UNIX 系统取证分析方法①

殷联甫　(嘉兴学院 数学与信息工程学院 浙江 嘉兴 314001)

摘　要：UNIX 作为目前最常用的主流操作系统之一，研究 UNIX 系统的取证分析方法具有非常重要的现实意义。本文首先介绍从 UNIX 系统中获取易失性数据的方法，然后介绍获取被入侵 UNIX 机器上的硬盘数据，建立取证映像（forensic image），然后进行取证分析的具体步骤和方法。

关键词：计算机犯罪；计算机取证；UNIX 取证分析

UNIX Forensic Analysis Method

YIN Lian-Fu

(College of Mathematics & Information Engineering, Jiaxing University, Jiaxing 314001, China)

Abstract: UNIX is one of the most popular operating systems, it has great practical significance to research the methodology of UNIX forensic analysis. This paper firstly introduces the method to capture the volatile data from UNIX systems, then introduces the concrete steps and method of UNIX forensic analysis.

Keywords: computer crime; computer forensics; UNIX forensics analysis

1　引言

UNIX 作为目前最常用的主流操作系统之一，研究 UNIX 系统的取证分析方法具有非常重要的意义。在对 UNIX 系统进行取证分析之前，首先必须获取取证数据。取证数据主要分为两大类，一类是易失性数据，另一类是非易失性数据。

易失性数据是指那些当计算机关机后就会全部消失的数据，这些数据一般都在内存中，主要包括网络连接状态、正在运行的进程状态等信息。所谓初始响应就是指收集受害者机器上的易失性数据，并据此进行取证分析的过程。非易失性数据是指那些当计算机关机后依然存在的数据，这些数据一般都在硬盘上。

本文首先介绍从 UNIX 系统中获取易失性数据的方法，然后介绍获取被入侵 UNIX 机器上的硬盘数据，建立取证映像(forensic image)，然后进行取证分析的具体步骤和方法。

2　UNIX系统初始响应方法[1]

2.1 创建初始相应工具包

为了能对 UNIX 系统做出初始响应，首先应准备好装有以下工具的光盘或软盘(要保证这些工具是绝对干净的)：

ls	dd	des	file	pkginfo
find	icat	lsof	md5sum	netcat
netstat	pcat	perl	ps	strace
strings	truss	df	vi	cat
more	gzip	last	w	rm
script	bash	modinfo	ismod	ifconfig

2.2 保存初始响应信息

初始响应信息可采用以下方式保存：

① 将数据保存在本地硬盘中；

② 将数据保存在软盘、USB 驱动器或磁带驱动器等远程介质中；

③ 手动记录信息；

④ 使用 netcat(或 cryptcat)命令，通过网络将查找到的数据传输到取证分析机。

尽量不要将数据保存在本地硬盘上，如果需要进行数据恢复或取证分析的话，保存在本地硬盘上的数据就会覆盖位于未分配空间中已被删除的数据，而这些数据可能会有调查或者提供证据的价值。建议使用

① 收稿时间:2009-12-14;收到修改稿时间:2010-01-12

netcat 命令，通过网络将这些数据传送到配有 USB 驱动器或其他具有足够空间的存储设备的取证分析机上。

2.3 收集数据

初始响应阶段至少应收集以下数据：

a. 系统日期与时间；

b．当前登录的用户清单；

c．整个文件系统的时间/日期戳；

d．当前正在运行的进程列表；

e．当前打开的套接字列表；

f．在打开的套接字上监听的应用程序；

g．当前或最近连接到系统的系统列表。

(1)执行可信 shell

所有响应的第一步是确定所执行的是可信任的 shell 命令。攻击者可在 UNIX 的 shell 中植入木马程序，记录下所有执行过的命令，或执行一些调查人员难以觉察到的恶意操作。因此，我们必须执行自己的可信 shell。

首先使用下面的命令将可信工具包(假设可信工具包在软盘上)加载到“/mnt/floppy”目录下：

```
# mount /dev/fd0  /mnt/floppy
```

