网络安全

安全技巧（六）

小未 主编

目　录

解读防火墙记录 1
深入浅出谈防火墙 30
防火墙原理入门 42
信息安全话题之一:文件加密 48
网络防黑初步 51
虚拟专网的加密算法说明 54
防火墙功能指标详解.....57
虚拟专网的加密算法说明 62
查看开放端口判断木马的方法.....65
未来电子战，中国获胜的几率有多大 69
如何定制企业防火墙安全机制.....74
选择网络防病毒系统需要考虑的六个方面.....81
Linux 网络安全之经验谈 84
SSL 的安全漏洞及解决方案 91
防范 WindowsXP 的安全策略 106
管理信息系统安全方案详解 110
提高系统安全的注册表修改秘籍.....122

解读防火墙记录

本文将向你解释你在防火墙的记录（Log）中看到了什么？尤其是那些端口是什么意思？你将能利用这些信息做出判断：我是否受到了 Hacker 的攻击？他/她到底想要干什么？本文既适用于维护企业级防火墙的安全专家，又适用于使用个人防火墙的家庭用户。

现在个人防火墙开始流行起来，很多网友一旦看到报警就以为受到某种攻击，其实大多数情况并非如此。

一、目标端口 ZZZZ 是什么意思

所有穿过防火墙的通讯都是连接的一个部分。一个连接包含一对相互“交谈”的 IP 地址以及一对与 IP 地址对应的端口。目标端口通常意味着正被连接的某种服务。当防火墙阻挡（block）某个连接时，它会将目标端口“记录在案”(logfile)。这节将描述这些端口的意义。

端口可分为 3 大类：

1）公认端口（WellKnownPorts）：从 0 到 1023，它们紧密绑定于一些服务。通常这些端口的通讯明确表明了某种服务的协议。例如：80 端口实际上总是 HTTP 通讯。

2）注册端口（RegisteredPorts）：从 1024 到 49151。它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其它目的。例如：许多系统处理动态端口从 1024 左右开始。

3)动态和/或私有端口(Dynamicand/orPrivatePorts)：从 49152 到 65535。理论上，不应为服务分配这些端口。

实际上,机器通常从 1024 起分配动态端口。但也有例外：SUN 的 RPC 端口从 32768 开始。

从哪里获得更全面的端口信息：

1．ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers

"AssignedNumbers"RFC，端口分配的官方来源。

2．http://advice.networkice.com/advice/Exploits/Ports/

端口数据库，包含许多系统弱点的端口。

3．/etc/services

UNIX 系统中文件/etc/services 包含通常使用的 UNIX 端口分配列表。WindowsNT 中该文件位于%systemroot%/system32/drivers/etc/services。

4．http://www.con.wesleyan.edu/~triemer/network/docservs.html

特定的协议与端口。

5．http://www.chebucto.ns.ca/~rakerman/trojan-port-table.html

描述了许多端口。

6．http://www.tlsecurity.com/trojanh.htm

TLSecurity 的 Trojan 端口列表。与其它人的收藏不同，作者检验了其中的所有端口。

7．http://www.simovits.com/nyheter9902.html

TrojanHorse 探测。

二、通常对于防火墙的 TCP/UDP 端口扫描有哪些？

本节讲述通常 TCP/UDP 端口扫描在防火墙记录中的信息。记住：并不存在所谓 ICMP 端口。如果你对解

读 ICMP 数据感兴趣，请参看本文的其它部分。

0 通常用于分析操作系统。这一方法能够工作是因为在一些系统中“0”是无效端口，当你试图使用一种通常的闭合端口连接它时将产生不同的结果。一种典型的扫描：使用 IP 地址为 0.0.0.0，设置 ACK 位并在以太网层广播。

1tcpmux 这显示有人在寻找 SGIIrix 机器。Irix 是实现 tcpmux 的主要提供者，缺省情况下 tcpmux 在这种系统中被打开。Iris 机器在发布时含有几个缺省的无密码的帐户，如 lp,guest,uucp,nuucp,demos,tutor,diag,EZsetup, OutOfBox,和 4Dgifts。许多管理员安装后忘记删除这些帐户。因此 Hacker 们在 Internet 上搜索 tcpmux 并利用这些帐户。

7Echo 你能看到许多人们搜索 Fraggle 放大器时，发送到 x.x.x.0 和 x.x.x.255 的信息。

常见的一种 DoS 攻击是 echo 循环（echo-loop），攻击者伪造从一个机器发送到另一个机器的 UDP 数据包，而两个机器分别以它们最快的方式回应这些数据包。(参见 Chargen)

另一种东西是由 DoubleClick 在词端口建立的 TCP 连接。有一种产品叫做“ ResonateGlobalDispatch ”，它与 DNS 的这一端口连接以确定最近的路由。

Harvest/squidcache 将从 3130 端口发送 UDPecho：“如果将 cache 的 source_pingon 选项打开，它将对原始主机的 UDPecho 端口回应一个 HITreply。”这将会产生许多这类数据包。

11sysstat 这是一种 UNIX 服务，它会列出机器上所有正在运行的进程以及是什么启动了这些进程。这为入

侵者提供了许多信息而威胁机器的安全，如暴露已知某些弱点或帐户的程序。这与 UNIX 系统中“ ps ”命令的结果相似

再说一遍：ICMP 没有端口，ICMPport11 通常是 ICMPtype=11

19chargen 这是一种仅仅发送字符的服务。UDP 版本将会在收到 UDP 包后回应含有垃圾字符的包。TCP 连接时，会发送含有垃圾字符的数据流知道连接关闭。Hacker 利用 IP 欺骗可以发动 DoS 攻击。伪造两个 chargen 服务器之间的 UDP 包。由于服务器企图回应两个服务器之间的无限的往返数据通讯一个 chargen 和 echo 将导致服务器过载。同样 fraggleDoS 攻击向目标地址的这个端口广播一个带有伪造受害者 IP 的数据包，受害者为了回应这些数据而过载。

21ftp 最常见的攻击者用于寻找打开“ anonymous ”的 ftp 服务器的方法。这些服务器带有可读写的目录。Hackers 或 Crackers 利用这些服务器作为传送 warez(私有程序)和 pr0n(故意拼错词而避免被搜索引擎分类)的节点。

22sshPcAnywhere 建立 TCP 和这一端口的连接可能是为了寻找 ssh。这一服务有许多弱点。如果配置成特定的模式，许多使用 RSAREF 库的版本有不少漏洞。(建议在其它端口运行 ssh)

还应该注意的是 ssh 工具包带有一个称为 make-ssh-known-hosts 的程序。它会扫描整个域的 ssh 主机。你有时会被使用这一程序的人无意中扫描到。

UDP（而不是 TCP）与另一端的 5632 端口相连意味着存在搜索 pcAnywhere 的扫描。5632（十六进制的 0

x1600）位交换后是 0x0016（使进制的 22）。

23Telnet 入侵者在搜索远程登陆 UNIX 的服务。大多数情况下入侵者扫描这一端口是为了找到机器运行的操作系统。此外使用其它技术，入侵者会找到密码。

25smtp 攻击者（spammer）寻找 SMTP 服务器是为了传递他们的 spam。入侵者的帐户总被关闭，他们需要拨号连接到高带宽的 e-mail 服务器上，将简单的信息传递到不同的地址。SMTP 服务器（尤其是 sendmail）是进入系统的最常用方法之一，因为它们必须完整的暴露于 Internet 且邮件的路由是复杂的（暴露+复杂=弱点）。

53DNSHacker 或 crackers 可能是试图进行区域传递（TCP），欺骗 DNS（UDP）或隐藏其它通讯。因此防火墙常常过滤或记录 53 端口。

需要注意的是你常会看到 53 端口做为 UDP 源端口。不稳定的防火墙通常允许这种通讯并假设这是对 DNS 查询的回复。Hacker 常使用这种方法穿透防火墙。

67 和 68Bootp 和 DHCPUDP 上的 Bootp/DHCP：通过 DSL 和 cable-modem 的防火墙常会看见大量发送到广播地址 255.255.255.255 的数据。这些机器在向 DHCP 服务器请求一个地址分配。Hacker 常进入它们分配一个地址把自己作为局部路由器而发起大量的“中间人”（man-in-middle）攻击。客户端向 68 端口（bootps）广播请求配置，服务器向 67 端口（bootpc）广播回应请求。这种回应使用广播是因为客户端还不知道可以发送的 IP 地址。

69TFTP(UDP)许多服务器与 bootp 一起提供这项服务，便于从系统下载启动代码。但是它们常常错误配置而从系统提供任何文件，如密码文件。它们也可用于向

系统写入文件。

79fingerHacker 用于获得用户信息，查询操作系统，探测已知的缓冲区溢出错误，回应从自己机器到其它机器 finger 扫描。

98linuxconf 这个程序提供 linuxboxen 的简单管理。通过整合的 HTTP 服务器在 98 端口提供基于 Web 界面的服务。它已发现有许多安全问题。一些版本 setuidroot，信任局域网，在/tmp 下建立 Internet 可访问的文件，LANG 环境变量有缓冲区溢出。此外因为它包含整合的服务器，许多典型的 HTTP 漏洞可能存在（缓冲区溢出，历遍目录等）

109POP2 并不象 POP3 那样有名，但许多服务器同时提供两种服务（向后兼容）。在同一个服务器上 POP3 的漏洞在 POP2 中同样存在。

110POP3 用于客户端访问服务器端的邮件服务。POP3 服务有许多公认的弱点。关于用户名和密码交换缓冲区溢出的弱点至少有 20 个（这意味着 Hacker 可以在真正登陆前进入系统）。成功登陆后还有其它缓冲区溢出错误。

111sunrpcportmaprpcbindSunRPCPortMapper/RPCBIND。访问 portmapper 是扫描系统查看允许哪些 RPC 服务的最早的一步。常见 RPC 服务有：rpc.mountd,NFS,rpc.statd,rpc.csmd,rpc.ttybd,amd 等。入侵者发现了允许的 RPC 服务将转向提供服务的特定端口测试漏洞。

记住一定要记录线路中的 daemon,IDS,或 sniffer，你可以发现入侵者正使用什么程序访问以便发现到底发生了什么。

113Identauth 这是一个许多机器上运行的协议，用

于鉴别 TCP 连接的用户。使用标准的这种服务可以获得许多机器的信息（会被 Hacker 利用）。但是它可作为许多服务的记录器，尤其是 FTP,POP,IMAP,SMTP 和 IRC 等服务。通常如果有许多客户通过防火墙访问这些服务，你将会看到许多这个端口的连接请求。记住，如果你阻断这个端口客户端会感觉到在防火墙另一边与 e-mail 服务器的缓慢连接。许多防火墙支持在 TCP 连接的阻断过程中发回 RST，着将回停止这一缓慢的连接。

119NNTPnews 新闻组传输协议，承载 USENET 通讯。当你链接到诸如：news://comp.security.firewalls/.的地址时通常使用这个端口。这个端口的连接企图通常是人们在寻找 USENET 服务器。多数 ISP 限制只有他们的客户才能访问他们的新闻组服务器。打开新闻组服务器将允许发/读任何人的帖子，访问被限制的新闻组服务器，匿名发帖或发送 spam。

135oc-servMSRPCend-pointmapperMicrosoft 在这个端口运行 DCERPCend-pointmapper 为它的 DCOM 服务。这与 UNIX111 端口的功能很相似。使用 DCOM 和/或 RPC 的服务利用机器上的 end-pointmapper 注册它们的位置。远端客户连接到机器时，它们查询 end-pointmapper 找到服务的位置。同样 Hacker 扫描机器的这个端口是为了找到诸如：这个机器上运行 ExchangeServer 吗？是什么版本？

这个端口除了被用来查询服务（如使用 epdump）还可以被用于直接攻击。有一些 DoS 攻击直接针对这个端口。

137NetBIOSnameservicenbtstat(UDP)这是防火墙管理员最常见的信息，请仔细阅读文章后面的 NetBIOS 一

节

139NetBIOSFileandPrintSharing 通过这个端口进入的连接试图获得 NetBIOS/SMB 服务。这个协议被用于 Windows“文件和打印机共享”和 SAMBA。在 Internet 上共享自己的硬盘是可能是最常见的问题。

大量针对这一端口始于 1999，后来逐渐变少。2000 年又有回升。一些 VBS（IE5VisualBasicScripting）开始将它们自己拷贝到这个端口，试图在这个端口繁殖。

143IMAP 和上面 POP3 的安全问题一样，许多 IMAP 服务器有缓冲区溢出漏洞运行登陆过程中进入。记住：一种 Linux 蠕虫（admw0rm）会通过这个端口繁殖，因此许多这个端口的扫描来自不知情的已被感染的用户。当 RadHat 在他们的 Linux 发布版本中默认允许 IMAP 后，这些漏洞变得流行起来。Morris 蠕虫以后这还是第一次广泛传播的蠕虫。

这一端口还被用于 IMAP2，但并不流行。

已有一些报道发现有些 0 到 143 端口的攻击源于脚本。

161SNMP(UDP)入侵者常探测的端口。SNMP 允许远程管理设备。所有配置和运行信息都储存在数据库中，通过 SNMP 客获得这些信息。许多管理员错误配置将它们暴露于 Internet。Crackers 将试图使用缺省的密码“public”“private”访问系统。他们可能会试验所有可能的组合。

SNMP 包可能会被错误的指向你的网络。Windows 机器常会因为错误配置将 HPJetDirectremotemanagement 软件使用 SNMP。HPOBJECTIDENTIFIER 将收到 SNMP 包。新版的 Win98 使用 SNMP 解析域名，你会看见这

种包在子网内广播（cablemodem,DSL）查询 sysName 和其它信息。

162SNMPtrap 可能是由于错误配置

177xdmcp 许多 Hacker 通过它访问 X-Windows 控制台，它同时需要打开 6000 端口。

513rwho 可能是从使用 cablemodem 或 DSL 登陆到的子网中的 UNIX 机器发出的广播。这些人为 Hacker 进入他们的系统提供了很有趣的信息。

553CORBAIIOP(UDP)如果你使用 cablemodem 或 DSLVLAN，你将会看到这个端口的广播。CORBA 是一种面向对象的 RPC（remoteprocedurecall）系统。Hacker 会利用这些信息进入系统。

600Pcserverbackdoor 请查看 1524 端口

一些玩 script 的孩子认为他们通过修改 ingreslock 和 pcserver 文件已经完全攻破了系统--AlanJ.Rosenthal.

635mountdLinux 的 mountdBug。这是人们扫描的一个流行的 Bug。大多数对这个端口的扫描是基于 UDP 的，但基于 TCP 的 mountd 有所增加（mountd 同时运行于两个端口）。记住，mountd 可运行于任何端口（到底在哪个端口，需要在端口 111 做 portmap 查询），只是 Linux 默认为 635 端口，就象 NFS 通常运行于 2049 端口。

1024 许多人问这个端口是干什么的。它是动态端口的开始。许多程序并不在乎用哪个端口连接网络，它们请求操作系统为它们分配“下一个闲置端口”。基于这一点分配从端口 1024 开始。这意味着第一个向系统请求分配动态端口的程序将被分配端口 1024。为了验证这一点，你可以重启机器，打开 Telnet，再打开一个窗口运行“natstat-a”，你将会看到 Telnet 被分配 1024 端口。请

求的程序越多，动态端口也越多。操作系统分配的端口将逐渐变大。再来一遍，当你浏览 Web 页时用“ netstat ”查看，每个 Web 页需要一个新端口。

Version0.4.1,June20,2000

http://www.robertgraham.com/pubs/firewall-seen.html

Copyright1998-2000byRobertGraham(mailto:firewall-seen1@robertgraham.com

Allrightsreserved.Thisdocumentmayonlybereproduced(wholeor

inpart)fornon-commercialpurposes.Allreproductionsmust

containthiscopyrightnoticeandmustnotbealtered,exceptby

permissionoftheauthor.

1025 参见 1024

1026 参见 1024

1080SOCKS

这一协议以管道方式穿过防火墙，允许防火墙后面的许多人通过一个 IP 地址访问 Internet。理论上它应该只允许内部的通信向外达到 Internet。但是由于错误的配置，它会允许 Hacker/Cracker 的位于防火墙外部的攻击穿过防火墙。或者简单地回应位于 Internet 上的计算机，从而掩饰他们对你的直接攻击。WinGate 是一种常见的 Windows 个人防火墙，常会发生上述的错误配置。在加入 IRC 聊天室时常会看到这种情况。

1114SQL

系统本身很少扫描这个端口，但常常是 sscan 脚本

的一部分。

1243Sub-7 木马（TCP）

参见 Subseven 部分。

1524ingreslock 后门

许多攻击脚本将安装一个后门 Shell 于这个端口(尤其是那些针对 Sun 系统中 Sendmail 和 RPC 服务漏洞的脚本，如 statd,ttdbserver 和 cmsd)。如果你刚刚安装了你的防火墙就看到在这个端口上的连接企图，很可能是上述原因。你可以试试 Telnet 到你的机器上的这个端口，看看它是否会给你一个 Shell。连接到 600/pcserver 也存在这个问题。

2049NFS

NFS 程序常运行于这个端口。通常需要访问 portmapper 查询这个服务运行于哪个端口，但是大部分情况是安装后 NFS 运行于这个端口，Hacker/Cracker 因而可以闭开 portmapper 直接测试这个端口。

3128squid

这是 SquidHTTP 代理服务器的默认端口。攻击者扫描这个端口是为了搜寻一个代理服务器而匿名访问 Internet。你也会看到搜索其它代理服务器的端口：8000/8001/8080/8888。扫描这一端口的另一原因是：用户正在进入聊天室。其它用户（或服务器本身）也会检验这个端口以确定用户的机器是否支持代理。请查看 5.3 节。

5632pcAnywere

你会看到很多这个端口的扫描，这依赖于你所在的位置。当用户打开 pcAnywere 时，它会自动扫描局域网 C 类网以寻找可能得代理(译者 指 agent 而不是 proxy)。Hacker/cracker 也会寻找开放这种服务的机器，所以应该

查看这种扫描的源地址。一些搜寻 pcAnywere 的扫描常包含端口 22 的 UDP 数据包。参见拨号扫描。

6776Sub-7artifact

这个端口是从 Sub-7 主端口分离出来的用于传送数据的端口。例如当控制者通过电话线控制另一台机器，而被控机器挂断时你将会看到这种情况。因此当另一人以此 IP 拨入时，他们将会看到持续的，在这个端口的连接企图。（译者：即看到防火墙报告这一端口的连接企图时，并不表示你已被 Sub-7 控制。）

6970RealAudio

RealAudio 客户将从服务器的 6970-7170 的 UDP 端口接收音频数据流。这是由 TCP7070 端口外向控制连接设置的。

13223PowWow

PowWow 是 TribalVoice 的聊天程序。它允许用户在此端口打开私人聊天的连接。这一程序对于建立连接非常具有“进攻性”。它会“驻扎”在这一 TCP 端口等待回应。这造成类似心跳间隔的连接企图。如果你是一个拨号用户，从另一个聊天者手中“继承”了 IP 地址这种情况就会发生：好象很多不同的人在测试这一端口。这一协议使用“OPNG”作为其连接企图的前四个字节。

17027Conducent

这是一个外向连接。这是由于公司内部有人安装了带有 Conducent"adbot"的共享软件。Conducent"adbot"是为共享软件显示广告服务的。使用这种服务的一种流行的软件是 Pkware。有人试验：阻断这一外向连接不会有任何问题，但是封掉 IP 地址本身将会导致 adbots 持续在每秒内试图连接多次而导致连接过载：

机器会不断试图解析 DNS 名—ads.conducent.com，即 IP 地址 216.33.210.40；216.33.199.77；216.33.199.80；216.33.199.81；216.33.210.41。（译者：不知 NetAnts 使用的 Radiate 是否也有这种现象）

27374Sub-7 木马(TCP)

参见 Subseven 部分。

30100NetSphere 木马(TCP)

通常这一端口的扫描是为了寻找中了 NetSphere 木马。

31337BackOrifice“elite”

Hacker 中 31337 读做“elite”/ei 'li:t/（译者：法语，译为中坚力量，精华。即 3=E,1=L,7=T）。因此许多后门程序运行于这一端口。其中最有名的是 BackOrifice。曾经一段时间内这是 Internet 上最常见的扫描。现在它的流行越来越少，其它的木马程序越来越流行。

31789Hack-a-tack

这一端口的 UDP 通讯通常是由于"Hack-a-tack"远程访问木马（RAT,RemoteAccessTrojan）。这种木马包含内置的 31790 端口扫描器，因此任何 31789 端口到 317890 端口的连接意味着已经有这种入侵。（31789 端口是控制连接，317890 端口是文件传输连接）

32770~32900RPC 服务

SunSolaris 的 RPC 服务在这一范围内。详细的说：早期版本的 Solaris（2.5.1 之前）将 portmapper 置于这一范围内，即使低端口被防火墙封闭仍然允许 Hacker/cracker 访问这一端口。扫描这一范围内的端口不是为了寻找 portmapper，就是为了寻找可被攻击的已知的 RPC 服务。

33434~33600traceroute

如果你看到这一端口范围内的 UDP 数据包（且只在此范围之内）则可能是由于 traceroute。参见 traceroute 部分。

41508Inoculan

早期版本的 Inoculan 会在子网内产生大量的 UDP 通讯用于识别彼此。参见

http://www.circlemud.org/~jelson/software/udpsend.html

http://www.ccd.bnl.gov/nss/tips/inoculan/index.html

(二）下面的这些源端口意味着什么？

端口 1~1024 是保留端口，所以它们几乎不会是源端口。但有一些例外，例如来自 NAT 机器的连接。参见 1.9。

常看见紧接着 1024 的端口，它们是系统分配给那些并不在乎使用哪个端口连接的应用程序的“动态端口”。

ServerClient 服务描述

1-5/tcp 动态 FTP1-5 端口意味着 sscan 脚本

20/tcp 动态 FTPFTP 服务器传送文件的端口

53 动态 FTPDNS 从这个端口发送 UDP 回应。你也可能看见源/目标端口的 TCP 连接。

123 动态 S/NTP 简单网络时间协议（S/NTP）服务器运行的端口。它们也会发送到这个端口的广播。

27910~27961/udp 动态 QuakeQuake 或 Quake 引擎驱动的游戏在这一端口运行其服务器。因此来自这一端

口范围的 UDP 包或发送至这一端口范围的 UDP 包通常是游戏。

61000 以上动态 FTP61000 以上的端口可能来自 Lin

uxNAT 服务器（IPMasquerade）

三、我发现一种对于同一系列端口的扫描来自于 Internet 上变化很大的源地址这通常是由于“诱骗”扫描（decoyscan），如 nmap。其中一个是攻击者，其它的则不是。

利用防火墙规则和协议分析我们可以追踪他们是谁？例如：如果你 ping 每个系统，你就可以将获得的 TTL 与那些连接企图相匹配。这样你至少可以哪一个是“诱骗”扫描（TTL 应该匹配，如果不匹配则他们是被“诱骗”了）。不过，新版本的扫描器会将攻击者自身的 TTL 随机化，这样要找出他们回更困难。

你可以进一步研究你的防火墙记录，寻找在同一子网中被诱骗的地址（人）。你通常会发现攻击者刚刚试图对你连接，而被诱骗者不会。

四、特洛伊木马扫描是指什么？

特洛伊木马攻击的第一步是将木马程序放置到用户的机器上。常见的伎俩有：

1)将木马程序发布在 Newsgroup 中，声称这是另一种程序。

2)广泛散布带有附件的 E-mail

3)在其 Web 上发布木马程序

4)通过即时通讯软件或聊天系统发布木马程序（ICQ,AIM,IRC 等）

5)伪造 ISP（如 AOL）的 E-mail 哄骗用户执行程序（如软件升级）

6)通过“文件与打印共享”将程序 Copy 至启动组

下一步将寻找可被控制的机器。最大的问题是上述方法无法告知 Hacker/Cracker 受害者的机器在哪里。因

此，Hacker/Cracker 扫描 Internet。

这就导致防火墙用户(包括个人防火墙用户)经常看到指向他们机器的扫描。他们的机器并没有被攻击，扫描本身不会造成什么危害。扫描本身不会造成机器被攻击。真正的管理员会忽略这种“攻击”

以下列出常见的这种扫描。为了发现你的机器是否被种了木马，运行“NETSTAT－an”。查看是否出现下列端口的连接。

PortTrojan

555phAsezero

1243Sub-7,SubSeven

3129MastersParadise

6670DeepThroat

6711Sub-7,SubSeven

6969GateCrasher

21544GirlFriend

12345NetBus

23456EvilFtp

27374Sub-7,Seven

30100NetSphere

31789Hack‘a‘Tack

31337BackOrifice,andmanyothers

50505SocketsdeTroie

更多信息查看:http://www.commodon.com/threat/threat-ports.htm

1.什么是 SUBSEVEN（sub-7）

Sub-7 是最有名的远程控制木马之一。现在它已经成为易于使用，功能强大的一种木马。原因是：

1〕它易于获得，升级迅速。大部分木马产生后除了修改 bug 以外开发就停止了。

2〕这一程序不但包含一个扫描器，还能利用被控制的机器也进行扫描。

3〕制作者曾比赛利用 sub-7 控制网站。

4〕支持“端口重定向”，因此任何攻击者都可以利用它控制受害者的机器。

5〕具有大量与 ICQ,AOLIM,MSNMessager 和 Yahoomessenger 相关的功能，包括密码嗅探，发送消息等。

6〕具有大量与 UI 相关的功能，如颠倒屏幕，用受害者扩音器发声，偷窥受害者屏幕。

简而言之它不仅是一种 hacking 工具而且是一种玩具，恐吓受害者的玩具。

Sub-7 是由自称“Mobman”的人写的，他的站点是 http://subseven.slak.org/。

Sub-7 可能使用以下端口：

1243 老版本缺省连接端口

2772 抓屏端口

2773 键盘记录端口

6711???

