Standard Operating Procedure -- Pueblo High-Tech Crimes Unit
Investigative Protocol -- Hacking and Intrusions
1 Apr 2000

Investigating Cyber Crime/Hacking and Intrusions

Cmdr. Dave Pettinari
Pueblo County Sheriff's Office
Pueblo High-Tech Crimes Unit
davepet@cops.org

Framework for Conducting an Investigation of a Computer Security Incident

What is the threat? How proficient does the "hacker" need to be?

- Computers are easily manipulated and easily "boobytrapped" to intentionally destroy data.
- You do not need to be a "computer wizard" to seize a computer to destroy data and wreak havoc. Hacker tools are readily available on the Internet, as well as complete instructions and plans.
- Hackers can usually uncover ways of circumventing firewalls.
- When you have an ongoing intrusion, you don't know initially whether it's just somebody's kid engaged in hacking for the fun or it or a precursor to a much more sophisticated, destructive attack. You have to investigate them all as though they were potentially the most serious case possible, and pray they are not.
- Most intrusions are kids hacking
    - Log files reveal expertise
        - Beginner
        - Intermediate
        - Advanced
- Hacker pyramid
    - On the bottom are the “bottom feeders” – 97%.
        - Anyone can do; like putting together a swing set with instructions
        - When spotted, put these folks in the “watch” file and track them if they try it repeatedly
    - 2-percenters
        - Take Internet exploits that extra step; persistent
    - 1 percenters
        - The folks you won’t see in log files. Never caught.

How can a hacker work his wiles and cover his tracks?

- The hacker may start his hunt with a vulnerability scanner such as SATAN and other commercially available programs. Since SATAN has been widely publicized, "in-the-know" systems administrators have run SATAN against their own systems and fixed vulnerabilities they found. But others have not, and there are other products continually produced that circumvent previously known safeguards.
- The proficient hacker (and, again, he doesn't have to be a computer genius, but merely follow a few simple instructions!) **telnets** from his current hacked account into another of his pirated accounts, then telnets from that location to yet another account that he has hacked, remotely logging on to it in preparation to run port scans looking for targetable systems. This process forces investigating law enforcement to obtain search warrants in a number of different jurisdictions, immensely complicating the investigation.
- Knowing that almost every large corporation has at least one unauthorized modem on its network, the hacker sets up a war-dialer program that will call each of the extensions to the phone system at the company until it pulls up the modem, giving him a login screen to the company's computer system. A war dialer searches ranges of telephone numbers to find those phone numbers specifically connected to a computer.

- Using a "brute force" program, he repeatedly hammers the system, trying to "guess" passwords for "root," a top-level account that has the run of the system and controls the computer. These programs keep working automatically until they exhaust every word in an unabridged dictionary, all names in an encyclopedia, and each entry from a local phone book, for example.
- The hacker "secures his beachhead," using FTP (file transfer protocol) to plant a root kit and sniffer onto his latest victim. He sets the program to capture and record everything typed in at the systems administrator console, as well as any log-on session from any computer on the network.
- The hacker next goes on a hunt for a password file, hoping that some of the passwords he finds will also work on other machines inside the company's network.
- The hacker locates the password file, but discovers only "x" characters where the encrypted passwords should have been. The information the hacker seeks is contained in a shadowed file. Even so, he easily runs the ftp program and tricks it into crashing, causing a "core dump." The legitimate purpose of a core dump is to allow programmers to perform an autopsy on the digital remains in search of clues to a program's failure. But, as the hacker knows, a core dump has other uses, such as placing encrypted passwords in the shadowed file into RAM (Random Access Memory), where he can easily harvest them.
- Using other software, the hacker creates a root shell, from which he can then run other commands and programs.
- The root kit the hacker installed will hide evidence of his activities only from the time when the program was activated, so the hacker must mop up by deleting previous actions of his busy night by deleting entries in the computer system's logs.
- At this point, the hacker "owns" the company.

Three possible courses of action for companies and corporations

- Completey handle the incident internally
- Take civil action
- Report the incident to authorities

Do you want to involve law enforcement?