然后进入/mnt/floppy 目录，输入以下命令来执行自己的可信 shell：

```
# ./bash
```

接下来就可以执行下面的可信命令了。

(2)执行 date 命令

执行 date 命令可以记录系统的时间与日期。本地日期与时间的设置对后面的时间/日期戳关联很重要，它们还可以显示出你处于系统中的时间。

(3)执行 ifconfig 命令

执行 ifconfig 命令可以获取每个网卡的信息，包括网络地址和状态等。分析这些数据可以发现入侵者是否修改了 IP 地址或者启动了网络监控程序。命令格式如下：

```
# ifconfig -a
```

(4)执行 ps 命令

执行 ps 命令可以显示每个进程的名称、命令行参数、已运行时间以及调用该进程的用户等信息，从中可以发现恶意进程。命令格式如下：

```
# ps -aux
```

(5)执行 netstat 命令

执行 netstat 命令可以获取打开的网络套接字(sockets)等信息。一般情况下，入侵者经常在被入侵系统中留下后门程序，通过分析打开的网络套接字信息可以发现后门程序。命令格式如下：

```
# netstat -an
```

(6)执行 w 命令

执行 w 命令可以显示当前登录用户的信息。使用 w 命令可显示出登录用户的用户 ID 以及他们是从哪个系统登录的、当前在系统中执行什么操作等，还能显示日期与系统时间。

(7)执行 ls 命令

与 Windows 系统一样，UNIX 系统中每个文件和目录都有三项时间/日期戳可以收集：访问时间(atime)、修改时间(mtime)与 inode 更改时间(ctime)。可以使用带有相应命令行参数的可信 ls 命令来获取文件的这些时间。以下命令行将告诉你如何获得时间/日期戳，并将输出结果保存在可信软盘上：

```
ls    alRu / > /floppy/atime
ls    alRc / > /floppy/ctime
ls    alR  / > /floppy/mtime
```

3 UNIX系统取证分析

3.1 数据获取

当我们获取受害者机器上的硬盘数据时，必须获取硬盘上的所有数据，包括未分配空间中的数据，只有这样我们才能恢复所有被删除的文件。使用 UNIX 系统中的 dd 工具可以完成此项工作。这里我们将硬盘上所有数据的备份称为取证映像。(forensic image)，接下来的取证分析工作也将在取证映像上进行，而不是在原始盘上进行。

一般情况下，我们可以用三种方法来获取硬盘数据：

(1)利用 netcat 工具通过网络获取。也就是通过网络将取证分析机与受害者机器相连，用 netcat 工具传输数据；

(2)将受害者机器的硬盘卸下，将其安装到可信的取证分析机上；

(3)用可信的操作系统直接启动受害者机器，将硬盘数据拷贝到外接硬盘。

3.1.1 设备识别

获取硬盘数据的第一步是识别硬盘的设备名。在 UNIX 系统中，所有 ATA/IDE 硬盘的设备名为/dev/hd?，而所有 SCSI 硬盘的设备名为/dev/sd?，其中”?”可由英文字母来代替，表示硬盘的编号，如/dev/hda、/dev/hdd 等。可用以下命令来识别系统中的硬盘：

```
# dmesg | grep  e [hs]d
```

3.1.2 数据获取

如果你已经将受害者机器的硬盘卸下，并将其安装到可信的取证分析机上，或者你已经用可信的操作系统重新启动受害者机器，那么你可以根据以下步骤来获取数据：

(1)确定源盘和存放源盘映像的目标盘。此处源盘用 SRC 表示，目标盘用 DST 表示。

(2)安装目标盘：

mount /dev/DST /mnt

(3)计算源盘数据的 hash 值：

dd if=/dev/SRC bs=2048 | md5sum

将计算结果记下来留待后用。

(4)将源盘中的全部内容拷贝到目标盘，保存在一个文件中：

dd if=/dev/SRC bs=2048 of=/mnt/disk1.dd

(5)计算目标盘上结果文件的 hash 值：

md5sum /mnt/disk1.dd

将该值与第(3)步取得的 hash 值进行比较，若两者一致表示拷贝成功，否则表示拷贝失败，转到第(4)步重新拷贝。

3.1.3 映像文件分解

由于目前大多数取证工具的分析对象是硬盘中的分区而不是整个硬盘，因此当我们成功获取取证映像以后，必须将一个个的分区分离出来。在进行分离之前，我们必须首先了解各个分区的位置和长度，可以使用两种方法：

