第 1 章　阅读日志文件

你小的时候应该看过周六下午关于西部牛仔的电视节目吧？还记得其中的这样一些镜头吗？跟踪者只需将耳朵放在铁轨上就能熟练地分辨出火车何时经过，或者根据沙滩上的足迹就能准确地说出一匹马上驮了几个人。不必惊讶，你也可以成为这样的人，不过时间要调转到 21 世纪。记号到处都是，而且一清二楚，你的任务就是发现它们并做出相应解释。

本书首先介绍由 IDS（Intrusion Detection System ，入侵检测系统）、防火墙和其他操作系统所创建的一组日志格式。刚开始学习时，可能会觉得它比较枯燥，不过毕竟这是一本关于攻击特征和分析的书。既然要学习当一名跟踪者，那么就从现在开始吧。

路由器、IDS 都需要在日志中记录所发生的事件，甚至运行各种网络转储工具的不同 UNIX 版本也会记录日志，不过具体的记录方式则各有千秋。正确地理解日志文件，同时识别其文件来源，对于有效地利用其中的数据是至关重要的。

在学习完本章之后，你应该能够做到以下几点：

- 理解如何正确地解释日志文件
- 识别文件来源
- 了解信息的危险程度

本章包括了以下几种日志格式：

- TCPdump
  Snort
  Cisco ACL（access control list，存取控制列表）日志文件
- Syslog
- 商业 IDS
- 防火墙日志文件

在实现入侵检测时可以使用一组免费的系统（如 TCPdump，Snort 和 Portsentry），其中包括基于主机和基于网络两种类型。在查看 GIAC（Global Incidents Analysis Center，全球事件分析中心）（www.sans.org/giac.htm）的信息或者 SecurityFocus（www.securityfocus.com）的事件列表时，你会发现这些工具即为实现入侵检测的主要工具。这一章首先讨论 TCPdump。

1.1　TCPdump

TCPdump 是由劳伦斯巴克利国家实验室的网络研究组开发的，在实现网络数据流转储时，这是最常用的工具。尽管 TCPdump 一般总作为 IDS（如 Snort 和 Shadow）的基础，不过它也可以独立运行。程序本身提供了多个选项，从而使用户可以选择不同的冗余度实现网络数据流的转储。在 Linux 下单独运行 TCPdump 将得到以下输出结果（见图 1.1）。注意

这里的数据流是无恶意的，它只是一个友好的 Web 数据包。

这里只列出了其中的几行，但“麻雀虽小，五脏俱全”，在此已经包括了一些重要的信息。先来逐一地分析这个例子：

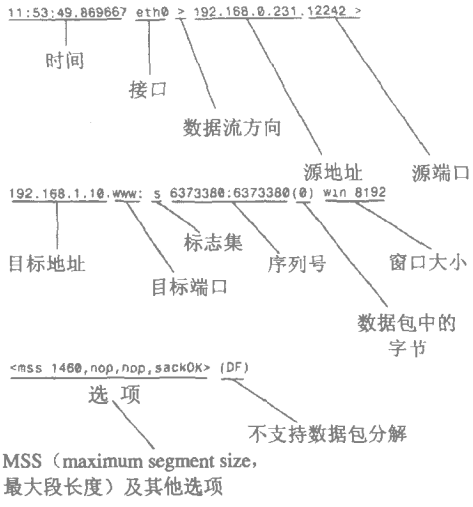


图 1.1 TCPdump 跟踪格式

11:53:49.869667

这是发现数据包的时间，.869667 的作用是更加准确地记录事件，因为在某 1 秒内很可能发生许多事件。其设计思想是为每个数据包设置一个惟一的时间戳。这意味着如果在一个文件中收集 24 小时以内的跟踪记录，那么若在一个数据包集合中寻找某个数据包，就起码需要提供一个查找关键字。TCPdump 并不会设置日期戳，因此必须利用文件名来处理日期。

eth0

这是一个被监控接口。根据操作系统不同，接口名将有所变化。例如， Linux 中一般为 ethX，Solaris 中则一般为 hmeX，而基于 BSD 的系统则根据网卡类型的不同而有所调整。

192.168.0.231.12242

这是源 IP 地址和源端口（12242）。大多数情况下，你可以根据端口判断哪个系统是客户，哪个系统是服务器。当客户向服务器请求某种服务时，如 HTTP 或 FTP，它往往会把其源端口（大于“特权端口”或“常用端口”范畴，一般把端口号为 1023 或更小的端口称为“常用端口”）设置为一个临时端口，此端口号一般为 1024 或更大。客户则通过一个小一些的常用端口（一般为 80 或 21）向服务器请求服务。

192.168.1.10.www

此为目标 IP 地址和目标端口。在这个例子中，TCPdump 将解析/etc/services 以得到端口分配，并由此知道端口 80 用于实现 Web 通信，因此将把 www 替换为相应的端口号。如果这是一个未知的服务，则会以数字形式显示目标端口。要记住，虽然这里是 www，但并不表示它一定是 Web 通信。例如，如果客户知道要到端口 80 获得 FTP，则可以在端口 80 运行一个 FTP 服务器。不过 TCPdump 总会把它报告为 Web 通信。

