Fadia道德黑客丛书

ANKIT FADIA 著
孟庆华 译

An Ethical Hacking Guide to Corporate Security

公司安全

——道德黑客攻防指导

电子科技大学出版社

公司安全

——道德黑客攻防指导

法迪亚　著

孟庆华　译

电子科技大学出版社

图书在版编目（CIP）数据

公司安全——道德黑客攻防指导 / 法迪亚著；孟庆华译. —成都：电子科技大学出版社，2007.6

ISBN 978-7-81114-480-2

Ⅰ. 公… Ⅱ. ①法…②孟 … Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 081132 号

公司安全——道德黑客攻防指导

法迪亚 著

孟庆华 译

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）

策划编辑：郭　庆

责任编辑：杜亚提

主　　页：www.uestcp.com.cn

电子邮箱：uestcp@uestcp.com.cn

发　　行：新华书店经销

印　　刷：成都理工大学印刷厂

成品尺寸：185mm×260mm　印张　11.5　字数　280　千字

版　　次：2007 年 6 月第一版

印　　次：2007 年 6 月第一次印刷

书　　号：ISBN 978－7－81114－480－2

定　　价：28.00 元

Ankit Fadia 生命中的里程碑

10岁——父母在家给他配置了一台个人电脑。

12 岁——表现出对计算机的超常天赋，成为无师自通的少年黑客。

14岁——出版了第一本个人专著——An Unofficial Guide to Ethical Hacking（良性入侵——道德黑客非官方指导），轰动业界，迅即被翻译成11 种语言，在全球15个国家出版发行，并被亚洲和北美的一些著名高校选作教学用书。

16岁——9 · 11 事件后，成立了法迪亚道德黑客国际研究院，曾为机密情报机构破译了由本 · 拉登恐怖分子网络发送的加密的电子邮件。自从那时FADIA就介入了与国际安全和计算机网络有关的多个机密工程，负责处理机密情报机构的亚洲行动。

21岁——成为道德黑客的年轻领袖，出版了11 本畅销书，在25 个国家发表了超过1000 次研讨会,获得了45 个奖励。

22岁——致力于数字智能、安全咨询和培训等方面研究，规划并开发出法迪亚道德黑客培训认证体系，并在新加坡管理大学的信息系统学院、美国圣何塞州立大学得到了成功的应用。

2007年——来到中国。

前　言

随着计算机与互联网的迅速普及，人类对计算机的依赖达到了前所未有的程度，计算机的安全直接关系到个人、企业、国家乃至人类社会的生存和发展。而对计算机与互联网构成最严重威胁的，正是防不胜防的网络黑客。纵观当今的互联网业界，病毒木马泛滥、黑客攻击猖獗，各种病毒变体花样百出，恶意攻击手段层出不穷。如何防黑、反黑、制黑，已成为所有互联网用户共同面对的巨大挑战。

上海兴韦教育集团及旗下的上海托普信息技术学院，利用自身的产业背景和专业优势，首度全面引进了国际互联网界资深反恐反黑精英、少年成名的网络安全大师 ANKIT FADIA 的系列专著——“法迪亚道德黑客丛书”。力图从黑客攻防两个角度，将国际最前沿的网络安全技术介绍给国内读者，帮助国内网络用户知黑、防黑、反黑，共同营造和维护健康、安全的互联网世界。

本书是“法迪亚道德黑客丛书”中，专门针对公司、企业类用户的网络安全专著。本书从黑客攻击和安全防护两个角度对公司安全的各个层次作了深入细致的探讨，对于公司的核心技术和商业机密提供了全方位的安全保障。内容涉及公司安全的各个方面：E-mail 安全、即时通信安全、知识产权威胁、身份攻击、输入验证攻击、拒绝服务攻击、缓冲区攻击和社会工程攻击。此书已被新加坡管理大学指定为计算机安全的专用教材。

本书主要由孟庆华博士主持翻译、统稿、审校。朱莹博士参与翻译了第一、二、五、九章，陆星家博士参与翻译了第三、四、八章，齐金鹏博士参与翻译了第六、七章。由于译者水平有限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

有关全套“法迪亚道德黑客丛书”的出版情况，敬请登陆 http://www.e-hacker.info.

