计算机取证—Linux 系统初始响应方法

Computer Forensics—Initial Response to Linux System

殷联甫 （嘉兴学院信息工程学院 314001）

摘 要： Linux 系统作为目前最常用的操作系统，研究 Linux 系统上的计算机取证方法具有非常重要的现实意义。本文介绍了在 Linux 系统进行初始响应所需的常用工具及基本步骤，并给出了几个常见工具的具体使用方法。

关键词： 初始响应 计算机取证 计算机犯罪调查

1 引言

Linux 系统作为目前最常用的操作系统，研究 Linux 系统上的计算机取证方法具有非常重要的现实意义。一般情况下，当发现 Linux 系统受到入侵而需要对系统进行取证分析时，首先需要关闭系统，然后对硬盘进行按位（bit－level）备份以作进一步的分析。但一旦关机，有些重要的入侵证据往往会丢失，这些证据一般存在于被入侵机器的寄存器、缓存或内存中，主要包括正在运行的进程、打开的 TCP/UDP 端口、已被删除但仍在内存中运行的程序映象、缓冲区的内容等信息。这些证据往往被称为易失性数据（volatile information）。系统关闭后这些数据就会全部丢失，而且不可能恢复。

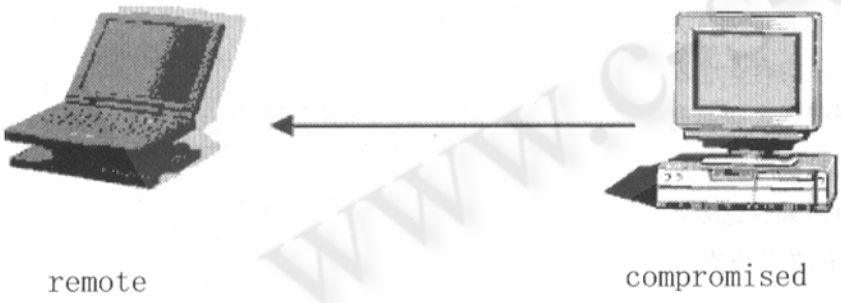

图 1 利用 netcat 收集证据

初始响应就是在关闭系统之前收集受害者机器上的易失性数据的过程。主要的易失性数据包括：

（1）系统日期和时间；

（2）当前运行的活动进程；

（3）当前的网络连接；

（4）当前打开的端口；

（5）在打开的套接字（open sockets）上监听的应用程序；

（6）当前登录的用户。

2 初始响应的准备工作

2.1 建立一个司法鉴定工作站

在初始响应过程中，不能将收集到的证据直接写回到被入侵机器的硬盘上，这样做可能会删除一些重要的入侵证据。一个最简单的方法是将收集到的证据写到软盘上，但软盘的容量太小，有时无法容纳所有的证据。我们常用的方法是在网络中接入一台工作站，该工作站称为司法鉴定工作站，再利用所谓的“TCP/IP 瑞士军刀”工具 netcat，通过网络将收集到的证据传送到司法鉴定工作站上。本文约定将司法鉴定工作站简称为“remote”，将被入侵系统简称为“compromised”，如图 2.1 所示。所有在司法鉴定工作站上运行的命令加上前缀“（remote）”，在被入侵系统上运行的命令加上前缀“（compromised）”。

2.2 创建一个初始响应工具包

在数据收集过程中，我们必须牢记以下几条准则：

（1）不能运行被入侵系统上的程序来收集证据，这样做可能会修改系统命令或系统库，使收集到的证据不可靠。因此，我们必须准备好静态编译工具，通过运行静态编译工具来收集证据。

（2）不能运行那些可能会修改文件或目录的元数据（meta－data）的程序。

（3）对于收集到的数据，必须计算它们的 hash 值，以防止数据被篡改。

以下是常用的 Linux 系统初始响应工具：

（1）nc（http://www.atstake.com/research/tools/network_utilities/nc110.tgz）

编译方法：$ tar zxvf nc110.tgz；make linux

（2）dd（http://www.gnu.org/software/fileutils/fileutils.html）

（3）datecat（http://www.gnu.org/software/coreutils/）

编译方法：$ tar zxvf coreutils－5.0.tar.gz；configure CC＝gcc － static，make

（4）pcat（http://www.porcupine.org/forensics/tct）

编译方法：$ tar zxvf tct－1.14.tgz；make CC＝gcc － static

（5）Hunter.o（http://www.phrack.org/phrack/61/p61－0x03_Linenoise.txt）

为了使模块更具独立性，我们必须从源代码中删除以下内容：

```
# ifdef CONFIG_MODVERSIONS
# define MODVERSIONS
# include <linux/ modversions .h>
# endif
```

编译方法：$ gcc － c hunter.c － I/usr/src/linux/include/

（6）insmod（http://www.kernel.org/pub/linux/utils/kernel/modutils/for kernel 2.4）

编译方法：$ ./configure－enable－insmod_static；make

（7）NetstatArproute（http://freshmeat.net/projects/net－tools/）

编译方法：$ bzip2 － d net－tools－1.60.tar.bz2

$ tar xvf net－tools－1.60.tar.bz2

$ make config

$ make CC＝gcc － static

（8）dmesg（http://ftp.cwi.nl/aeb/util－linux/util－linux－2.12.tar.gz）

编译方法：$ ./configure；make CC＝gcc －static

上述工具全部编译完成后，必须将它们拷贝到一张可读写光盘上。为了在接下来的数据收集过程中能运行一个可靠的 shell，初始响应工具还必须包括静态编译的 bash shell 命令解释程序。