6776 我并不清楚这个端口是干什么用的，但是它被作为一些版本的后面(即不用密码也能连接)。

7215"matrix"chat 程序

27374v2.0 缺省端口

54283Spy 端口

五、来自低端口的 DNS 包

Q：我看见许多来自 1024 端口以下的 DNS 请求。这些服务是“保留”的吗？他们不是应该使用 1024-655

35 端口吗？

A：他们来自于 NAT 防火墙后面的机器。NAT 并不需要保留端口。（RyanRussell>http://www.sybase.com/）

Q：我的防火墙丢弃了许多源端口低于 1024 的包，所以 DNS 查询失败。

A：不要用这种方式过滤。许多防火墙有类似的规则，但这是一种误导。因为 Hacker/Cracker 能伪造任何端口。

Q：这些 NAT 防火墙工作不正常吗？

A：理论上不是，但实际上会导致失败。正确的方式是在任何情况下完全保证 DNS 通讯。（尤其在那些‘代理”DNS 并强迫 DNS 通过 53 端口的情况下）

Q：我以为 DNS 查询应该使用 1024 端口以上的随机端口？

A：实际上，一般 DNS 客户将使用非保留端口。但是有许多程序使用 53 端口。在任何情况下，NAT 都会完全不同，因为它改变了所有 SOCKET（IP＋portcombo）

六、一旦我拨号连接到 ISP 后，我的个人防火墙就开始警告“有人在探测你的 xxxx 端口”。

这种情况很常见。因为你使用 ISP 分配给你的 IP，而在你使用之前刚有人使用。你看到的是上一个用户的“残留”信息。

常见的例子是聊天程序。如果有人刚刚挂断，刚才和他聊天的人会继续试图连接。一些程序的“超时”设置很长。如 POWWOW 或 ICQ。

另一个例子是多人在线游戏。你会看到来自游戏提供者的通讯（如 MPlayer），或其它不知名的游戏服务器。

这些游戏通常基于 UDP，因此无法建立连接。但为了获得较好的用户感觉，他们对于建立连接又很“执着”。以下是一些游戏的端口：

7777Unreal,KlingonHonorGuard

7778UnrealTournament

22450Sin

26000Quake

26900Hexen2

26950HexenWorld

27015Half-life,TeamFortressClassic(TFC)

27500QuakeWorld

27910Quake2

28000-28008StarsiegeTRIBES(TRIBES.DYNAMIX.COM)

28910Heretic2

另一个例子是多媒体广播、电视。如 RealAudio 客户端使用 6970－7170 端口接收声音数据。

你需要连接的来源。例如 ICQ 服务器运行于 4000 端口，而其客户端使用更高的随机端口。这就是说你会看到你会看到从 4000 端口到高端随机端口的 UDP 包。换句话说，不要试图查询端口列表找到随机高端端口的用途。重要的是源端口。

Sub-7 也有类似问题。它使用不同的 TCP 连接用于不同的服务。如果受害者的机器下线，它会持续企图连接受害者机器的端口，特别是 6776 端口。

Version0.4.1,June20,2000

http://www.robertgraham.com/pubs/firewall-seen.html

Copyright1998-2000byRobertGraham(mailto:firewall-seen1@robertgraham.com.

Allrightsreserved.Thisdocumentmayonlybereproduced(wholeorinpart)fornon-commercialpurposes.Allreproductionsmustcontainthiscopyrightnoticeandmustnotbealtered,

exceptbypermissionoftheauthor.

(接上篇)

七、IRC 服务器在探测我

最流行的聊天方式之一是 IRC。这种聊天程序的特点之一就是它能告诉你正在和你聊天的人的 IP 地址。聊天室的问题之一是：人们匿名登陆并四处闲逛，往往会遭遇跑题的评论、粗鲁的话语、被打断谈话、被服务器“冲洗”或被其它客户踢下线。

因此，服务器端和客户端都默认禁止在聊天室内使用匿名登陆。特别需要指出的是，当有人进入聊天室时要检查他们是否通过其它代理服务器连接。最常见的这种扫描是 SOCKS。假设你来的那个地方支持 SOCKS，那么你完全有可能有一台完全独立的机器，你试图通过明处的代理服务器隐藏你在暗处的真实身份。Undernet’s 关于这方面的策略可参考 http://help.undernet.org/proxyscan.

同时，crackers/hackers 会试图扫描人们的机器以确定他们是否运行某种服务，可被他们用做跳板。同样，通过检查 SOCKS，攻击者希望发现某人打开了 SOCKS，例如一个家庭的个人用户 SOCKS 实现共享连接，但将其错误设置成 Internet 上所有用户都能通过它。

八、什么是“重定向”端口

一种常见的技术是把一个端口重定向到另一个地

址。例如默认的 HTTP 端口是 80，许多人把他们重定向到令一个端口，如 8080(这样，如果你打算访问本文就得写成 http://www.robertgraham.com:8080/pubs/firewall-seen.html)

实现重定向是为了让端口更难被发现，从而使 Hacker 更难攻击。因为 Hacker 不能对一个公认的默认端口进行攻击而必须进行端口扫描。

大多数端口重定向与原端口有相似之处。因此，大多数 HTTP 端口由 80 变化而来：81，88，8000，8080，8888。同样 POP 的端口原来在 110，也常被重定向到 1100。

也有不少情况是选取统计上有特别意义的数，象 1234，23456，34567 等。许多人有其它原因选择奇怪的数，42，69，666，31337。近来，越来越多的远程控制木马(RemoteAccessTrojans,RATs)采用相同的默认端口。如 NetBus 的默认端口是 12345。

BlakeR.Swopes 指出使用重定向端口还有一个原因，在 UNIX 系统上，如果你想侦听 1024 以下的端口需要有 root 权限。如果你没有 root 权限而又想开 web 服务，你就需要将其安装在较高的端口。此外，一些 ISP 的防火墙将阻挡低端口的通讯，所以即使你拥有整个机器你还是得重定向端口。

九、我还是不明白当某人试图连接我的某个端口时我该怎么办？

你可以使用 Netcat 建立一个侦听进程。例如，你想侦听 1234 端口：

NETCAT－L－p1234

许多协议都会在连接开始的部分发送数据。当使用

Netcat 侦听某个端口时，你能想办法搞清在使用什么协议。如果幸运的话，你会发现是 HTTP 协议，它会为你提供大量信息，使你能追踪发生的事情。

“－L”参数是让 Netcat 持续侦听。正常情况下 Netcat 会接受一个连接，复制其内容，并退出。加上这个参数后，它可以持续运行以侦听多个连接。

二．ICMP

TCP 和 UDP 能承载数据，但 ICMP 仅包含控制信息。因此，ICMP 信息不能真正用于入侵其它机器。Hacker 们使用 ICMP 通常是为了扫描网络，发动 DoS 攻击，重定向网络交通。(这个观点似乎不正确，可参考 shotgun 关于木马的文章，译者注)

一些防火墙将 ICMP 类型错误标记成端口。要记住，ICMP 不象 TCP 或 UDP 有端口，但它确实含有两个域：类型(type)和代码(code)。而且这些域的作用和端口也完全不同，也许正因为有两个域所以防火墙常错误地标记了他们。更多关于 ICMP 的知识请参考 InfosecLexiconentryonICMP。

关于 ICMP 类型/代码的含义的官方说明请参阅 http://www.isi.edu/in-notes/iana/assignments/icmp-parameters。该文献描述官方含义，而本文描述 Hacker 的企图，详见下文。

类型代码名称含义

0*Echoreplay 对 ping 的回应

3*DestinationUnreachable 主机或路由器返回信息：一些包未达到目的地

0NetUnreachable 路由器配置错误或错误指定 IP 地址

1HostUnreachable 最后一个路由器无法与主机进行 ARP 通讯

3Portunreachable 服务器告诉客户端其试图联系的端口无进程侦听

4FragmentationNeededbutDFset 重要：如果你在防火墙丢弃记录中发现这些包，你应该让他们通过否则你的客户端将发现 TCP 连接莫名其妙地断开

4*SourceQuenchInternet 阻塞

5*Redirect 有人试图重定向你的默认路由器，可能 Hacker 试图对你进行“ man-in-middle ”的攻击，使你的机器通过他们的机器路由。

8*EchoRequestping

9*RouterAdvertisementhacker 可能通过重定向你的默认的路由器 DoS 攻击你的 Win9x 或 Solaris。邻近的 Hacker 也可以发动 man-in-the-middle 的攻击

10*TimeExceededInTransit 因为超时包未达到目的地

0TTLExceeded 因为路由循环或由于运行 tracerout e，路由器将包丢弃

1Fragmentreassemblytimeout 由于没有收到所有片断，主机将包丢弃

11*ParameterProblem 发生某种不正常，可能遇到了攻击

(一)type=0(Echoreply)

发送者在回应由你的地址发送的 ping，可能是由于以下原因：

有人在 ping 那个人：防火墙后面有人在 ping 目标。

自动 ping：许多程序为了不同目的使用 ping，如测

试联系对象是否在线，或测定反应时间。很可能是使用了类似 VitalSign‘ sNet.Medic 的软件，它会发送不同大小的 ping 包以确定连接速度。

诱骗 ping 扫描：有人在利用你的 IP 地址进行 ping 扫描，所以你看到回应。

转变通讯信道：很多网络阻挡进入的 ping(type=8)，但是允许 ping 回应(type=0)。因此，Hacker 已经开始利用 ping 回应穿透防火墙。例如，针对 internet 站点的 DdoS 攻击，其命令可能被嵌入 ping 回应中，然后洪水般的回应将发向这些站点而其它 Internet 连接将被忽略。

(二)Type=3(DestinationUnreachable)

在无法到达的包中含有的代码(code)很重要记住这可以用于击败“ SYN 洪水攻击 ”。即如果正在和你通讯的主机受到“ SYN 洪水攻击 ”，只要你禁止 ping(type=3)进入，你就无法连接该主机。

有些情况下，你会收到来自你从未听说的主机的 ping(type=3)包，这通常意味着“ 诱骗扫描 ”。攻击者使用很多源地址向目标发送一个伪造的包，其中有一个是真正的地址。Hacker 的理论是：受害者不会费力从许多假地址中搜寻真正的地址。

解决这个问题的最好办法是：检查你看到的模式是否与“ 诱骗扫描 ”一致。比如，在 ICMP 包中的 TCP 或 UDP 头部分寻找交互的端口。

1)Type=3,Code=0(DestinationNetUnreachable)

无路由器或主机：即一个路由器对主机或客户说，：“ 我根本不知道在网络中如何路由！包括你正连接的主机 ”。这意味着不是客户选错了 IP 地址就是某处的路由表配置错误。记住，当你把自己 UNIX 机器上的路由表

搞乱后你就会看到“无路由器或主机”的信息。这常发生在配置点对点连接的时候。

2)Type=3,Code=3(DestinationPortUnreachable)

这是当客户端试图连击一个并不存在的 UDP 端口时服务器发送的包。例如，如果你向 161 端口发送 SNMP 包，但机器并不支持 SNMP 服务，你就会收到 ICMPDestinationPortUnreachable 包。

解码的方案

解决这个问题的第一件事是：检查包中的端口。你可能需要一个嗅探器，因为防火墙通常不会记录这种信息。这种方法基于 ICMP 原始包头包含 IP 和 UDP 头。以下是复制的一个 ICMPunreachable 包：

0000BA5EBA1100609707C0FF08004500

00386FDF00008001B4120A00010B0A00

01C90303C2D200000004500004707F0

000080111BE30A0001C90A00010B08A7

79190033B836

其中字节 0303 是 ICMP 的类型和代码。最后 8 个字节是原始 UDP 头，解码如下：

08A7UDP 源端口 port=2215，可能是临时分配的，并不是很重要。

7919UDP 目标端口 port=31001，很重要，可能原来用户想连接 31001 端口的服务。

0033UDP 长度 length=51，这是原始 UDP 数据的长度，可能很重要。

B836UDP 校验和 checksum=0xB836，可能不重要。

你为什么会看到这些？

“诱骗 UDP 扫描”：有人在扫描向你发送 ICMP 的

机器。他们伪造源地址，其中之一是你的 IP 地址。他们实际上伪造了许多不同的源地址使受害者无法确定谁是攻击者。如果你在短时间内收到大量来自同一地址的这种包，很有可能是上述情况。检查 UDP 源端口，它总在变化的话，很可能是 Scenario。

“陈旧 DNS”：客户端会向服务器发送 DNS 请求，这将花很长时间解析。当你的 DNS 服务器回应的时候，客户端可能已经忘记你并关闭了用于接受你回应的 UDP 端口。如果发现 UDP 端口值是 53，大概就发生了这种情况。这是怎么发生的？服务器可能在解析一个递归请求，但是它自己的包丢失了，所以它只能超时然后再试。当回到客户时，客户认为超时了。许多客户程序(尤其是 Windows 中的程序)自己做 DNS 解析。即它们自己建立 SOCKET 进行 DNS 解析。如果它们把要求交给操作系统，操作系统就会一直把端口开在那里。

“多重 DNS 回应”：另一种情况是客户收到对于一个请求的多重回应。收到一个回应，端口就关闭了，后序的回应无法达到。此外，一个 Sun 机器与同一个以太网中的多个 NICs 连接时，将为两个 NICs 分配相同的 MAC 地址，这样 Sun 机器每桢会收到两个拷贝，并发送多重回复。还有，一个编写的很糟糕的客户端程序(特别是那些吹嘘是多线程 DNS 解析但实际上线程不安全的程序)有时发送多重请求，收到第一个回应后关闭了 Socket。但是，这也可能是 DNS 欺骗，攻击者既发送请求由发送回应，企图使解析缓存崩溃。

“NetBIOS 解析”:如果 Windows 机器接收到 ICMP 包，看看 UDP 目标端口是否是 137。如果是，那就是 windows 机器企图执行 gethostbyaddr()函数，它将将会同

时使用 DNS 和 NetBIOS 解析 IP 地址。DNS 请求被发送到某处的 DNS 服务器，但 NetBIOS 直接发往目标机器。如果目标机器不支持 NetBIOS，目标机器将发送 ICMPunreachable。

“Traceroute”：大多数 Traceroute 程序(Windows 中的 Tracert.exe 除外)向关闭的端口发送 UDP 包。这引起一系列的背靠背的 ICMPPortUnreachable 包发回来。因此你看到防火墙显示这样 ICMP 包，可能是防火墙后面的人在运行 Traceroute。你也会看到 TTL 增加。

3)Type=3,Code=4(FragmentationNeededandDon‘tFragmentwasSet)

这是由于路由器打算发送标记有(DF,不允许片断)的 IP 报文引起的。为什么？IP 和 TCP 都将报文分成片断。TCP 在管理片断方面比 IP 有效得多。因此，饿堆趋向于找到“PathMTU”(路由最大传输单元)。在这个过程将发送这种 ICMP 包。

假设 ALICE 和 BOB 交谈。他们在同一个以太网上(maxframesize=1500bytes)，但是中间有连接限制最大 IP 包为 600byte。这意味着所有发送的 IP 包都要由路由器切割成 3 个片断。因此在 TCP 层分割片断将更有效。TCP 层将试图找到 MTU(最大传输单元)。它将所有包设置 DF 位(Don‘tFragment)，一旦这种包碰到不能传输如此大的包的路由器时路由器将发回 ICMP 错误信息。由此，TCP 层能确定如何正确分割片断。

你也许应该允许这些包通过防火墙。否则，当小的包可以通过达到目的地建立连接，而大包会莫名其妙的丢失断线。通常的结果是，人们只能看到 Web 页仅显示一半。

路由最大传输单元的发现越来越整合到通讯中。如IPsec 需要用到这个功能。

(三)Type=4(SourceQuench)

这种包可能是当网络通讯超过极限时由路由器或目的主机发送的。但是当今的许多系统不生成这些包。原因是现在相信简单包丢失是网络阻塞的最后信号(因为包丢失的原因就是阻塞)。

现在 sourcequenches 的规则是(RFC1122)：

路由器不许生成它们

主机可以生成它们

主机不能随便生成它们

防火墙应该丢弃它们

但是，主机遇到 SourceQuench 仍然减慢通讯，因此这被用于 DoS。防火墙应该过滤它们。如果怀疑发生 DoS，包中的源地址是无意义的，因为 IP 地址肯定是虚构的。

已知某些 SMTP 服务器会发送 SourceQuench。

(四)Type=8(EchoakaPING)

这是 ping 请求包。有很多场合使用它们；它可能意味着某人扫描你机器的恶意企图，但它也可能是正常网络功能的一部分。参见 Type=0(EchoResponse)

很多网络管理扫描器会生成特定的 ping 包。包括 ISS 扫描器，WhatsUp 监视器等。这在扫描器的有效载荷中可见。许多防火墙并不记录这些，因此你需要一些嗅探器捕捉它们或使用入侵检测系统(IDS)标记它们。

记住，阻挡 ping 进入并不意味着 Hacker 不能扫描你的网络。有许多方法可以代替。例如，TCPACK 扫描越来越流行。它们通常能穿透防火墙而引起目标系统不

正常的反应。

发送到广播地址(如 x.x.x.0 或 x.x.x.255)的 ping 可能在你的网络中用于 smurf 放大。

(五)Type=11(TimeExceededInTransit)

这一般不会是 Hacker 或 Cracker 的攻击

1)Type=11,Code=0(TTLExceededInTransit)

这可能有许多事情引起。如果有人从你的站点 trace route 到 Internet，你会看到许多来自路由器的 TTL 增加的包。这就是 traceroute 的工作原理：强迫路由器生成 TTL 增加的信息来发现路由器。

防火墙管理员看到这种情况的原因是 Internet 上发生路由循环。路由器 Flapping(持续变换路由器)是一个常见的问题，常会导致循环。这意味着当一个 IP 包朝目的地前进时，这个包被一个路由器错误引导至一个它曾经通过的路由器。如果路由器在包经过的时候把 TTL 域减一，这个包只好循环运动。实际上当 TTL 值为 0 时它被丢弃。

造成这种情况的另一个原因是距离。许多机器(Windows)的默认 TTL 值是 127 或更低。路由器也常常会把 TTL 值减去大于 1 的值，以便反应诸如电话拨号或跨洋连接的慢速连接。因此，可能由于初始 TTL 值太小，而使站点无法到达。此外，一些 Hacker/Cracker 也会使用这种办法使站点无法到达。

2)Type=11,Code=1(FragmentReassemblyTimeExceeded)

当发送分割成片断的 IP 报文时，发送者并不接收所有片断。通常，大多数 TCP/IP 通讯甚至不分割片断。你看到这种情况必定是采用了分割片断而且你和目的地之

间有阻塞。

(六)Type=12(ParameterProblem)

这可能意味着一种进攻。有许多足印技术会生成这种包。

深入浅出谈防火墙

随着计算机网络技术的突飞猛进，网络安全的问题已经日益突出地摆在各类用户的面前。仅从笔者掌握的资料表明，目前在互联网上大约有将近 20%以上的用户曾经遭受过黑客的困扰。尽管黑客如此猖獗，但网络安全问题至今仍没有能够引起足够的重视，更多的用户认为网络安全问题离自己尚远，这一点从大约有 40%以上的用户特别是企业级用户没有安装防火墙(Firewall)便可以窥见一斑,而所有的问题都在向大家证明一个事实，大多数的黑客入侵事件都是由于未能正确安装防火墙而引发的。