译　者

兴韦—法迪亚网络与信息安全中心（中国）

上海托普信息技术学院

2007 年 5 月 18 日

目　录

第一章　电子邮件入侵

威胁等级：高
难易等级：高
突发等级：低

商业威胁

知识产权盗取、社会工程学攻击、商业间谍信息刺探、关键商业设施病毒攻击、诽谤企业财团老板、在线滥用。

引　言

电子邮件是因特网最普遍的使用方式之一，常见的几种有：和亲戚朋友们保持联系、在几分钟之内结束商务交易、给地址簿中所有的地址转发大量的邮件。电子邮件已经在各个领域内迅速取代了传统信件，并且已经成为绝大部分人所喜爱的通信方式。然而，一封电子邮件所包含的信息绝不如它第一眼看起来那么安全。随着电子邮件的迅速普及，里面存在很多危险因素、弊端和问题。

电子邮件已经普及，特别是在商业领域中使用广泛，绝大部分生意都离不开电子邮件。但是，尽管电子邮件正在迅速普及为大众喜爱的通信方式，但是只有少量的人真正意识其内在的安全隐患。在最近几年中，因特网上电子邮件诈骗犯罪数量激增。因此，采取必要的防范措施对电子邮件欺诈行为进行控制已经变得尤为重要。大多数因特网用户使用标准电子邮件客户端程序来收发信件，诸如：Outlook Express、Eudora Pro、Opera 等等。在过去，电子邮件客户端程序高度发达，速度很快，易于使用。在使用电子邮件客户端程序时，用户不会去关心其内部系统的操作。事实上，在因特网上每收发一封电子邮件，都有一系列特定的、预先定义好的规则被执行。为了深入理解电邮的工作原理、特点和安全风险，首先需要知道一些不同的协议：

（1）简单邮件传输协议（SMTP Port 25）

（2）邮局协议（POP Port 110）

每当用户写好一封电子邮件并在因特网上发送，就相应地执行了简单邮件传输协议（SMTP）。

商业范畴

电子在很多场合经常被滥用，内部心怀不满的员工和外部恶意攻击者盗取知识产权、进行滥用攻击、利用社会工程学来散播虚假行情、敲诈勒索、发送垃圾信息、盗取身份、发布炸弹邮件等。攻击者有时也为了用电子邮件伪装身份或身份劫持的手段，以侵犯雇员、客户或者媒体代表。

电子邮件威胁

几乎全球的雇员每天都收发公司或者个人的电子邮件，最常见的和电子邮件有关的威胁如下：

（1）几乎没有几家公司使用加密的电子邮件。因特网上的大多数邮件以明文的形式发送而导致被一个简单的 sniffer 程序记录和破解。因此，电子邮件为坏蛋分子提供了提取信息进行盗窃的作案机会。电子邮件不仅使私人谈话处于危险之中，更使敏感的生意信息被简单的 sniffer 软件工具所破获。

（2）几乎所有基于 ISP 或者网络的正规电子邮件系统都依靠外部的未经认证的系统来发送从出发地到目的地的邮件。这意味着当邮件从一个地方被送至另一个地方时，坏蛋分子就有很多方法获取邮件的敏感内容。

（3）对攻击者来说，给受害者发送匿名垃圾邮件非常容易。绝大部分因特网上的性骚扰和精神恐吓犯罪都是通过 IM 或者电子邮件施行的。办公室的在线性骚扰行为已经很普遍，因此，公司和个人在使用电子邮件时应当非常小心。

（4）大多数雇员使用主流电子邮件客户端程序来收发邮件，诸如 Outlook Express、Microsoft Outlook、Eudora Pro 等等。电子邮件的流行也导致了病毒的大量孳生。如今，大量的蠕虫病毒首选电子邮件系统作为传播媒体。由此不幸的是，因特网上的主要蠕虫病毒利用上述电子邮件客户端许多安全漏洞达到了传播目的。因此，公司必须采取必要措施来阻止蠕虫病毒在邮件客户端上的传播。

（5）另一个电子邮件客户端的常见问题是：当用户在进行身份确认时，其用户名和密码一起以明文的形式送至邮件服务器，这样，攻击者很容易使用 sniffer 软件窃取密码并进行恶意犯罪。而且，如果用户使用了保存密码等功能，即在本地机上保存了该电子邮件账户和密码，那么攻击者只要用一个简单的密码破解工具就能破解该用户的密码。

（6）伪造电子邮件已成为普遍的严重问题：攻击者发送伪造的邮件给第三方，即客户、合作人或者消费者，使被伪造者含冤。这样的伪造邮件攻击很容易造成一系列的误解导制取消订单、破坏合作关系、毁坏公司名誉、导致大量的商业资金损失等。