TCP 和 UDP

在 UNIX 系统中，如果你查看/etc/services 文件，会注意到一些端口号出现了两次（一次使用的是 TCP 协议，另一次则使用 UDP 协议）。虽然它们的端口号相同，但一般认为这是完全不同的两个端口。正式情况下，端口需要结合端口号和协议规范来定义。例如，telnet 服务端口可以记为 23/TCP。

我们知道，TCP 是面向连接的协议，而 UDP 是无连接的协议。面向连接的协议虽然能够提供可靠的服务，但为了保证所发送数据包的准确性，势必会带一些额外的数据流。这种协议一般用于在网络之间传送信息。无连接的协议不会为保证数据包传输而增加负载，如果传送信息的优先级比较低，或者网络本身比较可靠，一般不会丢失数据包的话，那么使用这种协议就是适合的。无连接协议还可以用于网络间短消息的传递，这是因为其重发的耗费比较低。

A.J.

S—标志字段

这是一个标志字段。其值可能是 P，R，S 或 F，分别对应 PSH，RST，SYN 和 FIN。注意这里没有 URG 和 ACK 标志，如果要设置，则可以连同合适的序列号分别记为 urg 或 ack。在标志字段中若有一个句号或一个点号（.），则表示 PSH，RST，SYN 和 FIN 中任何一种标志都没有设置。攻击者往往就通过设置异常的标志（如 SYN-FIN）来逃避 IDS 的检查。如果一个数据包的标志是不符合规范的，就应该知道其中必有文章，因此需要对此特别注意。第 15 章将更为详细地讨论异常数据包的有关内容。

6373380:6373380（0）

前一部分为初始序列号，其后是一个完全相同的结束序列号。（0）表示此数据包中的字节数。初始序列号可以用于跟踪记录数据包发送的顺序。同时初始序列号还可以知道三段握手中的第二台计算机应该从何时开始计算。设置了初始序列号后，针对数据包中的各字节，每台主机都会将序列号增 1，这样就能够保证通信双方实现同步。对于 TCP，在全双工连接方式中，连接双方都有一个序列号，从而可以跟踪记录双方的数据发送情况。

Win 8192

设置窗口大小可以控制既定时间内能够发送的数据量。不同操作系统可以处理不同大小的数据包，而且处理速度也不同。每台计算机都要通过设置窗口大小指出其能够接收的最大数据包长度。对此，可以使用套接字 API 中的“窗口广播”功能，它将分配发送和接收缓冲区，另外还会定义窗口的最大长度。这是一种流控制机制，与 MSS（maximum segment size，最大段长度）是不同的。如果客户发送给服务器的数据包超出了窗口大小，服务器通常会丢掉数据包，因此无法处理完整的数据流（反之，服务器向客户发送数据包时情况也是类似的）。

<mss 1460,nop,nop,sackOK>

此字段可以设置各种 TCP 选项。这里将 MSS 设置为 1460 字节。这些选项将在连接建立时设置。MSS 表示当前连接中可以接受的 TCP 段最大长度。TCP 选项必须占满 32 位，如果没有达到，则要填入 NOP（No Operation codes ，无操作码），以此区别 0。

（DF）

在此可以找到关于数据包分解的信息。如果发送的数据报大小超过了路由能够处理的最大长度，则要用到数据子包。每个物理层都有一个最大的 ITU（interface transmission unit，接口传输单元）。在源地址与目标地址之间的最小 ITU 一般称为相应连接的 MTU（maximum transmission unit ，最大传输单元）。IP 层将检查接口，找到 MTU，如果有必要还要对 IP 数据报进行分解。所有的中间路由器都要完成类似的工作。实现数据包的分解并非是 TCP 的功能，而且 MTU 也不是由接收主机设置，它是在路由做出决策并配置接口时进行设置的。TCP 最好不要进行分解，而 UDP 则一般都要对数据包进行分解。如果数据包中确实有数据子包，则在 DF 的位置上要替换为相应的数据子包 ID 和位移，以帮助 TCP 数据包实现重组。这里的 DF 的含义是不支持数据包分解。

下一节将学习目前使用最广泛的 IDS Snort 的日志格式。

1.2 Snort

Snort 是由 Martin Roesch 基于 libpcap 数据包收集程序所开发的 IDS，它是免费的。Snort 的警示信息与 TCPdump 格式类似，不过更易读。以下是 Robert Coursey 的实习报告中所列的一个实际的 Snort 警示信息（见图 1.2）。

在 Snort 警示信息中，要注意以下几个问题。首先，在警示信息名前面和后面必须有 [**]. 这是 Snort 的特点。其次，可以注意到它与 TCPdump 格式是如此相似。在警示信息名中可以找出产生 Snort 警示信息的过滤条件。在 Snort 或 TCPdump 日志中能够看到数据包的 16 进制有效负载，其值取决于怎样调用实用程序。以下 Snort 警示信息来自 John Springer 的实习报告，其中就记录了有效负载（见图 1.3）。