防火墙的概念及作用

防火墙的本义原是指古代人们房屋之间修建的那道墙，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。应该说，在互联网上防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域(即 Internet 或有一定风险的网络)与安全区域(局域网)的连接，同时不会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、核准了的信息进入，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，对网络的入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：一是可以限制他人进入内部网络，过滤掉不安全服务和非法用户；二是防止入侵者接近你的防御设施；三是限定用户访问特殊站点；四是为监视 Internet 安全提供方便。由于防火墙假设了网络边界和服务，因此更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。

防火墙的架构与工作方式

防火墙可以使用户的网络划规划更加清晰明了，全面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）。如果没有防火墙的话，你可能会接到许许多多类似的报告，比如单位内部的财政报告刚刚被数万个 Email 邮件炸烂，或者用户的个人主页被人恶意连接向了 Playboy，而报告链接上却指定了另一家色情网站……一套完整的防火墙系统通常是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中的一个服务器进程，它能够代替网络用户完成特定的 TCP/TP 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/TP 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。整个过程可以对胜户完全透明。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，例如一次性口令或回应式系统等。

屏蔽路由器的最大优点就是架构简单且硬件成本较低，而缺点则是建立包过滤规则比较困难，加之屏蔽路由器的管理成本及用户级身份认证的缺乏等。好在路由器生产商们已经认识到并开始着手解决这些问题，他们正在开发编辑包过滤规则的图形用户界面，制订标准的用户级身份认证协议，以提供远程身份认证拨入用户服务(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纲。

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 Dualhomed 防火墙、被屏蔽主机型

防火墙以及被屏蔽子网型防火墙。

通常架设防火墙需要数千甚至上万美元的投入，而且防火墙需要运行于一台独立的计算机上，因此只用一台计算机连入互联网的用户是不必要架设防火墙的，况且这样做即使从成本方面讲也太不划算。目前观之，防火墙的重点还是用来保护由许多台计算机组成的大型网络，这也是黑客高手们真正感兴趣的地方。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，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。当用户将单位内部的局部网连入互联网时，大家肯定不愿意让全世界的人随意翻阅你单位内部人员的工资单、各种文件资料或者是数据库，但即使在单位内部也存在数据攻击的可能性。例如一些心怀叵测的电脑高手可能会修改工资表和财务报告。而通过设置防火墙后，管理员就可以限定单位内部员工使用 Email、浏览 WWW 以及文件传输，但不允许外界任意访问单位内部的计算机，同时管理员也可以禁止单位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。

防火墙的体系结构

1、屏蔽路由器(ScreeningRouter)

屏蔽路由器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。屏蔽路由器的缺点是一旦被攻隐后很难发现，而且不能识别不同的用户。

2、双穴主机网关(DualHomedGateway)

双穴主机网关是用一台装有两块网卡的堡垒主机的做防火墙。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。与屏蔽路由器相比，双穴主机网关堡垒主机的系统软件可用于维护护系统日志、硬件拷贝日志或远程日志。但弱点也比较突出，一旦黑客侵入堡垒主机并使其只具有路由功能，任何网上用户均可以随便访问内部网。

3、被屏蔽主机网关(ScreenedGatewy)

屏蔽主机网关易于实现也最为安全。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(ScreenedSubnet)

被屏蔽子网就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 DNS，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。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，攻击者得先侵入堡垒主机，然后进入内网主机，再返回来破坏屏蔽路由器，并且整个过程中不能引发警报。

防火墙的基本类型

如今市场上的防火墙林林总总，形式多样。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。

包过滤防火墙(IPFiltingFirewall)：

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。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炎墙对黑客来说是比较容易的，他们在这一方面已经积了大量的经验。"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(FakeI

P)，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 地十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(RoutingInformationProtcol)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入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 秒钟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知上万个虚假请求时，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。此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。它阻挡别人进入内部网络，但也不告诉你何人进入你的系统，或者何人从内部进入网际网路。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。

代理服务器(ProxyServer)：

代理服务器通常也称作应用级防火墙。包过滤防火墙可以按照 IP 地址来禁止未授权者的访问。但是它不适合单位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。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度或者特定服务，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。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。

下面笔者向网友们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(ApplicationGatewayProxy)

应用代理服务器可以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、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

回路级代理服务器也称一般代理服务器，它适用于多个协议，但无法解释应用协议，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。其中，套接字服务器(SocketsServer)就是回路级代理服务器。套接字(Sockets)是一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"SocketsifideAPI"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

代管服务器技术换言之就是把不安全的服务，诸如 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 通道(IPTunnels)

如果某公司下属的两个子公司相隔较远，通过 Internet 进行通信时，可以采用 IPTunnels 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。

5、网地址转换器(NetworkAddressTranslate)

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 InternetIP 地址有限，而且受保护网络往往有自己的一套 IP 地址规划。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(SplitDomainNameSever)

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(Mailforwarding)

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，特别是从外面来的访问者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。而内部客户根本感觉不到它的存在，可以自由访问外部站点。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。但代理服务器同时也存在一些不足，特别是它会使网络的访问速度变慢，因为它不允许用户直接访问网络，而代理又要处理入和出的通信量，因此每增加一种新的媒体应用，则必须对代理进行设置。笔者在一套办公应用软件的设计方面，就因为代理服务器的原因折腾了很长时间，结果还是由于设置与容错方面的问题暂时搁浅了。

状态监视器(StatefulInspection)：

状态监视器作为防火墙技术其安全特性最佳，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，并作下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就是可以监测 RemoteProcedureCall 和 UserDatagrqamProtocol 类的端口信息。问题当然也有，即状态监视器的配置非常复杂，而且会降低网络的速度。

目前防火墙已经在 Internet 上得到了广泛的应用，

而且由于防火墙不限于 TCP/IP 协议的特点，也使其逐步在 Internet 之外更具生命力。客观的讲，防火墙并不是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，但了解防火墙技术并学会在实际操作中应用防火墙技术，相信会在新世纪的网络生活中让每一位网友都受益菲浅。

防火墙原理入门

防火墙能增强机构内部网络的安全性。防火墙系统决定了哪些内部服务可以被外界访问；外界的哪些人可以访问内部的服务以及哪些外部服务可以被内部人员访问。防火墙必须只允许授权的数据通过，而且防火墙本身也必须能够免于渗透。

防火墙的五大功能

一般来说，防火墙具有以下几种功能：

1.允许网络管理员定义一个中心点来防止非法用户进入内部网络。

2．可以很方便地监视网络的安全性，并报警。

3．可以作为部署 NAT（NetworkAddressTranslation，网络地址变换）的地点，利用 NAT 技术，将有限的 IP 地址动态或静态地与内部的 IP 地址对应起来，用来缓解地址空间短缺的问题。

4.是审计和记录 Internet 使用费用的一个最佳地点。网络管理员可以在此向管理部门提供 Internet 连接的费用情况，查出潜在的带宽瓶颈位置，并能够依据本机构的核算模式提供部门级的计费。

两种防火墙技术的对比

包过滤防火墙

优点

价格较低

性能开销小，处理速度较快

缺点

定义复杂，容易出现因配置不当带来问题

允许数据包直接通过，容易造成数据驱动式攻击的潜在危险

代理防火墙

内置了专门为了提高安全性而编制的 Proxy 应用程序，能够透彻地理解相关服务的命令，对来往的数据包进行安全化处理

速度较慢，不太适用于高速网（ATM 或千兆位以太网等）之间的应用

5．可以连接到一个单独的网段上，从物理上和内部网段隔开，并在此部署 WWW 服务器和 FTP 服务器，将其作为向外部发布内部信息的地点。从技术角度来讲，就是所谓的停火区（DMZ）。

防火墙的两大分类

尽管防火墙的发展经过了上述的几代，但是按照防火墙对内外来往数据的处理方法，大致可以将防火墙分为两大体系：包过滤防火墙和代理防火墙（应用层网关防火墙）。前者以以色列的 Checkpoint 防火墙和 Cisco 公司的 PIX 防火墙为代表，后者以美国 NAI 公司的 Gauntlet 防火墙为代表。

1．包过滤防?

第一代：静态包过滤

这种类型的防火墙根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括 IP 源地址、IP 目标地址、传输协议(TCP、UDP、ICMP 等等)、TCP/UDP 目标端口、ICMP 消息类型等。包过滤类型的防火墙要遵循的一条基本原则是“最小特权原则”，即明确允许那些管理员希望通过的数据包，禁止其他的数据包。

图 1 简单包过滤防火墙

第二代：动态包过滤

这种类型的防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为所谓包状态监测（StatefulInspection）技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更绿跄俊?

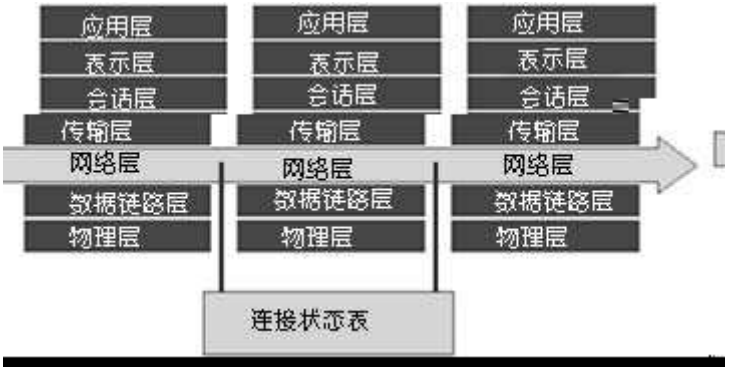


图 2 动态包过滤防火墙

2．代理防火墙

第一代：代理防火墙

代理防火墙也叫应用层网关（ApplicationGateway**）防火墙。这种防火墙通过一种代理（**Proxy**）技术参与到一个** TCP **连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器技术。**

所谓代理服务器，是指代表客户处理在服务器连接请求的程序。当代理服务器得到一个客户的连接意图时，它们将核实客户请求，并经过特定的安全化的 Proxy **应用程序处理连接请求，将处理后的请求传递到真实的服务器上，然后接受服务器应答，并做进一步处理后，将答复交给发出请求的最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接的作用。**

代理类型防火墙的最突出的优点就是安全。由于每一个内外网络之间的连接都要通过 Proxy **的介入和转**

换，通过专门为特定的服务如 Http 编写的安全化的应用程序进行处理，然后由防火墙本身提交请求和应答，没有给内外网络的计算机以任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。包过滤类型的防火墙是很难彻底避免这一漏洞的。就像你要向一个陌生的重要人物递交一份声明一样，如果你先将这份声明交给你的律师，然后律师就会审查你的声明，确认没有什么负面的影响后才由他交给那个陌生人。在此期间，陌生人对你的存在一无所知，如果要对你进行侵犯，他面对的将是你的律师，而你的律师当然比你更加清楚该如何对付这种人。

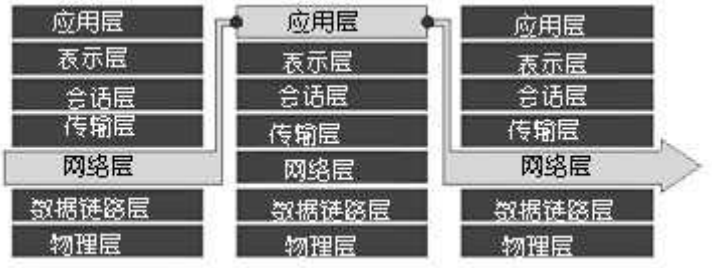


图 3 传统代理型防火墙

代理防火墙的最大缺点就是速度相对比较慢，当用户对内外网络网关的吞吐量要求比较高时，（比如要求达到 75-100Mbps 时）代理防火墙就会成为内外网络之间的瓶颈。所幸的是，目前用户接入 Internet 的速度一般都远低于这个数字。在现实环境中，要考虑使用包过滤类型防火墙来满足速度要求的情况，大部分是高速网（ATM 或千兆位以太网等）之间的防火墙。

第二代：自适应代理防火墙

自适应代理技术（Adaptiveproxy）是最近在商业应

用防火墙中实现的一种革命性的技术。它可以结合代理类型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高 10 倍以上。组成这种类型防火墙的基本要素有两个：自适应代理服务器（AdaptiveProxyServer）与动态包过滤器（DynamicPacketfilter）。

图 4 自适应代理防火墙

在自适应代理与动态包过滤器之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应 Proxy 的管理界面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

小资料

防火墙的发展史

第一代防火墙

第一代防火墙技术几乎与路由器同时出现，采用了包过滤（Packetfilter）技术。下图表示了防火墙技术的简单发展历史。

第二、三代防火墙

1989 年，贝尔实验室的 DavePresotto 和 HowardTrickey 推出了第二代防火墙，即电路层防火墙，同时提出了第三代防火墙——应用层防火墙（代理防火墙）的初步结构。

第四代防火墙

1992 年，USC 信息科学院的 BobBraden 开发出了基于动态包过滤（Dynamicpacketfilter）技术的第四代防火墙，后来演变为目前所说的状态监视（Statefulinspection）技术。1994 年，以色列的 CheckPoint 公司开发出了第一个采用这种技术的商业化的产品。

第五代防火墙

1998 年，NAI 公司推出了一种自适应代理（Adaptiveproxy）技术，并在其产品 GauntletFirewallforNT 中得以实现，给代理类型的防火墙赋予了全新的意义，可以称之为第五代防火墙。

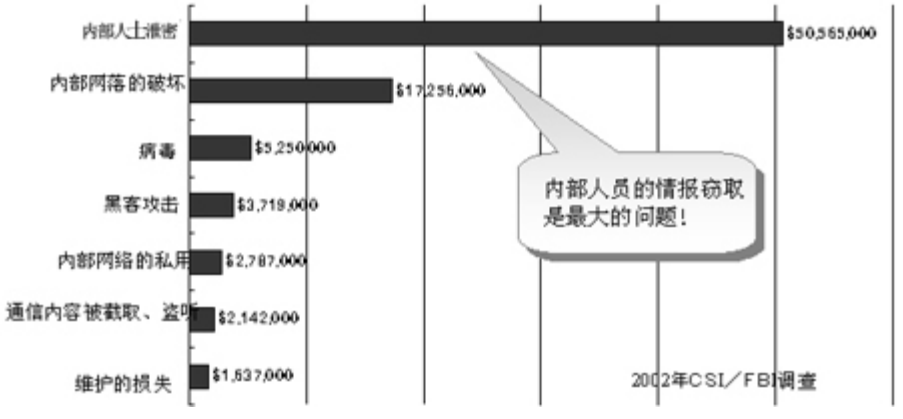
信息安全话题之一:文件加密

公司的电子文件在某种意义上是公司知识产权积累的一种形式，如何保护好电子文件的安全意味着如何保

护好企业知识产权。特别是随着通信技术的发展，电子邮件、移动硬盘、无限上网等很容易把电子文档复制、拷贝、泄露到公司外部给公司带来巨大的损失。文件加密是一种很好解决方式。

在中国市场上，防止文件泄露的文件加密软件类产品很多。但几乎都是用户对自己的计算机上的文件进行加密，然后只有本人可以利用的方式。但在网络的环境下，很多时候都是大家共用很多文件。那么如果只有本人才能利用自己加过密的文件的方式,就会有很多麻烦。例如：如果其他人想利用加密文件的话，就不得不告诉他密码。一旦告诉了他密码，对方就会拥有了文件操作的所有权限。这样既达不到保密的效果，又影响了正常的工作效率。公司的网络环境的优势也就得不到发挥，所以当前的加密软件产品已经满足不了网络环境下的新的需求。

首先，我们看一看下面的一组数据：



所以内部员工的泄密是受害金额最大，防护工作是企业网络安全工作重点的重点。现在，信息泄密的渠道

主要有 3 种：

(1)网络泄密

(2)软盘、移动硬盘泄密

(3)打印泄密

结合上述三种泄密的方式，如何才能做到电子文件的安全呢？首先需要提高企业管理水平，同时还要采用一些技术措施：(1)文件加密(2)严格的授权(3)操作监控

下面就是的新的电子文件安全管理解决方案，具体如下：

1、文件加密

新的文件加密系统解决方案为:所有文件加密，但文件的密钥存放在服务器上，阅览文件需要严格的身份认证。这样，很多人可以利用该加密文件。但不经过身份验证不能取到密钥。即便电子文件通过移动硬盘或电子邮件流失到网络外部，泄密人员也取不到内部网络上的密钥。达到了防止电子邮件或移动硬盘泄密的效果。

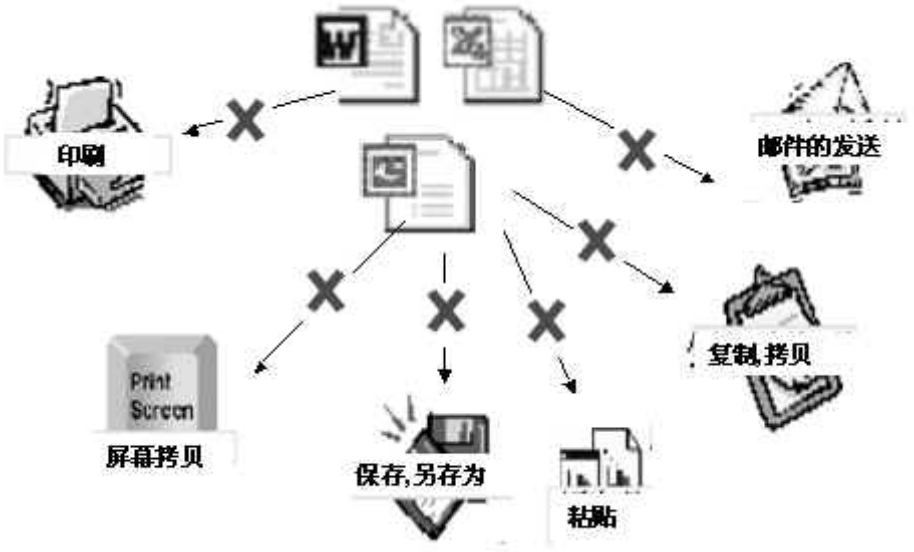
2、严格控制文件的操作，保证不同级别的人员和部门拥有不同权限，包括打印、保存、另存为等权限。具体措施如下：

(1)防止文件的打印、拷贝(只有受权者才可以打印拷贝)同时控制文件的打印次数、阅览次数；

(2)控制保存和另存为(只有受权者才可以保存)，并且防止屏幕拷贝；.

(3)设置文件的利用有效时间

(4)重要电子文档在限定用户阅读范围基础上，附加指定在哪些机器上允许阅读（根据机器名、某段 IP 地址、MAC 地址的一个或多个组合）



3、监控文件利用者的操作，并且留有详细的操作记录，同时可以结合水印技术,追查泄密的渠道。

信息安全是一项任重道远的工作，还需要政府、企业的管理人员提高管理水平和安全意识 ;只有这样一来，才能做到万无一失、防患于未然！

网络防黑初步

只要将你的微机连上 Internet，你就可能会遭到黑客的攻击。网络凶险，黑客猖狂，人在网络，要想使自己的微机不那么轻易地被黑掉，必须未雨绸缪，防患于未然，学些防黑的武功。

一、提高警惕，树立安全意识

步入了网络，注定要和黑客过招。许多网民因到网吧上网，没有注意到安全两个字，而被黑客盗了 QQ 号，

有更多的人用自己的微机上网时悄然被黑客入侵了电脑，当作病毒的试验场，将系统搞垮或把硬盘格式化了，更甚的，盗走了重要的数据，如存折的帐号、密码等。所以你只要用上电脑，就要提高了警惕，树立起安全的意识了，学会保护自己。

二、认识黑客

黑客(hacker)原指那些既有反抗精神又身怀绝技的计算机精英，他们不断挖掘计算机程序最大潜力，为断证明自己，在解决问题和克服限制永远不知疲倦。不过出现另类的骇客(cracker)却不遗余力大行其道专门搞破坏，除了破坏，还是破坏，惟恐天下不乱，这种人已背叛了老一辈黑客崇尚创造的精神了，并与原褒义的黑客混为一谈，让人谈黑变色。黑客虽然是破坏分子的象征，是病毒的制造者，但却是值得我们的尊敬的，正因为有着这些专寻系统的漏洞和软件的 bug 而攻击的黑客，才有对立的反黑专家出来反斗争，他们在展开一场你追我赶的争斗，促使计算机不断完善，飞速发展，日新月异。如 Windows2000 出现不久，黑客即寻到输入法的漏洞攻入别人的电脑了，不过不要怕，只要下载最新的补丁，就可将此一漏洞修补了。总之黑客是寻找计算机的系统漏洞攻击的,因此如何堵塞系统漏洞是防黑的主要课题。

三、利用防黑的工具去防黑

黑客如此厉害，我们不是无可奈何的。只要我们懂得利用防黑的工具去防黑，构建安全的防御体系，你的微机也可“固若金汤”的。

1、安装防火墙阻塞黑客的入侵。天网个人防火墙以及 ZoneAlarm 防火墙是非常出色的个人防火墙，而且是免费的。成为真正的网络卫士，能有效的防止黑客入侵，

抵御来自外部网络的攻击，保证内部系统的资料不被盗取。

2、利用代理服务器上网。代理服务器起到防火墙的作用，起到了屏障的作用。因此，可以提高微机的安全性。如 SyGate 代理服务器易于安装使用，支持多种 Internet 接入方式，包括 ISDN，ASDL 和 CableModem，对个人来说，非常理想的。

3、有道说“预防是理想的，但检测是必须的”。与 Internet 相连，黑客入侵的危险就是存在的。新的漏洞层出不迭，要不被黑客攻击的方法很少。一旦被攻击，没有临视软件，就很难发现攻击者都作了什么。因此可使用 WhatsUpGold 监视软件，对黑客实行及时监控，确保电脑处在安全的状态。

四、关闭一些黑客容易入侵的端口

黑客主要是通过计算机的开放端口连接系统，入侵对方的计算机的。关闭一些危险的端口就能另计算减少系统的漏洞。合法用户的端口开得越多，进入系统的途径就越多。因此，为使系统正常运作，关闭一些无用的端口，尽量保持少的端口是十分必要的。

用 netstat 命令在本地运行以检测哪些端口是打开的，最保险的方法还是对系统进行外部的端口扫描，检查一下每一个端口都在运行什么。任何无法确认的端口都应被关闭，应记录最终端口列表，以确定没有额外的端口出现。

可使用端口扫描器 nmap 扫描端口，不过不论用什么扫描器都应扫描从 1-65,535 的所有 TCP 和 UDP 端口。还有在进行扫描之前，应对系统拥有写入权限。以避免在扫描时，触犯系统的内的协议器件，出现难以预计的

后果或触发入侵检测系统和防火墙，而被认为是一种入侵。

还有要注意连接的安全，不要将打打印机与文件共享同网络协议随意捆绑，若局域网要将打印机与文件共享，应该设立非 Internet 网络协议，这样才更安全。发现黑客攻击时，立即断线，重新拔号上网，这样 IP 地址改变了，黑客又要浪费很多时间去搜寻你的 IP 了。在外部路由或防火墙上设置过滤规则，确认日志系统可以处理很强的负载等。

