巧妙收集入侵Windows系统的证据 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/259/2021_2022__E5_B7_A7_E5_A6_99_E6_94_B6_E9_c100_259089.htm 随着网络的不断扩大，网络安全更加会成为人们的一个焦点，同时也成为是否能进一步投入到更深更广领域的一个基石。当然网络的安全也是一个动态的概念，世界上没有绝对安全的网络，只有相对安全的网络。相对安全环境的取得可以通过不断地完善系统程序(及时给系统漏洞打上不同的补丁和给系统升级)、装上防火墙，同时对那些胆敢在网络上破坏秩序做出不义行为的人给予恰如其分的处理。这必然要牵涉到证据的收集，本文正是对这一方面的内容针对Windows系统进行研究。 一、Windows系统特性 Windows操作系统维护三个相互独立的日志文件：系统日志、应用程序日志、安全日志。 1.系统日志 系统日志记录系统进程和设备驱动程序的活动。它审核的系统事件包括启动失败的设备驱动程序、硬件错误、重复的IP地址，以及服务的启动、暂停和停止。系统日志包含由系统组件记录的事情。例如在系统日志中记录启动期间要加载的驱动程序或其他系统组件的故障。由系统组件记录的事件类型是预先确定的。系统日志还包括了系统组件出现的问题，比如启动时某个驱动程序加载失败等。 2.应用程序日志 应用程序日志包括关于用户程序和商业通用应用程序的运行方面的错误活动，它审核的应用程序事件包括所有错误或应用程序需要报告的信息。应用程序日志可以包括性能监视审核的事件以及由应用程序或一般程序记录的事件，比如失败登录的次数、硬盘使用的情况和其它重要的指针.比如数据库

程序用应用程序日志来记录文件错误.比如开发人员决定所要记录的事件。 3.安全日志 安全日志通常是在应急响应调查阶段最有用的日志。调查员必须仔细浏览和过滤这些日志的输出，以识别它们包含的证据。安全日志主要用于管理员记载用户登录上网的情况。在安全日志中可以找到它使用的系统审核和安全处理。它审核的安全事件包括用户特权的变化、文件和目录访问、打印以及系统登录和注销。安全日志可以记录诸如有效的登录尝试等安全事件以及与资源使用有关的事件，例如创建、打开或删除应用文件。管理员可以指定在安全日志中记录的事件。例如如果你启用了登录审核，那么系统登录尝试就记录在安全日志中。 二、寻找“ 显形 ”证据 系统工具提供了对系统进一步的监视，在性能监视器中可以看到其图形化的变化情况。而计数器日志、跟踪日志和警报则提供了对本地或远端系统的监视记录，并可根据预定的设定进行特定的跟踪和报警。还可利用不同的用于配置、管理COM组件及应用的组件服务工具记录或查找相关信息。 1.查看三大日志 在计算机上维护有关应用程序、安全性系统事件的日志，可以使用事件查看器查看并管理事件日志。它用于收集计算机硬件、软件和系统整体方面的错误信息，也用来监视一些安全方面的问题。它可根据应用程序日志、安全日志和系统日志来源将记录分成3类。 事件查看器显示以下几种事件类型：error是指比较严重的问题，通常是出现了数据丢失或功能丢失。例如如果在启动期间服务加载失败，则会记录错误。Warning给出警告则表明情况暂时不严重，但可能会在将来引起错误，比如磁盘空间太少等。Information描述应用程序、驱动程序或服务的成功操作的事件。例如成功

地加载网络驱动程序时会记录一个信息事件。Success audit审核访问尝试成功。例如将用户成功登录到系统上的尝试作为成功审核事件记录下来。Failure audit审核安全尝试失败。例如如果用户试图访问网络驱动器失败，该尝试就会作为失败审核事件记录下来。 注意启动系统时事件日志服务会自动启动，所有用户都可以查看应用程序日志和系统日志，但是只有管理员才能访问安全日志。默认情况下会关闭安全日志，所以管理员要记住设定启用。管理员既可以使用组策略启用安全日志记录，也可以在注册表中设置策略使系统在安全日志装满时停止运行。 基于主机的检测器可以检测到系统类库的改变或敏感位置文件的添加。当结合所有现有的基于网络的证据片断时，就有可能重建特定的网络事件，诸如文件传输、缓冲区溢出攻击，或在网络中使用被盗的用户帐号和密码等。 当调查计算机犯罪时，会发现很多潜在证据的来源，不仅包括基于主机的日志记录，而且还包括网络的日志记录以及其它的传统形式，如指纹、证词和证人。大多数的网络流量在它经过的路径上都留下了监查踪迹。路由器、防火墙、服务器、IDS检测器及其它的网络设备都会保存日志，记录基于网络的突发事件。DHCP服务器会在PC请求IP租用时记录网络访问。现代的防火墙允许管理员在创建监查日志时有很多种粒度。IDS检测器可以根据签名识别或异常的检测过滤器来捕获一个攻击的一部分。基于网络的日志记录以多种形式存储，可能源自不同的操作系统，可能需要特殊的软件才能访问和读取，这些日志在地理上是分散的，而且常常对当前系统时间有严重错误的解释。调查人员的挑战就在于查找所有的日志，并使之关联起来。从不同系统获得地理上分散

的日志、为每个日志维护保管链、重建基于网络的突发事件，这一切都需要消耗大量的时间和密集的资源。