（7）攻击者通常针对人或者计算机两个方面，利用电子邮件可进行社会工程学攻击。他们通过社会工程学攻击等来获取更多信息。

（8）大多在线电子邮件供应商对入侵式非法攻击束手无策，诸如 DOS 攻击、缓存器溢出等等一系列行为。

（9）用户最头痛的要属垃圾邮件了。最近一份报告显示因特网上有多于 70% 的邮件都

是垃圾邮件。垃圾邮件不仅阻塞了你的收件箱，还导致了大量时间和资源的浪费。

商业威胁、诈骗和犯罪

（1）你的雇员正在通过电子邮件把公司的敏感信息泄露给坏蛋分子吗？

（2）你确信自己的官方机密要函没有被恶意攻击者所注意和记录吗？坏蛋分子是否在伪造看似从你的账户发送的邮件给客户？由此而影响了你的声誉？

（3）你女儿是否收到大量乱七八糟的性骚扰邮件？

实例分析

某国：教育部

某天某国某院校的一名学生准备了一份诽谤部分教授和学生的新闻爆料。他设法用伪造的电子邮件地址将该新闻发送给国家主流媒体机构。他伪造的电子邮件地址看起来似乎是从该校的通信社发出来的。除了一部分报社记者在刊登这则新闻之前曾与校方代表通气，其他几个媒体并未及时与校方沟通就擅自发布了该条新闻。新闻文章在当地媒体见报后，校方官员为之震惊并要求给予调查。但是不幸已经发生，回天乏力。

- 给学校以及相关人员带来不幸。
- 使一部分人处于窘困尴尬的境地。
- 给这部分人的工作生活带来麻烦。

各种各样：涉及个人生活

电子邮件已在世界范围内成为办公室、家庭所喜爱使用的通信方式。如今，大量朋友之间的私人联系和商业公务活动几乎都通过电子邮件进行。电子邮件的普及使用使得在全球范围内出现了各式各样的有关电子邮件的网络犯罪。本节将列出在全球范围内最常见的几种和电子邮件有关的网络犯罪：

- 讹诈、恶作剧或者对个人情感生活的骚扰。
- 性骚扰。
- 恐吓受害者家属而进行敲诈勒索。
- 用伪造的电子邮件在夫妻或者好友之间挑拨离间。

某国某市：个案

一名警察署官员的女儿刚考进大学不久突然收到一系列对其进行性骚扰恐吓的电子邮件，声称如果不将××罪犯释放的话，将无休止地骚扰下去，而该名罪犯就是被这位女孩的父亲关押进监狱的。当然警署不可能答应攻击者的无理要求。召集计算机法律专家开始着手调查此案，他们分析受害者收到的骚扰邮件，找出证据对其进行起诉。然而调查显示受害人收到的都是伪造地址的电子邮件。这表明攻击者是在某个连接到远处的邮件服务器的子网吧内，发送假签名的骚扰邮件给受害者的。此事持续了将近数月，受害人不断地收到骚扰邮件，但计算机专家们依然无法找到罪犯。计算机专家们想尽了一切办法：与当地

ISP运营商联系、向当地的网吧业主询问，但都收效甚微。攻击者很精明，他从来不在同一家网吧出现两次。所幸的是，后来攻击者发送骚扰邮件的频率慢慢下降，最后也不再收到了。此案再次说明了攻击者在网吧利用伪造的电子邮件，可以使自己的身份不被暴露和发现地进行犯罪活动。网络犯罪有数不尽的害处：

- 给受害者及其家属带来精神上的折磨。
- 受害者不得不频繁地更换电子邮件地址以防止再收到骚扰邮件。
- 给这部分人的工作生活带来麻烦。

某国某市：个案

在某国某市，有位在跨国公司供职的工程师。他收入颇丰并且享有较高的威望和地位。某天他收到来自另外一家跨国企业一封电子邮件，声称可以给他更高职位和薪水的工作，而且该工作也更具挑战性并充满了乐趣。接下来的几封邮件允诺他在公司当一个大项目的经理，于是，他大胆地辞去了现有的稳定工作，准备接受那份激动人心的新工作。当他兴冲冲地前往邮件合同里所显示的新公司地址时，却发现根本就没有这个岗位，而且使他最受打击的是，所谓给他发邮件的未来老板根本就不在那家公司。

- 受害者失去了他原本的稳定工作。
- 人财两空。
- 不得不重新开始找工作。
- 受害人原来的公司失去了一名经验丰富的人才。

某国某市：零售部门

某国某市零售巨头之一发现其第一季度利润猛增了17%。投资人和董事会主管因此而兴奋无比，庆祝了一番。但就在公司大获成功之际，某天早上公司所有的员工、合伙人、供应商，以及数以百万计的客户收到了一封冒充公司总裁写的邮件。不仅如此，恶意攻击者还给供应商和合伙人发送伪造的电子邮件取消或者更改订单。虽然公司尽一切可能立即采取了抵制措施，但已经影响了客户感情。由于一系列的相关原因，该零售业巨头当年利润严重下滑。