黑客是无所不能的,这些防线只是增设黑客的障碍，使得一些中低级的黑客无法入侵你的微机，但高级黑客却是无孔不入了，在互联网上来去无痕，连美国的国防部、微软公司等具有高等防黑设备的单位、公司照样如入“无人之境”。要想成为真正的防黑高手，必须不断寻找与黑客相关的书籍、杂志、网站学习，常与黑客交流，还要熟悉各种网络协议，熟悉黑客的攻击原理及工具，熟悉网络的设备与配置，熟悉操作系统的漏洞，尝试寻找系统的漏洞，摸清其原理，找出修补的方法。

虚拟专网的加密算法说明

一、IPSec 认证

IPSec 认证包头（AH）是一个用于提供 IP 数据报完整性和认证的机制。其完整性是保证数据报不被无意的或恶意的方式改变，而认证则验证数据的来源（识别主机、用户、网络等）。AH 本身其实并不支持任何形式的加密，它不能保证通过 Internet 发送的数据的可信程度。

AH 只是在加密的出口、进口或使用受到当地政府限制的情况下可以提高全球 Intenret 的安全性。当全部功能实现后，它将通过认证 IP 包并且减少基于 IP 欺骗的攻击机率来提供更好的安全服务。AH 使用的包头放在标准的 IPv4 和 IPv6 包头和下一个高层协议帧（如 TCP、UDP、ICMP 等）之间。

AH 协议通过在整个 IP 数据报中实施一个消息文摘计算来提供完整性和认证服务。一个消息文摘就是一个特定的单向数据函数，它能够创建数据报的唯一的数字指纹。消息文摘算法的输出结果放到 AH 包头的认证数据（Authentication_Data）区。消息文摘 5 算法（MD5）是一个单向数学函数。当应用到分组数据中时，它将整个数据分割成若干个 128 比特的信息分组。每个 128 比特为一组的信息是大分组数据的压缩或摘要的表示。当以这种方式使用时，MD5 只提供数字的完整性服务。一个消息文摘在被发送之前和数据被接收到以后都可以根据一组数据计算出来。如果两次计算出来的文摘值是一样的，那么分组数据在传输过程中就没有被改变。这样就防止了无意或恶意的窜改。在使用 HMAC－MD5 认证过的数据交换中，发送者使用以前交换过的密钥来首次计算数据报的 64 比特分组的 MD5 文摘。从一系列的 16 比特中计算出来的文摘值被累加成一个值，然后放到 AH 包头的认证数据区，随后数据报被发送给接收者。接收者也必须知道密钥值，以便计算出正确的消息文摘并且将其与接收到的认证消息文摘进行适配。如果计算出的和接收到的文摘值相等，那么数据报在发送过程中就没有被改变，而且可以相信是由只知道秘密密钥的另一方发送的。

二、IPSec 加密

封包安全协议（ESP）包头提供 IP 数据报的完整性和可信性服务 ESP 协议是设计以两种模式工作的：隧道（Tunneling）模式和传输（Transport）模式。两者的区别在于 IP 数据报的 ESP 负载部分的内容不同。在隧道模式中，整个 IP 数据报都在 ESP 负载中进行封装和加密。当这完成以后，真正的 IP 源地址和目的地址都可以被隐藏为 Internet 发送的普通数据。这种模式的一种典型用法就是在防火墙－防火墙之间通过虚拟专用网的连接时进行的主机或拓扑隐藏。在传输模式中，只有更高层协议帧（TCP、UDP、ICMP 等）被放到加密后的 IP 数据报的 ESP 负载部分。在这种模式中，源和目的 IP 地址以及所有的 IP 包头域都是不加密发送的。

IPSec 要求在所有的 ESP 实现中使用一个通用的缺省算法即 DES－CBC 算法。美国数据加密标准（DES）是一个现在使用得非常普遍的加密算法。它最早是在由美国政府公布的，最初是用于商业应用。到现在所有 DES 专利的保护期都已经到期了，因此全球都有它的免费实现。IPSecESP 标准要求所有的 ESP 实现支持密码分组链方式（CBC）的 DES 作为缺省的算法。DES－CBC 通过对组成一个完整的 IP 数据包（隧道模式）或下一个更高的层协议帧（传输模式）的 8 比特数据分组中加入一个数据函数来工作。DES－CBC 用 8 比特一组的加密数据（密文）来代替 8 比特一组的未加密数据（明文）。一个随机的、8 比特的初始化向量（IV）被用来加密第一个明文分组，以保证即使在明文信息开头相同时也能保证加密信息的随机性。DES－CBC 主要是使用一个由通信各方共享的相同的密钥。正因为如此，它被认为是

一个对称的密码算法。接收方只有使用由发送者用来加密数据的密钥才能对加密数据进行解密。因此，DES－CBC 算法的有效性依赖于秘密密钥的安全，ESP 使用的 DES－CBC 的密钥长度是 56 比特。

防火墙功能指标详解

产品类型：从防火墙产品和技术发展来看，分为三种类型：基于路由器的包过滤防火墙、基于通用操作系统的防火墙、基于专用安全操作系统的防火墙。

LAN 接口：列出支持的 LAN 接口类型：防火墙所能保护的网络类型，如以太网、快速以太网、千兆以太网、ATM、令牌环及 FDDI 等。

支持的最大 LAN 接口数：指防火墙所支持的局域网络接口数目，也是其能够保护的不同内网数目。

服务器平台：防火墙所运行的操作系统平台（如 Linux、UNIX、WinNT、专用安全操作系统等）。

协议支持：支持的非 IP 协议：除支持 IP 协议之外，又支持 AppleTalk、DECnet、IPX 及 NETBEUI 等协议。

建立 VPN 通道的协议：构建 VPN 通道所使用的协议，如密钥分配等，主要分为 IPSec，PPTP、专用协议等。

可以在 VPN 中使用的协议：在 VPN 中使用的协议，一般是指 TCP/IP 协议。

加密支持：支持的 VPN 加密标准：VPN 中支持的加密算法,例如数据加密标准 DES、3DES、RC4 以及国内专用的加密算法。

除了 VPN 之外，加密的其他用途：加密除用于保护传输数据以外，还应用于其他领域，如身份认证、报文完整性认证，密钥分配等。

提供基于硬件的加密：是否提供硬件加密方法，硬件加密可以提供更快的加密速度和更高的加密强度。

认证支持：支持的认证类型：是指防火墙支持的身份认证协议，一般情况下具有一个或多个认证方案，如 RADIUS、Kerberos、TACACS/TACACS＋、口令方式、数字证书等。防火墙能够为本地或远程用户提供经过认证与授权的对网络资源的访问，防火墙管理员必须决定客户以何种方式通过认证。

列出支持的认证标准和 CA 互操作性：厂商可以选择自己的认证方案，但应符合相应的国际标准，该项指所支持的标准认证协议，以及实现的认证协议是否与其他 CA 产品兼容互通。

支持数字证书：是否支持数字证书。

访问控制：通过防火墙的包内容设置：包过滤防火墙的过滤规则集由若干条规则组成，它应涵盖对所有出入防火墙的数据包的处理方法，对于没有明确定义的数据包，应该有一个缺省处理方法；过滤规则应易于理解，易于编辑修改；同时应具备一致性检测机制，防止冲突。IP 包过滤的依据主要是根据 IP 包头部信息如源地址和目的地址进行过滤，如果 IP 头中的协议字段表明封装协议为 ICMP、TCP 或 UDP，那么再根据 ICMP 头信息（类型和代码值）、TCP 头信息（源端口和目的端口）或 UDP 头信息（源端口和目的端口）执行过滤，其他的还有 MAC 地址过滤。应用层协议过滤要求主要包括 FTP 过滤、基于 RPC 的应用服务过滤、基于 UDP 的应用服务

过滤要求以及动态包过滤技术等。

在应用层提供代理支持：指防火墙是否支持应用层代理，如 HTTP、FTP、TELNET、SNMP 等。代理服务在确认客户端连接请求有效后接管连接，代为向服务器发出连接请求，代理服务器应根据服务器的应答，决定如何响应客户端请求，代理服务进程应当连接两个连接（客户端与代理服务进程间的连接、代理服务进程与服务器端的连接）。为确认连接的唯一性与时效性，代理进程应当维护代理连接表或相关数据库（最小字段集合），为提供认证和授权，代理进程应当维护一个扩展字段集合。

在传输层提供代理支持：指防火墙是否支持传输层代理服务。

允许 FTP 命令防止某些类型文件通过防火墙：指是否支持 FTP 文件类型过滤。

用户操作的代理类型：应用层高级代理功能，如 HTTP、POP3。

支持网络地址转换(NAT)：NAT 指将一个 IP 地址域映射到另一个 IP 地址域，从而为终端主机提供透明路由的方法。NAT 常用于私有地址域与公有地址域的转换以解决 IP 地址匮乏问题。

在防火墙上实现 NAT 后，可以隐藏受保护网络的内部结构，在一定程度上提高了网络的安全性。

支持硬件口令、智能卡：是否支持硬件口令、智能卡等，这是一种比较安全的身份认证技术。

防御功能：支持病毒扫描：是否支持防病毒功能，如扫描电子邮件附件中的 DOC 和 ZIP 文件，FTP 中的下载或上载文件内容，以发现其中包含的危险信息。

提供内容过滤：是否支持内容过滤，信息内容过滤指防火墙在 HTTP、FTP、SMTP 等协议层，根据过滤条件，对信息流进行控制，防火墙控制的结果是：允许通过、修改后允许通过、禁止通过、记录日志、报警等。过滤内容主要指 URL、HTTP 携带的信息：JavaApplet、JavaScript、ActiveX 和电子邮件中的 Subject、To、From 域等。

能防御的 DoS 攻击类型：拒绝服务攻击(DoS)就是攻击者过多地占用共享资源，导致服务器超载或系统资源耗尽，而使其他用户无法享有服务或没有资源可用。防火墙通过控制、检测与报警等机制，可在一定程度上防止或减轻 DoS 黑客攻击。

阻止 ActiveX、Java、Cookies、Javascript 侵入：属于 HTTP 内容过滤，防火墙应该能够

从 HTTP 页面剥离 JavaApplet、ActiveX 等小程序及从 Script、PHP 和 ASP 等代码检测出危险代码或病毒，并向浏览器用户报警。同时，能够过滤用户上载的 CGI、ASP 等程序，当发现危险代码时，向服务器报警。

安全特性：支持转发和跟踪 ICMP 协议（ICMP 代理）:是否支持 ICMP 代理，ICMP 为网间控制报文协议。

提供入侵实时警告：提供实时入侵告警功能，当发生危险事件时，是否能够及时报警，报警的方式可能通过邮件、呼机、手机等。

提供实时入侵防范：提供实时入侵响应功能，当发生入侵事件时，防火墙能够动态响应，调整安全策略，阻挡恶意报文。

识别/记录/防止企图进行 IP 地址欺骗：IP 地址欺骗指使用伪装的 IP 地址作为 IP 包的源地址对受保护网络

进行攻击，防火墙应该能够禁止来自外部网络而源地址是内部 IP 地址的数据包通过。

管理功能：通过集成策略集中管理多个防火墙：是否支持集中管理，防火墙管理是指对防火墙具有管理权限的管理员行为和防火墙运行状态的管理，管理员的行为主要包括：通过防火墙的身份鉴别，编写防火墙的安全规则，配置防火墙的安全参数，查看防火墙的日志等。防火墙的管理一般分为本地管理、远程管理和集中管理等。

提供基于时间的访问控制：是否提供基于时间的访问控制。

支持 SNMP 监视和配置：SNMP 是简单网络管理协议的缩写。

本地管理：是指管理员通过防火墙的 Console 口或防火墙提供的键盘和显示器对防火墙进行配置管理。

远程管理：是指管理员通过以太网或防火墙提供的广域网接口对防火墙进行管理，管理的通信协议可以基于 FTP、TELNET、HTTP 等。

支持带宽管理：防火墙能够根据当前的流量动态调整某些客户端占用的带宽。

负载均衡特性 :负载均衡可以看成动态的端口映射，它将一个外部地址的某一 TCP 或 UDP 端口映射到一组内部地址的某一端口,负载均衡主要用于将某项服务(如 HTTP）分摊到一组内部服务器上以平衡负载。

失败恢复特性（failover)：指支持容错技术，如双机热备份、故障恢复，双电源备份等。

记录和报表功能：防火墙处理完整日志的方法：防火墙规定了对于符合条件的报文做日志，应该提供日志

信息管理和存储方法。

提供自动日志扫描：指防火墙是否具有日志的自动分析和扫描功能，这可以获得更详细的统计结果，达到事后分析、亡羊补牢的目的。

提供自动报表、日志报告书写器：防火墙实现的一种输出方式，提供自动报表和日志报告功能。

警告通知机制：防火墙应提供告警机制，在检测到入侵网络以及设备运转异常情况时，通过告警来通知管理员采取必要的措施，包括 E－mail、呼机、手机等。

提供简要报表（按照用户 ID 或 IP 地址）：防火墙实现的一种输出方式，按要求提供报表分类打印。

提供实时统计：防火墙实现的一种输出方式，日志分析后所获得的智能统计结果，一般是图表显示。

列出获得的国内有关部门许可证类别及号码：这是防火墙合格与销售的关键要素之一，其中包括：公安部的销售许可证、国家信息安全测评中心的认证证书、总参的国防通信入网证和国家保密局的推荐证明等。

虚拟专网的加密算法说明

一、IPSec 认证

IPSec 认证包头（AH）是一个用于提供 IP 数据报完整性和认证的机制。其完整性是保证数据报不被无意的或恶意的方式改变，而认证则验证数据的来源（识别主机、用户、网络等）。AH 本身其实并不支持任何形式的加密，它不能保证通过 Internet 发送的数据的可信程度。AH 只是在加密的出口、进口或使用受到当地政府限制

的情况下可以提高全球 Intenret 的安全性。当全部功能实现后，它将通过认证 IP 包并且减少基于 IP 欺骗的攻击机率来提供更好的安全服务。AH 使用的包头放在标准的 IPv4 和 IPv6 包头和下一个高层协议帧（如 TCP、UDP、ICMP 等）之间。

AH 协议通过在整个 IP 数据报中实施一个消息文摘计算来提供完整性和认证服务。一个消息文摘就是一个特定的单向数据函数，它能够创建数据报的唯一的数字指纹。消息文摘算法的输出结果放到 AH 包头的认证数据（Authentication_Data）区。消息文摘 5 算法（MD5）是一个单向数学函数。当应用到分组数据中时，它将整个数据分割成若干个 128 比特的信息分组。每个 128 比特为一组的信息是大分组数据的压缩或摘要的表示。当以这种方式使用时，MD5 只提供数字的完整性服务。一个消息文摘在被发送之前和数据被接收到以后都可以根据一组数据计算出来。如果两次计算出来的文摘值是一样的，那么分组数据在传输过程中就没有被改变。这样就防止了无意或恶意的窜改。在使用 HMAC－MD5 认证过的数据交换中，发送者使用以前交换过的密钥来首次计算数据报的 64 比特分组的 MD5 文摘。从一系列的 16 比特中计算出来的文摘值被累加成一个值，然后放到 AH 包头的认证数据区，随后数据报被发送给接收者。接收者也必须知道密钥值，以便计算出正确的消息文摘并且将其与接收到的认证消息文摘进行适配。如果计算出的和接收到的文摘值相等，那么数据报在发送过程中就没有被改变，而且可以相信是由只知道秘密密钥的另一方发送的。

二、IPSec 加密

封包安全协议（ESP）包头提供 IP 数据报的完整性和可信性服务 ESP 协议是设计以两种模式工作的：隧道（Tunneling）模式和传输（Transport）模式。两者的区别在于 IP 数据报的 ESP 负载部分的内容不同。在隧道模式中，整个 IP 数据报都在 ESP 负载中进行封装和加密。当这完成以后，真正的 IP 源地址和目的地址都可以被隐藏为 Internet 发送的普通数据。这种模式的一种典型用法就是在防火墙－防火墙之间通过虚拟专用网的连接时进行的主机或拓扑隐藏。在传输模式中，只有更高层协议帧（TCP、UDP、ICMP 等）被放到加密后的 IP 数据报的 ESP 负载部分。在这种模式中，源和目的 IP 地址以及所有的 IP 包头域都是不加密发送的。

IPSec 要求在所有的 ESP 实现中使用一个通用的缺省算法即 DES－CBC 算法。美国数据加密标准（DES）是一个现在使用得非常普遍的加密算法。它最早是在由美国政府公布的，最初是用于商业应用。到现在所有 DES 专利的保护期都已经到期了，因此全球都有它的免费实现。IPSecESP 标准要求所有的 ESP 实现支持密码分组链方式（CBC）的 DES 作为缺省的算法。DES－CBC 通过对组成一个完整的 IP 数据包（隧道模式）或下一个更高的层协议帧（传输模式）的 8 比特数据分组中加入一个数据函数来工作。DES－CBC 用 8 比特一组的加密数据（密文）来代替 8 比特一组的未加密数据（明文）。一个随机的、8 比特的初始化向量（IV）被用来加密第一个明文分组，以保证即使在明文信息开头相同时也能保证加密信息的随机性。DES－CBC 主要是使用一个由通信各方共享的相同的密钥。正因为如此，它被认为是一个对称的密码算法。接收方只有使用由发送者用来加

密数据的密钥才能对加密数据进行解密。因此，DES－CBC 算法的有效性依赖于秘密密钥的安全，ESP 使用的 DES－CBC 的密钥长度是 56 比特。

查看开放端口判断木马的方法

当前最为常见的木马通常是基于 TCP/UDP 协议进行 client 端与 server 端之间的通讯的，既然利用到这两个协议，就不可避免要在 server 端（就是被种了木马的机器了）打开监听端口来等待连接。例如鼎鼎大名的冰河使用的监听端口是 7626，BackOrifice2000 则是使用 54320 等等。那么，我们可以利用查看本机开放端口的方法来检查自己是否被种了木马或其它黑客程序。以下是详细方法介绍。

1．Windows 本身自带的 netstat 命令

关于 netstat 命令，我们先来看看 windows 帮助文件中的介绍：

Netstat

显示协议统计和当前的 TCP/IP 网络连接。该命令只有在安装了 TCP/IP 协议后才可以使用。

netstat[-a][-e][-n][-s][-pprotocol][-r][interval]

参数

-a

显示所有连接和侦听端口。服务器连接通常不显示。

-e

显示以太网统计。该参数可以与-s 选项结合使用。

-n

以数字格式显示地址和端口号（而不是尝试查找名称）。

-s

显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。

-pprotocol

显示由 protocol 指定的协议的连接；protocol 可以是 tcp 或 udp。如果与-s 选项一同使用显示每个协议的统计，protocol 可以是 tcp、udp、icmp 或 ip。

-r

显示路由表的内容。

interval

重新显示所选的统计，在每次显示之间暂停 interval 秒。按 CTRL+B 停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

好了，看完这些帮助文件，我们应该明白 netstat 命令的使用方法了。现在就让我们现学现用，用这个命令看一下自己的机器开放的端口。进入到命令行下，使用 netstat 命令的 a 和 n 两个参数：

C:\>netstat-an

ActiveConnections

ProtoLocalAddressForeignAddressState

TCP0.0.0.0:800.0.0.0:0LISTENING

TCP0.0.0.0:210.0.0.0:0LISTENING

TCP0.0.0.0:76260.0.0.0:0LISTENING

UDP0.0.0.0:4450.0.0.0:0

UDP0.0.0.0:10460.0.0.0:0

UDP0.0.0.0:10470.0.0.0:0

解释一下，ActiveConnections **是指当前本机活动连接，**Proto **是指连接使用的协议名称，**LocalAddress **是本地计算机的** IP **地址和连接正在使用的端口号，**ForeignAddress **是连接该端口的远程计算机的** IP **地址和端口号，**State **则是表明** TCP **连接的状态，你可以看到后面三行的监听端口是** UDP **协议的,所以没有** State **表示的状态。看 我的机器的** 7626 **端口已经开放,正在监听等待连接，像这样的情况极有可能是已经感染了冰河！急忙断开网络，用杀毒软件查杀病毒是正确的做法。**

2．**工作在** windows2000 **下的命令行工具** fport

使用 windows2000 **的朋友要比使用** windows9X **的幸运一些,因为可以使用** fport **这个程序来显示本机开放端口与进程的对应关系。**

Fport **是** FoundStone **出品的一个用来列出系统中所有打开的** TCP/IP **和** UDP **端口，以及它们对应应用程序的完整路径、**PID **标识、进程名称等信息的软件。在命令行下使用，请看例子：**

D:\>fport.exe

FPortv1.33-TCP/IPProcesstoPortMapper

Copyright2000byFoundstone,Inc.

http://www.foundstone.com

PidProcessPortProtoPath

748tcpsvcs->7TCPC:\WINNT\System32\tcpsvcs.exe

748tcpsvcs->9TCPC:\WINNT\System32\tcpsvcs.exe

748tcpsvcs->19TCPC:\WINNT\System32\tcpsvcs.exe

416svchost->135TCPC:\WINNT\system32\svchost.exe

是不是一目了然了。这下，各个端口究竟是什么程序打开的就都在你眼皮底下了。如果发现有某个可疑程序打开了某个可疑端口，可千万不要大意哦，也许那就是一只狡猾的木马！

Fport 的最新版本是 2.0。在很多网站都提供下载，但是为了安全起见，当然最好还是到它的老家去下：http://www.foundstone.com/knowledge/zips/fport.zip

3.与 Fport 功能类似的图形化界面工具 ActivePorts

ActivePorts 为 SmartLine 出品，你可以用来监视电脑所有打开的 TCP/IP/UDP 端口，不但可以将你所有的端口显示出来，还显示所有端口所对应的程序所在的路径，本地 IP 和远端 IP(试图连接你的电脑 IP)是否正在活动。下面是软件截图：

是不是很直观？更棒的是，它还提供了一个关闭端口的功能，在你用它发现木马开放的端口时，可以立即将端口关闭。这个软件工作在 WindowsNT/2000/XP 平台下。你可以在 http://www.smartline.ru/software/aports.zip 得到它。

其实使用 windowsxp 的用户无须借助其它软件即可以得到端口与进程的对应关系，因为 windowsxp 所带的 netstat 命令比以前的版本多了一个 O 参数，使用这个参数就可以得出端口与进程的对应来。

上面介绍了几种查看本机开放端口，以及端口和进程对应关系的方法，通过这些方法可以轻松的发现基于 TCP/UDP 协议的木马，希望能给你的爱机带来帮助。但是对木马重在防范，而且如果碰上反弹端口木马，利用驱动程序及动态链接库技术制作的新木马时，以上这些方法就很难查出木马的痕迹了。所以我们一定要养成良