- Law enforcement can do things you can't
  - Subpoenas to look for things that you can't without allegations of invading privacy
  - Search warrants to seize and impound computers indefinitely
  - Tap phone lines
  - Begin surveillance
  - Use undercover officers and operations to investigate
  - Question employees, detain suspects, examine company records

But…

- Does the local agency have the training, budget or manpower to see the investigation through to the end?
- The company loses control of its investigation; it becomes **law enforcement's** investigation. Law enforcement operates by different rules, and is not bound to protect any company's interest, but works to protect the public's interest. It becomes a state matter, not a private matter, and the criminal justice system kicks in. Law enforcement officers will almost always work hard to do what is in your organization's best interests, as long as it doesn't conflict with their official duties and objectives.
- For the investigator to be effective, he must have your FULL cooperation. Investigators can't create cases out of thin air.
- Be prepared to air "dirty laundry" in public, if it comes to that.

It is ALWAYS A GOOD IDEA to call law enforcement in when your case involves:

- Cyber terrorism
- Corporate espionage
- Financial fraud

Likelihood of success in these investigations is low -- FBI estimates

- Typical computer criminal has a 99% probability of getting away with his or her crime; only 1% of all computer crimes are successfully prosecuted.
  - Fewer than 10% of all computer crimes result in a successful investigation
  - 10% or less of that number are prosecuted
  - Only about 10% of that number are actually punished
    - One reason: Electronic evidence can be created, altered, stored, copied, and moved with unprecedented ease. Many perpetrators are skillful at covering their digital tracks.
    - **You may never catch the culprit because:**
      - The trail was cold -- too much time passed since the incident, and the digital evidence evaporated
      - Logging was incomplete or nonexistent
      - The investigation cost more than the loss, and there was no point in continuing
      - The universe of possible perpetrators was too large
      - The event was inconclusive -- it may or may not have been a security incident
      - You couldn't conclusively point to a suspect
      - You didn't have enough evidence to prove your case beyond a reasonable doubt
      - Political pressure stopped the investigation
      - Cover-up

Laws that apply

Colorado Computer Crimes statute

18-5.5-102 - Computer crime.

(1) Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; using the property or services of another without authorization; or committing theft commits computer crime.

(2) Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network described in section 18-5.5-101 or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) If the loss, damage, or thing of value taken in violation of this section is less than one hundred dollars, computer crime is a class 3 misdemeanor; if one hundred dollars or more but less than five hundred dollars, computer crime is a class 2 misdemeanor; if five hundred dollars or more but less

than fifteen thousand dollars, computer crime is a class 5 felony; if fifteen thousand dollars or more, computer crime is a class 3 felony.

Federal case

There are various federal laws if it is a "federal interest" computer:

- Computers involved in crimes that cross state lines
- Computers materially involved in any crime that is a federal crime (gambling, kidnapping)
- Threats or attacks a federal government computer system (HUD, Air Force)
- Computers involved in banking
- Federal laws that might apply:
  - Fraud and Related Activity in Connection with Computers, 18 U.S.C. Section 1030. The latest amendment is found in the National Infrastructure Protection Act of 1996. Section 1030 is the main anti-intruder law. Includes language such as "intentionally accesses or exceeds authorized access to a computer." Violations are felonies.
  - …"accused knowingly caused the transmission of a program, information, code or command, and by doing so, caused damage to a protected computer." Protected computer could be one used by financial institution or U.S. government, or "any computer used in interstate or foreign commerce or communication." Enacted in response to the Morris Internet worm. This measure also covers possession of unauthorized passwords, computer extortion, etc. See language on Page 49 of Computer Crime Investigator's Handbook for AFOSI on people fired who damaged private systems.
  -

- **If federal, FBI and Secret Service have jurisdiction…but…**

  - **These agencies are understaffed in this area, so they are naturally more concerned with national security threats and federal system computers. They may not have the wherewithal to respond even to a federal interest computer case.**

  - **Does another agency, perhaps a local agency, have a "claim" in the case?**

Managing Intrusions

Four-step process

- Avoidance
- Testing
- Detection
- Investigation

What are the company's information security policies, standards, and practices?
Consider the following:

- Investigating and prosecuting computer-related crime is expensive and time-consuming.
- Need to proceed with great care in case you need to defend yourself against wrongful termination, invasion of privacy, or discrimination.
- If law enforcement is involved, there are rules of evidence, issues of privacy, and burdens of proof that must be born.