- 公司及总裁的声誉受损。
- 带来经济损失。
- 恶意中伤使得商业竞争加剧。
- 销售量下降。
- 与合伙人、联盟及其他人的良好信誉合作关系受损。

电子邮件威胁的种类

如上所列，因特网上有多种跟电子邮件有关的威胁。其中比较常见的攻击如下：

（1）骚扰邮件。

（2）伪造邮件。

（3）垃圾邮件。

骚扰邮件

引言

想要真正解决性骚扰邮件问题，我们首先得明白电子邮件在因特网上是怎样传播的。电子邮件在因特网上从源计算机传送到目的计算机跟我们日常生活中的传统邮件方式差不多。

在通常情况下，电子邮件发送者连接到邮件服务器，相当于现实生活中的邮局，将邮件发送到某个指定的地址。接着，从源邮件服务器发出的电子邮件通过一系列中间邮件服务器，最终到达真正的目的地址。换句话说，每封邮件从某个特定的邮件服务器产生，并途径一系列不同的中间邮件服务器，最终到达真正的目的地。

发送者发件箱→源邮件服务器→些中间邮件服务器→目的邮件服务器→目的收件箱

这就是说，如果能够精确定位到某封电子邮件的源邮件服务器，那么就可以查明发送这封电子邮件的人的身份。当某封电子邮件在因特网上被传送时，其中包含了真正的邮件内容信息和其经过的路径信息。在邮件头部包含了这封邮件的路径信息如图 1-1 所示。这意味着只要逆向地读取该邮件的路径信息，就可以轻易寻找到其源头。所以每当收到骚扰邮件后，可以打开邮件的头部，读取信息，追溯其发源处。但统计显示，人们收到此类邮件的最普通的反应就是按下“删除”键，把该邮件删了。毕竟忽视和逃避不是解决此类问题的办法。

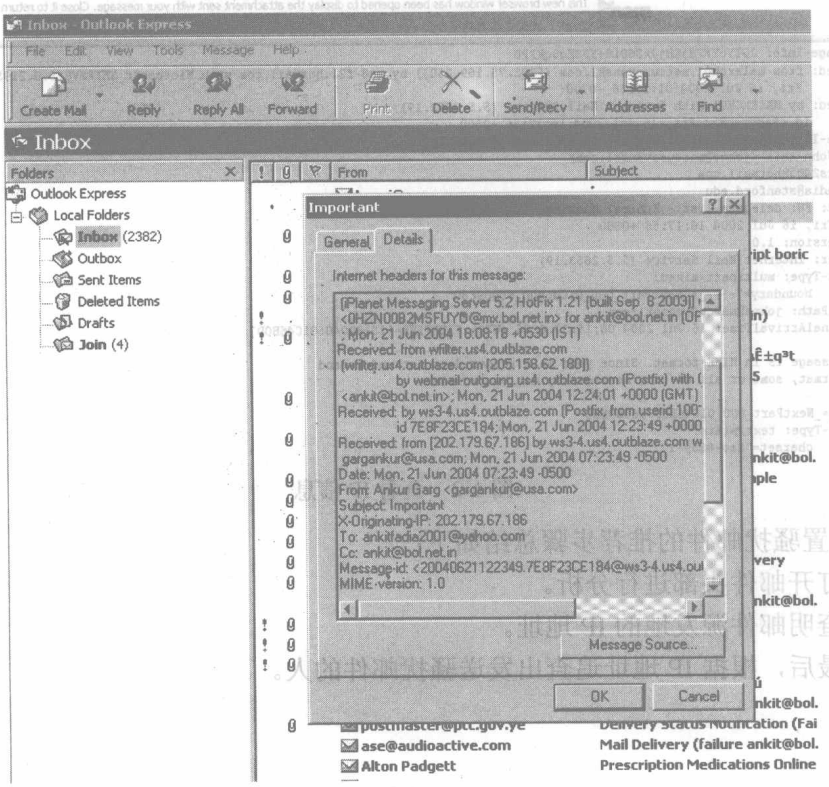

图 1-1　邮件头部信息

当收到骚扰邮件的理想解决办法是按照以下步骤试着追查到发送该邮件人的身份：

（1）查看所收到骚扰邮件的头部信息。

（2）确认用来发送该邮件的计算机的 IP 地址。

（3）根据 IP 地址查明罪犯的身份。

攻击原理

研究分析电子邮件头部，首先应当找出如下的内容：

X－源－IP：XX.xx.XX.xx

上面一行包括了发送邮件系统的 IP 地址。找到源 IP 地址后，立即开始追查，不用再去阅读邮件头部的其他信息，如图 1-2 所示。

只要使用邮件客户端软件或者邮件网页上的“选择/功能”按钮，就能激活整个电子邮件头部，使之与邮件客户端所提供的服务无关，变成“完整头部/高级头部”。当邮件头部被激活后，每封邮件就将显示各自的头部信息。总之，每当收到骚扰邮件和猥亵邮件，所需要做的就是研究其头部信息，以查出发送者的 IP 地址。可以采用前面所讨论过的 LINK 技术来查明其 IP 地址。