好的上网习惯，不要随意运行邮件中的附件，安装一套杀毒软件，像国内的瑞星就是个查杀病毒和木马的好帮手。从网上下载的软件先用杀毒软件检查一遍再使用，在上网时打开网络防火墙和病毒实时监控，保护自己的机器不被可恨的木马入侵。

未来电子战，中国获胜的几率有多大

信息战的定义

一个全新的战争样式，它模糊了战与非战、军事战争和商战、个人违法活动和国家行为的界限。正如《星期日泰晤士报》载文所指出的："每块芯片都是一种潜在的武器，每台计算机都是射入敌人心脏的一支潜在的箭。"

美国国防信息基础结构（DII）中信息战的定义为：保证任何时间、任何地方整个国防部所需信息的有效性、完整性和安全性，保证全部必需的作战、工程及安全等科目和情报（或反情报）支持及应用。

美军野战条令 FM100－6 定义：

在保护己方的信息、信息处理、信息系统和计算机网络的同时，为扰乱敌人的信息、信息处理、信息系统和计算机网络以取得对敌信息优势而采取的行动。

我国沈伟光将信息战定义为：广义是指军事集团抢占信息空间和争夺信息资源的战争；狭义是指：战争中交战双方在信息领域的对抗。

我国王普丰对信息战的定义为：信息战争是在战争中大量使用信息技术和信息武器的基础上，构成信息网

络化的战场，进行全时空的信息较量的一种战争形态。核心是争夺战场信息的控制权，并以此影响和决定战争的胜负。

信息战的实质

利用现代信息手段，通过夺取信息优势来达到自己的军事目的，它既包括了攻击对方的认识和信念，也包括了利用信息优势在实际战斗中打败对方。

在未来的网络战中，

谁先掌握过硬的信息技术和病毒技术，

谁就将赢得未来信息战争的主动权。

信息战的形式之一

进攻性信息战

进攻性信息战

电子战进攻

计算机网络进攻

截获和利用敌方的信息

军事欺骗

进攻性心理战

物理摧毁

微处理芯片攻击

利用电磁辐射窃取信息

高功率微波（HPM）武器

信息战的形式之二

防御性信息战

防御性信息战

电子战防卫

计算机、通信和网络安全防护

反情报

防御性的军事欺骗及反欺骗

防御性心理战

防物理摧毁

信息战技术发展预测

计算机与网络对抗技术

包括黑客战、病毒战、计算机辐射侦察与防御等。

现代通信（大通信）对抗技术

包括全球定位系统（GPS）等系统的使用技术和对抗技术、"灵境"与虚拟现实技术、系统理论与技术、定向能武器技术

几种典型的信息武器（信息进攻）

计算机病毒、蠕虫、特洛伊木马、逻辑炸弹、暗门

网络分析仪、探测软件、密码破译分析

“黑客”行动

“芯片捣鬼”、芯片细菌

灵巧树、智能石、电波辐射

电子干扰机等电子战进攻装备

高能／定向能武器、精确制导武器

几种典型的信息武器（信息防御）

计算机病毒对抗（防病毒措施）、数据加密、网络安全设计（如风险分析）与测评、网络的安全监控与告警、网络“防火墙”、信息设施防护、安全／开放的信息网络、移动计算机安全技术；

防电磁（屏蔽）、防窃听／窃录／窃照、病毒免疫卡

大型数握库的安全技术、标准报文卡、访问控制、用户识别、审计跟踪、数据加密、安全密钥管理、网络安全协议、多级安全、光学加密。

辐射探测器、信息犯罪侦察与惩罚、反情报、反欺

骗

信息战---攻击的对象与切入点

信息战中进攻的对象

电信网络

微波传输网络

卫星网络(含 GPS 等)

野战通信网络

计算机网络，尤其是有拨号服务的网络

信息战---攻击的对象与切入点

信息战中计算机网络进攻的切入点

连接 PSTN 的计算机网络

穿过防火墙

穿过 NAT

越过审计和访问控制

路由器(路由攻击，网络实时操作系统的攻击)

信息战的出现

即将成为事实……

美国国家安全局、中央情报局

早已开始研究芯片武器

1999 年两岸黑客网络上先开火

网络安全"木桶"理论

网络安全系统的强度取决于其中最为薄弱的一环。这是由攻击和防守的特性决定的。相对于攻击来说，防守的任务更为艰巨，任何一个节点、某一个软件、其中的某个服务、某个用户的脆弱口令等等都可能造成整个防御系统的失效。

网络安全体系失败的原因之一

从芯片、操作系统到应用程序，任何一个环节都可

能被开发者留下“后门”。

在 CPU 芯片中植入无线发射接收功能；在操作系统、数据库管理系统或应用程序中能够预先安置从事情报收集、受控激发破坏的程序。这些"内奸"，可以接收特殊病毒、接收来自网络或无线电指令来触发 CPU 的自杀功能、搜集和发送敏感信息、将敏感信息隐藏在网络协议层中传输等。最近揭发出来的 PIII 芯片序列号和 MSOffice 文档中隐藏 MAC 地址等内幕已经告诉了我们许多东西。

网络安全体系失败的原因之二

网络设备和软件不可能是完美的，在设计开发过程中必然会出现缺陷和漏洞。

网络安全体系失败的原因之三

管理的失败

网络管理员配置不当或者网络应用升级不及时造成的安全漏洞、使用脆弱的用户口令、随意使用普通网络站点下载的软件、在防火墙内部架设拨号服务器却没有对帐号认证等严格限制、用户安全意识不强，将自己的帐号随意转借他人或与别人共享等等，这些管理落实上的问题都是无论多么精妙的安全策略和网络安全体系都不能解决的，都会使网络处于危险之中。

信息战的技术准备

加紧发展具有战略威慑作用的信息武器装备，如病毒枪（炮）、芯片攻击武器、网络攻击平台、高功率微波武器等。

培养具有特色的“网络战士”。

加强安全管理，建立规范的安全管理工作程序，并把安全管理贯彻到采购、设计、开发、实施、安装、测

试、维护、培训的各个环节。

分析系统的安全需求。

网络监测与入侵检测系统将不断监测进出的各种信息。

信息战的技术准备（续）

开发网络安全探测系统。

研究商用系统构件安全性增强技术、用非可信构件建造可信系统技术。

从安全体系上研究如何将国产系统与国外系统“参合”起来使用，以及商用系统构件安全性增强技术，使系统的效能和安全性达到最佳的平衡。其中的一个具体问题是在整个网络信息系统的哪几个位置上安插国产设备就可以最大限度地阻止安全事故的发生和危害的传播。

如何定制企业防火墙安全机制

前言:

随着互联网发展日渐蓬勃，由于黑客的非法入侵时及病毒摧毁计算机所造成的威胁有越来越严重的趋势，企业对于功能更强大的防火墙的需求也越来越迫切。许多的企业也因为之前没有对网络架构作好网络防护措施，付出了惨痛而昂贵的代价。在使用防火墙产品以防止黑客的非法入侵时,除了产品的安全性与执行效能外，另外善解人意的 GUI 接口、完整的服务功能、厂商技术支持能力等，缺一不可。在享受丰盛的 Internet/Intranet 各种建置及所带来的效率与成本回收的成果之时，如果

企业没有一个良好的安全防范机制，企业内部网络资源将不堪一击，这不是在危言耸听。

1、防火墙来是怎样防止非法者的入侵

防火墙是 Internet 上公认网络存取控制最佳的安全解决方案，网络公司正式将防火墙列入信息安全机制；防火墙是软硬件的结合体，架设在网络之间以确保安全的连接。因此它可以当做 Internet、Intranet 或 Extranet 的网关器，以定义一个规则组合或安全政策，来控制网络间的通讯。并可有效率的记录各种 Internet 应用服务的存取信息、隐藏企业内部资源、减少企业网络曝露的危机等。所以正确安全的防火墙架构必须让所有外部到内部或内部到外部的封包都必须通过防火墙，且唯有符合安全政策定义的封包，才能通过防火墙；既然防火墙是 Internet/Intranet 相关技术服务进出的唯一信道，要正确的使用防火墙就必须先了解防火墙的技术为何？安全性是否符合各种应用服务的需求？认证方式有哪些及网络传输资料的加解/密功能（VPN）方式？最重要的是厂商能否提供完整且长期的服务与技术支持能力？

2、目前防火墙的技术

防火墙的安全性与研发的技术息息相关，现在市场上的防火墙主要的技术可分为封包过滤（PacketFilter）、代理应用闸信道（ApplicationGateway/Proxy）及多阶层状态检查（MultilayerStatefulInspection）等，说明如下：

（1）封包过滤

就如同 Router 的技术,在网络层具备良好的效能和延伸能力，但只能提供 Ip 地址的过滤功能；封包过滤可知道每一个 Ip 的来源地址，但不知道使用者为何人?同样的,它会检测网络层的封包，而不会去管是什么应用程

序，所以封包过滤是防火墙中功能最不安全的，因为他们不会监测到应用程序，无法知道封包传送内容，很容易被非经授权的使用者侵入。

（2）代理应用闸信道

此为最传统的防火墙技术，任何进出 Internet 的应用服务都必须经过防火墙的代理后，再转送到目的地；藉由代理的过程中，来检测各阶层的应用服务，但是这样做却破坏主从架构模式。此外，此种技术只支持有限制的应用程序，每一个服务或应用程序都须要专属的 Proxy，因此有新的 Internet 服务时，使用者必须等待厂商开发新的代理应用程序才能使用；由于每一种代理（Proxy）需要不同的应用程序或 daemon 来执行，会因为过多的资料复制和内容交换会造成执行效能不佳。

（3）多阶层状态检查

这是一种新的防火墙专利技术，结合了封包过滤网络层的执行效能及代理应用闸信道的安全性。任何的封包会都在网络层中被拦劫，然后防火墙会从全部的应用层级中萃取出跟状态有关的数据，而且放在动态状态表来判续后续的封包 提供了应用层的资料内容安全检测，而且不会破坏主从架构模式，可以在资料保全和流量间作智能的控制，具有最大的扩展及延伸能力。

3、定制安全机制

（1）存取控制-定义安全政策

存取控制可定义使用者或应用服务的对象进/出企业网络，以保护企业内部资源；例如：一个企业组织只可决定于上班时间限制存取 Internet 特定的网站，只允许于午餐时间存取，或当系统在执行备援时，禁止存取重要的服务者等。

执行存取控制参数必须是简单且直接的，以一个明确的图形使用者接口（GUI）操作，最好全部的组件都是使用对象导向的方式来定义。而每一个规则能包含任何网络对象、服务、动作和追踪机置，并可判断规则的冲突性。防火墙除必须提供安全的存取控制外，还必须抵挡恶意的攻击。例如 IPSpoofing、DenialofService、PingofDeath 等等。

（2）认证机制

防火墙认证的应用为当使用者与目的主机联机时，在通讯被允许进行之前，认证的机制服务可安全的确认他们身份的有效性，且不需要修改服务器或客户端应用软件。认证服务是可完全的被整合到企业整体的安全政策内，并能经由防火墙图形使用者接口集中管理。所有的认证会期也都能经由防火墙日志浏览器来监视和追踪。

一般防火墙所提供的认证机制与方法多寡不一，以 CheckPointFireWall-1 为例，提供使用者的认证：针对 FTP、TELNET、HTTP 和 RLOGIN 提供透通的使用者认证；客户端认证：可针对特定 IP 地址的使用者授予存取的权限；透通的会期认证：提供以会期为基础的任何一种应用服务的认证等.

认证的机制包括固定的密码，如 OS 及防火墙的密码；以及动态的 OneTimePassword 的密码，如 S/key、SectrID、RADIUS 等。如要使用固定的密码认证，建议使用防火墙的密码较安全，但是固定密码还是容易被监听，最好是使用 OneTimePassword 的方式，以防止被窃取。

（3）内容的安全性

防火墙所提供的内容安全能力，可达到最高层次的应用服务协议检测，以保护使用者企业资源。以 Check PointFireWall-1 而言，包含计算机病毒和恶意 Java 与 ActiveXApplets 的内容安全性检查，经由图形的接口可集中管理。另外提供开放平台的安全企业连接（OPSEC）架构的 API，可整合第三者厂商内容过滤的应用。主要的应用如下：

A、URL 过滤

可维护公司宝贵的网络频宽和增加网络另一层次的控制，允许网络管理者存取 Internet 特定网页，并可确保员工只能下传和存取的网页信息。

B、电子邮件的支持

通过 SMTP 的连接提供高度的控制以保护网络。可在一个标准的应用程序地址之后，隐藏一个外出的邮件地址，或可隐藏内部的网络结构与真正的内部的使用者，或丢弃超过所给与邮件信息的容量等。

C、FTP 的支持

FTP 指令（如 PUT/GET）的内容安全性，可限制文件名称和档案反病毒检查等。

（4）网络地址转译

网络地址转译对 Internet 而言，可隐藏内部的网络地址，克服了 IP 地址数量的限制，可维护一个企业的内部地址的完整性，对映内部非注过册 IP 地址以一个合法有效的 IP 对外，可完整存取 Internet。防火墙提供两种操作模式：

A、动态的模式

当维持已注册 IP 地址给予使用者存取 Internet 的时候和隐藏内部实际 IP 地址的网络资源，可使用动态的模

式达到地址转译。动态的模式可将内部所有 IP 地址的连接，经过防火墙与单一个合法的 IP 地址对外。

B、静态的模式

可应用在一个网络 IP 地址很早就被分派使用和你需要提供「真正的」地址，以

便人们在 Internet 能存取他们，静态模式的地址转译可解决上述问题。静态的模式提供一个对一个的对映在对外公开 IP 地址和内部真正的 IP 地址之间。

（5）加密（虚拟私人网络）

私人的网络利用一些公用网络的设施称为虚拟私人网络或者 VPN。一个 VPN 与一个专属的私人的网络相比较，优点显然是是减少昂贵的费用与更多的弹性。在公开的网络环境中，公司的信息可能在网际网络传输过程中遭受窃听与篡改，可利用加密功能在 Internet 上建立安全的通讯频道，可确保在公司内部的资源具备完整的隐私性、真实性与资料完整性。

由于每一家的防火墙加密机制大都不同，在标准 IP Sec 的加密未完全产品化之前，彼此之间的整合性还是有问题。而加密软件的出口至今还是受美国的限制，一般商业的使用维持 40Bits，金融项目申请可达 56Bits。VPN 可应用在远程使用者与防火墙之间及防火墙与防火墙之间的加解密。

（6）产品的后续支持及厂商的技术能力

Internet 有新的安全产品出现，就有人会研究新的破解方法，所以一个好的防火墙提供者就必须要有一个庞大的组织作为使用者安全的后盾，也应该要有众多的使用者所建立的口碑为防火墙作见证。现今国内防火墙产品大部分是代理国外的软件，搭配硬件出售，很多防火

墙的代理商都是销售单一防火墙产品，无法提供完整的安全解决方案，因企业内部有 Intranet、Database 等软件，如厂商无法提供整体的技术与安全政策，将会带给使用者更多的梦魇。所以在选购防火墙产品，你最好参考一下业界的评语、实际的安装经验或实地测试。

（7）内部人员考核与训练

这部分的安全政策属于人员安全的管理，主要目的在降低人员使用信息或操作信息设备时所可能发生的错误，如滥用、窃取、欺骗、遗失等问题。要避免前述的情况发生，首先应该从人员背景的调查与考核作起，尤其针对一些较敏感的信息之使用，应慎选适当人员来负责。其次，企业制定的安全政策为的就是希望让企业内部所有人员熟悉与了解。因此，最佳的方法，便是赋予人员应有的信息安全责任，并通过日常的信息安全教育训练来达到此一目的。除了以各种方式公布安全政策外，企业可以部门为单位，实施信息安全养成教育，由负责信息安全事宜的同仁来担任，解释企业信息安全政策的内容，告诉使用平时应该注意哪些细节，了解怎么做、什么事可以做、什么事不可以做。举例来说，有关计算机帐号的管理政策中明定，员工计算机中毒时，应该实时通知信息部门人员协助处理，并作详细的回报与记录，以避免计算机病毒扩散，造成企业内部更严重的损失。像这样的政策，如果只是公布，而没有对员工作适当的教育训练，一旦真的发生中毒的事件，必定是手忙脚乱，无法顺利排解问题，相反的，只会造成更多的问题。

小结：

需要特别说明的是，一个良好的防火墙安全机制如果不能有效地实施，那么一切还是形同虚设。一个专业

知识有限的黑客，有时甚至是通过一次电话拨号连接，就能轻易地侵入和攻击一个企业的电脑网络，使企业直接损失上百万。如果严格执行了，那么，黑客渗透进来的成本就更高，他们就需要更多的资源，而这些都是大多数潜在的黑客做不到的。所以人还是最关键的因素。

选择网络防病毒系统需要考虑的六个方面

由于 Internet 技术及信息技术的普及和发展，病毒的传染速度越来越快。一个和 Internet 相连的企业，最主要的病毒入口就是 Internet，主要的传染方式是群件系统；控制 Internet 入口处的病毒侵入，就抑制了最主要的病毒源；好的群件系统防病毒系统，将病毒的传染域隔离到孤立的某一台机器，这样病毒的破坏就会控制到最小范围。

在大的企业里，为了保证防病毒系统的一致性、完整性和自升级能力，必须有一个完善的病毒防护管理体系，负责病毒软件的自动分发、自动升级、集中配置和管理、统一事件和告警处理、保证整个企业范围内病毒防护体系的一致性和完整性。那么，选择一个好的防病毒系统到底需要考虑哪几个方面呢？

一、完整的产品体系和高的病毒检测率

一个好的防病毒系统应该能够覆盖到每一种需要的平台。我们都知道，病毒的入口点是非常多的。我们一般需要考虑在每一种需要防护的平台上都部署防病毒软件。大体上分为以下几类平台：

1．客户端。不管客户端使用什么操作系统，都必须

具有相应的防病毒软件进行安装防范。

2．邮件服务器。电子邮件目前已经成为病毒传播的重要途径。对邮件服务器进行集中邮件病毒防范是非常有意义的。一个好的邮件或群件病毒防范系统可以很好地和服务器的邮件传输机制结合在一起，完成在服务器上对病毒的清除工作。另外，由于目前邮件病毒的传输方式已经从以前的单纯附件携带方式扩展为内容携带方式，所以一个好的邮件防病毒系统应该具有清除邮件正文中的病毒的能力。

3．其他服务器。网络中除了邮件服务器外，还存在大量的其他服务器如文件服务器、应用服务器等等。用户在日常工作时会经常同这些服务器进行文件传输等工作，也就形成了另外一种病毒的传播途径。这些服务器也需要安装相应的防病毒软件。

4．网关。网关是隔离内部网络和外部网络的设备如防火墙、代理服务器等。在网关级别进行病毒防范可以起到对外部网络中病毒进行隔离的作用。

比如，NAI 公司的 McAfeeAVD(ActiveVirusDefense)网络防病毒系统就是典型的例子，该系统包括桌面防病毒产品、服务器防病毒产品、邮件防病毒产品等，其全球用户数目已达到了 6 千万以上。当然，一个好的防病毒软件必须具备极高的病毒检测率和清除率。另外，防病毒软件还必须能够对各种格式的文件包括各种格式的压缩文件进行病毒的清除。

二、功能完善的防病毒软件控制台

所谓网络防病毒所讲的不仅仅是可以对网络服务器进行病毒防范，更加重要的是能够对防病毒软件通过网络进行集中的管理和统一的配置。一个能够完成集中分

发软件、进行病毒特征码升级的控制台是非常必要的。为了方便集中管理，防病毒软件控制台首先需要解决的就是管理容量问题。也就是每一台控制台能够管理到的客户机的最大数目。另外，对于一个企业内部的不同部门，我们有可能需要设置不同的防病毒策略。一个好的控制台应该允许管理员按照 IP 地址、计算机名称、子网甚至 NT 域进行安全策略的分别实施。

三、减少通过广域网进行管理的流量

在一个需要通过广域网进行管理的企业中，由于广域网的带宽有限，防病毒软件的安装和升级流量问题也是必须要考虑到的。好的防病毒软件应从各个方面考虑，尽量减少带宽占用问题。首先，自动升级功能允许升级发生在非工作时间，尽量不占用业务需要的带宽；其次，对于必须频繁升级的特征码，应采用必要的措施将其进行压缩，比如增量升级方式等。

四、方便易用的报表功能

一个网络中的病毒活动状况对于网络管理员来说是非常重要的。通过了解网络中的病毒活动情况，管理员可以了解哪些病毒活动比较频繁、哪些计算机或者用户的文件比较容易感染病毒以及发现的病毒的清除情况等等，以便修改病毒防范策略以及了解病毒的来源情况，方便进行用户、文件资源的安全管理。实用、界面友好的报表是一个网络防病毒软件必备的功能。

五、对计算机病毒的实时防范能力

传统意义上的实时计算机病毒防范是指防病毒软件能够常驻内存，对所有活动的文件进行病毒扫描和清除。这当然是一个防病毒软件必备的功能。这里说的防范能力是另外一种意义的自动病毒防范能力。目前由于病毒

活动频繁，再加上网络管理员一般都工作忙碌，有可能会导致病毒特征码不能及时更新。这就需要防病毒软件本身能够具有一定程度的未知病毒识别能力。

六、快速及时的病毒特征码升级

能够提供一个方便、有效和快速的升级方式是防病毒系统应该具备的重要功能之一。正是由于防病毒软件需要不断进行升级，所以对防病毒软件厂商的技术力量和售后服务的要求也是格外重要。

综上所述，目前的防病毒工作的意义早已脱离了各自为战的状况，技术也不仅仅局限在单机的防病毒。目前，如果需要对整个网络进行规范化的网络病毒防范，我们必须了解最新的技术,结合网络的病毒入口点分析，很好地将这些技术应用到自己的网络中去，形成一个协同作战、统一管理的局面，这样的病毒防范体系，才能够称得上是一个完整的、现代化的网络病毒防御体系。

Linux 网络安全之经验谈

§关于分区：

一个潜在的黑客如果要攻击你的 Linux 服务器，他首先就会尝试缓冲区溢出。在过去的几年中，以缓冲区溢出为类型的安全漏洞是最为常见的一种形式了。更为严重的是，缓冲区溢出漏洞占了远程网络攻击的绝大多数，这种攻击可以轻易使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权！