在这里可以看到常见的 Snort 信息，连同 16 进制转储，以及 Snort 将 16 进制转换为可读格式。非商业系统的引入使我们可以更细致地了解基于主机的工具 Syslog 和 Portsentry。

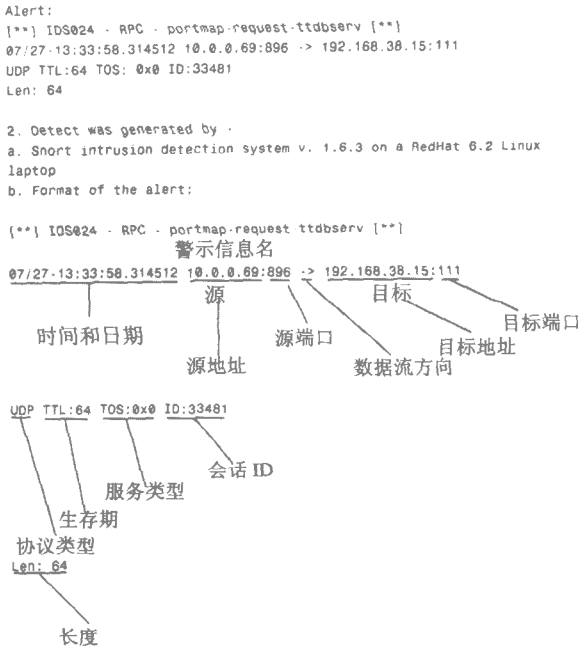


图 1.2　Snort 警示信息

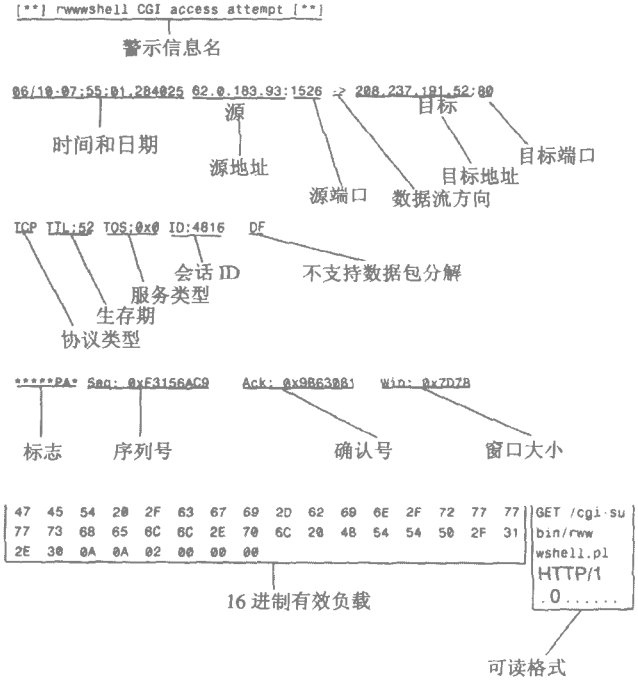
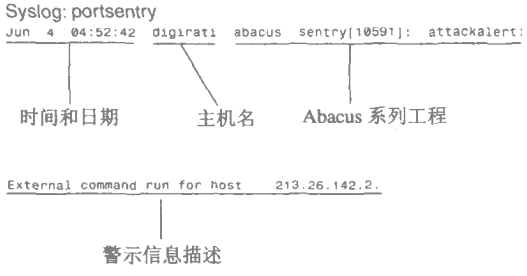


图 1.3　带有有效负载的 Snort 警示信息

1.3 Syslog

Syslog 是一个系统内置的报告程序，可以维护系统日志。 Syslog 所生成的文件一般保存在/var/log 下。许多安全工具都将其检测结果报告给 Syslog。Todd Garrison 在实习中通过登录 Syslog 得到以下结果。第 2 章详细讨论了在实习报告中采用的格式。此实例来自“Syslog：Portsentry”，可以算是提前对实习报告的介绍，需要明确的一点就是实习报告是本书的核心所在（见图 1.4）。




```
Jun  4 04:52:42 digirati  abacus_sentry[10591]: attackalert: Host
➥213.26.142.2 has been blocked via wrappers.
Jun  4 04:52:42 digirati abacus_sentry[10591]: attackalert: Host
➥213.26.142.2 has been blocked via dropped route.
Jun  4 04:52:42 digirati abacus_sentry[10591]:  attackalert: Connect
➥from host: 213.26.142.2/213.26.142.2 to TCP port: 111
Jun  4 04:52:42 digirati  abacus_sentry[10591]: attackalert: Host:
➥213.26.142.2 is already blocked. Ignoring
Jun  4 04:52:42 digirati abacus_sentry[10591]:  attackalert: Connect
➥from host: 213.26.142.2/213.26.142.2 to TCP port: 111
Jun  4 04:52:42 digirati  abacus_sentry[10591]: attackalert: Host:
➥213.26.142.2 is already blocked. Ignoring
                    (. . .)
Jun  4 04:52:51 digirati kernel: Packet log: input DENY
➥eth0 PROTO=6 213.26.142.2:4293 192.168.245.5:111 L=52
➥S=0x00 I=51379 F=0x4000 T=48
Jun  4 04:53:02 digirati kernel: Packet log: input DENY
➥eth0 PROTO=6 213.26.142.2:884 192.168.245.5:111 L=52 S=0x00
➥I=51626 F=0x4000 T=48
Jun  4 04:53:02 digirati kernel: Packet log: input DENY
➥eth0 PROTO=6 213.26.142.2:4293 192.168.245.5:111 L=52
➥S=0x00 I=51627 F=0x4000 T=48
Jun  4 04:53:03 digirati kernel: Packet log: input DENY
➥eth0 PROTO=6 213.26.142.2:4293 192.168.245.5:111 L=40
➥S=0x00 I=51647
—
                    (. . .)
```