Prevention tools

- TCP/IP attack simulator
  - SafeSuite
    - Performs more than 100 different attacks typical of hacker attacks.

Detection

- What capabilities do you have to detect intrusions in real-time? (like military ASIMS systems)
  - A watchdog system that sits in the background and oversees all activities involving the device under surveillance.
  - Best tools allow extensive, robust logging, protected from tampering. They also allow for responses from the system under attack that may be able to gather information about the attacker that can assist you during the investigation.
    - Intruder Alert
      - Everywhere an intruder goes, he or she leaves tracks.
    - RealSecure
  - Automated Security Incident Measurement (ASIM)
    - AFCERT system (Air Force Computer Emergency Response Team), Kelly AFB, Texas
    - ASIM systems are placed where base networks connect through gateways to external networks
    - Sniffer that monitors computer communications traffic passing through the gateway
    - Programmed to detect changing hacker threats
  - AFCERT sends info from this system to AFOSI DETs and they review for suspicious activity that may cause them to initiate an intrusion investigation
  - Reports to DET include date, POC, description of incident, recommended actions to improve security, warning level
  - Many of the commercially available intrusion and abuse detection tools are excellent, but they can be expensive. However, you can download a very good basic tool, called TripWire, free from the Internet.

Investigation – Intrusion management defaults to investigation when all other measures failed to prevent an attack. But investigations may be futile unless luck and circumstances are with you.

- **Investigative process**
  - Legal coordination
  - Checking records, such as system documentation and logs, as well as information about suspects
  - Interviewing informants
    - Does the suspect frequent hacker newsgroups such as Cypherpunks, Bugtraq, Best-of-Security?
  - Conducting system surveillance
  - Preparing a search warrant
  - Searching the suspect's premises
  - Seizing evidence

- **If we had to be reactive…**
  - Eliminate the obvious – not every computer failure from now on will be your suspect taking action. Computers fail for a variety of reasons.
  - Hypothesize the attack
    - Map all possible vectors, access routes into the victim computer
    - Analyze access controls
      - Many computer systems contain many security features that people simply don't realize are there. In most cases, all systems administrators have to do is turn them

on. For example, account lockout features are critical for good security. Are they turned on?
    - Analyze logs
        - One great advantage are systems that run what is called a mirror log. Each time your audit program creates a log entry, an identical entry is created in a separate computer. When attackers attempt to erase their tracks, they will delete the entries in the primary log, but the mirrored log remains unchanged. You will be able to see virtually every step they took.
    - Evaluate known exploits in this system
- Reconstruct the crime
- Perform a traceback to the suspected computer
- Analyze the source, target, and intermediate computers
- Collect evidence, including, possibly, the computers themselves
- Follow up on findings and prepare evidence

Log Files

The "smoking gun" in intrusion investigations. Nearly all that come to AFOSI are ASIM logs. But also firewall log files, router log files. By default, many systems log files are not turned on. Some sys admins think they slow a system down; may be true. NT installations often don't have the log files turned on. UNIX and Linux have an out-of-the-box logging capability.

ASIM logs are socket or packet layering logs. Decode every single byte that goes through the network looking for strings that are threatening. Generates a log file, or an alert (real-time or logging alert). Transcript logs – everything that went on in that system. Connection logs show you the connections that took place, and the strings that hit and alerted ASIMS. Depending on the warning level, 1-10, it will actually record what happened.

Initiating transcript log shows where the bad guy came from and the commands he typed. Compare to destination transcript log to see commands as well as the output. Commands will not match exactly because packets are dropped as recording the information, an echo on the system (echoes extra characters back to the terminal).

Full transcript logs give you the commands in context of everything else going on in the system.

You have to ask AFCERT for the transcript logs to go along with the initiating and destination logs they provide.

To get a sniffer on a suspect, 52 request, like a wiretap, to put Sniffy, their sniffer, to check for only those suspect IP addresses in the investigation.

- **Information to gather**:
    - How would the intruder enter the system?
        - What type of security do you have on direct-connect maintenance modems on critical host computers? (For PCs and NT computers, there is a wealth of remote access programs, such as PCAnywhere, LapLink, ReachOut, and CarbonCopy that an intruder can use to "drive" your system.)
        - Do you have weak password accounts that can be easily hacked into with a password cracker?
        - Do you have back doors in your UNIX or NT operating system?
            - Will let the intruder back into the computer system even if systems administrator changes all the passwords.

