系统调用是用户程序与系统打交道的唯一入口，因此系统调用的安全直接关系到系统的安全。如果一个用户恶意地不断调用fork()将导致系统负载增加，因此我们有必要收集一些有危险的系统调用记录，将有利于系统管理进行事后追踪，从而提高系统的安全性。更详细内容，请点击链接系统调用日志收集程序_x86_64环境3.14版本内核(上)