图 1.4 Portsentry Syslog

Abacus

Abacus 系列工程是 Psionic 软件公司推出的，其目的是开发一组工具以提供基于主机的安全，并使 Internet 用户无须进行入侵检测。详细信息请参见 www.psionic. com/abacus/。

跟 踪 源

这里攻击的目标网络与以前讨论的有所不同，以前攻击的网络一般都是专门设计的，

即为了便于分析攻击而设置了相应的“漏洞”，而我们所攻击的则是正在使用的实际网络。我的家用网络上建立了多个网站，另外配置也相当复杂。防火墙为 IPchains，并通过 ARP 代理或路由方法将/29 网络分离出来。

要如此配置往往比较困难，我之所以会这样配置是因为当时我买不起 2 层防火墙，我的 ISP 也没有为我分配两个 IP 地址段，所以要建立一个防护领域，这是最佳的方式。防火墙起到了欺骗的作用：对于一些明显不安全的服务，这里并没有将相应的连接丢掉，而是将相应请求重定向到本地，再使用 Portsentry，就会动态地避开那些可能发动攻击的 IP 地址。

Portsentry 只处理实际的连接，其作用是使我不至于因为伪装的攻击而无法到达外部网络（例如，通过假冒成根一层次的命名服务，就会使我的 DNS 无法正常工作）。

在同一台主机上，我还运行了 Snort，如果有人首次探测网络，利用 Snort 我就可以及时发现，并跟踪其整个攻击过程。直到大约 21 世纪中期，Snort 才有端口扫描检测功能，因此运行 Snort 时结合 Portsentry 之类的工具尤为重要。这种情况很常见，因为对于入侵检测而言，还没有哪一种技术堪称“全能”。

Portsentry 自动响应了连接之后，入侵者就无法进一步地攻击我的网络了，而且同时还将相关事件记录下来，提醒我注意该攻击。这种防护是比较完善的，但是它本身也可能造成 DoS（denial of service，拒绝服务）攻击。例如，一次我朋友来我这里，把她的笔记本电脑（系统平台为 Windows）插到集线器中。在收到 DHCP 分配的地址之后，它就开始广播 SMB 浏览请求，防火墙对此反应，其结果却是中止其主机访问 Internet。希望系统管理员注意这一点。

检测工具

利用 Psionic 的 Logcheck 来标志攻击源，所用的 Syslog 消息是由 Linux 平台上的 Portsentry 和 IPchains 创建的。

1.4 商业入侵检测系统

目前市面上有许多商业 IDS。不过在本书中它们所占的比重很小，这是因为尽管许多申请入侵分析师的学生在完成实习时选用了商业 IDS，但通过率却相当低。以下几节简单介绍了 3 个常用的 IDS，包括：Dragon，RealSecure 和 NFR（Network Flight Recorder）。

Dragon IDS

Dragon IDS 是由 Network Security Wizards 公司（最近被 Cabletron Systems 公司收购）开发的，它是一种很常用的商业 IDS。以下内容选自 Todd Garrison 的实习报告（见图 1.5）。

数据源 1（Dragon IDS）

```
04:52:30   [T]   24.95.236.118   10.0.15.67    [SNMP:MIBIISA3]
➥(udp,dp=161,sp=1123)   (dragon)

04:52:30   [T]   24.95.236.118   10.0.15.67
时间              源 IP          目标 IP
[SNMP:MIBIISA3]  (udp,dp=161,sp=1123)  (dragon)
攻击名            IP/UDP 选项          IDS 名

04:52:30   [T]   24.95.236.118   10.0.15.67   [SNMP:MIBIISA3]   (udp,dp=161,sp=1123)   (dragon)
04:53:01   [T]   24.95.236.118   10.0.15.67   [SNMP:CISCO]   (udp,dp=161,sp=1123)   (dragon)
04:53:03   [T]   24.95.236.118   10.0.15.67   [SNMP:PUBLIC]   (udp,dp=161,sp=1123)   (dragon)
04:53:03   [T]   24.95.236.118   10.0.15.67   [SNMP:PUBLIC]   (udp,dp=161,sp=1123)   (dragon)

                                 (. . .)

dragon
(Towards)
     04:52:26
        SOURCE: 24.95.236.118   winterspringsubr-c5s1-
118.cfl.rr.com
        DEST:   10.0.15.67   solaris.evilscan.com
      IP HEADER:
            Version                         4
            Header Length                   5
            Type of Service                 0
            Total Length                    72 bytes
            ID Number                       0xE6B9
            Reserved Bit                    0
            Don't Frag Bit                  0
            More Frags Bit                  0
            Fragment Offset                 0
            Time To Live                    38
            Protocol                        UDP
            Checksum                        0xD1E3
            Source Address                  24.95.236.118
            Destination Address             10.0.15.67

      UDP HEADER:
            Source Port                     1123
            Destination Port                snmp (161)
            Message Length                  52
            Checksum                        0x2A24
      UDP PAYLOAD:
      30 82 00 28 02 01 00 04 06 63 69 73 63 6f 31 a0 1b 02 01 0c 0 . . (. . . . .cisco1. . . . .
      02 01 00 02 01 00 30 10 30 82 00 0c 06 08 2b 06 01 02 01 01   . . . . . 0 . 0 . . . . .+. . . . .
      05 00 05 00                                                   . . . .

      EVENT1: [SNMP:CISCO]  (udp,dp=161,sp=1123)
```

