C2 Auditing

Many UNIX systems allow the administrator to enable a comprehensive type of auditing, logging, known as a *C2 audit*. This is so named because it is logging of the form specified by the U.S. Department of Defense regulations to meet the certification at the C2 level of trust. Those regulations were specified in a document called the *Trusted Computer System Evaluation Criteria*, often referred to as the "Orange Book" in the "Rainbow Series." The Orange Book is now depreciated in favor of the Common Criteria. Nonetheless, *C2* Auditing is still a commonly used term.

C2 auditing generally means assigning an audit ID to each group of related processes, starting at login. Thereafter, certain forms of system calls performed by every process are logged with the audit ID. These include calls to open and close files, change directory, alter user process parameters, and so on.

Despite the mandate for the general content of such logging, there is no generally accepted standard for the format. Thus, each vendor that provides C2-style logging seems to have a different format, different controls, and different locations for the logs. If you feel the need to set such logging on your machine, we recommend that you read the documentation carefully. Furthermore, we recommend that you be careful about what you log so as not to generate lots of extraneous information and that you log to a disk partition with lots of space.

The last suggestion reflects one of the biggest problems with C2 auditing: it can consume a huge amount of disk space on an active system in a short amount of time. The other main problem with C2 auditing is that it is useless without some interpretation and reduction tools, and these are not generally available from vendors. The DoD regulations require only that the logging be done, not that it be usable. Vendors have generally provided only as much as is required to meet the regulations and no more.