计算机取证工具分析

Analysis of Computer Forensic Tools

殷联甫　（嘉兴学院信息工程学院 314001）

摘要：本文主要对计算机取证过程中使用的常见工具进行详细的分析和说明。这些常用的工具包括 windows 系统中的实时响应工具，开放数据复制工具 ODD、电子证据保护工具 SafeBack 及取证复制工具 EnCase 等等。
关键词：计算机取证　计算机犯罪　计算机安全

1　引言

计算机取证作为计算机安全领域的一个新的热点正引起人们的普遍关注。计算机取证也称数字取证、电子取证，是指对计算机入侵、破坏、欺诈、攻击等犯罪行为，利用计算机软硬件技术，按照符合法律规范的方式进行识别、保存、分析和提交数字证据的过程。取证的目的是为了据此找出入侵者（或入侵的机器），并解释入侵的过程。

计算机取证过程中要用到很多工具，目前可用的取证工具也比较多，根据取证工具的功能，主要可以将取证工具分为三大类：第一类是实时响应工具，第二类是取证复制工具，第三类是取证分析工具。下面准备对每一类取证工具的功能、特点等做详细的分析说明。

2　实时响应工具

在计算机取证过程中，主要从被入侵机器的硬盘上寻找犯罪证据，然而有些重要的犯罪证据往往存在于被入侵机器的寄存器、缓存或内存中，这些证据包括当前登录的用户列表、整个文件系统的时间/日期戳、当前运行着的进程列表、当前打开的套接字列表、在打开的套接字上监听的应用程序等，这些数据往往被称为易失性数据，系统关闭后这些数据便会全部丢失，而且不可能恢复。收集易失性数据是计算机取证中的一个重要步骤，因为易失性数据有时会在计算机取证中起非常重要的作用。

2.1　收集易失性数据步骤

（1）运行可信的命令解释程序；

（2）记录系统时间和日期；

（3）确定哪些人登录到该系统（包括远程用户）；

（4）记录所有文件的创建、修改和访问时间；

（5）确定打开的端口；

（6）列出与打开端口相关的应用程序；

（7）列出所有正在运行的进程；

（8）列出所有当前和最近的连接；

（9）记录系统时间和日期。

2.2　Windows 实时响应工具

计算机取证过程中用于收集易失性数据的工具便是实时响应工具。下面介绍 Windows 系统中一些常用的实时响应工具：

（1）cmd. exe（系统内置）

Windows NT 和 Windows 2000 的命令行工具。

（2）PsLoggedOn（www. foundstone. com）

显示本地连接和远程连接的所有用户。

（3）rasusers（Windows NT 资源工具包（NTRK））

显示对目标网络系统具有远程访问权限的所有用户。

（4）netstat（系统内置）

列出所有监听端口及与这些端口的所有连接。

（5）Fport（www. foundstone. com）

列出 Windows NT/2000 系统中打开 TCP/IP 端口的所有进程。

（6）PsList（www. foundstone. com）

列出在目标系统中正在运行的所有进程。

（7）ListDLLs（www. foundstone. com）

列出所有正在运行的进程及其命令行参数和各自运行所需的动态链接库。

(8) nbtstat(系统内置)

列出最近十分钟内的 NetBIOS 连接。

(9) Arp(系统内置)

显示最后一分钟内本系统中与目标系统进行通信的所有 MAC 地址。

(10) kill(Windows NT 资源工具包(NTRK))

中止正在运行的进程。

(11) Md5sum(www.cygwin.com)

为一个给定的文件创建 md5 散列。

(12) rmtshare(Windows NT 资源工具包(NTRK))

显示远程计算机上可供访问的共享目录。

(13) netcat(www.atstake.com/research/tools/network_utilities)

用于在两个不同的系统之间创建通信信道。

(14) cryptcat(http://sourceforge.net/projects/cryptcat)

用来创建一个加密的通信信道。

(15) PsLogList(www.foundstone.com)

转储事件日志的内容。

(16) ipconfig(系统内置)

显示接口配制信息。

(17) Psinfo(www.foundstone.com)

显示本地网络系统结构等信息。

(18) PsFile(www.foundstone.com)