图 1.5　Dragon IDS 警示信息

跟踪源

这里检测的网络是专为检测攻击、研究攻击方法而建立的。

检测工具

此攻击通过 Dragon IDS（www.securitywizards.com）检测。数据包的第一部分显示了一些总的信息，包括时间、源 IP 地址、目标 IP 地址、攻击名、一些基本的 IP/UDP 选项和产生攻击的 IDS 名。

下面的部分将分析最具卖点的商业 IDS，RealSecure。

RealSecure

RealSecure 由 ISS（Internet Security Systems）公司出品，这是一个很常用的商业入侵检测产品。其日志很容易读懂，因此无须过多的解释。

以下内容由 Merik Karman 的实习报告中选取，它说明了 RealSecure 的检测过程（见图 1.6）。相应数据是从 RealSecure 系统记录的网络事件数据库中抽取的，其中表示优先级为 High，随后是一个日期一时间戳，源地址为 207.126.127.68，源端口为 49224，目标地址即为我的外部 DNS/SMTP 服务器的地址，目标端口为 25。目标端口后面的一行表示主机结构为 Intel 且操作系统为 Linux。

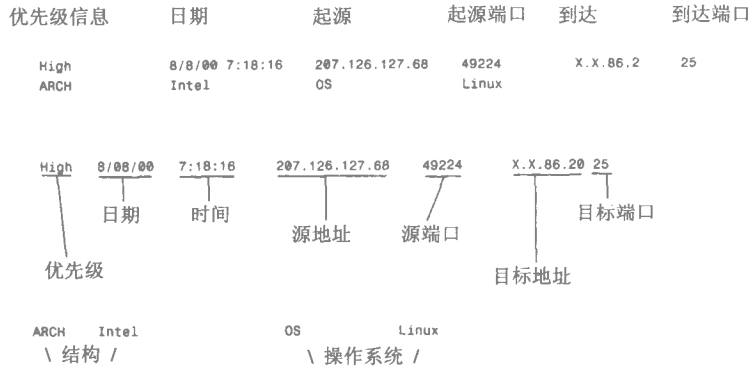


图 1.6 RealSecure 警示信息

NFR

NFR 是计算机安全市场上另一个竞争产品。其功能与 ISS 和 Network Security Wizards 公司所提供的大致相同，它也是一个基于网络的 IDS，可以根据规则生成攻击警示信息（NFR 把这些规则称为“基干”，其中包括多个“过滤条件”）。

以下即为一个 NFR 警示信息：

```
Time:               13-Apr-2000 12:48:18
NFR:                ponch
Source IP:          192.168.0.2
Source Port:        42531
Dest. IP:           192.168.0.4
Dest Port:          21
Module:             FTP Monitor
Reason:             FTP password
Possible Version:   1.3
```

以上警示信息取自 NFR 系统，这是用 ISS（RealSecure 的生产商）的 S3 产品扫描得到的。这个过滤条件要基于 S3 扫描工具固定编码的特征写入触发器（特别是静态的 FTP 口令）。

以上每一项都可以根据其字面理解：时间（和日期）、 NFR（远程捕获此数据流的实际 NFR 名）、源 IP、源端口、目标 IP、目标端口、模块（实现监控的实际进程）、原因（触发

产生此警示信息的原因）以及可能的版本（可以大致猜出扫描软件的版本）。

并非 NFR 生成的所有警示信息都类似，实际上每组警示信息所报告的信息量就有所不同。作为 NFR 报告的补充，Web 日志资料还可以提供更详细的信息，甚至包括浏览器类型和 Web 服务器版本。不过这里只返回基本信息。以上资料有特定的输出形式，即无须分析员专门对警示信息进行逐项解释，最终输出的警示信息本身就很容易理解。

1.5 防火墙与边界防护

与本章提到的其他设备有所不同，防火墙需要基于某种规则对数据流进行阻塞。也就是说，只要数据包违反了安全策略就会被检测出来。 IDS 则根据这些资料报告检测信息。

这一章将简单介绍路由器和防火墙日志（包括 Cisco，Firewall-1 和 PIX），并提供一个关于主机或个人防火墙（BlackIce ）的实例。第 6 章将详细讨论有关内容。