为了防止此类攻击,我们从安装系统时就应该注意。如果用 root 分区纪录数据，如 log 文件和 email，就可能

因为拒绝服务产生大量日志或垃圾邮件，从而导致系统崩溃。所以建议为/var 开辟单独的分区，用来存放日志和邮件，以避免 root 分区被溢出。最好为特殊的应用程序单独开一个分区，特别是可以产生大量日志的程序，还有建议为/home 单独分一个区，这样他们就不能填满/分区了，从而就避免了部分针对 Linux 分区溢出的恶意攻击。

§关于 BIOS：

记着要在 BIOS 设置中设定一个 BIOS 密码，不接收软盘启动。这样可以阻止不怀好意的人用专门的启动盘启动你的 Linux 系统，并避免别人更改 BIOS 设置，如更改软盘启动设置或不弹出密码框直接启动服务器等等。

§关于口令：

口令是系统中认证用户的主要手段，系统安装时默认的口令最小长度通常为 5，但为保证口令不易被猜测攻击，可增加口令的最小长度，至少等于 8。为此，需修改文件/etc/login.defs 中参数 PASS_MIN_LEN（口令最小长度）。同时应限制口令使用时间，保证定期更换口令，建议修改参数 PASS_MIN_DAYS（口令使用时间）。

§关于 Ping：

既然没有人能 ping 通你的机器并收到响应，你可以大大增强你的站点的安全性。你可以加下面的一行命令到/etc/rc.d/rc.local，以使每次启动后自动运行，这样就可以阻止你的系统响应任何从外部/内部来的 ping 请求。

echo1>/proc/sys/net/ipv4/icmp_echo_ignore_all

§关于 Telnet：

如果你希望用户用 Telnet 远程登录到你的服务器时

不要显示操作系统和版本信息（可以避免有针对性的漏洞攻击），你应该改写/etc/inetd.conf 中的一行象下面这样：

telnetstreamtcpnowaitroot/usr/sbin/tcpdin.telnetd-h

加-h标志在最后使得telnet后台不要显示系统信息，而仅仅显示 login。

§关于特权账号：

禁止所有默认的被操作系统本身启动的且不需要的帐号，当你第一次装上系统时就应该做此检查，Linux提供了各种帐号，你可能不需要，如果你不需要这个帐号，就移走它，你有的帐号越多，就越容易受到攻击。

为删除你系统上的用户，用下面的命令：userdelusername

为删除你系统上的组用户帐号，用下面的命令：groupdelusername

在终端上打入下面的命令删掉下面的特权用账号：

userdeladm

userdellp

userdelsync

userdelshutdown

userdelhalt

userdelmail

如果你不用 sendmail 服务器，就删除这几个帐号：

userdelnews

userdeluucp

userdeloperator

userdelgames

如果你不用 Xwindows 服务器，就删掉这个帐号。

userdelgopher

如果你不允许匿名 FTP，就删掉这个用户帐号：

userdelftp

§关于 su 命令：

如果你不想任何人能够 su 为 root 的话,你应该编辑/etc/pam.d/su 文件，加下面几行：

authsufficient/lib-

/security/pam_rootok-

.sodebug

authrequired/lib-

/security/pam_wheel-

.sogroup=isd

这意味着仅仅 isd 组的用户可以 su 作为 root。如果你希望用户 admin 能 su 作为 root.就运行下面的命令：

usermod-G10admin

suid 程序也是非常危险的，这些程序被普通用户以 euid=0（即 root）的身份执行，只能有少量程序被设置为 suid。用这个命令列出系统的 suid 二进制程序：

suneagle#find/-perm-4000-print

你可以用 chmod-s 去掉一些不需要程序的 suid 位。

§关于账户注销：

如果系统管理员在离开系统时忘了从 root 注销，系统应该能够自动从 shell 中注销。那么，你就需要设置一个特殊的 Linux 变量“ tmout ”，用以设定时间。同样，如果用户离开机器时忘记了注销账户，则可能给系统安全带来隐患。你可以修改/etc/profile 文件，保证账户在一段时间没有操作后，自动从系统注销。编辑文件/etc/profile，在“ histfilesize= ”行的下一行增加如下一行:

tmout=600

则所有用户将在 10 分钟无操作后自动注销。注意：修改了该参数后，必须退出并重新登录 root，更改才能生效。

§关于系统文件：

对于系统中的某些关键性文件如 passwd、passwd.old、passwd._、shadow、shadown._、inetd.conf、services 和 lilo.conf 等可修改其属性，防止意外修改和被普通用户查看。如将 inetd 文件属性改为 600：

#chmod600/etc/inetd.conf

这样就保证文件的属主为 root，然后还可以将其设置为不能改变:

#chattr+i/etc/inetd.conf

这样，对该文件的任何改变都将被禁止。你可能要问：那我自己不是也不能修改了？当然，我们可以设置成只有 root 重新设置复位标志后才能进行修改:

#chattr-i/etc/inetd.conf

§关于用户资源：

对你的系统上所有的用户设置资源限制可以防止 DoS 类型攻击，如最大进程数，内存数量等。例如，对所有用户的限制，编辑/etc/security/limits.con 加入以下几行：

*hardcore0

*hardrss5000

*hardnproc20

你也必须编辑/etc/pam.d/login 文件，检查这一行的存在：

sessionrequired/lib/security/pam_limits.so

上面的命令禁止 corefiles“ core0 ”,限制进程数为“ nproc50 “ ，且限制内存使用为 5M “ rss5000 ”。

§关于 NFS 服务器：

由于 NFS 服务器漏洞比较多，你一定要小心。如果要使用 NFS 网络文件系统服务，那么确保你的/etc/exports 具有最严格的存取权限设置，不意味着不要使用任何通配符，不允许 root 写权限，mount 成只读文件系统。你可以编辑文件/etc/exports 并且加：

/dir/to/exporthost1.mydomain.com(ro,root_squash)

/dir/to/exporthost2.mydomain.com(ro,root_squash)

其中/dir/to/export 是你想输出的目录，host.mydomain.com 是登录这个目录的机器名，ro 意味着 mount 成只读系统，root_squash 禁止 root 写入该目录。最后为了让上面的改变生效，还要运行/usr/sbin/exportfs–a

§关于开启的服务：

默认的 linux 就是一个强大的系统，运行了很多的服务。但有许多服务是不需要的，很容易引起安全风险。这个文件就是/etc/inetd.conf，它制定了/usr/sbin/inetd 将要监听的服务，你可能只需要其中的两个：telnet 和 ftp，其它的类如 shell,login,exec,talk,ntalk,imap,pop-2,pop-3,finger,auth,etc.除非你真的想用它。否则统统关闭之。

你先用下面的命令显示没有被注释掉的服务：

grep-v"#"/etc/inetd.conf

这个命令统计面前服务的总数：

ps-eaf|wc-l

需要提醒你的是以下三个服务漏洞很多，强烈建议你关闭它们：S34yppasswdd（NIS 服务器）、S35ypserv（NIS 服务器）和 S60nfs（NFS 服务器）。

我们可以运行#killall-HUPinetd 来关闭不需要的服务。当然，你也可以运行

#chattr+i/etc/inetd.conf

如果你想使 inetd.conf 文件具有不可更改属性，而只有 root 才能解开，敲以下命令

#chattr-i/etc/inetd.conf

当你关闭一些服务以后，重新运行以上命令看看少了多少服务。运行的服务越少，系统自然越安全了。我们可以用下面命令察看哪些服务在运行：

netstat-na--ip

如果你用的是 Redhat 那就方便多了。^_^Redhat 提供一个工具来帮助你关闭服务，输入/usr/sbin/setup，然后选择"systemservices"，就可以定制系统启动时跑哪些服务。另外一个选择是 chkconfig 命令，很多 linux 版本的系统都自带这个工具。脚本名字中的数字是启动的顺序，以大写的 K 开头的是杀死进程用的。

§关于日志：

所有的日志都在/var/log 下（仅对 linux 系统而言），默认情况下 linux 的日志就已经很强大了，但除 ftp 外。因此我们可以通过修改/etc/ftpaccess 或者/etc/inetd.conf，来保证每一个 ftp 连接日志都能够纪录下来。下面是一个修改 inetd.conf 的例子，假如有下一行：

ftpstreamtcpnowaitroot/usr/sbin/tcpdin.ftpd-l-L-i-o

注释：

-l 每一个 ftp 连接都写到 syslog

-L 纪录用户的每一个命令

-i 文件 received,纪录到 xferlog

-o 文件 transmitted,记录到 xferlog

不过你也不要太相信日志，因为绝大部分黑客都有“擦脚印”的“好”习惯啰！如果你不放心，最好安装一个 Sniffer 吧。

§关于 TCP_WRAPPERS：

默认的，RedhatLinux 允许所有的请求，这是很危险的。如果用 TCP_WRAPPERS 来增强我们站点的安全性简直是举手之劳，你可以将禁止所有的请求放入“ ALL: ALL ”到/etc/hosts.deny 中，然后放那些明确允许的请求到/etc/hosts.allow 中，如:

sshd:192.168.1.10/255.255.255.0gate.openarch.com

对 IP 地址 192.168.1.10 和主机名 gate.openarch.com，允许通过 ssh 连接。配置完了之后，用 tcpdchk 检查，你可以直接执行：tcpdchk。在这里，tcpchk 是 TCP_Wrapper 配置检查工具，它检查你的 tcpwrapper 配置并报告所有发现的潜在/存在的问题。

§关于补丁：

你应该经常到你所安装的 Linux 系统发行商的主页上去找最新的补丁。例如：对于 Redhat 系统而言可以在：http://www.redhat.com/corp/support/errata/上找到补丁。幸运的是，在 Redhat6.1 以后的版本带有一个自动升级工具 up2date，它能自动够测定哪些 rpm 包需要升级，然后自动从 Redhat 的站点下载并完成安装。

SSL 的安全漏洞及解决方案

如果你在互联网上访问某些网站时在浏览器窗口的下方有一个锁的小图标，就表示它表示该网页被 SSL 保

护着。但用 SSL 防护的网站真的能够防范黑客吗？现在国内有很多人对 SSL 存在这么一个认识误区：SSL 很安全，受到 SSL 防护网页服务器的资料就一定是万无一失的，这也导致这样一个局面，只要有着 SSL 防护的网站服务器很少接受审查以及监测。其实不然，对于安全要求不甚高的交易或认证，SSL 还是一个相当不错的安全机制，然而若应用在特殊要求方面，它还存在有这样那样的问题。在下面的文中我将为大家简单介绍 SSL 存在的安全漏洞及解决方案，希望本文对你有所帮助。

一、认识 SSL

一般人认为 SSL 是保护主机或者只是一个应用程序，这是一个误解，SSL 不是设计用来保护操作系统的。SSL 是 SecureSocketsLayer 通讯协议的简称，它是被设计用来保护传输中的资料，它的任务是把在网页以及服务器之间的数据传输加密起来。这个加密（encryption）的措施能够防止资料窃取者直接看到传输中的资料，像是密码或者信用卡号码等等。在这里谈到 SSL，你就必须了解数字证书（DigitalCertificates）的概念。

数字证书是一种能在完全开放系统中准确标识某些主体的机制。一个数字证书包含的信息必须能鉴定用户身份，确保用户就是其所持有证书中声明的用户。除了唯一的标识信息外，数字证书还包含了证书所有者的公共密钥。数字证书的使用允许 SSL 提供认证功能－－保证用户所请求连接的服务器身份正确无误。在信用卡号或 PIN 号码等机密信息被发送出去前让用户确切知道通讯的另一端的身份是毫无疑问的重要的。很明显的，SSL 技术提供了有效的认证。然而大多数用户并未能正确意识到通过 SSL 进行安全连接的必需性。除非越来越多

的用户了解 SSL 和安全站点的基本知识，否则 SSL 仍不足以成为保护用户网络连接的必需技术。除非用户能够充分意识到访问站点时应该注意安全连接标识，否则现有的安全技术仍不能称为真正有效。

目前几乎所有处理具有敏感度的资料，财务资料或者要求身分认证的网站都会使用 SSL 加密技术（当你看到 https 在你的网页浏览器上的 URL 出现时，你就是正在使用具有 SSL 保护的网页服务器。）。在这里我把 SSL 比喻成是一种在浏览器跟网络服务器之间“受密码保护的导管”（cryptographicpipe），也就是我们常说的安全通道。这个安全通道把使用者以及网站之间往返的资料加密起来。但是 SSL 并不会消除或者减弱网站所将受到的威胁性。在 SSL 这个安全通道的背后，一般没有受到 SSL 防护的网站一样具备了相同的网页服务器程序，同样的网页应用程序，CGI 的 script 以及后端数据库。目前普遍存在这么一个错误的认识：很多系统管理者却认为，受到 SSL 防护的网页服务器自动就变得安全了。其实不然，事实上，受到 SSL 防护的网页服务器同样还是会受到与一般其它网站服务器遭受攻击的威胁，受到 SSL 防护的网页服务器不一定是万无一失的。

二、SSL 的安全漏洞

虽然一个网站可能使用了 SSL 安全技术，但这并不是说在该网站中正在输入和以后输入的数据也是安全的。所有人都应该意识到 SSL 提供的仅仅是电子商务整体安全中的一小部份解决方案。SSL 在网站上的使用可能会造成管理员对其站点安全性的某些错觉。使用了 SSL 的网站所可能受到的攻击和其它服务器并无任何区别，同样应该留意各方面的安全性。简言之，加密和数

字证书，SSL 的主要组成，从来都无法保护服务器－－它们仅仅可以保护该服务器所收发的数据。SSL 常见安全问题下面三种：

1、攻击证书

类似 Verisign 之类的公共 CA 机构并不总是可靠的，系统管理员经常犯的错误是过于信任 Verisign 等的公共 CA 机构。例如，如果 Verisign 发放一个证书说我是“某某某”，系统管理员很可能就会相信“我是某某某”。但是，对于用户的证书，公共 CA 机构可能不象对网站数字证书那样重视和关心其准确性。例如，Verisign 发放了一个“keyman"组织的证书，而我是其中一员“JACK”。当一个网站要求认证用户身份时，我们提交了“JACK”的证书。你可能会对其返回的结果大吃一惊的。更为严重的是，由于微软公司的 IIS 服务器提供了“客户端证书映射”（ClientCertificateMapping）功能，用于将客户端提交证书中的名字映射到 NT 系统的用户帐号，在这种情况下我们就能够获得该主机的系统管理员特权！

如果黑客不能利用上面的非法的证书突破服务器，他们可以尝试暴力攻击（brute-forceattack）。虽然暴力攻击证书比暴力攻击口令更为困难，但仍然是一种攻击方法。要暴力攻击客户端认证，黑客编辑一个可能的用户名字列表，然后为每一个名字向 CA 机构申请证书。每一个证书都用于尝试获取访问权限。用户名的选择越好，其中一个证书被认可的可能性就越高。暴力攻击证书的方便之处在于它仅需要猜测一个有效的用户名，而不是猜测用户名和口令。

2、窃取证书

除上面的方法外，黑客还可能窃取有效的证书及相

应的私有密钥。最简单的方法是利用特洛伊木马。这种攻击几乎可使客户端证书形同虚设。它攻击的是证书的一个根本性弱点：私有密钥－－整个安全系统的核心－－经常保存在不安全的地方。对付这些攻击的唯一有效方法或许是将证书保存到智能卡或令牌之类的设备中。

3、安全盲点

系统管理员没办法使用现有的安全漏洞扫描（vulnerabilityscanners）或网络入侵侦测系统（intrusiondetectionsystems，IDS），来审查或监控网络上的 SSL 交易。网络入侵侦测系统是通过监测网络传输来找寻没有经过认证的活动。任何符合已知的攻击模式或者并未经过政策上授权的网络活动都被标起来以供系统管理者检视。而要让 IDS 能够发生作用，IDS 必须能够检视所有的网络流量信息，但是 SSL 的加密技术却使得通过 http 传输的信息无法让 IDS 辨认。再者，虽然我们可以用最新的安全扫描软件审查一般的网页服务器来寻找已知的安全盲点，这种扫描软件并不会检查经过 SSL 保护的服务器。受到 SSL 保护的网页服务器的确拥有与一般服务器同样的安全盲点，可是也许是因为建立 SSL 连结所需要的时间以及困难度，安全漏洞扫描软件并不会审查受到 SSL 保护的网页服务器。没有网络监测系统再加上没有安全漏洞审查，使得最重要的服务器反而成为受到最少防护的服务器。

三、解决方法

至于如何保护证书的安全，你可以采用 IDS（IntrusionDetectionSystem），它是一种用于监测攻击服务器企图的技术和方法。典型的 IDS 监视网络通讯，并将其与保存在数据库中的已知攻击“特征”或方法比较。如果

发现攻击，IDS 可以提醒系统管理员、截断连接或甚至实施反攻击等。问题在于如果网络通讯是加密的，IDS 将无法监视。这反而可能会使攻击更为轻松。假设在一个典型的被防火墙和 IDS 防护的 DMZ 环境中，黑客能轻松地探测被 SSL 保护的网站，因为 SSL 对数据的加密使得 IDS 无法正常监测攻击。通常一台单一的网站服务器会同时使用 SSL 和普通的 TCP 协议。由于黑客攻击的服务器而不是网络连接，他们可以选择任意一种途径。通过 SSL 途径，黑客知道 SSL 加密为他们带来的好处，这样更容易避开 IDS 系统的监测。在这里我主要介绍的是如何解决系统管理员没办法使用现有的安全漏洞扫描或网络入侵侦测系统而存在的网页服务器安全盲点的情况，目前解决这个困扰的常用方法大致有以下三种：

1、通过 Proxy 代理服务器的 SSL

我们可以在一个 SSLProxy 代理程序上使用这项资料审查技术。SSLProxy 是一个在连接埠 80 上接收纯文字的 HTTP 通讯请求的软件，它会将这些请求通过经由 SSL 加密过的连结，转寄到目标网站。我们在连接埠 80 开一个听取的 socket，通过上述的 OpenSSL 指令，将所有进入这个 proxy 的数据传送出去。这在 Unix 上，只是个小技巧：你只须将以下的指令加到你们的/etc/inetd.conf 档案里面，这个 inetd.conf 包含所有 inetd 所提供的网络服务的设定：

wwwstreamtcpnowaitroot/usr/sbin/tcpd/usr/local/bin/ssl_proxy.sh

而/usr/local/bin/ssl_proxy.sh 的内容则如下所述：

#!/bin/sh

/usr/local/ssl/bin/openssls_client-no_tls1-quiet-conne

ct168.172.100.10:4432>/dev/null

168.172.100.10 是 SSL 防护下的网站的地址所在。其中“ -no_tls1 ”以及“ -quiet ”选项将 SSL 交谈（handshake）的标题显示关掉，并且也删除了 SSL 对于尚未经过授权的网站认证所发出的警告。

如果你要想测试你的 proxy 连结，那么你只要以纯文字的方式，在执行 SSLproxy 的系统的连接端口 80 建立联机。这个 proxy 会使用 SSL 来转寄接收的请求到目标网站。

$telnet182.197.110.180GET/HTTP/1.0

在这里，服务器正在 182.197.110.1 的地址执行 SSL proxy 机制，而真正受到 SSL 保护的地址则是在 168.172.100.10。通过这个 SSLproxy 机制，我们只要将安全扫描软件指向 proxy 的 IP 地址，就可以使用它来审查一个 SSL 服务器。

在这里，你可以使用 whisker 程序（网址：http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2）来审查 SSL 防护的网站服务器。Whisker 是一个由 RainForestPuppy 写出来的 script，可以用来检查已知的比较容易受到入侵的网站应用程序以及 CGIscript。

./whisker.pl-h168.172.100.2

--whisker/v1.3.0a/rainforestpuppy/ADM/wiretrip--

-Loadedscriptdatabaseof1691lines

=-=-=-=-=-=

=Host:168.172.100.2

=Server:Microsoft-IIS/4.0

+404ObjectNotFound:GET/cfdocs/

+404ObjectNotFound:GET/cfide/Administrator/starts

top.html

+404ObjectNotFound:GET/cfappman/index.cfm

+404ObjectNotFound:GET/cgi-bin/

+403AccessForbidden:HEAD/scripts/

+403AccessForbidden:HEAD/scripts/cpshost.dll

+404ObjectNotFound:HEAD/samples/search/queryhit.htm

+404ObjectNotFound:HEAD/adsamples/config/site.csc

+403AccessForbidden:HEAD/scripts/counter.exe

+403AccessForbidden:HEAD/scripts/samples/

以上情况是在 182.197.110.1 上执行 whisker，然后 whisker 使用 SSL 将所有的 HTTP 请求转寄到 168.172.100.10。

SSLproxy 的观念已经存在一阵子了。目前有一个名为 sslproxy.c 的程序可以执行以上的功能（网址：http://www.obdev.at/Products/sslproxy.html）。另外还有一个最近才出来，执行 SSLproxy 还有它额外功能的工具程序，叫做 stunnel（http://www.stunnel.org/），是由 BrianHatch 开发的。然而，因为使用命令列模式操作 OpenSSL 软件相对来说比较简单的，所以我将在下面介绍这种方式。

2、OpenSSL

OpenSSL（相关资料网址：http://www.openssl.org/）包含了一套程序以及函式库，提供前端使用者 SSL 功能，并且允许软件工程师将 SSL 模块与他们的程序结合。在众多由 SSL 提供的产品里面，最能够用来让我们在这里讨论的是命令列模式的（command-line）SSL 客户端以及伺服端工具软件。OpenSSL 程序是一个指令列接口的

程序，它是用来以手动的方式起始 SSL 连结。OpenSSL 让你重新导引与其它程序之间的资料输入以及输出。

使用普遍可得的安全扫描软件来审查 SSL 服务器在研究技术文件时，我们在 Apache 提供给 OpenSSL 的接口模块 mod_ssl(相关资料网址：http://www.modssl.org/)读到了一些有趣的信息。其中有一段常见问题讨论到有关测试在 SSL 保护下的网站服务器。你可以利用 Telnet 连到网页服务器第 80 号连接埠，然后下达如下的 httpget 指令，从网页服务器取得网页：

```
telnet www.ramsec.com 80
Trying 216.182.36.154...
Connected to www.ramsec.com.
Escape character is '^]'.
GET / HTTP/1.0
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Content-Location: http://216.182.36.154/index.html
Date: Mon, 10 Jul 2000 11:43:59 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Thu, 23 Mar 2000 01:41:15 GMT
ETag: "305fc7e06894bf1:38441"
Content-Length: 886
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
```

因为 SSL 通联必须要经过一个安全的连接埠，而在这里我们使用的是没有安全防护的连接埠 80，因此，这个技巧在 HTTPS 通讯协议上是行不通的。然而，如果我们用的是 OpenSSL 程序，我们就可以在 SSL 连接上做同样的一件事情。