显示由远程打开的文件。

(19) PsService(www.foundstone.com)

显示当前进程和当前线程的相关信息。

(20) auditpol(Windows NT 资源工具包(NTRK))

显示当前安全审查的参数设置。

(21) doskey(系统内置)

显示打开的 cmd.exe 命令解释程序的命令记录。

3 取证复制工具

在计算机取证过程中,当收集易失性数据的工作结束后,接下来的主要工作是对被入侵机器的硬盘数据进行备份,这个过程就是取证复制过程,也就是制作司法鉴定复件或者制作合格的司法鉴定复件的过程。

所谓司法鉴定复件是指包含每个比特源信息的文件,采用原始的比特流格式。5GB 的硬盘将产生 5GB 的司法鉴定复件,除非读取源数据时发生错误,否则文件内不会有多余数据。目前制作司法鉴定复件的工具主要有 UNIX 系统的 dd 命令和美国国防部计算机司法鉴定实验室版本的 dd(叫 dfcldd)(http://prdownloads.sourceforge.net/biatchux)以及一种新的、开放源代码的 Open Data Duplicator(开放数据复制)工具。

合格的司法鉴定复件是包含每一比特的源信息、但可能采用其他形式保存的文件,其中内含扇区 Hash 值和空扇区压缩就是两种最常见的其他形式。目前制作合格的司法鉴定复件的工具主要有 SafeBack 和 EnCase 两种。多数情况下,在恢复或解释合格的司法鉴定复件文件时,需要使用专用工具。

3.1 UNIX 系统命令 dd(http://www.gnu.org)

dd 工具用于将二进制数据流从一个文件复制到另外一个文件中。以这种方式进行比特复制是所有取证复制工具的基础。dd 是通用的工具,源代码可以公开得到。此外,dd 可以在几乎所有的 UNIX 平台上编译。

3.2 开放数据复制工具(http://sourceforge.net/projects/odessa)

开放数据复制工具(ODD)是一种新的开放源代码工具。这种工具采用客户机/服务器模式,允许调查人员对一个局域网上的多台计算机系统同时进行司法鉴定复制。ODD 的另一特性是能够在处理数据时对数据执行额外功能。ODD 具有计算校验和与 HASH 值、执行字符串搜索和根据文件头提取文件的模块(插件)的功能。

ODD 是开放数字证据搜索和捕获架构(ODESSA,Open Digital Evidence Search and Seizure Architecture,http://odessa.sourceforge.net)框架的数据复制部分。ODESSA 项目的目标是向计算机司法鉴定界提供一套开放的、可扩展的证据处理和数据分析工具套件。

3.3 SafeBack

SafeBack 是颇具历史意义的电子证据保护工具,它是世界上惟一的处理电子证据的工业标准。它的主要用途是保护计算机硬盘驱动器上的电子证据,也可以用来复制计算机硬盘驱动器上的所有存储区域。

SafeBack 对硬盘驱动器的大小和存储能力没有限制。它可以对硬盘驱动器上的分区创建镜像备份,也

可以对整个物理硬盘(可能包含多个分区和/或操作系统)创建镜像备份。SafeBack 创建的备份映像文件可以被写到任何可写的磁存储设备上,包括 SCSI 磁带设备。SafeBack 可以保护已备份或已拷贝的硬盘上的所有数据,包括未激活或"已删除"的数据。

Safeback 可以为所有硬盘驱动器制作司法鉴定的副本,但是这些硬盘驱动器必须能够被系统驱动器控制访问,系统驱动器包括 EIDE、ATA66 和 SCSI。在 Backup 模式下,Safeback 可以创建一个压缩格式的司法鉴定映像文件,这个文件可存储在几乎所有可用的磁性介质上。该文件可以无缝地处理多种可移动设备(例如,大量 zip 盒式磁带)或磁带设备(只要首先解决硬件和驱动程序问题)。

Safeback 是悉尼的 Chuck Guzis 在 1991 年前后编写的,开始时是作为一个证据处理工具来设计的,现在已经成为了一个法律标准。2000 年 3 月,New Technologies Inc. (NTI) 获得了 Safeback 的所有权,该工具可在 NTI 的网站找到:http://www. forensics – intl. com,并可下载试用版本。