Cisco ACL

在当今的网络环境中，应用最广的设备当属 Cisco 路由器和网关了。在做分析时，你通常会碰到 Cisco 设备产生的日志文件（因此这里将重点介绍这种日志文件格式）。以下资料取自 Cisco ACL 日志（见图 1.7）：

对此我们同样会逐项地分析。

Feb 1 00:15:06 rt1

典型的日期与时间信息，后面是主机名 rt1。

1136:08:00:42

这是 Cisco 的可配置时间戳。可以表示运行时间、日期和时间、以微秒计的日期和时间、在本地时区的日期和时间以及指定时区的日期和时间。

%SEC-6-IPACCESSLOGDP:list 102

SEC 是一个功能码，一般包括 2~5 个大写字母，用来表示消息功能，这里 SEC 是指 IP 安全。6 为攻击级别。IPACCESSLOGDP 是一组大写字母,用于惟一地标识消息。最后 list 102 表示哪一个 ACL 中的规则产生了此警示信息。

Denied

表示路由器所采取的操作，在这种情况下，被禁止的数据流为 ICMP（根据检测结果得知）。

源与目标

源地址为 192.168.0.202 ，目标 IP 地址为 192.168.135.2。

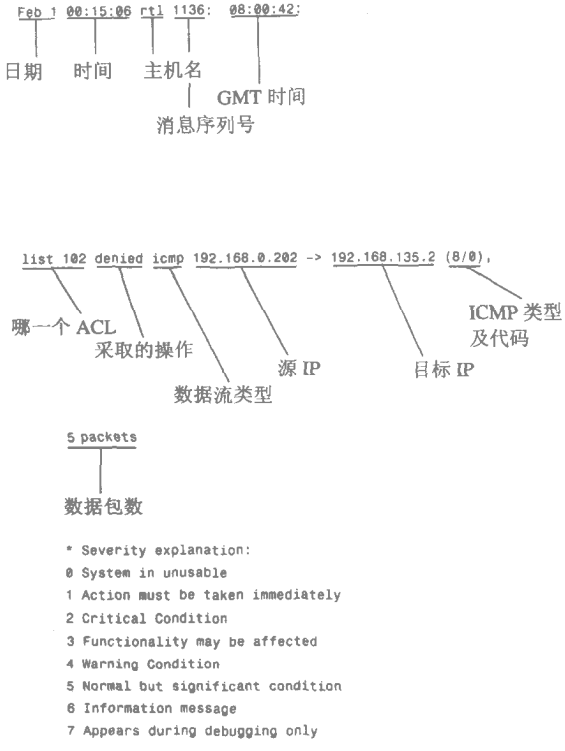


图 1.7 Cisco 存取控制日志的详细内容

ICMP 类型与代码

检测结果中（8/0）表示的是 ICMP 类型与代码。这里 ICMP 类型 8 所附带的代码号为 0，它表示一个回应请求。因为 ICMP 没有端口号，这一点与 TCP 和 UDP 有所不同，有人往往因此而小题大做，实际上，类型和代码完全可以起到与端口同样的作用。

表 1.1 列出了 ICMP 的类型和代码，摘自 Cisco 的《Catalyst 6000 Family Software Configuration Guide（5.3）》[①]。

表 1.1 ICMP 的类型和代码

类　型	代　码	定　义
3	13	禁止通过管理手段调整
6	—	地址转换
31	0	转换错误
3	10	禁止 dod 主机
3	9	禁止 dod 网络

① CiscoSystems 公司，《Catalyst 6000 Family Software Configuration Guide（5.3）》，客户号：DOC-787074.www.cisco.com。

续表

类　型	代　码	定　义
8	0	回应
0	0	回应应答
12	—	通用参数问题
3	8	独立主机
3	14	无法到达前一主机
5	1	主机重定向
5	3	主机 tos 重定向
3	12	无法到达主机 tos
3	7	未知主机
3	1	无法到达主机
16	0	信息应答
15	0	信息请求
18	0	掩码应答
17	0	掩码请求
32	0	移动重定向
5	0	网络重定向
5	2	网络 tos 重定向
3	11	无法到达网络 tos
3	0	无法到达网络
3	6	求知网络
12	2	无选项空间
12	1	选项丢失
3	4	过大的数据包
12	0	参数问题
3	3	无法到达端口
3	15	无法到达优先权
3	2	无法得到协议
11	1	重组超时
5	—	重定向
9	0	路由器广播
10	0	路由器请求
4	0	源停止
3	5	源路由失败
11	—	超时
14	0	时间戳应答
13	0	时间戳请求
30	0	跟踪路由
11	0	TTL 超时
3	—	无法到达

Firewall-1

Check Point 出品的 Firewall-1（fw1）是一个通用的防火墙，广泛用于局域网和广域网中。其日志格式相当直接，很类似于 Cisco 的 ACL 日志。

