KILLING THE MONITORING SOFTWARE

Modifying the log files can hide what a hacker has done in the past, but hackers still need to hide their presence while they're logged on to a computer. So, after the log files, the second target that hackers go after are the programs that can help system administrators notice any changes on their computers. In the world of Unix and Linux, the most common commands that hackers try to alter include the following:

- `find`—Looks for groups of files
- `ls`—Lists the contents of the current directory
- `netstat`—Shows the network status, including information about ports
- `ps`—Displays the current processes that are running
- `who`—Displays the names of all the users currently logged on
- `w`—Prints system usage, currently logged-on users, and what each user is doing

Planting Trojaned programs

When they introduce malicious programs onto a computer, hackers simply substitute the computer's current programs or binaries with their own hacked or Trojaned versions. If an unsuspecting system administrator uses these hacked versions, the commands may appear to work normally, but they secretly hide the hacker's activities from view. The longer it takes system administrators to find the hacker, the more time the hacker has to cause damage or to open additional back doors to ensure that he can return at a later time.

Of course, when a hacker replaces the original programs or binaries with his own deceptive versions of those same programs, he risks giving away his presence. This danger occurs because every file contains two unique properties: a creation date and time, and a file size. If a system administrator notices that a program's creation date was yesterday, that's a sure sign that the programs have been altered.

To protect their files from alterations, system administrators use *file integrity programs* that calculate a number, called a checksum, based on the file's size. The moment someone changes a file's size, even by a small amount, the checksum changes.

To avoid being detected by a file integrity checker, a skilled hacker may run the file integrity checker program and recalculate new checksums for all the files, including the modified ones. Now, if a system administrator didn't keep track of the old checksum values, the file integrity checker won't notice any differences.

With a little bit of tweaking, hackers can make their altered versions of certain programs the exact same size as the files they're replacing. This means that if they just change the date and time of this altered file to match that of the real file, any checksum comparisons won't notice the substitution.