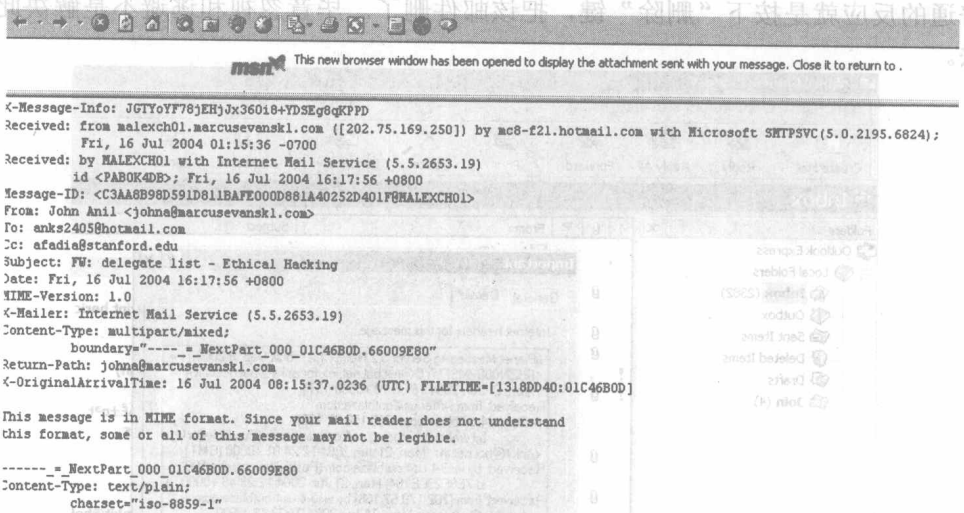

图 1-2　查看 IP 信息

如何处置骚扰邮件的推荐步骤总结如下：

（1）打开邮件头部进行分析。

（2）查明邮件源发地的 IP 地址。

（3）最后，根据 IP 地址追查出发送骚扰邮件的人。

攻击原理

大多数的邮件客户端会生成一个脚本文件，记录所有用户给邮件服务器发出的发送该邮件的 SMTP 命令。在多数情况下，这个脚本文件通常都存储在邮件客户端的默认目录下面，其中的数据由 Windows 注册文件生成。例如，Outlook Express 在一个名称为 smtp.log 的脚本文件里记录了所有的 SMTP 命令，这个脚本文件储存在 c:/windows/application data 文件目录下。以下就是摘自 Outlook Express 脚本文件的内容：

Outlook Express 5.00.2314.1300
SMTP Log started at 10/08/1999 150033
SMTP 150115 [rx] 220 delhi1.mtnl.net.in ESMTP Sendmail 8.9.1
(1.1.20.3/16Sep99-0827PM) Fri, 8 Oct 1999 145017 +0530 (IST)
SMTP 150115 [tx] HELO hacker
SMTP 150115 [rx] 250 delhi1.mtnl.net.in Hello [203.xx.248.175], pleased
to
meet you
SMTP 150116 [tx] MAIL FROM <ankit@bol.net.in>
SMTP 150116 [rx] 250 <ankit@bol.net.in>... Sender ok
SMTP 150116 [tx] RCPT TO <billgates@hotmail.com>
SMTP 150116 [rx] 250 <billgates@hotmail.com>... Recipient ok
SMTP 150116 [tx] DATA
SMTP 150116 [rx] 354 Enter mail, end with "." on a line by itself
SMTP 150120 [tx]

SMTP 150123 [rx] 250 OAA0000014842 Message accepted for delivery
SMTP 150123 [tx] QUIT
SMTP 150123 [rx] 221 delhi1.mtnl.net.in closing connection

要注意的是，从邮件客户端“已发送”文件夹里删除邮件并未在脚本文件中删除 SMTP 命令。因此，计算机法庭调查员只要阅读存储着的应用脚本文件，往往就能够再次模拟网络犯罪。

Fadia 精选的主流电子邮件威胁工具

1．工具名称：NeoTracePro

特点： 非常棒的软件工具，它可以使你追查到 IP 地址的地理位置，在世界地图上找到主机所在地。它非常精确、快速，具有一系列很有用的功能。可以在线使用许多高级功能，如图 1-3 所示。