以下资料取自 Ken-Wellmaker 的实习报告，其中显示了 NetBIOS 扫描，这就是通过 Firewall-1 发现的。格式如下（见图 1.8）：

日期
时间
操作
数据流方向
数据流类型
源 IP 地址
目标 IP 地址
目标端口
源端口
长度

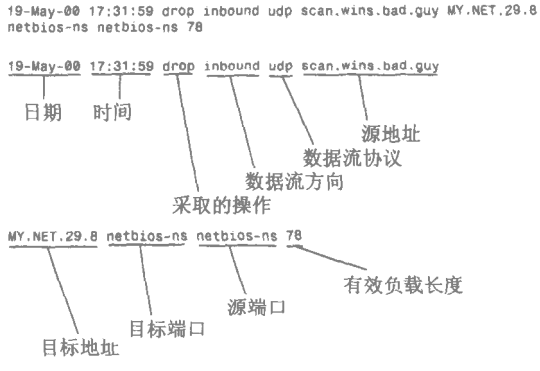


图 1.8 Firewall-1 防火墙警示信息

PIX 防火墙

另一种常用的防火墙系统为 PIX，也是 Cisco 的产品。以下资料取自 PIX 防火墙日志。PIX 防火墙日志的格式如下（见图 1.9）：

日期
时间
防火墙 IP
PIX 警示信息
操作
原因

源地址/端口
目标地址／端口

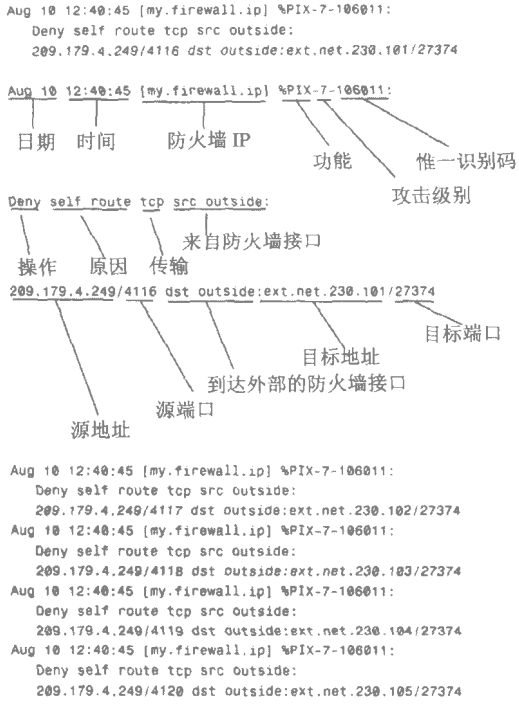


图 1.9　PIX 防火墙警示信息

BlackIce

BlackIce 防护器是由 Network Ice 公司推出的一种软件型防火墙，可以运行于 Windows 平台。能够对该防护器进行配置，即可以按要求设置警示信息内容和操作类型，并能将 IDS 的报告（过滤功能）与防火墙的“操作”功能相结合。以下即显示了 BlackIce 系统所做出的警示信息形式（见图 1.10）：

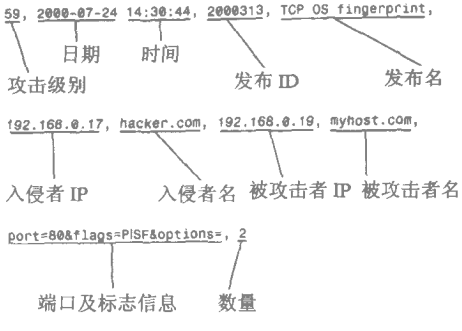


图 1.10　BlackIce 日志

攻击级别

攻击级别值介于 1~99 之间，其中 99 表示最严重的攻击。其实攻击级别本身的意义并不明确，因为即使是级别为 1 的攻击也有可能危及系统的安全。此例中攻击级别为 59。

时间戳

日期和时间信息为 2000-07-24-14:30:44。要记住，如果要向 ISP 和 CIRT 发送日志文件，一定要同时提供时区信息。

发送 ID 为 200313，这是攻击类型的数字标识。具体的攻击号可以参见 http://advice.networkice.com/advice/intrusions。

源与目标

与所有日志文件一样，BlackIce 提供了源和目标信息（可能还包括查找信息）。在这种情况下，192.168.0.17 是攻击者的 IP 地址，hacker.com 为攻击者 IP 地址的 DNS 解析名，192.168.0.19 为被攻击者的 IP 地址，myhost.com 则为被攻击者 IP 地址的 DNS 解析名。

参数字段

参数字段中包括了攻击的有关信息。在此例中 port=80&flags=P|SF&options= 显示了目标端口 80，为数据包所设置的 TCP 标志（PSF），以及可能设置的其他 TCP 选项。在此字段中包括了许多信息，这还取决于所生成的警示信息类型。通过查询 advICE 数据库，可以了解到此字段信息的具体含义，该数据库可以在 http://advice.networkice.com/Advice/default.htm 查到。

1.6 小 结

哇呜！需要了解这么多技术，是不是负担太重了？不要担心，在学习本书后面的章节时，你将进一步了解有关的技术细节。第 2 章将讨论关联记录的重要性，同时还将介绍实习分析报告的格式，这也是本书的核心。