3.4 EnCase

Encase 是 Guidance Software 公司的产品(可以从 Guidance Software 公司的 http://www. encase. com 站点上购买,可以下载试用版本),该工具被广泛应用于法律执行部门与商业化组织的取证复制工作。EnCase 是当今最为流行的单机司法鉴定分析软件。该软件的流行主要是由于其易用性。EnCase 提供一个 Windows 界面和一整套复杂的特性,这些特性极大地提高了司法鉴定检查的效率。

4 取证分析工具

取证复制过程结束以后,接下来的主要工作就是取证分析。取证分析工具倾向于同时具有数据收集及分析的功能。目前,常见的取证分析工具主要有 AccessData 公司的 FTK (Fornesic Toolkit)、The Coroner's Toolkit (TCT 工具包)、EnCase (EnCase 同时具有取证复制和取证分析的功能)、ForensiX、New Technologies Inc. (NTI) 等。

4.1 FTK

AccessData 公司(http://www. accessdata. com)的 FTK(Fornesic Toolkit,取证工具包)通过把大量数据集缩小成一个由重要信息组成的子集的方法来帮助分析者进行分析。FTK 是一个商业软件,可以从 AccessData 公司购买,但也可以从 AccessData 公司的网站下载试用版本。

FTK 能够自动提取出 Microsoft Office 文档、电子邮件、Internet 活动等,这些工作是自动完成的,为你节省了大量的时间,使得你能够把精力集中到对一些重要数据的分析上。FTK 的不足是它仅能分析微软 Windows 文件系统,因此,如果你正在调查的系统属于 UNIX 操作系统,就必须使用其他工具包来执行分析工作,比如采用 EnCase 或者 TCT 工具包。

4.2 The Coroner's Toolkit(TCT 工具包)

Dan Farmer 和 Wietse Venema 设计的 The Coroner's Toolkit (TCT) 主要用来调查被"黑"的 Unix 主机,它提供了强大的调查能力,它的特点是可以对运行着的主机的活动进行分析,并捕获目前的状态信息。TCT 的前端工具 grave – robber 可以收集大量的正在运行的进程、网络连接以及硬盘驱动器方面的信息。数据基本上以挥发性顺序收集,收集所有的数据是个很缓慢的过程,要花上几个小时的时间。运行 grave – robber 最合适的方法是只对运行的系统收集可变的数据,然后关闭系统,对驱动器做映像,这时使用 grave – robber 的 – f 选项来对映像数据进行分析。

4.3 ForensiX

ForensiX 是 Fred Cohen (http://www. all. net) 博士编写的,主要运行于 Linux 环境,是一个以收集数据及分析数据为主要目的的工具。它与配套的硬件组成自己的专门工作平台。它利用了 Linux 支持多种文件系统的特点,提供在不同的文件系统里自动装配映像或媒体的能力、能够发现分散空间里的数据、可以分析 Unix 系统是否含有木马程序。其中的 Webtrace 是一套网络搜索工具,可以自动搜索互联网上的域名,为网络取证进行必要的收集工作。

4.4 New Technologies Inc. (NTI)

NTI(http://www. forensics – intl. com)是取证软件最为固定的商家之一。NTI 的取证产品以命令的形式执行软件,所以速度很快,软件包的体积小,适合于在软盘上使用。

(下转第 94 页)

(上接第 90 页)

5 结束语

了解和掌握计算机取证过程各个阶段所使用的常见工具,有助于计算机取证工作的顺利进行,也有助于国内相关部门开发出实用、有效的计算机取证工具。

参考文献

1 殷联甫,计算机取证技术研究,计算机系统应用,2004,7:25~28。

2 丁丽萍、王永吉,论计算机取证工具软件及其检测。
http://www.quzheng.com/modules.php?name=Articles&file=article&sid=5.2004

3 Thomas Rude. DD and Computer Forensics. http://www.crazytrain.com/dd.html.2005.

4 [美]Kevin Mandia,Chris Prosise 著,常晓波译,应急响应:计算机犯罪调查,清华大学出版社,2002。