下载链接地址： http://www.neotrace.com

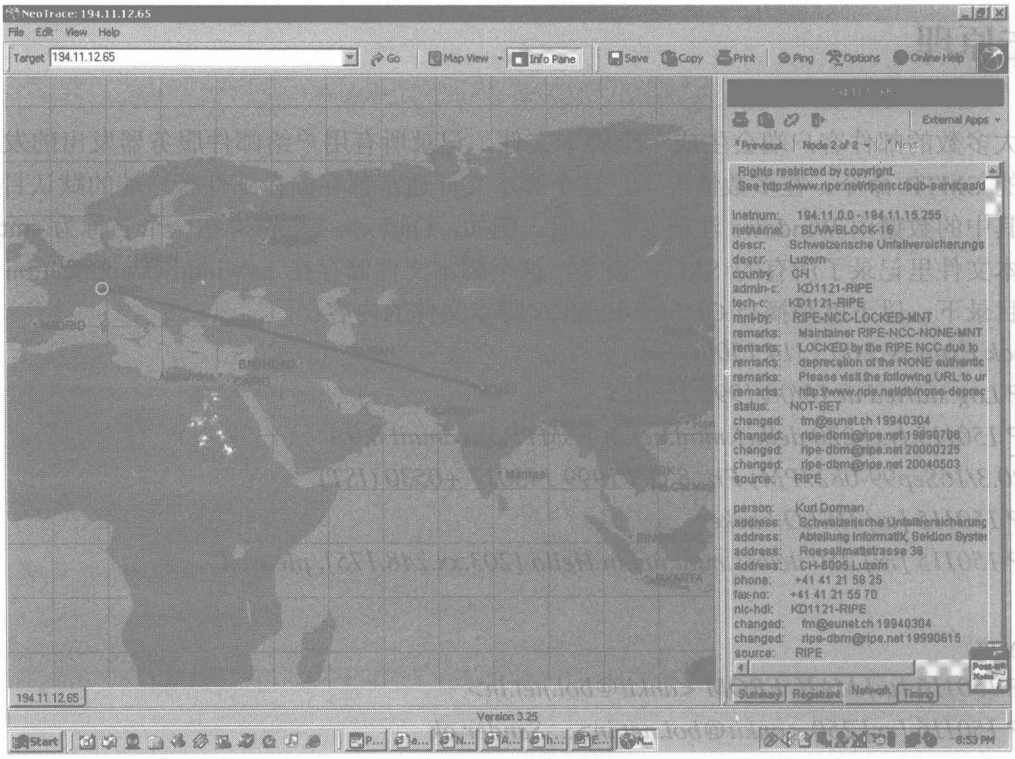

图 1-3 NetoTracepro 界面

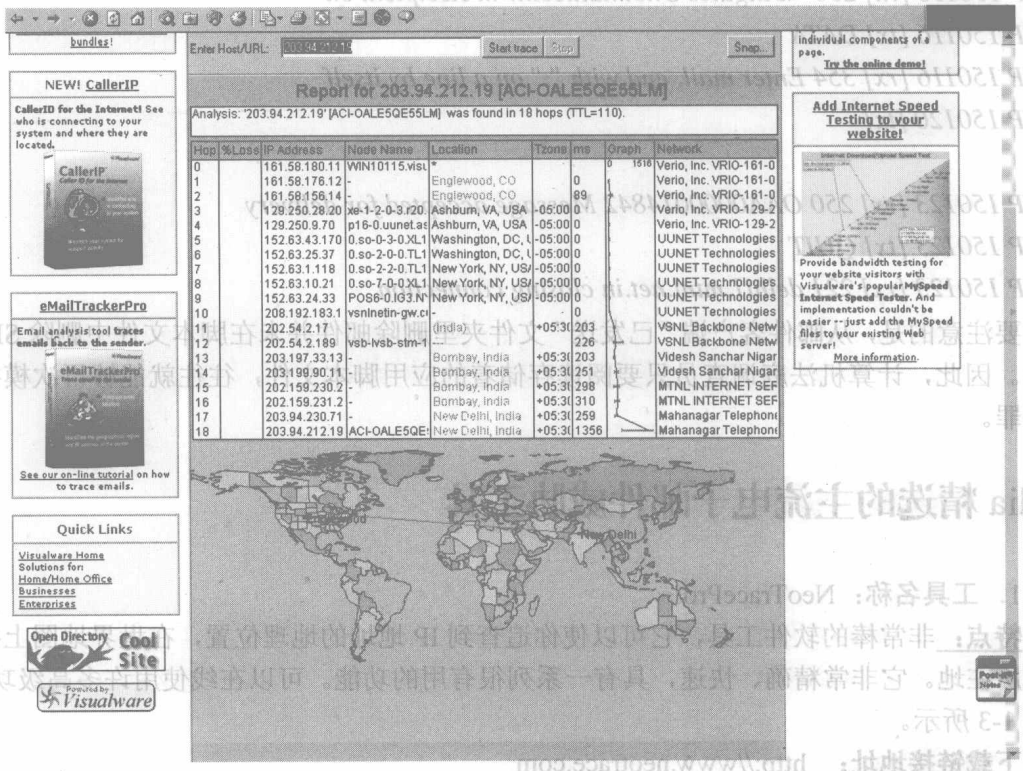

图 1-4 VisualRoute

2. 工具名称： VisualRoute

特点：另一个可以让你追查到因特网上主机 IP 地址的地理位置的可视化软件。同类软件中的 JAVA 版本可以免费获得，如图 1-4 所示。

下载链接地址： http://visualroute.visualware.com

3. 工具名称： eMailTrackerPro

特点： 该工具软件使用户能对邮件发送者在世界地图上进行地理定位。在追踪主机的 IP 地址不同，这个软件能找到电子邮件的源发送系统，如图 1-5 所示。

下载链接地址： http://www.visualware.com/personal/download/index.html