3　初始响应的具体步骤和方法

3.1　介质安装

介质安装阶段的主要工作是将包含初始响应工具的可读写光盘安装到被入侵系统上，同时设定运行环境，为在被入侵系统上运行初始响应工具做准备：

（compromised）#mount － n /mnt/cdrom

运行光盘上的 bash shell：

（compromised）#/mnt/cdrom/bash

我们采用 netcat 工具和管道方法，将在被入侵系统上收集到的数据传送到司法鉴定工作站上（假定该司法鉴定工作站的 IP 地址是 192.168.1.100），下面是一个收集当前日期信息的例子：

首先在司法鉴定工作站上打开一个 TCP 端口：

（remote）#nc － l － p 8888 > date_compromised

上面的命令在司法鉴定工作站上打开了一个监听端口，同时将接收到的数据重定向到文件 date_compromised 中。参数“－l”表示监听模式，当监听方接收到数据后将关闭端口，停止监听。如果希望监听方接收到数据后继续监听，可以选用参数“－L”。参数“－p”指定监听端口，你可以选择任何端口。

然后在被入侵系统上必须运行以下命令：

（compromised）#/mnt/cdrom/date l/mnt/cdrom/nc 192.168.1.100 8888 － w 3

为了保证数据的一致性，我们还必须计算收集到的数据文件的 hash 值：

（remote）#md5sum date_ compromised > date_compromised.md5

3.2　收集当前日期信息

（remote）#nc － l － p port > date_compromised

（compromised）#/mnt/cdrom/date － u l/mnt/cdrom/nc（remote）port

（remote）#md5sum date_compromised > date_compromised.md5

在上面的命令中，“port”表示端口号，“remote”表示司法鉴定工作站的 IP 地址，下同。

3.3 收集 cache 表的信息

由于 cache 表中信息的存在时间较短，因此我们首先收集该信息。

收集 Mac 地址 cache 表信息：

(remote)#nc - l - p port > arp_compromised

(compromised) #/mnt/cdrom/arp - an l/mnt/cdrom/nc (remote) port

(remote) #md5sum arp_compromised > arp_compromised. md5

收集内核 route cache 表信息：

(remote)#nc - l - p port > route_compromised

(compromised) #/mnt/cdrom/route - Cn l/mnt/cdrom/nc (remote) port

(remote)#md5sum route_compromised > route_compromised. md5

3.4 收集当前的连接和打开的 TCP/UDP 端口的信息

(remote)#nc - l - p port > connections_compromised

(compromised)#/mnt/cdrom/netstat - anl/mnt/cdrom/nc (remote) port

(remote)#md5sum connections_compromised > connections_compromised. md5

打开的 TCP/UDP 端口信息保存在/proc 伪文件系统中(文件/proc/net/tcp 和/proc/net/udp)，当前连接的信息保存在文件/proc/net/netstat 中。

3.5 收集物理内存映像信息

收集物理内存映像(physical memory image)信息对于计算机取证来说意义重大，因为调查分析人员往往可以从物理内存映像中找到入侵者的犯罪证据。我们可以直接拷贝/dev/mem 设备文件或 kcore 文件来取得物理内存映像。Kcore 文件表示 Linux 系统中的 RAM 信息，该文件可以从伪文件系统中找到，一般安装在/proc 目录下。Kcore 文件的大小与当前物理内存的大小基本一致。使用 kcore 文件的优点在于该文件使用 ELF 格式，可以用 gdb 工具进行调试。

下面我们利用伪文件系统来获取物理内存映像：

(remote)#nc - l - p port > kcore_compromised

(compromised) #/mnt/cdrom/dd < /proc/kcore l/mnt/cdrom/nc (remote) port

(remote)#md5sum kcore_compromised > kcore_compromised. md5

3.6 收集活动进程信息

(remote)#nc - l - p port > lsof_compromised

(compromised)#/mnt/cdrom/lsof - n - P -ll/mnt/cdrom/nc (remote) port

(remote) #md5sum lsof_compromised > lsof_compromised. md5

3.7 收集可疑进程信息

(remote)#nc - l - p port > proc_id_compromised

(compromised)#/mnt/cdrom/pcat proc_id l/mnt/cdrom/nc (remote) port

(remote)#md5sum proc_id_compromised > proc_id_compromised. md5

4 结束语

初始响应是计算机取证的关键步骤之一，通过初始响应可以获取非常有用的计算机犯罪信息。Linux 系统作为目前最常用的操作系统，研究 Linux 系统上的初始响应方法具有非常重要的现实意义。

参考文献

1 [美]Keith J. Jones, Mike Shema, Bradley C. Johnson 著，宋震，易晓东，肖国尊等译.《黑客大曝光》姊妹篇：阻击黑客，北京电子工业出版社，2003 年.

2 [美]Mike Shema, Bradley C. Johnson 著，赵军锁，姜南等译.《黑客大曝光》姊妹篇：反黑客工具包(第二版). 北京：电子工业出版社，2005 年.

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

4 [美]Kevin Mandiis Pra, Chrosise, Matt Pepe 著，汪青青，付宇光等译. 应急响应 & 计算机司法鉴定. 清华大学出版社，2004.

5 Mariusz Burdach. Forensics Analysis of a Live Linux System, Part One. http://www. istroop. org/Article_Print. asp? ArticleID =723. 2004