下面是 OpenSSL 连结的细节

openssl：s_client-connectwww.ramsec.com:443

CONNECTED(00000003)

depth=0/C=US/ST=Washington/L=NewCastle/O=RampartSecurityGroup LLC/OU=Web/OU=Termsofuseatwww.verisign.com/RPA

(c)99/CN=secure.ramsec.com

verifyerror:num=20:unabletogetlocalissuercertificate

verifyreturn:1

depth=0/C=US/ST=Washington/L=NewCastle/O=RampartSecurityGroup LLC/OU=Web/OU=Termsofuseatwww.verisign.com/RPA

(c)99/CN=secure.ramsec.com

verifyerror:num=27:certificatenottrusted

verifyreturn:1

depth=0/C=US/ST=Washington/L=NewCastle/O=RampartSecurityGroup LLC/OU=Web/OU=Termsofuseatwww.verisign.com/RPA

(c)99/CN=secure.ramsec.com

verifyerror:num=27:certificatenottrusted

verifyreturn:1

depth=0/C=US/ST=Washington/L=NewCastle/O=RampartSecurityGroup LLC/OU=Web/OU=Termsofuseatwww.verisign.com/RPA

(c)99/CN=secure.ramsec.com

verifyerror:num=21:unabletoverifythefirstcertificate

verifyreturn:1

Certificatechain

0s:/C=US/ST=Washington/L=NewCastle/O=Rampart SecurityGroup

LLC/OU=Web/OU=Termsofuseatwww.verisign.com/RPA

(c)99/CN=secure.ramsec.com

i:/C=US/O=RSADataSecurity,Inc./OU=SecureServer Certification

Authority

Servercertificate

-----BEGINCERTIFICATE-----

MIIClTCCAgICEGJTOhcnU+VNQDZ7fqS1K8UwDQYJKoZIhvcNAQEEBQAwXzELMAkG

A1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMS4wLAYD

VQQLEyVTZWN1cmUgU2VydmVyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTAw

MDEyNDAwMDAwMFoXDTAxMDEyMzIzNTk1OVowgbsxCzAJBgNVBAYTAlVTMRMwEQYD

VQQIEwpXYXNoaW5ndG9uMRMwEQYDVQQHFApOZXcgQ2FzdGxlMSMwIQYDVQQKFBpS

YW1wYXJ0IFNlY3VyaXR5IEdyb3VwIExMQzEMMAoGA1UECxQDV2ViMTMwMQYDVQQL

FCpUZXJtcyBvZiB1c2UgYXQgd3d3LnZlcmlzaWduLmNvbS9SUEEgKGMpOTkxGjAY

BgNVBAMUEXNlY3VyZS5yYW1zZWMuY29tMIG
fMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQD+0K9xpPTh79iWWXc5JmTeJrg5YNdmwP
5EwfKSPqOk2E8QSRNk8+Huv7h7
h636cDbmIh+J+VuRO5x5YP8apUCcqRfIMmQevTF
zaIyCf3Mwm/OKNTs+4tqA5kjT
SedbBUGaaY2A1VcK0uby1djc+oX8XoCMoRWy+V
GBkBrLK51t2QIDAQABMA0GCSqG
SIb3DQEBBAUAA34AhT7v59KwTvldIHJV7U4Doc
a+/wQ6ivbyd35K9hC/wxwE/jnO
oBXFKaJvV6mHk9hVz37CtLauUGYIZb3x7Cw6Gaj
hhPicLi0l6ndH4VF9C4tbUb4t
2yw/6Jy9i+TfsO/Ldcu4KV0688vfORWm663+6miLY
HKGNqFMaR3QaXc=

-----ENDCERTIFICATE-----

subject=/C=US/ST=Washington/L=NewCastle/O=Ra
mpartSecurityGroup
LLC/OU=Web/OU=Termsofuseatwww.verisign.com/
RPA
(c)99/CN=secure.ramsec.com

issuer=/C=US/O=RSADataSecurity,Inc./OU=SecureS
erver
Certification
Authority

NoclientcertificateCAnamessent

SSLhandshakehasread801bytesandwritten312bytes

New,TLSv1/SSLv3,CipherisRC4-MD5

Serverpublickeyis1024bit

SSL-Session:

Protocol:TLSv1

Cipher:RC4-MD5

Session-ID:

020000001E9F693D9F9D5FF87E6DF24A0BAFC853
91992415991DF3AB74522BCB

Session-ID-ctx:

Master-Key:

08FD7A5E6D058A45D0855AD359C0428F3BB5A68
5E6D74DFB9CDAB6D6A2ED7D53

E97147155DC7B9C61B946BE6

Key-Arg:None

StartTime:963184785

Timeout:300(sec)

Verifyreturncode:0(ok)

GET/HTTP/1.0

HTTP/1.1200OK

Server:Microsoft-IIS/4.0

Content-Location:http://216.182.36.154/index.html

Date:Mon,10Jul200011:41:25GMT

Content-Type:text/html

Accept-Ranges:bytes

Last-Modified:Thu,23Mar200001:41:15GMT

ETag:"305fc7e06894bf1:38441"