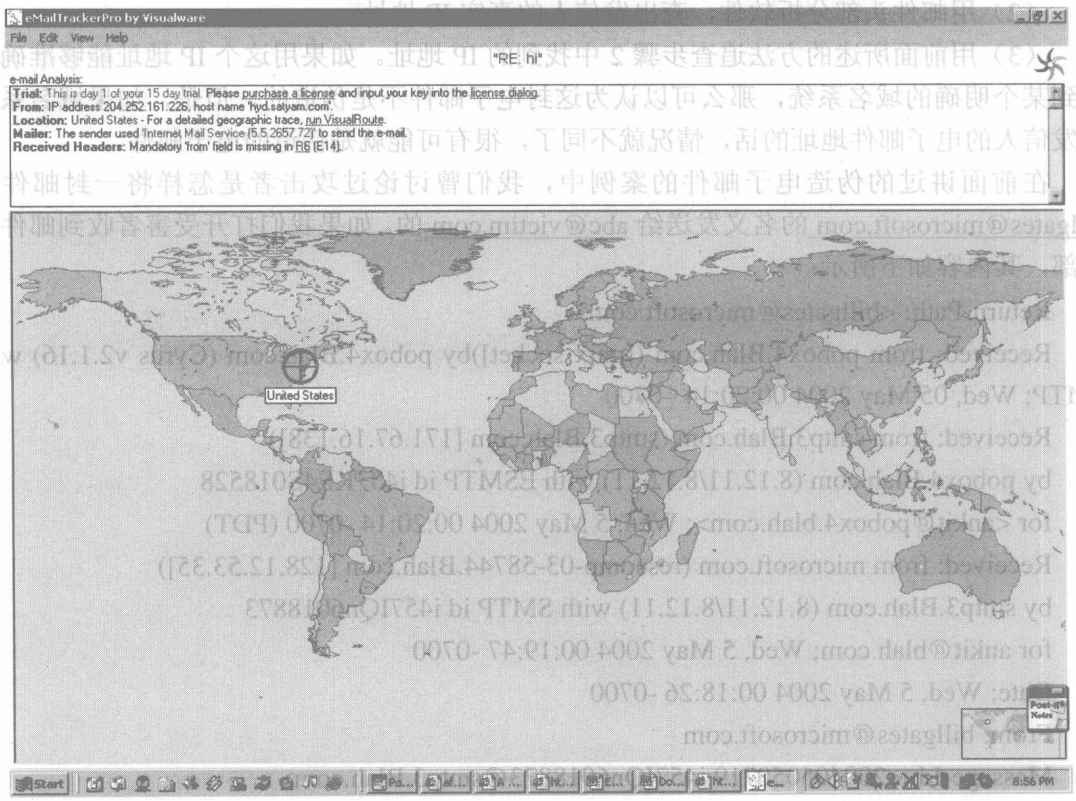

图 1-5 eMailTrackerPro

对 策

所幸的是，伪造的电子邮件并不如其看上去地那么完美。有很多技术手段可以查明某封电子邮件是否属于伪造信件。如果你怀疑某封电子邮件是伪造的，那么按照以下的简单检查步骤就有可能发现邮件的真实来源。为了说明这个问题，让我们回到前面的章节开始讲述电子邮件的伪造过程：

helo microsoft.com

250 mailserver.com Hello abc-03-3414.isp.com [128.12.53.35], pleased to meet you

攻击者用如上所写的一行命令告诉邮件服务器伪造的主机名：“*helo microsoft.com*”. 那

么邮件服务器是怎样响应这行命令的呢？ 服务器给予攻击者热忱欢迎，同时也验明其真正的 IP 地址，或者查清攻击者使用的系统主机名。于是，攻击者所使用系统的 IP 地址为：abc-03-3414.isp.com [128.12.53.35].