(1)使用 UNIX 中的 fdisk 工具

```
# fdisk -lu disk1.dd

Disk disk1.dd: 0 heads, 0 sectors, 0 cylinders
Units = sectors of 1 * 512 bytes

Device    Boot    Start       End    Blocks   Id  System
disk1.dd1   *        63    208844    104391   83  Linux
disk1.dd2         208845   2249099   1020127+  83  Linux
disk1.dd3        2249100   4289354   1020127+  83  Linux
disk1.dd4        4289355  39873329  17791987+   5  Extended
disk1.dd5        4289418   4819499    265041   82  Linux swap
disk1.dd6        4819563  39873329  17526883+  83  Linux
```

在上面的命令中，参数“-l”表示列出各个分区的位置和长度，参数“-u”表示位置和长度的单位是扇区。

(2)使用 The Sleuth Kit 中的 mmls 工具

在上面的命令中，参数“-t dos”指定分区的类型。mmls 工具的优点在于它不仅能列出各个分区的位置和长度，还能列出未分配空间的位置和长度。各个分区的位置和长度的单位也是扇区。

```
# mmls -t dos disk1.dd
DOS Partition Table
Units are in 512-byte sectors

     Slot  Start      End        Length     Description
00:  -----  0000000000 0000000000 0000000001 Primary Table
01:  -----  0000000001 0000000062 0000000062 Unallocated
02:  00:00  0000000063 0000208844 0000208782 Linux (0x83)
03:  00:01  0000208845 0002249099 0002040255 Linux (0x83)
04:  00:02  0002249100 0004289354 0002040255 Linux (0x83)
05:  00:03  0004289355 0039873329 0035583975 Extended (0x05)
06:  -----  0004289355 0004289355 0000000001 Extended Table
07:  -----  0004289356 0004289417 0000000062 Unallocated
08:  01:00  0004289418 0004819499 0000530082 Linux Swap (0x82)
09:  01:01  0004819500 0039873329 0035053830 Extended (0x05)
10:  -----  0004819500 0004819500 0000000001 Extended Table
11:  -----  0004819501 0004819562 0000000062 Unallocated
12:  02:00  0004819563 0039873329 0035053767 Linux (0x83)
```

当我们了解各个分区的位置和长度以后，我们可以使用 dd 工具从映像文件中提取出各个分区的内容：

```
# dd if=disk1.dd skip=63 count=208782 of=hda1.dd
# dd if=disk1.dd skip=208845 count=2040255 of=hda2.dd
```

上面的命令从映像文件 disk1.dd 中提取出最前面的两个分区的内容，分别存入文件 hda1.dd 和 hda2.dd 中。

3.2 取证分析[2,3]

数据获取完毕以后，接下来的工作就是取证分析，取证分析一定要在获取的映像文件上进行。

3.2.1 准备工作

在取证分析之前，首先必须将获取的各个分区映像文件安装到取证分析机上。我们假设将 hda1.dd 安装在取证分析机的/home/user01/analysis 目录上：

mount o ro,loop,nodev,noexec hda1.dd /home/user1/analysis

然后进入/home/user01/analysis 目录就可以开始进行分析了。

3.2.2 取证分析

(1)查找隐藏文件

入侵者在入侵过程中往往会创建一些不易被用户发现的文件，因此取证分析的第一步首先是在取证映像中查找隐藏文件，找出隐藏文件后，通过查看隐藏文件的内容来推断入侵者的行为。入侵者常用的一种隐藏技术是将普通文件加入到/ dev 目录中。我们可以用 find 命令加上“type f”选项来查找/dev 目录中的普通文件。

另一种隐藏文件的方法是将文件名的第一个字母改为“.”，因为用普通的 ls 命令不能列出以字母“.”开头的文件。但我们可以用 find 命令加上“- name”选项来找出所有以字母“.”开头的文件。

(2)分析隐藏文件

找到隐藏文件后必须分析隐藏文件的内容来推断入侵者的入侵行为。我们可以用 UNIX 系统中的 strings 命令(该命令的主要功能是提取出文件中的 ASCII 码字