        - Often allows the hacker the run of the system without being logged.
    - What would we need to justify trap and trace of the phone line the intruder would use?
        - Once the attacker has dialed in and is online, you don't have any options for tracing that don't involve the phone company, which requires law enforcement, a court order, and trap and trace. Would it be less troublesome, less costly and more effective to strengthen defenses in advance?
    - How would we gather evidence of the intrusion in progress?
        - How would you document damage to your system in order to explain its extent?
    - Would you be able to document effort you spend in investigating this incident and determining the damage?

Analyzing a computer involved in an intrusion

- Boot from a sterile DOS investigative disk
- Take a physical image of the hard drive
- Look at the last date of change on critical files
- Examine configuration and start-up files for things that don't seem right
- Look for hacking tools (password crackers, copies of passwords, etc.)
- Examine the password file for unauthorized accounts
- Search the mirror image of the hard drive for keywords appropriate to the incident. Include hidden areas, slack space, and cache.
- Look for changes to files, critical file deletions, and unknown new files
- Use the NTI tool IPFilter to collect a list of all e-mail addresses, FTP sites and URLs, visited from the computer, and use DM or Excel to calculate the number of times they were visited

Cyber Forensics

- KEY QUESTION: DO YOUR SYSTEMS ADMINISTRATORS HAVE ADEQUATE LOGGING PRACTICES TO CAPTURE ATTACK ATTEMPTS?
    - Log examination is probably the single most productive part of the investigation, ***IF*** logs are kept properly.
        - Search an electronic copy for user IDs (password is invariably nearby)
        - Search for target word or phrase unique to the investigation
    - Times of login and logout -- use LASTLOG
    - Anomalies in the LASTLOG (use CHKLASTLOG)
    - Source IP address -- use SYSLOG or other logs that record IP addresses.
    - Capture attacks with a sniffer (record every transaction involving IP addresses)

Target-Hardening

- Does your company see itself as a possible target for information warriors?
- Does your company have a cyber security section?
- **Protective measures you can take:**
    - Plug into threat-warning networks (e.g., NIPC)
    - Analyze intrusions -- Cybercrime requires study and a great degree of coordination; be willing to share "dirty laundry."
    - Put in place a good security policy that defines what is and is not allowed in terms of network and Internet access.

- Establish several hardened firewalls.
- Train systems admins in security, and how to plug holes and investigate intrusions. To protect an organization completely, sys admins must audit the network on a regular basis.
- Install a good quality intrusion detection system (IDS). The firewalls guard your perimeter, while IDS monitors what is happening on your network, guarding against slip-ups by the firewall, as well as internal mischief. Network administrators should use one product from each of the following categories:
    - **Vulnerability Scanners** -- "Hacker in a box" programs the systems administrator can use to probe his or her network resources proactively.
    - **Host-based IDS** -- Use an agent that scrutinizes logs, critical system files and auditable resources looking for unauthorized changes or suspicious patterns of activity. Whenever anything out of the ordinary is spotted, alerts are "sounded" and traps raised automatically.
    - **Network-based IDS** -- Monitor traffic on the computer in real time, examining packets in detail to spot denial of service attacks or dangerous packet payloads before they reach their destination and do damage. This network-based scanner should be capable of both raising alerts and terminating the offending connection immediately.
- Pull the plug on perpetrators
    - Have them investigated, arrested, prosecuted and convicted -- ruins the "reward system"

Good reading for the corporate security investigator

- "Investigating Computer-Related Crime" by Peter Stephenson
- "Corporate Security," by Ira Winkler

Other Resources

Visit web sites, and perhaps join:

- Computer Security Institute (CSI)
- International Computer Security Association (ICSA)
- National Infrastructure Protection Center (NIPC)
- Newsgroups dedicated to hackers:
    - Cypherpunks
    - Best-of-Security
    - Bugtraq
    - Good hacking resource site: -- http://www.anticode.com/cgi-bin/showdsc.anticode?cat=computer-forensics/windows.html