# UNIX Investigations

Cmdr. Dave Pettinari
Pueblo County Sheriff's Office
davepet@cops.org

**Information provided by Dir. Jim Concialdi in training at Pueblo County Sheriff's Office Pueblo High-Tech Crimes Unit Oct. 20, 1999**

UNIX generally has to do with very large mainframe systems. While we might not see too many of those type investigations, with the increasing use of Linux, which uses very similar commands, we will see computers using this similar operating system.

UNIX commands aren't simple, because you can have several commands for the same thing, and variations that do different things. For example, to list a file, there are several ways to go:

- Ls
- cat
- pg
- more

Sample commands:

ls -- list command, like dir in DOS.
ls -l = long list (lists permissions)

permissions -- rxx/rxx/rxx dave
read/write/execute
user/group/world

Chmod 640 (Number in first place changes world access, second place group access, third place user access). 0 takes away all the permissions. 000 indicates no permissions whatsoever. No one else can see or access this file until permissions are changed.

To take away all permissions:

Chmod 000 edna

Full permissions -- 777,

Cannot change a read-only file if you don't have the permissions. To change permissions, you use numbers from 1 through 7. You can even take away access in an entire directory.

ls -l /* | grep `----------' finds every file in the system where there are no permissions.

mv is the move command to move a file.

last | more or pg -- shows you all the folks who were the last ones on the system, and where they logged in from.

last dave tells you the last time "dave" was on the system.

Find _/_ -name "*Jim*" Find any files where the suspect is listed as the owner.
ls -l * | grep "edna" will find the user's name in the file listing.

Ask the systems administrator to use the "find" command to fine every file on the system tied to the suspect.

Look for information in the suspect user's temp directory.
cd /tmp

After finding these files, make copies of them and load them to a different directory, probably under root, and have the systems admin lock the suspect user out of the system. You might also want to have him copy evidentiary files to a removable media, print them, then make evidentiary files "read only." Be aware that copying files changes their permissions, and changes the access times. So you might first want to print out directory structures, and save files to removable media.

To lock a user out of the system, sys admin changes his password.

passwd dave

file filename -- read the file by printing it to the screen.

ps -fu username -- find any processes the suspect has running now. Kill these processes with the kill command.

See detailed UNIX command sheet.

UNIX is context sensitive, so you never want to use capital letters in a command line.

Definitions:

PID -- process identifier. Every process has one. The first PID to fire off when you log into a UNIX system is sched (scheduler). Sched keeps track of all the processes, in order.

CRON -- tells thing when to fire off (chronological). Literally thousands of files fire off to run the system. It's important for you to ask the system administrator to see if the suspect has any cron files, which could be used to do certain things after he is locked out of the system. Go over to the cron directory and do a listing to see if the suspect has a cron tab file. ls -l shows ownership of the cron files.
/usr/spool/cron/cron tabs

Ask the system administrator to move this file and restart cron.

**Taking down a UNIX system…**

If you come onto a scene and the UNIX computer is up, don't pull the plug, because you might have root access. If you shut it down, you will not have login and password. Besides, UNIX does not like to be reset or have its plug pulled. It needs to be shut down in an orderly fashion.

If you see the root prompt, get a UNIX expert in immediately to reset the root password, prior to shutdown.

$ is the standard UNIX prompt

Standard Operating Procedures -- Pueblo High-Tech Crimes Unit
Investigative and Technical Protocols -- UNIX-based Incidents
20 Oct 1999

# -- superuser, or root

To get into a system, "crash it" -- come in on the single-user mode as root, reset the password, and then go to multiple user mode.

Password access is problematical. Formerly, passwords could be seen in the /etc/passwd file. Now, though, you can no longer see the 15-character passwords, but maybe just a *. With C2 security, a hacker can't get in, because the password files are encrypted, and the computer must check three different places and match them up before accessing.

**To properly shut down a system:**

- Tell everyone to get off the system. (wall "Everyone please log out of the system now." If they don't, "kill" them.
- "shutdown" -- the command to shut the system.

Our system at the sheriff's office is set up so that "root" can only be used at certain terminals. You might have the password, but can't get in except on the terminals set aside for this purpose.

who tells you who is on the system right now.

who -Htcu | more -- more info on people on the system, node, activity (period indicates current activity, such as typing), and PID (process identifier).

who -Htu |sort |more -- alphabetizes by login name.

pwd -- print working directly (like the dir *. Command in DOS)

Tells you who is on the system.

Real-time monitoring - A systems administrator can watch what a user is doing on the system at that very moment.

To verify files weren't changed in copying, use the "diff" command to see if there is any difference, and print out file listing that shows file size has not changed.

Go to the suspect's mail files and read his e-mail

/usr/spool/mail
mailx to read

Check for backups of the main UNIX system. Might contain evidence that was deleted from the main system. Also be aware that a programmed erase routine can also fire off a command to send blank files to the backup machine, obliterating evidence that exists there.

Sample protocol if you are taking down a single user who is suspect:

1. Get the systems administrator to lock out this person's password so user can't get back in. id command to check user's ID.
2. CD to his home directory.
3. ls -l -- Tells you what the suspect has in this directory.
4. Print out files in the suspect directory, and copy to removable media.
5. Copy the entire directory and put it someplace else, probably in the root directory. cp is the copy command. Remember that copying changes permissions.