符串)或 Autopsy 工具来分析隐藏文件的内容。

(3)分析启动文件和配置文件

大多数入侵者经常将后门程序隐藏在系统的配置文件和启动文件中，这样的话，每当系统启动时，后门程序就会自动执行。因此，通过分析系统的启动文件和配置文件，我们便可以发现可疑程序。

a. 分析启动文件

由于许多安装程序只是简单地在启动文件的后面加上几条命令，因此我们只要检查启动文件的最后面几行命令就可以发现可疑程序。启动文件中的正常命令一般都包含在 if 语句结构中，不包含在 if 语句结构中的命令一般可认定为可疑程序，但也不是绝对的，因为入侵者很容易做假。

b. 分析配置文件

通过分析配置文件，也可以找到许多非常有用的入侵线索。配置文件/etc/passwd 中包含了系统中所有用户的登录信息，入侵者在入侵系统时可能会在系统中创建新的用户或帐号，分析文件/etc/passwd 内容，可以发现可疑用户信息，尤其是那些 UID 为 0 的用户最值得怀疑，因为它们是 root 用户，具有很高的权限。

c. 分析历史文件

除了启动文件和配置文件，历史文件也能提供一些线索。历史文件位于用户的/home 目录中（如文件.bash_history），记录了用户以前执行过的所有命令。当入侵者入侵系统后，经常会删除该文件或将其链接到/dev/null 中，通过恢复该文件或分析/dev/null，我们可以发现许多有用的线索。

(4)分析日志文件

从日志文件中我们可以找到非常有用的入侵线索。UNIX 系统使用 syslog 守护程序来建立系统日志。应用程序或者网络上的其他主机将信息发送给守护程序，守护程序再将这些信息存入日志文件。在分析日志文件之前，首先要查看日志配置文件/etc/syslog.conf，该文件指出了日志文件的路径。一般情况下日志文件保存在/var/adm 或/var/log 目录下。下面是/var/log 目录下的一些日志文件：

a. boot：该日志文件存放系统启动信息，其内容可读性较好。

b. lastlog：该日志文件存放每个用户的最后登录信息，包括登录的时间和地点，入侵者盗用其他用户帐号的情况可从该文件中反映出来。该文件是一个二进制文件。

c. maillog：该文件存放邮件系统的日志信息。

d. messages：该日志文件存放大部分应用程序的日志信息，通常包括启动任务信息、登录信息等，还能显示出谁试图登录系统获得超级管理员权限。该文件可以提供较多的入侵线索，但该文件容易经常被删除或修改。

e. secure：记录系统自启动以来所有用户的登录时间和地点以及登录的途径。

f. wtmp/wtmpx：存放用户登录的历史信息，保存了系统所有的登录、退出信息以及系统的启动、停机记录，据此可发现有用的入侵线索。该文件是一个二进制文件，可以用 last 命令加上“-f”选项来读出 wtmp 文件的内容。

(5)分析空闲空间和交换空间(swap space)

文件被删除以后，文件内容仍然保存在硬盘上的数据块中，不过此时系统已经将这些数据块的状态标识为空闲。我们可以在空闲数据块中寻找犯罪证据。

我们可以使用 The Sleuth Kit 中的 dls 工具来提取空闲数据块中的数据。dls 工具检查每个数据块的状态，并输出空闲数据块中的数据。

从空闲空间中提取出数据后，我们可以用 foremost(http://foremost.sourceforge.net) 工具来分析这些数据。foremost 工具可以从这些数据中查找特定的文件头和文件脚，从而将文件恢复出来。

我们也可以从交换空间中寻找犯罪证据。虽然目前没有专门的取证工具来分析交换空间，但我们可以用 strings 命令。我们可以从交换空间中发现 shell 历史记录、环境变量和进程内存等信息。

4 结语

UNIX 作为目前最常用的主流操作系统之一，研究 UNIX 系统的取证分析方法具有非常重要的现实意义。本文只是对 UNIX 系统的取证分析方法作了非常初步的研究，有兴趣的读者可以在这方面作更进一步的探索和研究。

参考文献

1 Mandia K, Prosise C, Pepe M. 汪青青,付宇光等译.应急响应&计算机司法鉴定(第 2 版).北京:清华大学出版社, 2004.

2 Carrier B. UNIX Computer Forensics. [2007-10-12]. http://searchenterpriselinux.techtarget.com/searchEnterpriseLinux/downloads/Honeynet_Ch12.pdf.

3 Keith R, Jones J. Performing Investigations on a Live Host.[2007-11-15].http://www.usenix.org/publications/login/2001-11/pdfs/jones.pdf.