc/inetd.conf. Intruders may turn on a service that you previously thought you had turned off, or replace the inetd program with a Trojan horse program.

- Examine the /etc/passwd file on the system and check for modifications to that file. In particular, look for the unauthorized creation of new accounts, accounts with no passwords, or UID changes (especially UID 0) to existing accounts.

- Check your system and network configuration files for unauthorized entries. In particular, look for '+' (plus sign) entries and inappropriate non-local host names in /etc/hosts.equiv, /etc/hosts.lpd, and in all .rhosts files (especially root, uucp, ftp, and other system accounts) on the system. These files should not be world-writable. Furthermore, confirm that these files existed prior to any intrusion and were not created by the intruder. Look everywhere on the system for unusual or hidden files (files that start with a period and are normally not shown by 'ls'), as these can be used to hide tools and information (password cracking programs, password files from other systems, etc.). A common technique on UNIX systems is to put a hidden directory in a user's account with an unusual name, something like '...' or '.. ' (dot dot space) or '..^G' (dot dot control-G). Again, the find(1) program can be used to look for hidden files, for example:

```
find / -name ".. " -print -xdev
find / -name ".*" -print -xdev | cat -v
```

Also, files with names such as '.xx' and '.mail' have been used (that is, files that might appear to be normal). Examine all machines on the local network when searching for signs of intrusion. Most of the time, if one host has been compromised, others on the network have been, too. This is especially true for networks where NIS is running or where hosts trust each other through the use of .rhosts files and/or /etc/hosts.equiv files. Also, check hosts for which your users share .rhosts access.

Some future requirements and problems[2]

Law enforcement is going to want more help from ISPs, regardless of their location. They will want real time access to packet streams and authentication sessions to tap specific sessions, giving stronger links between a user and his activities. Some ISPs already assist in these matters when they can, but it is a difficult job. The Internet's growth leaves hardware running at full speed, with no spare facilities for this activity. For a busy router, hardware assist will be necessary. This will only be provided by the router manufacturers, and only in response to ISP or legal demands. Since this would increase the costs of the router, it may take legal requirements similar to the CALEA [CITE] requirements for the telephone system.

Such efforts will probably not work in the long run. Ubiquitous encryption is coming, and will frustrate many of these efforts. When they are not used for game graphics and voice recognition, fast CPUs have plenty of power to apply strong state-of-the-art encryption to network traffic streams. There is little hope that even a governmental entity will have the resources to penetrate these sessions directly.

Even weakened or broken cryptography presents a large economic obstacle to real-time wiretaps. 40-bit encryption is considered weak, but it is not easily amenable to real-time cracking. And our best (i.e., most expensive) hardware is required to extract even plain-text packets from modern packet streams.

Can a defendant be forced to reveal passwords and unlock cryptographic keys? In the U.S. there are fifth amendment issues to this problem. The pass-phrase to a PGP key file can unlock encrypted files, revealing stolen information or pornography. This is a hard step for law enforcement, who have on occasion have asked for assistance from the governmental cryptography community.

What happens when an ISP is under investigation? It becomes much more

[2] [2] Internet Forensics and Cyber Crime in Court, Bill Cheswick

difficult to investigate them. Often, specific circuit numbers have to be obtained from a telephone company to determine connectivity. Can you trust the logs of a compromised ISP?

Given an IP address, can we tell where the computer is? There are network servers that attempt to provide this information from the WHOIS database, inverse DNS lookups, and information. This is an important and unsettled question, because it relates to the jurisdictions involved in an attack.

Systems can be made strongly resistant to hacking attacks. A careful system designer can avoid sniffed passwords and defaced web pages. But I see no general solution to denial-of-service attacks. Any service available to the public can be abused by the public, and these attacks are going to grow in frequency and severity. Smurf attacks [CITE] and the more sophisticated distributed trinoo [CITE] technologies can be launched with little chance of catching the instigators.

Conclusion

Computer technology has made fraud a growth industry of the 1990s and into the next century. We have seen in the above pragraphs that it takes more than computer know-how to effectively search for, preserve, and present evidence of computer fraud. There is a need to develop skills in Internet Forensics with computer expertise which can help determine how the fraud was committed, assess the damages, and provide the expert testimony needed--as well as assist in devising ways to prevent similar fraudulent activity in the future.

Adding to the technical challenges, there is also a lot of cross-functional education needs to be addressed for the management, regulatory and legal fraternity to address the growing requirements of Internet forensics. The science of Internet forensics is a growing requirement and would require be researching and practicing to reach a stage of maturity.

Given the above, one can conclude that it's a really difficult task to identify the systems that are compromised, traceback the attack mechanism and collate evidence that is acceptable in court of law, ie assuming that adequate legal mechanism is in place. One needs to answer all these before even contemplating as to **"can one nail the intruder?"**

References:

1. http://project.honeynet.org, Honeynet Project Series, 23 May 2000, (20th July 2001)
2. Know Your Enemy: II, Honeynet Project Series, (20th July 2001)
3. Know Your Enemy: III; Honeynet Project Series, (20th July 2001)
4. Know Your Enemy: Forensics; Honeynet Project Series, (20th July 2001)
5. Know Your Enemy: Motives; Honeynet Project Series,(20th July 2001)
6. Know Your Enemy: Worms at War; Honeynet Project Series, (20th July 2001)
7. http://www.cert.org/tech_tips/intruder_detection_checklist.html#A7, Cert.org, (20th July 2001)
8. http://www.cla.org/RuhBook/chp11.htm, Mark D. Rasch, The Internet and Business: A Laywer's Guide to the Emerging Legal Issues, published by the Computer Law Association, (21st July 2001)
9. Internet Forensics and Cyber Crime in Court, Article by Bill Cheswick, Bell Laboratories, (21st July 2001)
10. What lawyers and managers should know about computer forensics, Veritect, www.veritect.com, (21st July 2001)