换句话说，即使攻击者通过给服务器提供假域名来伪造电子邮件头部，服务器仍然能够识别攻击者真正的 IP 地址。一旦邮件服务器在 helo 命令行确认了攻击者真实身份，就会自动将攻击者的 IP 地址添加到发送出去的邮件头部。就是说，当收到可疑邮件时，按照下面的步骤，你可以轻而易举地验明邮件的身份。

（1）查看可疑邮件的头部。

（2）用邮件头部分析软件，查出发信人的真实 IP 地址。

（3）用前面所述的方法追查步骤 2 中找到的 IP 地址。如果用这个 IP 地址能够准确定位到某个明确的域名系统，那么可以认为这封电子邮件不是伪造的。但是，如果域名系统是发信人的电子邮件地址的话，情况就不同了，很有可能就是伪造的电子邮件。

在前面讲过的伪造电子邮件的案例中，我们曾讨论过攻击者是怎样将一封邮件以 billgates@microsoft.com 的名义发送给 abc@victim.com 的。如果我们打开受害者收到邮件的头部，其内容如下所示：

Return-Path: <billgates@microsoft.com>

Received: from pobox4.Blah.com ([unix socket])by pobox4.Blah.com (Cyrus v2.1.16) with LMTP; Wed, 05 May 2004 00:20:14 –0700

Received: from smtp3.Blah.com (smtp3.Blah.com [171.67.16.138])

by pobox4.Blah.com (8.12.11/8.12.11) with ESMTP id i457KE4S018528

for <ankit@pobox4.blah.com>; Wed, 5 May 2004 00:20:14 -0700 (PDT)

Received: from microsoft.com (rescomp-03-58744.Blah.com [128.12.53.35])

by smtp3.Blah.com (8.12.11/8.12.11) with SMTP id i457IQn6018873

for ankit@blah.com; Wed, 5 May 2004 00:19:47 -0700

Date: Wed, 5 May 2004 00:18:26 -0700

From: billgates@microsoft.com

Message-Id: <200405050719.i457IQn6018873@smtp3.Blah.com>

To: abc@victim.com

这封邮件在收件客户端或者供应商提供的收邮件网页上显示的是从 billgates@microsoft.com 发过来的。但只要检查邮件头部，就可以很明显地看出来是封伪造的邮件。关键的地方如下：

Received: from microsoft.com (rescomp-03-58744.Blah.com [128.12.53.35]) by smtp3.Blah.com (8.12.11/8.12.11) with SMTP id i457IQn6018873 for ankit@blah.com; Wed, 5 May 2004 00:19:47 -0700

从上面那行就能看出这封邮件不是从“microsoft.com”这个域名发送的。请注意圆括号内的内容显示了发送邮件的真正 IP 地址： *128.12.53.35.* 用软件查明这个 IP 地址不是微软系统，而是斯坦福大学的计算机。所以，可以立即下结论：这封邮件是伪造的，是某人从斯坦福大学发出来的。

实例分析

以下是一些电子邮件的头部，并给出了简单的分析其是否属于伪造信件：

例 1：

Return-Path: <Bltoddy@aol.com>

Received: from smtp3.Blah.com (8.12.11/8.12.11) by pobox4.Blah.com (Cyrus v2.1.16) with LMTP; Mon, 22 Mar 2004 12:28:42 -0800

Received: from Bltoddy.blah.com ([203.11.12.56])by smtp3.Blah.com (8.12.11/8.12.11) with ESMTP id i2MKSfQI025425 for <ankit@blah.com>; Mon, 22 Mar 2004 12:28:42 -0800

From: Bltoddy@aol.com

Message-ID: <9f.4a120032.2e27987d@aol.com>

Date: Thu, 15 Jul 2004 04:21:17 EDT

Subject: Hi

To: ankit@blah.com

MIME-Version: 1.0

Content-Type: multipart/related; boundary="part1_9f.4a120032.2e27987d_boundary"

1．发件人地址： Bltoddy@aol.com

2．源 IP 地址： 203.11.12.56

3．源邮件服务器： smtp3.Blah.com

4．邮件客户端： 无。

5．路径：

信源→邮件服务器→下一个邮件服务器→目的地址

用可视化的软件来定位邮件的源 IP 地址，就可以看到是发件人的域名而不是邮件服务器。因此，上面所示的是一封伪造的电子邮件。

例 2：

Return-Path: <Nikhil@abcd.com>

Received: from pobox4.Blah.com ([unix socket])by pobox4.Blah.com (Cyrus v2.1.16) with LMTP; Tue, 06 Jul 2004 02:29:32 –0700

X-Sieve: CMU Sieve 2.2

Received: from leland3.Blah.com (leland3.Blah.com [171.67.16.108])

by pobox4.Blah.com (8.12.11/8.12.11) with ESMTP id i669TWKq018389

for <ankit@pobox4.blah.com>; Tue, 6 Jul 2004 02:29:32 -0700 (PDT)

Received: from njpmail.abcd.com (njpmail.abcd.com [204.179.188.132])

by leland3.Blah.com (8.12.11/8.12.11) with ESMTP id i669TS8P008290

for <ankit@blah.com>; Tue, 6 Jul 2004 02:29:30 -0700

Received: from hyd.abcd.com (hyd.abcd.com [204.252.161.226])

by njpmail.abcd.com (8.11.6/8.11.6) with ESMTP id i668f9x09227

for <ankit@blah.com>; Tue, 6 Jul 2004 04:41:22 -0400