对于不同设备所生成的日志，无论其位置和格式如何，好的分析员都必须对其中的基本信息相当熟悉。一次攻击往往需要借助于多个设备完成，如果是这样，分析员必须充分结合攻击者所用的各个设备，这样才能掌握有关攻击源和攻击组成的诸多信息，并加以利用。

要熟悉日志中的一般信息，最好的办法是多了解一些硬件设备的跟踪情况。你可以从开发商主页上开始起步，在此可以找到不同的日志格式。开发商在提供技术支持时，通常将其设备日志资料放在主页上。如果你没有看过 GIAC 日报（www.sans.org/giac.htm），建议你起码每周查看一次，其中提交了许多不同的日志类型，所以是一个很有用的资源。如果你非常用功，而且深入分析了所有内容，就能获得一些很重要的技能，这些本领要是丢失了就太可惜了，毕竟，你也不知道什么时候需要去解释一个日志文件中的攻击特征。

第 2 章　实习报告导言

本书中的主要内容大部分是由那些报考 GIAC 入侵检测专业资格证书的人提供的。可以看到，其中一些分析员在这个领域中堪称一流，根据其实践工作即可明确地看出他们对入侵检测领域知识掌握的熟练程度。

在本书中，由于对网络和系统攻击特征的分析均采用统一格式，因此本章将对分析报告中各部分的作用详细地加以解释。这里涉及到 10 个内容，即由这些内容组成了 GIAC 入侵分析实习报告的标准跟踪和分析模式。具体包括：

- 作为实习报告的基础，首先需要有某个关键事件的网络或系统跟踪日志。系统跟踪日志一般可以在 GIAC 网站上找到，也可以取自学生自己建立的网络
- 检测源，如 Snort IDS
- 伪装源地址的可能性
- 攻击描述
- 攻击机制
- 关联记录
- 有明确目标的主动攻击证据
- 攻击级别
- 防范措施
- 多选问题

以下各节将详细讨论以上内容。

2.1　网络或系统跟踪

由第 1 章的介绍，我们已经了解了如何读取跟踪信息，因此这一章将不再对此多做说明。不知你是否访问过 GIAC 的网页（www.sans.org/giac.htm），并仔细研究过上面的跟踪情况？我非常喜欢阅读这些提交上来的跟踪情况和实习报告。当然不可避免地，有时候看到的内容确实很陈旧，但有时却可以发现一个新的模式或者新的攻击。然而，一个很重要的问题就是为什么会出现这些跟踪情况呢？如果你仔细考虑 Internet 边界上的数据流量，就会发现那里收集到大量的代码片断。那么为什么要收集这些跟踪情况（也称关键事件）呢？

通常，安全分析员要关注 GIAC 上的跟踪情况主要有两个原因：

- 分析员需要查找由 IDS 过滤得到的数据流
- 由于数据流违反了某个主机或边界防护设备的安全策略，那么就要在日志中记录该数据流

在多数情况下，如果关键事件记入日志，我们就能知道其本来面目。将数据流与规则

进行匹配，由此即可发现其中存在的问题。但实际上并没有这么简单。从理论上说，我们需要解决 3 个问题：过于谨慎、过于大意和误解。

过 于 谨 慎

过于谨慎（也可以理解为假警告）会经常出现。在查找数据流时，如果 IDS 的过滤条件符合数据流而并不与原来打算检测的关键事件相符，那么就属于这种情况。另外如果主机或网络防护对良性数据流加以拒绝并记入日志，也可称之为过于谨慎。

固定格式和自由格式

首批提交的 GIAC 入侵检测实习报告并没有严格的格式，即可根据个人情况自由设置。其结果很有意思。有些学生充分利用了自由格式的随意性，从而制作了很有新意的入侵分析实例。但实践经验比较少的学生则茫然不知所措，因此提交的报告可以算是一塌糊涂。另外由于需要对报告进行评分，而评判自由格式的报告就困难得多。所以随着时间推移，目前已经形成了一套标准的实习报告格式，这也是 GIAC 证书课程的基础。

过于大意

过于大意是指关键事件出现时，因没有设置有关规则对此加以检测，而使之遗漏；或者是由于主机或网络边界设备没有识别出关键事件，因此也没有将相应的数据流加以阻塞。很明显，你肯定不希望在 GIAC 上，或者学生的实习报告中看到这种情况。明智的分析员为了杜绝这种过于大意的现象发生，会不断地测试各种可能的过滤条件。他（她）还会花时间针对其他理解，重新对数据流进行访问。

误解

如果利用过滤条件能够检测到相应数据流，而且根据边界防范措施可以按需要通过或拒绝数据流，那么就会出现误解的情况，即虽然你认为对数据流有充分的了解，但实际上你的想法可能是错的。

2.2 分析实例

正是由于存在以上 3 个问题，所以才需要制定实习报告的格式。这种设计需要分析员对跟踪情况进行充分的检查。在上课时，我们就告诉学生不要因为一只鸭子有毛就急于称之为鸭子，最好再花些时间看看它会不会呷呷地叫，而且会不会摇摇摆摆地走路。同样地，我们也可以把 ICMP 主机不可到达消息比作鸭子，来说明从多角度进行分析的重要性。以下是一个简单的跟踪情况：