Content-Length:886

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
```

通过上面 OpenSSL 这项技术，我们就可以直接传送资料到有 SSL 保护的网站，然后用我们一般审查任何 HTTP 服务器安全性的方式来审查这个 SSL 网页服务器。

3、监测 SSL 服务器

现在的网络 IDS 只能够监视纯文字资料内容，所以我们只能够有两项选择：监视服务器上的 SSL 连结或者将整个连结资料转为纯文字格式。大部分的网页服务器都有一些基本的日志纪录功能。例如：Microsoft 的 IIS Webserver 有内建的日志制作功能，使用的是 W3svc1 格式，它可以侦测到很多一般的网络攻击状况。我通过前述的 SSLproxy 针对 WindowsNT4.0 上具备有 SSL 防护的 IIS 服务器，来作示范性的攻击。我们用的是由 Rain ForestPuppy 发现的一般性常见的 msadc 安全穿透技术。我们的 IIS 服务器在 C:\WINNT\system32\LogFiles 的目录下，记载了以下的日志：

12:25:4510.0.0.1GET/msadc/msadcs.dll200

12:25:4810.0.0.1POST/msadc/msadcs.dll200

然而，因为这些日志文件通常是存在网页服务器上面，因此，一个成功的攻击事件表示黑客很可能已经对日志文件下了手脚了。此外，安全管理员必须每天检查服务器上的日志文件（另外还有 IDS，防火墙等等），这实在不是个最佳的解决方案。

除了使用主机日志文件的以外，另一个方式是将 SSL 连结转换成纯文字格式。如此一来网络的 IDS 就能

够监视资料往来。有几种产品提供这项功能，不过他们主要是为了要提升数据处理效能，而不是为了网络安全的理由。建立以及维护 SSL 连结，必须耗用相当的 CPU 时间，如此一来会减损网页服务器的效能。市面上有几家厂商提供“电子商务加速器”，用来将与 SSL 交涉的工作移到不同的装置或处理器。你可以将 IDS 置放于加速器跟网页服务器之间，以监控纯文字格式的网络交通。用这种方式监控的话，有一个问题。那就是你必须有至少一个网络区隔（networksegment）。这个网络区隔必须是安全的，而且与其它的网络装置分开来。

四、结论

总的来说 SSL 仍然不失为一套全面完善的安全策略中有效的组成元素。然而，与网络安全的其它工具软件一样，仅使用单一的防护软件都是无效的。对 SSL 的过高评价有可能带来安全风险。它仅是网络安全工具的一种，必须和其它网络安全工具紧密结合，方能构造出全面、完善、安全可靠的网络。最后有两件重要的事情是你必须牢记在心的，首先，SSL 并不能够防护你的网站安全。它仅仅防护使用者的网页服务器以及目标网站之间的点对点数据链路，网页服务器跟后端的网页应用软件，仍旧会受到跟一般没有 SSL 防护的网站同样的攻击威胁；第二点，虽然 SSL 会使网络黑客很难用目前已知的攻击模式直接攻击 SSL 防护网站，不过，这些防卫仍旧是有可能用诸如 SSLproxy 等工具来加以突破，然而，相同的技术却也可以被用来监视以及审查系统的安全漏洞。

防范 WindowsXP 的安全策略

尽管 WindowsXP 刚刚推出没有多长时间，但是 WindowsXP 凭借其超强的稳定性和可靠的安全性还是吸引了不少用户在第一时间内去使用它。笔者在与 Windows XP 的短暂“接触”中，细心留意了一些安全方面的操作策略，现在把它整理成文，以期抛砖引玉。

1、屏蔽不需要的服务组件

尽管服务组件安装得越多，用户可以享受的服务功能也就越多。但是用户平时使用到的服务组件毕竟还是有限,而那些很少用到的组件不但占用了不少系统资源，会引起系统不稳定外，它还会为黑客的远程入侵提供了多种途径，为此我们应该尽量把那些暂不需要的服务组件屏蔽掉。具体的操作方法为：首先在控制面板中找到"服务和应用程序"图标，然后再打开"服务"对话框，在该对话框中选中需要屏蔽的程序，并单击鼠标右键，从弹出的快捷菜单中依次选择"属性"/"停止"命令，同时将"启动类型"设置为"手动"或"已禁用"，这样就可以对指定的服务组件进行屏蔽了。

2、起用电源保护功能

使用电脑处理文件时，最担心的就是计算机突然掉电，因为这种突然掉电不但会使自己的辛勤劳动成果顷刻间化为乌有，严重的话还能使计算机受到损伤。为了防止各种情况下的意外掉电，保证计算机的安全正常工作，我们应该在电源管理中启用按下电源按钮时询问或直接休眠的功能。如果您要启动电源保护功能的话，可

以用鼠标在 WindowsXP 的桌面上依次单击“我的电脑”/“控制面板”/“电源选项”，在弹出的设置框中选择“高级”标签，在对应的标签页面下找到“按下计算机电源按钮时”设置项，然后在设置框中选择“休眠”或者“问我要做什么”选项，如果选择“关机”选项的话，就相当于没有起用电源保护功能。

3、对重要信息进行加密

为防止其他人在使用自己的电脑时，偷看自己存储在电脑中的文件信息，WindowsXP 特意为我们普通用户提供了“文件和文件夹加密”功能，利用该功能我们可以对存储在电脑中的重要信息进行加密，这样其他用户在没有密码的情况下是无法访问文件或者文件夹中的内容的。在对文件进行加密时，我们首先打开 WindowsXP 的资源管理器，然后在资源管理器操作窗口中找到需要进行加密的文件或者文件夹，然后用鼠标右键单击选中的文件或文件夹，从弹出的快捷菜单中选择“属性”命令，随后 WindowsXP 会弹出文件加密对话框，单击对话框中的“常规”标签，然后再依次选择“高级”/“加密内容以便保护数据”就可以了。

4、锁定您的计算机

如果在使用电脑的过程中因有急事需要短暂离开电脑的话，许多人因担心自己的电脑会被别人占用，往往会采取先关机，后离开，然后回来再开机的办法来处理，但这样频繁开关机器对电脑是不利的。那我们有没有办法做到既不要关机又能防止其他人使用自己的计算机呢？办法当然是有的啦，您可以通过双击桌面快捷方式来迅速锁定键盘和显示器，而无需使用 CTRL+ALT+DEL 组合键或屏幕保护程序。在锁定您的计算机时，您可

以参照如下的步骤来执行：先用鼠标右键单击 Windows XP 的桌面，然后在右键菜单中依次选择"新建"/"快捷方式"，随后按照屏幕提示，在命令行的文本框中输入"rundll32.exeuser32.dll,LockWorkStation"命令字符，再在随后的向导窗口中输入对应该快捷方式的具体名称，在这里为方便以后调用，您可以直接为该快捷方式取名为"锁定计算机"就可以了。以后您只要双击桌面上的“ 锁定计算机 ”，就可以达到锁定的目的了。

5、使用“ 连接防火墙 ”功能

在网络时代中，病毒的传播方式、传播速度和破坏力发生了翻天覆地变化，而且黑客行为也正在全世界范围内活动。为了防止病毒和黑客的随意入侵，不少用户在自己的计算机中都安装了防火墙。而 WindowsXP 就加入了免费的"Internet 连接防火墙"功能，利用该功能，WindowsXP 能对出入系统的所有信息进行动态数据包筛选，允许系统同意访问的人与数据进入自己的内部网络，同时将不允许的用户与数据拒之门外，最大限度地阻止网络中的黑客来访问自己的网络，防止他们随意更改、移动甚至删除网络上的重要信息。在使用“ 连接防火墙 ”功能时，您可以依次单击开始菜单中的"设置"/"网络连接"菜单项，然后从弹出的窗口中选择需要上网的拨号连接，然后用鼠标右键单击该连接图标，并选择"属性"命令，在随后弹出的拨号属性窗口中再单击"高级"标签，在对应标签的页面中选中"Internet 连接防火墙"选项，然后再单击对应防火墙的“ 设置 ”按钮，来根据自己的要求设置一下防火墙，以便防火墙能更高效地工作。

6、随时起用屏保程序

看到“屏保”二字，大家肯定会很自然地想到计算机中的屏幕保护程序，它主要是通过采用不同方式轮流显示指定图片来达到屏幕保护的目的。但是只有当不操作电脑达到事先设置的时间后，系统才会启动屏幕保护程序，如果我们想在任意指定的时间内启动屏幕保护程序,该怎么办呢？我们可以按照下面的操作方法来实现：在 WindowsXP 的开始菜单中，依次单击"开始"/"搜索"/"文件或文件夹"，然后在弹出的搜索对话框中，点击"所有文件和文件夹"类型,并在对应文件名的文本框中输入"*.scr"字符，再在搜索范围下拉列表中，选择"本机磁盘(C:)"或计算机上存储系统文件的驱动器，最后单击"搜索"按钮。然后在找到的屏幕保护程序列表中，选择需要的屏保程序，然后给这个屏保程序建立一个存放在桌面上的快捷方式，以后要启动屏保程序时直接用鼠标双击桌面上的屏保快捷方式。

7、为自己分配管理权限

安装在 WindowsXP 操作系统中的许多程序，都要求用户具有一定的管理权限才能让用户使用程序，因此为了能够使用好程序，我们有时需要为自己临时分配一个访问程序的管理权限。在分配管理权限时，我们可以先普通用户身份登录到 WindowsXP 的系统中，然后用鼠标右键单击程序安装文件，同时按住键盘上的 Shift 键，从随后出现的快捷菜单中点击"运行方式"，最后在弹出的窗口中输入具有相应管理权限的用户名和密码就可以了。

8、消除系统假死现象

在操作 WindowsXP 中的应用程序时，由于操作不当或者系统本身的问题，导致了操作的程序很长时间没

有响应，许多人以为计算机肯定是死机了，于是不少人选择了直接关机或者使用 Ctrl+Alt+Delete 来重新启动计算机。其实在 WindowsXP 中，有些不能正常运行的程序会引起系统任务栏的假死，这种现象主要是由于当前执行的程序与系统无法兼容引起的。遇到这种现象时，我们可以找到该程序的执行文件，然后单击鼠标右键，在弹出的对话框中选择"兼容性"标签，再在"兼容模式"下选择相应需要的运行环境。

管理信息系统安全方案详解

随着企业信息化建设的进一步发展和完善，安全问题也日益引起人们的关注。本文通过开发和管理石烟管理信息系统的经验，提出了在 C/S 和 B/S 相结合的体系结构下，针对系统安全性所采取的若干方法和技术。

引言

石家庄卷烟厂计算机管理信息系统是由百联优利公司历时三年余的时间开发而成，其体系结构是 C/S（客户机/服务器 Client/Server）,但随着石烟 Intranet 和网站的建设，其体系结构正逐渐从 C/S 向 B/S（浏览器/服务器 Browser/Server）模式转变，目前采用的是 C/S 和 B/S 相结合的方式。

通过这两种体系结构的有效集成，能够最大程度地发挥出两者各自的优势，但无论应用系统体系结构如何变化，其安全问题，一直是人们关注的焦点。

下面，在简要概述了石烟整个系统构架后，对系统安全规划设计及实现方面所采取的措施进行探讨。

系统平台

一、网络环境平台

内部网络的拓朴结构采用快速交换以太网技术，网络主干为光纤，选用百兆和千兆的交换机，以无线方式与厂外业务单位联通，使用防火墙和路由器通过 DDN 线路和光纤与外围单位及本地 ISP 相连。

二、服务器系统平台

数据库服务器采用 AlphaDS20，Alpha 系列机型采用 COMPAQ 公司推出的 64 位 RISC 微处理器芯片，采用超标量多流水线技术，它具有高性能、高速充及寻址功能，Alpha 芯片拥有 64 位的浮点运算器，64 位整数运算器以及 64 位的地址空间，是真正的 64 位芯片。并采用 SCSI 硬盘构成 Raid5 磁盘阵列实现系统双机热备份，以保证系统运行的高效、安全及可靠。由于磁盘容错采用磁盘阵列，可跨越故障 ;以 RAID5 方式构成磁盘阵列，读磁盘的速度快，数据可靠性高，有效容量达到 66%～87%之间，性价比较高。

Web 系列服务器选用 IBM 公司的 Netfinity7100，其具有极为卓越的性能，面向业务通讯、电子商务、内部网、WEB 等各种应用服务。

防病毒服务器和 Proxy 服务器选用 DELL 公司的 DellPowerEdge4400Server。

三、主机系统平台

工作站经过升级后，均为 PIII600，10G，128M 以上。

四、系统平台

服务器操作系统：TrueUnix、Win2000Server 版、Linux

数据库服务器软件：ORACLE8.1.6、SQLServer、IIS、Exchange

工发工具软件：Developer/20006.0、Delphi5、Dreamdreaver、Flash、Photoshop

系统安全

由于这套系统涉及到企业至关重要的信息，其在保密性、准确性及防篡改等安全方面都有较高的要求，因此，本系统着重设计了一套严密的安全并取得了卓有成效的成果。

一、一般措施

1、实体安全措施

就是要采取一些保护计算机设备、设施（含网络、通信设备）以及其他媒体免地震、水灾、火灾、有害气体和其他环境事故（如电磁污染）破坏的措施、过程。这是整个管理信息系统安全运行的基本要求。

尤其是机房的安全措施，计算机机房建设应遵循国标 GB2887－89**《计算机场地技术条例》和** GB9361－88**《计算机场地安全要求》，满足防火、防磁、防水、防盗、防电击、防虫害等要求，配备相应的设备。**

2、运行安全措施

为保障整个系统功能的安全实现，提供一套安全措施，来保护信息处理过程的安全，其中包括：风险分析、审计跟踪，备份恢复、应急等。

制定必要的、具有良好可操作性的规章制度，去进行制约，是非常必要和重要的，而且是非常紧迫的。

形成一支高长自觉、遵纪守法的技术人员队伍，是计算机网络安全工作的又一重要环节。要在思想品质、职业道德、经营、管理、规章制度、教育培训等方面，

做大量艰苦细致的工作，强化计算机系统的安全管理，加强人员教育，来严格有效地制约用户对计算机的非法访问，防范法用户的侵入。只有严格的管理，才能把各种危害遏止最低限度。

3、信息安全措施

数据是信息的基础，是企业的宝贵财富。信息管理的任务和目的是通过对数据采集、录入、存储、加工，传递等数据流动的各个环节进行精心组织和严格控制，确保数据的准确性、完整性、及时性、安全性、适用性和共享性。

制定良好的信息安全规章制度，是最有效的技术手段。而且不仅仅是数据，还应把技术资料、业务应用数据和应用软件包括进去。

二、防病毒措施

计算机病毒泛滥，速度之快，蔓延之广，贻害社会之大，为有史以来任何一种公害所无可比拟。从 CIH 到红色代码和尼姆达，已充分说明了病毒的难以预知性、潜藏性和破坏性，另一方面也说明了防毒的重要性。

本系统中采用了 KILL98 网络看防病毒软件，运行在 Win2000 服务器上。

该软件是世界第二大软件公司 CA 与国内第一家反病毒软件开发公司中国金辰公司合作推出的新一代反病毒产品，KILL 运用主动内核技术，其基础是 CA 公司的 UnicenterTNG 无缝连接技术，这种技术可以保证反病毒模块从底层内核，在发生病毒入侵反应时，反病毒操作不会伤害及到操作系统内核，同时确保杀灭来犯病毒。

此外，KILL 还有很强的网管能力，其可利用 Vxd 技术，进行实时反病毒。软件可实现自动安装，只要连

接互联网，通过域管理方式可实现自动升级。

三、内部网络安全

1、针对局域网采取安全措施

由于局域网采用的是以广播为技术基础的以太网，任何两个节点之间的通信数据包，不仅为这两个节点的网卡所接收，也同时为处在同一以太网上的任何一个节点的网卡所截取。因此，只要接入以太网上的任一节点进行侦听，就可以捕获发生在这个以太网上的所有数据包，对其进行解包分析。从而窃取关键信息。这就是局域网固有的安全隐患。

为了解决这个问题，采取了以下措施：

1)网络分段

由于局域网采用以交换机为中心、路由器为边界的网络格局，又基于中心交换机的访问控制功能和三层交换功能，综合应用物理分段与逻辑分段两种方法，来实现对局域网的安全控制，其目的就是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法侦听，这是一重要的措施。

2)以交换式集线器代替共享式集线器

由于部分网络最终用户的接入是通过分支集线器而不是交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包还是会被同一台集线器上的其他用户所侦听。如一种危险的情况是：用户 TELNET 到一台主机上，由于 TELNET 程序本身缺加密功能，用户所键入的每一个字符（包括用户名、密码、关键配置等重要信息），都将被明文发送，这就是一个很大的安全隐患。

因此，应该以交换式集线器代替共享式集线器，使

单播包仅在两个节点之间传送，从而防止非法侦听。

3)VLAN（虚拟专用网）的划分

本系统中采取划分 VLAN 的方法，进一步克服了以太网的广播问题。

目前的 VLAN 技术主要有三种：基于交换机端口的 VLAN、基于节点 MAC 地址的 VLAN 和基于应用协议的 VLAN。基于交换机端口的 VLAN 虽然稍欠灵活，但却比较成熟，在实际就用中较多，且效果显著。所以石烟信息系统采取了这种方式。

在集中式网络环境下，我们是将中心的所有主机系统集中到一个 VLAN 里，在这个 VLAN 里不允许任何用户节点，从而较好地保护敏感的主机资源。在分布式网络环境下，我们按机构或部门的设置来划分 VLAN。各部门内部的所有服务器和用户节点都在各自的 VLAN 内，互不侵扰。VLAN 内部的连接采用交换实现，而 VLAN 与 VLAN 之间的连接则采用路由实现。

2、强化 Server 端的安全措施

在 C/S 结构中，C 端的重要性是显而易见的。虽然 C/S 系统的安全已比较成熟，然而这种安全体系统中还有其潜在问题，尤其是在一个复杂系统中，由于存在着大量的数据库实体及拥用不同操作权限的用户，存在多个用户对数据库实体的操作可以是增、删、改、查的任意组合。因此，即使用角色或工作组的方式为其授权，也会显得相当复杂，甚至存在着严重的安全漏洞。

针对这些状况，本系统采取了如下安全措施：

1)内核级透明代理

与传统的 CS 安全模式不同，该系统所采取的解决方案是：每个数据库应用只建立一个真正的数据库帐号，

他具有对系统应用所涉及的所有数据实体进行操作的全部权限。与此同时，为每一位系统操作人员分别创建了一个“应用系统帐号”，实际上只数据库中创建的的名为USERS用户表里的一条记录。这样，每次应用程序在客户端执行时，首先会以其真正数据库帐号登录数据库，然后执行自行编写的登录程序，与USERS表结合，实现就用系统登录。

这种安全体系使得应用系统成为数据库的趋势用户，而应用系统的所有操作人员（包括系统管理员）则是数据库的间接用户；换言之，应用系统除了完成其应用逻辑之外，还将系统用户和数据库彻底隔离开来，成为数据库的一道坚固的“防火墙”由于在这种安全体系中，真正的数据库帐号泄露及扩散的可能性几乎为零，所有的用户必须通过应用系统这一“单点”访问数据库，所以可以得出结论只要应用程序是安全、可靠的，则整个系统是安全可靠的。

这样，系统开发人员的精力可以主要集中到应用程序安全性的编写上。经过深入地研究、分析，系统采取两级帐号、两级登录的改进方案。第一级帐号是应用系统帐号，也就是实际用户所掌握的帐号，建立的方法如上段所述；第二级为数据库系统帐号。两个帐号使用相同的用户名，但口令不同，以此来隔离用户和数据库系统。

具体而言,用户先使用应用系统帐号登录应用系统，应用系统再将应用级帐号变换为数据库系统帐号，然后应用系统用数据库系统帐号登录数据库。仅在两级登录都成功的前提下，整个登录过程才算成功。系统在使用了两级登录都成功的前提下，整个登录过程才算成功。

系统在使用了两级登录的机制后，数据库系统便能识别登录应用系统的用户身份，因此，ORACLE 原有的所有功能得以继承。在改进后的系统中，作者只对应用层的事件加入日志，有关数据库的操作则直接从 ORACLE 日志表中获取

2)增强的用户授权机制

由于在这种安全体系中，应用系统成为隔离用户和数据库的防火墙，其本身就必须具务相当的安全特性。尤其是用户授权管理机制，其严密将直接影响整个系统的安全。

基于此，作者从功能出发将整个系统细分为若干个可分配的最小权限单元，这些权限具体表现在对数据库中所涉及的表、视图的数据操作（DML：插入修改删除、查询等）的划分上。然后再运用角色或工作组的概念，结合各种系统使用人员的工作性质，为系统创建了 4 类基本等级：系统管理员，高级操作员，一般操作员及简单操作员，并相应地为每个等级赋予了不同的权限，以此来简化权限管理工作。此外，为了增加系统安全管理的灵活性，授权管理模块还可以对属于某一等能用户的权限作进一步限制,达到所有权限均可任意组合的效果。

同时，为了进一步提高系统管理员的工作效率，系统为系统权限，用户及每种等级所对应的默认权限组合都建立了数据字典，以便在不同的应用环境下，管理员都能方便地增加等，或改变某种等难的默认权限，此外，为了能暂时封锁某一帐号的使用，安全系统还提供了帐号冻结及解冻的功能。

能过这种方式，在统一管理之下，又具有相录的灵活性，有助于系统管理员更为方便，更为严密地控制整

个系统的安全。

3)智能型日志

日志系统具有综合性数据记录功能和自动分类检索能力。在该系统中，日志将记录自某用户登录时起，到其退出系统时止，这所执行的所有操作，包括登录失败操作，对数据库的操作及系统功能的使用。日志所记录的内容有执行某操作的用户保执行操作的机器 IP 地址操作类型操作对象及操作执行时间等，以备日后审计核查之用

在这个系统中，不仅可以分类检索日志内容，系统还能根据已记录的日志内容，通过智能型揄，自动找出可能存在的不安全因素，并实时触发相应的警告，信息以及时通知系统管理员及用户。

以下例举几个智能性检查。

·潜在非法攻击检查

对于那些企图登录系统的黑客，在其三次登录指令性后，系统便会自行关闭。由于使用了智能型日志系统，系统管理员便会及时得知有非法用户攻击，尤其是针对同一帐号的攻击，在若干次尝试指失败以后，系统将会自动冻结该帐号。在与帐号持有人取得联系后，管理员便可以根据日志文件的具体内容,如攻击点的确切位置、攻击时间等，采取相应措施，如更改帐号口令或封锁工作站，确保系统的安全性。

·单帐号多用户检查

在同一时刻中，若有以同一帐号登录系统的用户出现，则说明某一帐号可能已被泄露，这在一定程度上将对系统安全构成威胁。为此系统将自动监视，统计这种情况度及时通知系统管理员，以杜绝帐号扩散的可能，

防患于未然。

·非工作时间操作检查

对于 8 小时工作时间之外的任何操作或是被管理定义成非工作时所执行的任何操作，智能型日志也会视之为可疑现象而警告系统管理员

4)完善的备份及恢复机制

诚然，日志能记录任何非法操作，然而要真正使系统从灾难中恢复出来，还需要一套完善的备份方案及恢复机制

为了防止存储设备的异常损坏，本系统中采用了可热插拔的 SCSI 硬盘所组成的磁盘容错阵列，以 RAID5 的方式进行系统的实时热备份。

为了防止人为的失误或破坏，本系统中建立了强大的数据库触发器以备份重要数据的删除操作，甚至更新任务。保证在任何情况上，重要数据均能最大程度地有效恢复。具体而言，对于删除操作，作者将被操作的记录全部存贮在备份库中。而对于更新操作，考虑到信息量过于庞大，仅仅备份了所执行的 SQL 语句。这样，既能查看到被的内容，又能相当程度地减小备份库存贮容量。

而在需要跟踪追溯数据丢失或破坏事件的全部信息时，则将系统日志与备份数据有机地结合在一起真正实现系统安全性。

四、广域网络的安全

由于广域网采用公网来进行数据传输，信息在广域网上传输时被截取和利用就比局域网要大得多。本系统中涉及到无线网络部分和远程访问部分，因此，必须采取必要的手段，使得在广域网上的发送和接收信息时能

够保证：

·除了发送方和接收方外，其他人是无法知悉的（隐私性）

·传输过程中不被篡改（真实性）

·发送方能确知接收方不是假冒的（非伪装性）

·发送方不能否认自己的发送行为（不可抵赖性）

为达到以上目的，我们采用了以下措施：

1、加密技术的运用

加密技术的基本思想是不依赖于网络中数据通道的安全性来实现网络系统的安全，而是通过对网络数据的加密来保障网络的安全可靠性。数据加密技术可以分为三类，即对称型加密、不对称型加密和不可逆加密。

本系统中选用了不可逆加密，因为其不存在密钥保管和分发问题，且由于本系统中需采取这种措施的数据量有限，所以这种加密方式是适用于系统的网络体系结构。

2、VPN(虚拟专网)技术的运用

VPN 技术和核心是采用隧道技术，将企业专用网的数据加密封装后，透过虚拟的公网隧道进行传输，从而防止敏感数据的被窃取。企业通过公网建立 VPN，就如同通过自己的专用网建立内部网一样，享有较高的安全性、优先性、可靠性和可管理性，而其建立周期、投入资金和维护费用却大大降低。

故在本系统的设计中，对于一些远程访问用户，本系统采用了 VPN 的技术。

五、针对外网采取安全措施

这里所指的外网，是指本系统中与 Internet 的互联与外部一些企业用户部分。

因为采用的是基于 TCP/IP 协议族，Internet 协议族自身的开放性极大地方便了各种计算机的组网和互联，并直接推动了网络技术的迅猛发展。但是由于在早期网络协议设计上对安全性的忽视，至使 Internet 在使用和管理上的无政府状态，逐渐使 Internet 自身的安全受到威胁。

外网安全的威胁主要表现在：非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒、线路窃听等。

针对上述情况，本系统采取了防火墙技术、入侵检测技术和网络防病毒技术相结合的方法。

本系统中采用的防火墙是天融信网络安全技术有限公司的产品，NGFW3000，是中国人设计的符合国情的防火墙系统，具有完全自主版权。其采用模块化结构设计，可扩展性好，方便用户定制与升级，而且运用面向对象的管理，支持 VPN 的无缝集成，多接口等。此外，还采取了一些相关产品如 SecutityMessager，SJW11，KILL98 等，以实现以防火墙技术、加密技术、安全认证技术、安全应用技术、入侵检测技术和防病毒技术相结全的综合安全体系。

结束语

石烟管理信息系统安全方案，是基于石烟具体实际情况和国内外最实用计算机安全技术的产物，随着用户在实际应用中需求的不断提高，我们将对系统的安全性进一步完善。

提高系统安全的注册表修改秘籍

现在的电脑给人有一种弱不禁风的感觉，不是今天受到这个病毒突袭，就是明天受到那个黑客的攻击，出错、死机变得象家常便饭一样了。为了让计算机“坚强”起来，不少人找来了杀毒软件、防火墙，希望通过这些软件来增强计算机的免役力。的确，这些软件在一定程度上增强了计算机抵抗外来攻击的能力，但对于计算机内部系统存在的漏洞就无能为力了。本文的目的主要是向大家介绍一下通过修改注册表的方法，来提高系统的安全。

一、隐藏一个服务器

为了保证局域网中服务器上的资源不受其他人的非法访问和攻击，我们从安全的角度考虑，有时需要把局域网中指定的服务器计算机名称隐藏起来，以便让其他局域网用户无法访问到，那么我们该如何实现呢？下面请看该设置的具体步骤：

1、打开注册表编辑器，并在编辑器对话框中用鼠标依次单击如下分支：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 键值。

2、用鼠标单击该键值下面的 Hidden 数值名称，如果未发现此名称，那么添加一个，其数据类型为 REG_DWORD。

3、接着用鼠标双击此项，在弹出的“DWORD 编辑器”对话框中输入 1 即可。

4、最后单击“确定”按钮，并退出注册表编辑窗口，重新启动计算机就可以在局域网中隐藏一个服务器了。

二、防止其他人非法编辑注册表

注册表是整个系统的灵魂所在，任何对注册表的错误修改都有可能让系统瘫痪。因此，如果您不是一位系统高手的话，最好不要轻易动手修改注册表。当然在公共场所，为了防止那些电脑“菜鸟”们，随意更改注册表设置，我们最好还是取消其他用户对注册表进行修改的权利。我们可以按照如下步骤来实现这样的目的：

1、首先在注册表编辑界面中，找到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\键值；

2、然后在 Policies 键值的下面新建一个 System 主键，如果该主键已经存在的话，可以直接进行下一步；

3、接着在对应 System 主键右边窗口的空白处再新建一个 DWORD 串值，并命名为 DisableRegistryTools；

4、把 DisableRegistryTools 的值设置为 1，设置好以后，重新启动计算机就可以达到防止其他人非法编辑注册表的目的了。

三、屏蔽“控制面板”的访问

由于通过控制面板，我们可以对计算机系统中的绝大部分软硬件进行设置和控制，因此为了防止其他人随意通过控制面板对 Windows 系统进行非法修改，我们就很有必要屏蔽其他用户对“控制面板”的访问了，要实现该功能，我们可以对注册表进行如下修改：

1、首先在开始菜单中的运行栏中输入 regedit 命令，打开注册表编辑器操作界面；

2、接着在该界面中，依次用鼠标访问\\HKEY_CUR

RENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 键值；

3、随后在对应 System 键值的右边窗口中，用鼠标右键单击该窗口的空白处，并从弹出的快捷菜单中选择“新建”/“DWORD”命令，来新建一个 DWORD 值；

4、把 DWORD 值的名称命名为 NoDispCPL，同时设置 NoDispCPL 的值为 1。

四、不允许其他人对桌面进行任意设置

如果在培训时，每台计算机的桌面设置都一样，那么老师说到什么图标或者执行什么操作，每个学员都能迅速找到目标；相反，一旦桌面中的设置被任意修改后，每一台计算机中的设置就会不一样，那么在教学时，就很难保证教学操作的同步性。为此，不少学校机房或者培训机房，都对锁定桌面进行了设置，下面是具体的设置步骤:

1、在 Windows 的运行对话框中输入 regedit 命令，来打开注册表编辑器窗口；

2、在编辑窗口中，用鼠标依次访问 Hkey－Users\Software\Microsoft\Windows\CurentVersion\Polioies\Explores 键值；

3、在对应 Explores 键值右边的窗口中，用鼠标双击“NoSaveSetting”子键，并将其键值从 0 改为 1！

4、重新启动计算机，上述设置就可以生效了。

五、抵御 BackDoor 的破坏

如果您的计算机上网了，那么您的计算机就会存在着被黑客攻击的危险，而一旦被攻击中的，您的计算机就会面临着瘫痪或者被监视的安全威胁，其中有一个名叫 BackDoor 的后门程序，专门拣系统的漏洞进行攻击。

为防止这种程序对系统造成破坏，我们有必要通过相应的设置来预防 BackDoor 对系统的破坏。设置时：

1、首先在注册表编辑器操作窗口中，用鼠标依次单击键值 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run；

2、在对应 Run 键值的右边窗口中，如果发现了“ Notepad ”键值，您只要将它删除就能达到预防 BackDoor 的目的了。

六、隐藏用户登录名

Win9x 以上的操作系统可以对以前用户登录的信息具有记忆功能，下次重新启动计算机时，我们会在用户名栏中发现上次用户的登录名，这个信息可能会被一些非法分子利用，而给用户造成威胁，为此我们有必要隐藏上机用户登录的名字。

1、在设置时，请用鼠标依次访问键值 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon；

2、在对应 Winlogon 键值右边的窗口中，用鼠标右键单击窗口的空白处，从弹出的快捷菜单中选择“ 新建 ”/“ 字符串 ”命令；

3、给新建字符串命名为"DontDisplayLastUserName",并把该字符串值设置为"1"；

4、设置完后，重新启动计算机就可以隐藏上机用户登录的名字了。

七、不允许用户拨号访问

如果用户的计算机上面有重要的信息，有可能不允许其他人随便访问。那么如何禁止其他人拨入访问你的计算机，减少安全隐患呢，具体步骤为：

1、打开注册表编辑器，并在编辑器中依次展开以下键值：

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]；

2、在编辑器右边的列表中用鼠标选择“NoDialIn”键值，如果没有该键值，必须新建一个DWORD值，名称设置为“NoDialIn”；

3、接着用鼠标双击“NoDialIn”键值，编辑器就会弹出一个名为“字符串编辑器”的对话框，在该对话框的文本栏中输入数值“1”，其中0代表禁止拨入访问功能，1代表允许拨入访问功能；

4、退出后重新登录网络，上述设置就会起作用。

八、屏蔽对软盘的网络访问

俗话说“病从口入”，计算机中的病毒有很多都是通过访问不干净的软盘而被感染得来的，如果我们允许用户通过网络来访问软盘的话，那么整个网络都有可能被感染病毒，最终的结果将会使网络中的所有计算机都中毒瘫痪。为了防止病毒入侵整个网络，我们必须严格管理计算机的输入设备，以断绝病毒的源头，为此就要禁止通过网络访问软盘。设置时，您可以按照如下操作步骤来进行：

1、在系统的运行对话框中输入regedit命令，打开注册表编辑器；

2、在注册表编辑器操作窗口中，依次打开键值HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon；

3、在对应Winlogon右边的窗口中，检查一下其中有没有包含键值AllocateFloppies，如果没有，用鼠标右

键单击窗口的空白处，从弹出的快捷菜单中选择“新建”/“DWORD 值”；

4、把新建的 DWORD 值取名为 AllocateFloppies，同时把它的值修改为 0 或 1，其中 0 代表可被域内所有管理员访问，1 代表仅可被当地登陆者访问。

九、禁止访问“文件系统”按钮

在“系统属性”对话框中，有一个名为“文件系统”的功能按钮，利用它您可以对计算机的硬盘、软盘以及其他移动设备进行相关设置。但为了防止非法用户随意篡改这些设备的设置，您有时需要把“系统属性”中“文件系统”的按钮隐藏起来，下面是具体的设置步骤：

1、打开注册表编辑器窗口，并在窗口中依次访问如下键支：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System；

2、在对应 System 键值的右边窗口中，用鼠标单击窗口的空白处，从弹出的快捷菜单中选择“新建”/“DWORD 串值”；

3、给新建的 DWORD 串值，取名为“NoFileSysPage”，并把它的值设置为“1”；

4、设置完后，重新启动计算机就可以使设置生效了。

十、让“网上邻居”图标隐藏起来

大家知道，通过网上邻居可以随意访问局域网中其他计算机上的内容，但如果其他计算机没有设置特别的访问权限的话，那些别有用心的破坏者很有可能利用网上邻居来非法删除其他计算机上的重要数据，给其他计算机造成了损失。为了避免这样的损失，我们可以利用注册表来隐藏“网上邻居”。

1、首先在打开的注册表编辑器操作窗口中，用鼠标

依次访问键值 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer；

2、在对应 Explorer 键值右边的操作窗口中，用鼠标单击窗口的空白处，从弹出的快捷菜单中，用鼠标依次访问“新建”/“DWORD 串值”；

3、给新建的 DWORD 串值命名为 NoNetHood，同时把该值设置为 1（十六进制）；

4、设置好后，重新启动计算机就可以使设置生效了。

十一、限制使用系统的某些特性

在网吧或公用场所中，有时为了保证系统的属性不被其他普通用户随意更改，我们就必须要限制使用系统的某些特性。要实现这个目的，我们可以利用修改注册表编辑器的方法来达到。

1、运行注册表编辑器，进入 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 键值；

2、如果不存在该键值，就新建一个；

3、然后将该键值下方的 DisableTaskManager 的值设为 1，表示将阻止用户运行任务管理器。

4、接着将 NoDispAppearancePage 设为 1，表示将不允许用户在控制面板中改变显示模式；

5、下面再将 NoDispBackgroundPage 设为 1，表示将不允许用户改变桌面背景和墙纸。

十二、限制用户使用指定程序

为防止用户非法运行或者修改程序，导致整个计算机系统处于混乱状态，我们可以通过修改注册表来达到让用户只能使用指定的程序的目的，从而保证系统的安全。

1、在注册表编辑器窗口中依次打开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 键值；

2、在对应 Explorer 键值右边的窗口中，新建一个 DWORD 串值，名字取为“ RestrictRun ”，把它的值设为“ 1 ”；

3、在 RestrictRun 的主键下分别添加名为“ 1 ”、“ 2 ”、“ 3 ”等字符串值，然后将“ 1 ”,“ 2 ”、“ 3 ”等字符串的值设置为我们允许用户使用的程序名。例如将“ 1 ”、“ 2 ”、“ 3 ”分别设置为 word.EXE、notepad.EXE、write.EXE，则用户只能使用 word、记事本、写字板了，这样我们的系统将会做到最大的保障，也可以限制用户运行不必要的软件了。

十三、不允许用户设置屏幕保护密码

许多电脑使用者在使用电脑时，都有一种独占性，他们不希望自己使用的电脑，再去让别人使用，于是他们常常会在短暂离开电脑时，给电脑设定了屏保密码；但遗憾的是，他们在用完电脑之后，又不能及时把这些屏保密码去除,这样很容易导致其他用户不能正常使用，严重的能使计算机无法启动。为了避免这些现象的发生，我们可以通过修改注册表，来设定用户无权进行屏保密码的设置。

1、打开注册表编辑器窗口，在该窗口中用鼠标访问 CURRENT_USER\ControlPanel\desktop\ScreenSaveUsePassword 键支；

2、在对应 ScreenSaveUsePassword 键值的右边窗口中，将 ScreenSaveUsePassword 的值设置为 0 就可以了。

十四、将文件系统设置为 NTFS 格式

在 Windows2000 以及 NT 系统中，用户可以将分区设置为 NTFS 格式来确保文件系统的安全，当然我们也可以通过修改注册表的方法来达到将文件系统设置为 NTFS 格式的目的，具体实现步骤如下：

1、打开注册表编辑器，并在编辑器中依次展开以下键值：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem；

2、在注册表编辑器中用鼠标单击“编辑”菜单，并在下拉菜单中选择“新建”菜单项，并在其弹出的子菜单中单击“DWORD 值”；

3、在编辑器右边的列表中输入 DWORD 值的名称为“NtfsDisableLastAccessUpdate”；

4、接着用鼠标双击 NtfsDisableLastAccessUpdate 键值，编辑器就会弹出一个名为“字符串编辑器”的对话框，在该对话框的文本栏中输入数值“1”，其中 0 代表“取消”该项功能，1 代表“启用”该项功能。

十五、抵御 WinNuke 黑客程序对计算机的攻击

WinNuke 是一个破坏力极强的程序，该程序能对计算机中的 Windows 系统进行破坏，从而会导致整个计算机系统瘫痪，所以我们有必要预防 WinNuke 的破坏性。我们可以在注册表中对其进行设置，以保证系统的安全。

1、在注册表编辑器操作窗口中，用鼠标依次单击键值 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP；

2、在对应 MSTCP 键值的右边窗口中，用鼠标单击窗口的空白处，从弹出的快捷菜单中选择“新建”/“DWORD 值”，并给 DWORD 值取名为“BSDUrgent”，如

果该键值已经存在，可以直接进行下一步；

3、然后将 BSDUrgent 值设置为 0，重新启动计算机后就可以实现目的了。

十六、恢复对注册表的错误修改

由于注册表是计算机的核心和灵魂，对注册表进行的任何一个错误修改都有可能使计算机不能正常启动。为了确保万无一失，我们在对注册表进行修改时，都要对注册表进行备份工作，一旦在修改注册表时出了一点小错误,就可将以前备份的注册表文件再导入注册表中，从而恢复注册表以前的内容，下面是具体的操作步骤：

1、在运行对话框中输入 regedit 命令，程序将弹出了一个注册表编辑器窗口；

2、在该窗口中用鼠标单击“注册表”菜单下的“导入注册表文件”，从弹出的文件对话框中找到备份的.reg 文件，最后再用鼠标单击该对话框中的“确定”按钮，就可以重新向注册表写入正确信息；

3、当注册表损坏或错误更改了软硬件设置，导致系统启动失败，并且自动修复无效，用“Scanreg.exe／Fix”也无法恢复时，可在纯 DOS 下运行“scanreg.exe／restory”进行恢复，有五个数据供选择，先选日期最近的恢复，若仍不行，再依次选择，直到系统正常运行为止。